UDC 343.13
DOI: 10.32518/sals4.2023.123

Соціально-правові студії. 2023. Т. 6, № 4
Social & Legal Studios. 2023. Vol. 6, No. 4

Investigating cryptocurrency financing crimes terrorism and armed aggression

Anatolii Movchan*
Doctor of Law, Professor
Lviv State University of Internal Affairs
79007, 26 Horodotska Str., Lviv, Ukraine
https://orcid.org/0000-0002-6997-6517

Oleksandr Shliakhovskyi
PhD in Law, Associate Professor
Lviv State University of Internal Affairs
79007, 26 Horodotska Str., Lviv, Ukraine
https://orcid.org/0000-0001-8181-1857

Vasyl Kozii
PhD in Law, Doctoral Student
Lviv State University of Internal Affairs
79007, 26 Horodotska Str., Lviv, Ukraine
https://orcid.org/0000-0001-8181-1857

Ihor Fedchak
PhD in Law, Associate Professor
Lviv State University of Internal Affairs
79007, 26 Horodotska Str., Lviv, Ukraine
https://orcid.org/0000-0002-4359-5988

Abstract. The article is devoted to the study of the problems of investigating crimes of financing terrorism and armed aggression with cryptocurrency, which is relevant considering the attack on Ukraine by the Russian Federation, as well as in connection with the significant spread and use of cryptocurrency for financing both terrorism and armed aggression. The purpose of the article is to study the problems of investigating crimes of cryptocurrency financing of terrorism and armed aggression and finding ways and means of solving problematic issues, because cryptocurrency financing of terrorism and armed aggression is an encroachment on national security. The methods of system analysis and technical-legal analysis, as well as the formal-logical method, were used in the research process. Thanks to this, approaches to understanding the way of committing crimes of the researched category have been determined. The shortcomings in the legal regulation of the circulation and use of cryptocurrency in Ukraine, as well as in the legal regulation of the investigation of crimes related to the illegal acquisition and use of cryptocurrency for criminal purposes, including for the financing of terrorism and armed aggression, are highlighted. Jurisdictional problems of criminal prosecution of persons who committed crimes of this category, their high latency due to the lack of proper legal procedures and methods of investigation, have been determined. The need to create specialized units in law enforcement agencies, whose competence will include the detection and investigation of the specified crimes, their active interaction with the Cyber Police, is substantiated. The attention and necessity of introducing a system of constant monitoring of social networks, the Internet, and media and conducting OSINT-intelligence from open sources with the aim of detecting and stopping such criminal activities, tracking and arresting and eventually seizing cryptocurrency, if such an opportunity is available, was emphasized. Practical recommendations for the investigation of crimes of cryptocurrency financing of terrorism and armed aggression have been formulated. The need for international legal cooperation in this area was emphasized; the need to involve specialists in the field of information technologies, programming, and blockchain engineering in the investigation process in general and in specific investigative actions. The requirements for the

Suggested Citation

Article's History: Received: 05.09.2023 Revised: 10.12.2023 Accepted: 23.12.2023

Movchan, A., Shliakhovskyi, O., Kozii, V., & Fedchak, I. (2023). Investigating cryptocurrency financing crimes terrorism and armed aggression. *Social & Legal Studios*, 6(4), 123-131. doi: 10.32518/sals4.2023.123.

*Corresponding author

recording of evidence in the protocols of investigative (search) actions during the investigation of crimes of this category are formulated, in particular, the need for hashing of files is specified. The practical significance of the study is that the obtained results can be used during the investigation of crimes of the studied category

Keywords: virtual assets; blockchain; crimes in the field of cryptocurrencies; search of evidence; OSINT-intelligence; tracking cryptocurrency transfers

Introduction

Over the past decades, cryptocurrencies (virtual assets) have been an integral part of the functioning of society. It is actively used by individuals and legal entities to pay for goods and services. Cryptocurrencies are also traded on online exchanges and exchange services, used as a means of saving, etc. Cryptocurrency is essentially a convenient financial instrument that, like many others, can be used both legitimately and for criminal purposes. In particular, cryptocurrencies are stolen by hacking cryptocurrency exchanges and wallets of individual owners, they are seized under the pretext of investing in fraudulent cryptocurrency projects, they are used to finance terrorism and armed aggression, and they are used to legalize the proceeds of crime. However, the legal regulation of cryptocurrencies in Ukraine is still in its infancy in the area of criminal justice. Investigating crimes of cryptocurrency financing of terrorism and armed aggression is something entirely new for law enforcement. There are virtually no successful cases in this area. There are also no scientific studies in Ukraine that directly address this topic.

As for foreign research, the works of such scholars as V. Dyntu and O. Dykyj (2021), who consider cryptocurrency as a tool for terrorist financing and note that the main issue in the fight against crime is the de-anonymisation of the Bitcoin owner/user, which allows the identification of the criminal.

A. Maurushat and D. Halpin (2022) consider cryptocurrencies as a tool for online fraud and analyse the challenges associated with investigating fraud with cryptocurrency investments. V. Karpuntsov and R. Veresha (2023), studying the legal aspects of the regulation of virtual assets in Ukraine, point out the need to address the issue of legal qualification of illegal actions with crypto assets, as well as the issue of theoretical and legal understanding of new legal relations. M. Utkina *et al.* (2023), studying the issues of financial intelligence (monitoring) of transactions with virtual assets, state that virtual assets are used in criminal offences such as money laundering and determine the role of financial intelligence in the effective fight against money laundering. M. Dumchikov *et al.* (2023) note that the methods of money laundering through virtual assets, in particular, include virtual asset conversion services. Their study allowed them to conclude that it is necessary to strengthen financial monitoring by financial control authorities of the activities of conversion service centres.

A. Trozze *et al.* (2023), studying the results of criminal prosecution for financial crimes related to the use of cryptocurrency, based on the analysis of the results of the trial of 37 resolved cases in the United States, concluded that the presence of only individual defendants (and not a corporate defendant or a combination of them) and the use of only cryptocurrency besides bitcoin to commit the crime reduced the likelihood of resolving the case by dismissal.

Particular attention is drawn to the scientific work of A. Pantazidis *et al.* (2023), dedicated to the use of virtual reality for training security officers. Thus, they propose a new interactive and realistic virtual reality-based game for training law enforcement officers to analyse and understand terrorist activities. The game is based on pragmatic models of terrorist actions and teaches its users to predict the signs of terrorist attacks, as well as provides tools for creating datasets for training artificial intelligence (AI) modules that can help analyse and predict potential terrorist activity. In addition, their study provides a perspective on the evolution of the game in metaverse environments, where blockchain infrastructures can be used to both increase the cyber resilience of the game and protect the reliability of the data generation process.

S. Mirkamol and E. Mansur (2023) consider cryptocurrencies as the money of the future. E. Badawi *et al.* (2022) investigated fraud through cyberattack, in which fraudsters promise victims free cryptocurrencies in exchange for a small mining fee. As part of their research, they identified more than 8,000 cryptocurrency addresses directly related to the scam, hosted in more than 1,000 domains. In total, these addresses received about $8.7 million, an average of $49.24 per transaction. The study by G.A. Siu *et al.* (2022) focuses on the evolution of investment fraud temptations and fraud-related keywords on the online cryptocurrency forum Bitcointalk over a 12-year period. A. Schmidt (2021), exploring the risks of virtual assets to money laundering and terrorist financing, recommends expanding the regulatory framework to include regulation that is native to the peer-to-peer nature of virtual assets to address the risks. However, the approaches to investigating such crimes, the specifics of their investigation, the requirements for recording evidence in the protocols of investigative (search) actions, and the specifics of tracking, seizure, withdrawal, and confiscation of cryptocurrencies used to finance terrorism and armed aggression remain unexplored.

The aim of the article is to study the problems of investigating crimes of cryptocurrency financing of terrorism and armed aggression and to find ways and means to resolve the problematic issues, since cryptocurrency financing of terrorism and armed aggression is an encroachment on national security.

Materials and methods

The study used the methods of system analysis and technical and legal analysis, as well as the formal logical method, which made it possible to determine the ways of committing crimes in the category under study.

Furthermore, in the course of the study, to clarify the state of legal regulation of the cryptocurrency sphere in Ukraine, the author used the methods of system analysis and technical and legal analysis to study such legal acts as the Law of Ukraine “On Virtual Assets” (2022) and the provisions of the Criminal Procedure Code of Ukraine, which allowed the author to draw conclusions about the insufficiency of legal regulation of these social relations. To determine the state of research on the topic of investigation of crimes related to cryptocurrency financing of terrorism and armed aggression, the author uses the method of systematic analysis and the formal logical method to analyse the works of Ukrainian and foreign scholars contained in scientific databases, which made it possible to identify the issues which are not covered by such studies, as well as the issues which require more in-depth research, to investigate them and to propose ways and means of solving the existing problems. In addition, the method of systematic analysis and the formal logical method made it possible to identify the peculiarities of investigating crimes in the investigated category, to formulate approaches to the process of their detection and investigation, to state the need for constant monitoring of social networks, the Internet, and the media, conducting OSINT-intelligence from open sources, tracking, arresting and seizing cryptocurrency, as well as to formulate requirements for recording evidence in the protocols of investigative actions, and to come to the conclusion that files should be hashed. In addition, in the course of the research, the Scopus scientific database was used to search for scientific papers using the search terms "cryptocurrency", "virtual assets", "financing of terrorism with cryptocurrency", "financing of armed aggression with cryptocurrency". In total, more than 400 scientific papers related to the field of cryptocurrencies in general were reviewed, but most of them were excluded as not relevant to the field of criminal justice. The work used 20 studies by scholars that were directly related to the subject of the study.

In the course of the research, such web resources as CoinmarketCap and Internet Archive were used. Thus, the use of CoinmarketCap allowed forming an idea of the cryptocurrency market, its players and the structure of the cryptocurrency industry in general. A study of the capabilities of the Internet Archive web resource made it possible to establish the feasibility of using it to archive files containing evidence of criminal activity by individuals or organized groups. The web resource also pays attention to such a tool as the Wayback Machine, which can help in the process of investigating crimes of the investigated category if pages on the Internet have been highlighted or modified to hide traces of criminal activity. The study examines the capabilities of the software Crystal, Chainalysis, CipherTrace, CryptoFinance, Bitcoin Abuse Databases, Walletexplorer.com, Graphsense.info in terms of its ability to detect criminal activity in blockchains by analysing and tracking transactions. The author also studied the possibilities and noted the use of such programs as Mozilla Firefox with the Easy YouTube Video Downloader Express extension, as well as Mediainfo and RapidCRC Unicode programs in the process of investigating crimes of the investigated category. This, in particular, made it possible to formulate recommendations that when reviewing data on the Internet, it is possible to use the "Screenshot" function of the Mozilla Firefox browser and save a screenshot of the entire web page to the storage medium, and then use the software to copy photos or video files, fully and consistently reflecting this in the protocol of the relevant investigative (detective) action.

In addition, the Unified State Register of Court Decisions was monitored, during which 103 guilty verdicts related to the use of cryptocurrency for criminal purposes were processed. Such a study made it possible to find out that every 10 verdicts relate to the commission of crimes related to the financing of terrorism and armed aggression (under Article 89, part 1 of Article 110-2, part 4 of Article 111-1, part 1 of Article 263, part 1, part 2 of Article 263-1 of the Criminal Code of Ukraine), which indicates a rather significant share of crimes in the studied category in the structure of crime in the field of cryptocurrencies in general.

Results and discussion

The study of cryptocurrencies in the context of fundamental rights allowed C. Rueckert (2019) to conclude that in the context of criminal prosecution, law enforcement agencies restrict freedom of telecommunications, data privacy (including the right to information self-determination), freedom of expression and freedom of information. Therefore, whenever some of these fundamental rights are violated, the regulatory concepts and approaches to investigation or prosecution should be provided for by law and should meet the test of necessity.

P. Xia *et al.* (2020) describe fraud in the exchange of cryptocurrencies. The study by R. Phillips and H. Wilder (2020), in particular, focuses on the issues of committing cryptocurrency fraud through phishing. L. Swartz's (2022) research is devoted to "network fraud" with cryptocurrencies. As an example, this article examines the 2017 initial coin offering (ICO) bubble. ICOs were supposed to be a new, radically disruptive way of crowdfunding to finance the development of a new, radically disruptive blockchain technology ecosystem. In total, ICOs raised approximately $5 billion in 2017 alone. But by all analyses – by observers and participants alike, both during the bubble and afterwards – the vast majority of ICOs turned out to be frauds.

Some countries, such as North Korea, have their own cyber forces, with separate units tasked with hacking cryptocurrency exchanges and wallets and illegally seizing cryptocurrency used to finance the regime and circumvent international sanctions when making payments for certain goods and services. Obviously, cryptocurrencies are also used to purchase weapons and military equipment, technologies, software, and to finance terrorist operations outside such countries. Typically, crimes in this category are highly latent, their investigation is extremely difficult, and it is impossible to bring the perpetrators to justice and seize and confiscate cryptocurrency. In particular, the hacking of the CoinEx cryptocurrency exchange in September 2023 (estimated damage of USD 55.5 million) could have been carried out by North Korean hackers from the Lazarus Group (Experts suspect hackers…, 2023).

According to Transparency International, cryptocurrencies are used to withdraw funds in Russia to circumvent sanctions. There are OTC brokers in Moscow who sell dollars in stablecoins, which are then exchanged for pounds sterling in the UK (Cryptocurrencies are widely used…, 2023). In October 2023, officers of the Cyber Police Department blocked an illegal online currency exchanger that used Russian payment systems. According to the National Police press service, the offenders used the website to bring Russian rubles into Ukraine and exchange electronic money and cryptocurrencies. Their cooperation with the aggressor country is being checked (An online currency exchanger…, 2023).

In accordance with data provided by Bloomberg, in May 2023, the US Department of Justice launched an investigation into the cryptocurrency exchange Binance over suspicions that it was used by Russians to circumvent sanctions (Binance faces us probe…, 2023). In November 2023, in this case, Binance agreed that Hamas and other terrorist organizations had conducted transactions on its services. As a result, the exchange will have to pay $4.3 billion to the US government, and its CEO and founder Changpeng Zhao will be fined $50 million and will resign as CEO (The largest cryptocurrency exchange…, 2023). Cryptocurrencies are also used to finance the war against Ukraine. In particular, according to cryptocurrency tracking companies Chainalysis, Elliptic, and TRM Labs, the main beneficiaries are paramilitary groups that supply military products and weapons (Digital danger: What is…, 2023).

As stated in the State Security Strategy approved by Decree of the President of Ukraine No. 56/2022 of 16 February 2022, the Russian Federation continues to wage hybrid warfare and systematically uses cyberattacks to achieve its strategic goals in Ukraine. The special services of individual states use organized criminal groups and corrupt officials to fuel separatist sentiment.

In particular, Russian organized crime conducts special hybrid operations abroad (Maliuk, 2023). According to the State Bureau of Investigation (SBI), the enemy is trying to undermine Ukraine’s defence capabilities through drug trafficking schemes. Thus, since February 2022, SBI and police officers have launched pre-trial investigations in almost 400 such criminal proceedings (SBI: The special services…, 2022).

German law enforcement officers shut down the largest marketplace in the darknet, Hydra, which was used to sell drugs, fake documents and money laundering through cryptocurrency. German law enforcement officers removed the physical servers in Germany and were able to confiscate about $25 million in bitcoins. Since the activities of the Hydra website are linked to the Russian Federation, German law enforcement officers provided their Ukrainian colleagues with access to the investigation materials, which allowed them to detain individuals involved in the activities of the marketplace in the country (Detentions of members of a criminal…, 2022).

The commission of such crimes leaves electronic digital traces, which, in particular, may include correspondence on the Internet, posts, photos, and videos on channels in various applications (Telegram, Viber, Signal, WhatsApp), content from social networks (Facebook, TikTok, YouTube). It can also include various links to blocking resources. All of the above is information in electronic (digital) form. The data in social networks and managers are subsequently deleted by criminals to make them untraceable and to hide the traces of the crimes. And here, the investigator, prosecutor, detective, or operative officer faces the crucial issue of recording electronic (digital) information using available procedural and technical tools. One of the ways to help is to inspect electronic documents and computer data, copy them, archive them and hash the files that are the subject of the inspection. Article 237 of the Criminal Procedure Code (CPC) of Ukraine (2012) provides investigators and prosecutors with the relevant powers.

To properly record evidence in criminal proceedings on crimes of this category, when conducting an inspection of documents in electronic form and computer data containing relevant information, the investigator, or prosecutor is entitled to engage specialists in the field of computer technology, programming, cybersecurity, and blockchain engineering. During the inspection, it is possible to use programs such as Mozilla Firefox with the Easy YouTube Video Downloader Express extension, as well as Mediainfo and RapidCRC Unicode. During the review, it is possible to use the “Screenshot” function of the Mozilla Firefox browser and save a screenshot of the entire web page to a storage device. Later, it is possible to use the software to copy photos or video files. It is important to record the metadata of the copied files. For this purpose, it is advisable to use MediaInfo. Hashing, i.e. calculating the hash codes of files, is performed using RapidCRC Unicode. Hash codes of files are subject to indication in the protocol. Web resources can be archived using the Internet Archive service (n.d.). It is also possible to use the Wayback Machine resource at the specified link, which can help if the pages on the Internet on the sites and, accordingly, the content have been highlighted or changed.

In general, when conducting reviews of electronic (digital) documents and computer data, it is necessary to consistently indicate what actions are performed, which files are reviewed, on which websites, social networks or messengers, via which links and with which software. Hashing the saved and viewed files and indicating the hashes of such files in the hash protocol allows verifying their authenticity at any time and confirming that no changes have been made to them. This is especially important considering their subsequent examination in court. When it comes to tracking transactions, i.e. cryptocurrency transfers from one address in the blockchain to another, it is important to include the addresses and hashes of transactions, the software used to track them, as well as the addresses of the relevant cryptocurrency blockchains and the results of a sequential search. In the case of cryptocurrency transfers to cryptocurrency wallets controlled by the pre-trial investigation authority, the software used for this purpose, the name, and amount of cryptocurrency, the addresses from which the transfer is made and the addresses to which the cryptocurrency is transferred, and the hashes of the relevant transactions shall also be indicated. In no case should private keys and mnemonic (Seed) phrases be indicated, as this would allow anyone to access and illegally take possession of the cryptocurrency.

At the same time, it is advisable to immediately make a duplicate of the relevant electronic document, as well as copies of information, including computer data, which, in accordance with the requirements of Part 4 of Article 99 of the CPC (2012) of Ukraine, are mandatorily recognized by the court as the original document. Such an algorithm of actions will allow the court to present a duplicate of the document as evidence, and in case of unforeseen loss or damage to the originals of the relevant electronic (digital) evidence, the duplicate will be recognized by the court as the original, and therefore as proper and admissible evidence.

On 17.02.2022, the Verkhovna Rada adopted the Law of Ukraine “On Virtual Assets”, which classifies virtual assets as intangible assets. However, the said Law has not yet entered into force, and therefore, the legal status of virtual assets is not defined at all. Similarly, the Tax Code of Ukraine (2012) refers to virtual assets only in part 10 of Article 170 (only the possibility of seizure of virtual assets is provided).

The term “virtual assets” is a legislative definition and a concept that is generally identical to the concept of “cryptocurrency”. As of 01.12.2023, the CoinmarketCap (n.d.) resource provides information on tens of thousands of cryptocurrencies and 684 exchanges that trade and exchange cryptocurrencies.

Any cryptocurrency is a set of characters. They make up the wallet address, the so-called public key, which is generated by the system and is required to transfer a certain amount of cryptocurrency to it. A transaction hash allows identifying a transaction in the blockchain of a particular cryptocurrency. At the same time, neither the Law of Ukraine "On Virtual Assets" (2022) nor the CPC of Ukraine (2012) currently provide answers to the question of how to prosecute, investigate and prove a person's guilt in court in the event of illegal possession of cryptocurrency and cryptocurrency financing of terrorism and armed aggression.

In particular, the European Financial and Economic Crime Threat Assessment (2023) published by Europol notes that improved investigative techniques have helped police identify suspicious transactions and the individuals involved. Nevertheless, the global nature, speed and mixing of cryptocurrency transactions pose a significant challenge to law enforcement investigations. It is also difficult to trace and freeze crypto assets and convert them into fiat currency. At the placement stage, money brokers open several accounts using money mules and fake identity documents, and the cash received from criminals is exchanged for cryptocurrency (Aleksandrov, 2022).

At the stratification stage, the illicit funds are separated from their original source by exchanging them for other coins. In this process, known as a "hopping chain", money is moved from one cryptocurrency to other regulated exchanges and jurisdictions to make it difficult to trace. The layering process may involve cryptocurrency mixers that eliminate the links between the source and destination addresses by using multiple intermediary wallets. In the integration stage, money mules are used to open multiple bank accounts in one or more countries in a short timeframe to quickly transfer funds from cryptocurrency wallets. In addition, criminals create online companies to accept payments in cryptocurrency. Crypto-ATMs are used to convert fiat currency into cryptocurrency and vice versa to launder the proceeds of crime and transfer funds abroad. Another popular technology channels criminal proceeds to cryptocurrency gambling platforms, where criminals can claim gambling winnings (Europol, 2023).

Instead, as of 01.12.2023, the Unified state register of court decisions (n.d.) recorded only 103 convictions related to the use of cryptocurrency for criminal purposes in Ukraine, of which 10 verdicts (nos. 201/2020/23, 204/4713/23, 204/7642/23, 204/7978/23, 204/5603/22, 405/6271/23, 204/2980/21, 405/2939/23, 204/9472/23, 495/823/21) were delivered in relation to the commission of crimes related to the financing of terrorism and armed aggression (under Art. 89, p.1 Art. 110-2, Art. 111-1(4), Art. 263(1), Art. 263-1(1), Art. 263-1(2) of the Criminal Code of Ukraine (2012). At the same time, expert research indicates that cryptocurrencies are widely used for criminal purposes. According to The Chainanalysis 2021 Crypto Crime Report, Ukraine ranks 3rd in the world in terms of the volume of transactions related to the purchase of drugs on the darknet (Karchevskyi, 2021).

At the same time, O. Samoilenko and K. Titunina (2023), studying crimes in the field of cryptocurrencies, point out the need to solve such tactical tasks as blocking transactions for the sale of cryptocurrencies by a certain person and identifying such a person or group of individuals. While agreeing with this statement, it should be noted that blocking cryptocurrency sales transactions is not always technically possible in the case of criminals located outside of jurisdictions and using cryptocurrency wallets installed on their gadgets and using decentralized exchanges and so-called mixers that hide the links between transactions.

The study of international cooperation in the investigation of economic crimes related to cryptocurrency trafficking allowed O. Kreminskyi *et al.* (2021) to identify the following consequences of international cooperation in the investigation of economic crimes related to cryptocurrency 1) the need to use a risk-oriented approach of the international community at the global level, coordinating government efforts to prevent economic crime; 2) the formation of a network of organizations that ensures an effective balance between existing threats and opportunities for cryptocurrency circulation; 3) the development of free, decentralized governance networks at the global level, which is an innovative and effective way to combat criminal activity, compared to traditional centralized forms of coercion in the era of rapid and unpredictable technological change.

Given that there are more than 8,000 Internet service providers in Ukraine, it is difficult to obtain a court order to block an illegal Internet resource. If it is located outside of Ukraine, a request for international legal assistance should be sent to the competent law enforcement agencies of foreign countries in addition to a court order. This procedure also lacks a clear mechanism and can take a long time (Movchan *et al.*, 2021).

In Ukraine, there are two types of blocking of Internet resources: the first is in accordance with the Law of Ukraine "On Sanctions" (2014). The second type of blocking was introduced after the introduction of martial law in Ukraine in February 2022. This is a blocking within the framework of the implementation of orders of the NCU (National Centre for Operational and Technical Management of Electronic Communication Networks of Ukraine), which operates under the State Special Communications Service (Belovolchenko, 2023).

To successfully investigate cryptocurrency financing of terrorism and armed aggression, law enforcement agencies need to identify criminals. Transactions can be analysed using criminal analysis methods and tools. In particular, to detect and track illegal activities in blockchain networks, methods of the Intelligence-Led Policing/ILP model (Detentions of members of a criminal…, 2022) and special software (in particular, Crystal, Chainalysis, CipherTrace, Crypto-Finance, Bitcoin Abuse Databases, Walletexplorer. com", "Graphsense.info"), the use of such software provides an opportunity to effectively analyse the relationships between transactions and establish patterns of criminal finance flows (Movchan & Taranukha, 2018).

The materials of criminal proceedings obtained with the use of special software are characterized by documentation and high information content, which makes it possible to prove the fact of a criminal offence. Their authenticity can also be confirmed by the conclusions of computer forensics.

As noted by M. Karchevskyi (2021), covert investigative (detective) actions carried out in the field of information and communication technologies allow detecting and procedurally recording information about cryptocurrency transactions by combining two main ways of recording information: visual, related to the external perception of information posted on a web resource, and technological, related to the use of special software for recording data. Given the importance of detecting, documenting and procedural use of information on cryptocurrency financing of terrorism and armed aggression, it is proposed to develop an appropriate instruction that provides for the tactical aspects of recording a criminal offence using the CIDA, as well as an algorithm for seizing cryptocurrency and preserving it until a decision is made on the case.

S.K. Taylor *et al.* (2021) propose the creation of crypto-wallets by law enforcement officers to seize cryptocurrency at the crime scene. While agreeing with the expediency of the above, it should be added that in this context, it is necessary to introduce security protocols that would eliminate the risk of accidental loss of cryptocurrency and its misappropriation by law enforcement officers. In addition, if cryptocurrency transactions are recorded and documented during the commission of a criminal offence, there is technically no way to seize the cryptocurrency and block the electronic wallet. In this case, it is proposed to create a separate electronic wallet, which will be managed by the relevant law enforcement agency (in particular, the National Police, the Security Service of Ukraine, the NABU, the BES, the SBI) in the person of a designated responsible employee. Thus, it is proposed to seize cryptocurrency in the form of a transaction to the specified wallet.

Thus, the results of the study indicate that there are difficulties in investigating crimes of cryptocurrency financing of terrorism and armed aggression, which are related to the lack of legal regulation in this area of social relations and the absence of established practice and successful cases. At the same time, understanding and awareness of the challenges that arise and the application of appropriate approaches and techniques in numerous instances allows achieving the set objectives, detecting and stopping such criminal activity, identifying perpetrators, tracking transactions, seizing, arresting and confiscating cryptocurrency used to finance terrorism and armed aggression

Conclusions

The study of scientific sources, legislation and practical cases relating to the investigation of crimes of cryptocurrency financing of terrorism and armed aggression fully allowed achieving the research objective and reaching reasonable conclusions that countering this phenomenon by criminal law means is a matter of national security of the State. The scientific novelty of the work lies in the conclusion that specialized units should be created in law enforcement agencies with the competence to detect and investigate these crimes and their active interaction with cyber police. Specialists in the field of information technology, programming, and blockchain engineering should be involved in the investigation of such crimes. Due to the high latency of such crimes, it is necessary to introduce a system for monitoring social networks, the Internet, and media and open-source intelligence (OSINT) to detect and stop such criminal activity, track, seize and confiscate cryptocurrency and confiscate it. For this purpose, it is proposed to create a separate electronic wallet, which will be managed by a law enforcement agency (in particular, the National Police, the Security Service of Ukraine, the NABU, the BES, the SBI) in the person of a designated responsible employee, and the seized cryptocurrency will be stored there until a court decision is made. Since the jurisdiction of the state may not always extend to certain cases of crimes in this category, international legal cooperation is also necessary. During the investigation, an important part of the process is the inspection of electronic documents and computer data, their copying, archiving and hashing of the files that are the subject of the inspection. In addition, if pages on the Internet have been highlighted or modified to hide traces of criminal activity, a resource such as the Wayback Machine should be used. To track and analyse cryptocurrency transactions, the following software should be used: Crystal, Chainalysis, CipherTrace, CryptoFinance, Bitcoin Abuse Databases, Walletexplorer.com, Graphsense.info. The use of such programs as Mozilla Firefox with the Easy tube Video Downloader Express extension, as well as Mediainfo and RapidCRC Unicode programs when reviewing data on the Internet allows using the "Screenshot" function of the Mozilla Firefox browser and saving a screenshot of the entire web page to the storage medium, and then use the software to copy them, fully and consistently reflecting everything in the protocol of the investigative (detective) action.

The practical significance of this study is that the findings obtained can be used in the process of detecting and suppressing the relevant criminal activity. At the same time, these issues require further in-depth research and the development of a whole scientific doctrine and practical recommendations for counteracting the state-level financing of terrorism and armed aggression by cryptocurrencies. This primarily concerns the detection, tracking, blocking, and seizure of cryptocurrencies intended for the financing of terrorism and armed aggression, as well as the application of criminal law measures to cryptocurrency exchanges and online resources used to finance terrorism and armed aggression.

Acknowledgements

The research was carried out by the authors independently, in equal parts, accordingly, there are no thanks to individual individuals or organizations for the excellent technical assistance, ideas, financial (material) support, etc., thanks to which the research became possible.

Conflict of interest

None.

References

[1] Aleksandrov, A. (2022). *How cryptocurrency helps finance terrorism and how to avoid it*. Retrieved from https://speka.media/yak-kriptovalyuta-dopomagaje-finansuvati-terorizm-ta-yak-cyogo-uniknuti-p1dg5p.

[2] An online currency exchanger using Russian payment systems was exposed. (2023). Retrieved from https://ua.korrespondent.net/ukraine/4631420-vykryto-onlain-obminnyk-valuit-iz-vykorystanniam-rosiiskykh-platizhnykh-system.

[3] Badawi, E., Jourdan, G.-V., & Onut, I.-V. (2023). The "Bitcoin Generator" scam. *Blockchain: Research and Applications*, 3(1), article number 100084. doi: 10.1016/j.bcra.2022.100084.

[4] Belovolchenko, A. (2023). *"It is impossible to reliably block something on the Internet." How Russian resources are blocked in Ukraine and why it affects legal sites*. Retrieved from https://dou.ua/lenta/articles/blocking-websites.

[5] Binance faces us probe of possible Russian sanctions violations. (2023). Retrieved from https://www.bloomberg.com/news/articles/2023-05-05/binance-faces-us-probe-of-possible-russian-sanctions-violations?srnd=premium&leadSource=uverify%20wal.
[6] CoinMarketCap. (n.d.). Retrieved from https://coinmarketcap.com.
[7] Criminal Procedure Code of Ukraine. (2012, Aprile) Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17?lang=en#Text.
[8] Cryptocurrencies are widely used in the Russian Federation to withdraw funds to circumvent sanctions. (2023). Retrieved from https://sprotyv.info/ekonomica/v-rf-masovo-vikoristovuyut-kriptovalyuti-dlya-vivedennya-koshtiv-v-obhid-sankczij.
[9] Decree of the President of Ukraine No. 56/2022 "On the Decision of the National Security and Defense Council of Ukraine dated December 30, 2021 "On the Strategy for Ensuring State Security". (2022, February). Retrieved from https://zakon.rada.gov.ua/laws/show/56/2022#Text.
[10] Detentions of members of a criminal organization selling prohibited goods on the darknet began in Ukraine. (2022). Retrieved from https://life.nv.ua/ukr/lyudi/sayt-gidra-v-ukrajini-pochalisya-zatrimannya-zlochinciv-darknetu-hydra-prodavala-narkotiki-50247570.html.
[11] Digital danger: What is known about the fight against the financing of the war in Ukraine through cryptocurrencies. (2023). Retrieved from https://financy.24tv.ua/kriptovalyuti-vikoristovuyut-dlya-finansuvannya-viyni-rosiyi_n2240031.
[12] Dumchikov, M., Reznik, O., & Bondarenko, O. (2023). Peculiarities of countering legalization of criminal income with the help of virtual assets: Legislative regulation and practical implementation. *Journal of Money Laundering Control*, 26(1), 50-59. doi: 10.1108/JMLC-12-2021-0135.
[13] Dyntu, V., & Dykyj, O. (2021). Cryptocurrency as an instrument of terrorist financing. *Baltic Journal of Economic Studies*, 7(5). doi: 10.30525/2256-0742/2021-7-5-67-72.
[14] Europol. (2023). *The other side of the coin: An analysis of financial and economic crime*. Luxembourg: Publications Office of the European Union.
[15] Experts suspected hackers from Lazarus in hacking CoinEx for $55 million. (2023). Retrieved from https://forklog.com.ua/news/eksperty-zapidozryly-u-zlami-coinex-na-55-mln-hakeriv-iz-lazarus.
[16] Internet Archive. (n.d.). Retrieved from https://web.archive.org.
[17] Karchevskyi, M. (2021). *Cryptocurrencies and BLOCKCHAIN technologies: Innovations in combating corruption*. Retrieved from https://justtalk.com.ua/post/kriptovalyuti-ta-tehnologii-blockchain-innovatsii-u-protidii-koruptsii.
[18] Karpuntsov, V., & Veresha, R. (2023). Legal aspects of virtual assets regulation in Ukraine. *Danube*, 14(3), 235-252. doi: 10.2478/danb-2023-0014.
[19] Kreminskyi, O., Kuzmenko, O., Antoniuk, A., & Smahlo, O. (2021). International cooperation in the investigation of economic crimes related to cryptocurrency circulation. *Studies of Applied Economics*, 39(6). doi: 10.25115/eea.v39i6.5247.
[20] Law of Ukraine No. 1644-VII "On Sanctions". (2014, August). Retrieved from https://zakon.rada.gov.ua/laws/show/1644-18#Text.
[21] Law of Ukraine No. 2074-IX "On Virtual Assets". (2022, February). Retrieved from https://zakon.rada.gov.ua/laws/show/2074-20.
[22] Maliuk, V.V. (2023). The use of organized criminal groups by the special services of the Russian Federation to carry out reconnaissance and subversive activities under martial law. In *Current issues and prospects for the use of investigative tools in the detection of crimes under martial law: Materials of the interdepartmental scientific and practical conference* (pp. 103-105). Kyiv: National Academy of Internal Affairs.
[23] Maurushat, A., & Halpin, D. (2022). Investigation of cryptocurrency enabled and dependent crimes. In D. Goldbarsht & L. de Koker (Eds.), *Financial Technology and the Law: Combating Financial Crime* (pp. 235-267). doi: 10.1007/978-3-030-88036-1_10.
[24] Mirkamol, S., & Mansur, E. (2023). Cryptocurrencies as the money of the future. In Y. Koucheryavy & A. Aziz (Eds.), *Internet of things, smart spaces, and next generation networks and systems: Proceedings of 22nd international conference, NEW2AN 2022* (pp. 244-251). Cham: Springer. doi: 10.1007/978-3-031-30258-9_21.
[25] Movchan, A.V., & Taranukha, V.Y. (2018). Constructing an automation system to implement intelligence-led policing into the National Police of Ukraine. *Cybernetics and Systems Analysis*, 54, 643-649. doi: 10.1007/s10559-018-0065-5.
[26] Movchan, A.V., Yankovyi, M.O., Ismailov, K.Yu., Melnikova, E.O., & Zaiets, O.M. (2021). Countering illegal drug trafficking on the Internet: Topical issues. *Pakistan Journal of Criminologythis*, 14(2), 95-108.
[27] Pantazidis, A., Gazis, A., Soldatos, J., Touloupou, M., Kapassa, E., & Karagiorgou, S. (2023). Trusted virtual reality environment for training security officers. In *2023 19th International conference on distributed computing in smart systems and the Internet of things (DCOSS-IoT)* (pp. 518-524). Pafos: IEEE. doi: 10.1109/DCOSS-IoT58021.2023.00086.
[28] Phillips, R., & Wilder, H. (2020). Tracing cryptocurrency scams: Clustering replicated advance-fee and phishing websites. In *2020 IEEE international conference on blockchain and cryptocurrency (ICBC)*. doi: 10.1109/ICBC48266.2020.9169433.
[29] Rueckert, C. (2019). Cryptocurrencies and fundamental rights. *Journal of Cybersecurity*, 5(11). doi: 10.1093/cybsec/tyz004.
[30] Samoilenko, O.A., & Titunina, K.V. (2023). Typical forensic means of investigating criminal offenses related to the use of cryptocurrencies. *Current Issues in Modern Science*, 7, 409-420. doi: 10.52058/2786-6300-2023-7(13)-409-420.
[31] SBI: The special services of the Russian Federation use the drug mafia to "put" Ukrainians on drugs. (2022). Retrieved from https://kp.ua/ua/incidents/a661548-dbr-spetssluzhbi-rf-vikoristovujut-narkomaniju-shchob-posaditi-ukrajintsiv-na-narkotiki.

[32] Schmidt, A. (2021). Virtual assets: Compelling a new anti-money laundering and counter-terrorism financing regulatory model. *International Journal of Law and Information Technology*, 29(4), 332-363. doi: 10.1093/ijlit/eaac001.

[33] Siu, G.A., Hutchings, A., Vasek, M., & Moore, T. (2022). “Invest in crypto!”: An analysis of investment scam advertisements found in Bitcointalk. In *2022 APWG symposium on electronic crime research (eCrime)*. Boston: IEEE. doi: 10.1109/eCrime57793.2022.10142100.

[34] Swartz, L. (2022). Theorizing the 2017 blockchain ICO bubble as a network scam. *New Media and Society*, 24(7), 1695-1713. doi: 10.1177/14614448221099224.

[35] Taylor, S.K., Ariffin, A., Zainol Ariffin, K.A., & Sheikh Abdullah, S.N.H. (2021). Cryptocurrencies investigation: A methodology for the preservation of cryptowallets. In *2021 3rd international cyber resilience conference (CRC)*. Langkawi Island: IEEE. doi: 10.1109/CRC50527.2021.9392446.

[36] The largest cryptocurrency exchange will pay a record fine of $4.3 billion. (2023). Retrieved from https://ua.korrespondent.net/business/financial/4642325-naibilsha-kryptovaluitna-birzha-splatyt-rekordnyi-shtraf-na-43-mlrd.

[37] Trozze, A., Davies, T., & Kleinberg, B. (2023). Explaining prosecution outcomes for cryptocurrency-based financial crimes. *Journal of Money Laundering*, 26(1), 172-188. doi: 10.1108/JMLC-10-2021-0119.

[38] Unified state register of court decisions. (n.d.). Retrieved from https://reyestr.court.gov.ua.

[39] Utkina, M., Samsin, R., & Pochtovyi, M. (2023). Financial intelligence (monitoring) of the transactions with virtual assets: New legislation and best practices of foreign countries. *Journal of Money Laundering Control*, 26(2), 349-360. doi: 10.1108/JMLC-12-2021-0136.

[40] Xia, P., Wang, H., Zhang, B., Ji, R., Gao, B., Wu, L., Luo, X., & Xu, G. (2020). Haracterizing cryptocurrency exchange scams. *Computers and Security*, 98, article number 101993. doi: 10.1016/j.cose.2020.101993.

Розслідування злочинів про фінансування криптовалютою тероризму та збройної агресії

Анатолій Васильович Мовчан

Доктор юридичних наук, професор
Львівський державний університет внутрішніх справ
79000, вул. Городоцька, 26, м. Львів, Україна
https://orcid.org/0000-0002-6997-6517

Олександр Анатолійович Шляховський

Доктор філософії в галузі права, доцент
Львівський державний університет внутрішніх справ
79000, вул. Городоцька, 26, м. Львів, Україна
https://orcid.org/0000-0001-8181-1857

Василь Васильович Козій

Кандидат юридичних наук, докторант
Львівський державний університет внутрішніх справ
79000, вул. Городоцька, 26, м. Львів, Україна
https://orcid.org/0000-0002-8221-6678

Ігор Андрійович Федчак

Кандидат юридичних наук, доцент
Львівський державний університет внутрішніх справ
79000, вул. Городоцька, 26, м. Львів, Україна
https://orcid.org/0000-0002-4359-5988

Анотація. Статтю присвячено дослідженню проблем розслідування злочинів про фінансування криптовалютою тероризму та збройної агресії, що актуально з огляду на напад на Україну російської федерації, а також у зв'язку зі значним поширенням та використанням криптовалюти для фінансування як тероризму, так і збройної агресії. Метою статті є дослідження проблем розслідування злочинів про фінансування криптовалютою тероризму та збройної агресії й пошук шляхів та способів вирішення проблемних питань, адже фінансування криптовалютою тероризму та збройної агресії є посяганням на національну безпеку. Під час дослідження використано методи системного аналізу та техніко-юридичного аналізу, а також формально-логічний метод, що дало змогу визначити способи вчинення злочинів досліджуваної категорії. Висвітлено недоліки у правовому регулюванні обігу і використання криптовалюти в Україні, а також у правовому регулюванні розслідування злочинів, пов'язаних із незаконним заволодінням та використанням криптовалюти в злочинних цілях, і передусім для фінансування тероризму та збройної агресії. Визначено юрисдикційні проблеми злочинів цієї категорії, їх високу латентність через відсутність належних правових процедур та методик розслідування. Обґрунтовано необхідність створення у правоохоронних органах спеціалізованих підрозділів, до компетенції яких буде відноситися виявлення та розслідування вказаних злочинів, їх активної взаємодії з кіберполіцією. Акцентовано увагу та необхідності запровадження системи постійного моніторингу соціальних мереж, мережі інтернет, медіа та проведення OSINT-розвідки з відкритих джерел з метою виявлення та припинення такої злочинної діяльності, відстеження, арешту і зрештою вилучення криптовалюти, у разі наявності такої можливості, та її подальшої конфіскації. Розроблено практичні рекомендації щодо розслідування злочинів про фінансування криптовалютою тероризму та збройної агресії. Наголошено на необхідності міжнародно-правового співробітництва у цій сфері, необхідності залучення до процесу розслідування загалом та до конкретних слідчих дій фахівців у сфері інформаційних технологій, програмування, інженерії блокчейну. Сформульовано вимоги до фіксації доказів у протоколах слідчих дій у ході розслідування злочинів цієї категорії, зокрема вказано про необхідність гешування файлів. Практичне значення дослідження полягає в тому, що одержані результати можуть використати працівники правоохоронних органів під час розслідування злочинів досліджуваної категорії, а також у подальших наукових дослідженнях за вказаною тематикою

Ключові слова: віртуальні активи; блокчейн; злочини у сфері криптовалют; пошук доказів; OSINT-розвідка; відстеження переказів криптовалюти