IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

Peculiarities of recording electronic evidence in criminal proceedings regarding crimes committed in Ukraine using cryptocurrencies

Vasyl Kozii
Prosecutors Training center of Ukraine

Inha Kalancha
Borys Grinchenko Kyiv Metropolitan University

Hanna Vlasova
Borys Grinchenko Kyiv Metropolitan University

Andriy Orlean
National Academy of Internal Affairs

Date of submission: June 2024
Accepted in: September 2024
Published in: March 2025

Abstract

The article is devoted to studying the problems of recording electronic evidence in criminal proceedings regarding crimes committed in Ukraine using cryptocurrencies, which is relevant in view of the significant spread and use of cryptocurrencies and crimes committed through their use. During the study, the methods of system analysis and technical-legal analysis were employed, alongside the formal-logical method. The shortcomings in the legal regulation of the investigation of crimes committed using cryptocurrencies were highlighted. Practical recommendations have been developed for involving experts in the fields of computer technologies, programming, and information security in the recording of electronic evidence in criminal proceedings concerning crimes committed with the use of cryptocurrencies. The requirements for recording electronic evidence while investigating crimes committed using cryptocurrencies (virtual assets) are formulated. In particular, the need to copy, archive and hash files is specified. The use of appropriate software is suggested. The practical significance of the study is that the obtained results can be used by operatives, investigators, prosecutors and detectives during the investigation of crimes of the studied category, as well as during further scientific research on the specified topic.

Keywords

criminal procedure; electronic evidence; digital evidence; virtual assets; blockchain; cryptocurrency; hashing

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

Peculiaridades del registro de pruebas electrónicas en procedimientos penales con respecto a delitos cometidos en Ucrania utilizando criptomonedas

Resumen

Este artículo se dedica a estudiar los problemas en el registro de pruebas electrónicas en procedimientos penales relacionados con delitos cometidos en Ucrania utilizando criptomonedas, lo que es relevante en vista de la significativa propagación y uso de criptomonedas y de delitos cometidos a través de su uso. Durante el estudio, se emplearon los métodos de análisis de sistema y análisis técnico-legal, junto con el método formal-lógico. Se destacaron las deficiencias en la regulación legal de la investigación de delitos cometidos utilizando criptomonedas. Se han desarrollado recomendaciones prácticas para involucrar a expertos en los campos de las tecnologías informáticas, la programación y la seguridad de la información en el registro de pruebas electrónicas en procedimientos penales relacionados con delitos cometidos con el uso de criptomonedas. Se formulan los requisitos para registrar pruebas electrónicas mientras se investigan delitos cometidos utilizando criptomonedas (activos virtuales). En particular, se especifica la necesidad de copiar, archivar y etiquetar (hash) archivos. Se recomienda el software adecuado a utilizar. La importancia práctica del estudio es que los resultados obtenidos pueden ser utilizados por operadores, investigadores, fiscales y detectives durante la investigación de delitos de la categoría estudiada, así como durante investigaciones científicas adicionales sobre el tema especificado.

Palabras clave

procedimiento penal; prueba electrónica; prueba digital, activos virtuales; cadena de bloques; criptomoneda; hash

Introduction

In recent years, cryptocurrencies (virtual assets) have become incredibly popular because they are an electronic form of value expression and can ensure the confidentiality of ownership. The cryptocurrency industry includes online exchanges, exchange services, various decentralized services and software – multi-cryptocurrency wallets designed for buying, storing and exchanging virtual assets.

The importance and prevalence of the cryptocurrency industry are astounding. As of 05-15-2024, there are more than 2.4 million different cryptocurrencies and 765 exchanges that trade and exchange them, with a market volume of more than 2.27 trillion US dollars (CoinMarketCap, 2024).

Cryptocurrencies are a highly convenient, confidential financial instrument. In many cases, they are used legally within a legal framework that does not prohibit their use for legal purposes – as a means of saving and multiplying capital, exchanging, etc.

At the same time, the confidentiality of cryptocurrencies is of great interest to criminals and even criminal regimes, as it can satisfy their illegal needs: the purchase of narcotic drugs and other prohibited substances, weapons, financing of terrorism and armed aggression, payment for illegal services, circumvention of sanctions imposed on individuals and states, etc. Additionally, cryptocurrencies, like any financial resource, may be subject to illegal appropriation. Such theft occurs through hacking cryptocurrency exchanges and individuals' wallets, deception under the pretext of investing in fraudulent projects, and the use of malicious software and phishing.

On 20 April 2023, the European Parliament adopted a historic decision for the crypto-assets market. It approved new general rules for the supervision and protection of consumer rights regarding cryptocurrencies - Markets in Crypto-assets Regulation (MiCA) (EU, 2023).

The legal regulation of cryptocurrencies in Ukraine is still at an initial stage. The Ukrainian legislator uses the term "virtual assets". The Law of Ukraine "On Virtual Assets", which classifies virtual assets as intangible assets, was adopted on 17 February 2022 (UKRAINE, 2022). However, as of mid-2024, it has not entered into force, and accordingly, the legal status of virtual assets in Ukraine is actually not defined.

In part 10 of Art. 170 of the Criminal Procedure Code of Ukraine, there is a reference to virtual assets in the context of the possibility of their seizure.

In the Criminal Code of Ukraine, the term "cryptocurrency" is mentioned only once, namely in Part 3 of the footnote to Art. 368-5, where it is classified as an asset and is accordingly recognized as a subject of unlawful gain (UKRAINE, 2001).

In general, the term "cryptocurrency" corresponds to the concept of "virtual assets". However, due to the disparity of terms, there will be room for discussion among scientists and practitioners.

In criminal justice, the investigation of crimes committed using cryptocurrency is new and incomprehensible for most law enforcement officers, except for specific units of the Cyber Police.

A key feature of investigating crimes committed using cryptocurrencies is that the evidence of their commission is in electronic form. And in many cases, to identify guilty individuals, an investigator, cyber police officer, operative or detective does not need to leave the office. Having a computer with Internet access, specialized software, relevant knowledge, skills and abilities is sufficient.

Kim, Ihm and Son (2021) propose using a two-level blockchain system to manage digital evidence and preserve it properly. In the criminal investigation process, the frequently changing information should be stored in the hot blockchain, and immutable data, such as video, in the cold blockchain.

Among related scientific works, the study of O.V. attracts attention. Kreminsky (2022), who considers the legalization (laundering) of criminally obtained income in the context of the use of virtual currencies, views it as the legalization of criminally obtained financial funds, involving the application of conversion with virtual currency. In connection with this, it was established that the process of legalization (laundering) of criminally obtained income in the context of the use of virtual currencies could proceed through distinct stages such as placement (at this stage it is easiest to detect illegally obtained funds), stratification (separation of illegal income from its sources through a chain of transactions or special manipulations aimed at masking the traces of this income) and integration (revealing the facts of legalization is possible only with the aid of agency work).

As for foreign research, the works of scholars such as Maurushat and Halpin (2022) attract attention, as they consider cryptocurrencies a tool for online fraud and analyse the challenges associated with investigating fraud involving cryptocurrency investments.

The study by Madhavan and Kalabaskar (2022) is dedicated to the digital forensic investigation of Ponzi schemes.

The research by Siu, Hutchings, Vasek and Moore (2022) examined the evolution of investment fraud lures and fraud-related keywords on the online cryptocurrency forum Bitcointalk over 12 years.

Schmidt (2021), examining the risks of virtual assets countering money laundering and terrorist financing, recommends expanding the regulatory framework to include regulations that are native to the peer-to-peer nature of virtual assets to eliminate risks.

Mandela, Mahmoud and Shaker (2023) examine the forensic aspects of the Darknet state concerns for law enforcement agencies and cybersecurity experts due to its association with illegal activities such as drug trafficking, money laundering and cybercrime. They rightly point out that Darknet forensics involves the collection, analysis, and preservation of digital evidence, which is problematic due to anonymity, encryption, and the use of cryptocurrencies.

In 2021, the Spanish government introduced the Anti-Money Laundering Directive into national law, which was approved by the European Council in 2018. At the same time, King Philip VI of Spain and the Parliament adopted and approved the definition according to which virtual currencies are a digital equivalent of value, not issued or guaranteed by a central bank or government body. In addition, Spanish Law No. 112/2021 was passed, which clearly defines the obligations of those who provide financial services related to these digital assets. Cryptocurrency operators, that is, exchanges, must fulfil three conditions to be able to operate in Spain:

1) register as a cryptocurrency operator with the Central Bank of Spain;

2) identify their customers through the "Know your customer" procedure;

3) verify the origin of the funds in circulation (AML) (Spain, 2021).

However, until now, in the scientific doctrine, issues related to the investigation of crimes of this category and the peculiarities of recording electronic evidence in such

cases, considering the specifics of Ukrainian criminal procedural legislation, remain little researched.

This article aims to study the peculiarities of recording electronic evidence in criminal proceedings concerning crimes committed using cryptocurrencies, analyse problematic issues in this area and develop an algorithm for recording electronic evidence in criminal proceedings involving crimes committed using cryptocurrencies in Ukraine.

1. Materials and methods used in the research

During the research, the methods of system analysis, technical-legal analysis, and formal-logical analysis were used, which made it possible to determine the methods of recording electronic evidence in criminal proceedings regarding crimes committed using cryptocurrencies.

To clarify the state of regulatory and legal regulation in the field of cryptocurrencies in Ukraine, the Law of Ukraine "On Virtual Assets" and the provisions of the Criminal and Criminal Procedure Code of Ukraine were studied using the methods of systemic analysis and technical-legal analysis. This made it possible to conclude the insufficiency of legal regulation of social relations in the specified sphere. The works of domestic and foreign scientists were processed and analysed to determine the state of research on the peculiarities of recording electronic evidence in criminal proceedings regarding crimes using cryptocurrencies.

This allowed us to identify issues that are not covered by the specified research, as well as issues that require thorough investigation, to propose ways and means of solving existing problems. System analysis methods and formal logic made it possible to determine the peculiarities of recording electronic evidence regarding crimes committed using cryptocurrencies in criminal proceedings. They also help form optimal approaches to such recording and conclude the need to archive and hash files containing information important for solving criminal proceedings.

During the research, the scientific database Scopus was used, which processed scientific works accessible by the search terms "electronic evidence", "cryptocurrency" and "virtual assets". In total, more than 500 scientific papers related to this sphere were developed. However, most were not used because they did not directly relate to this topic. Accordingly, the study used more than 20 studies related to the subject.

During the research, such web resources as CoinmarketCap, Blockchair and Internet Archive were used. Thanks to the CoinmarketCap resource, knowledge was gained about the virtual assets industry as a whole, market capitalization, its main players, links to cryptocurrency exchanges and blockchains tracked by the specified resource, and familiarization with them. Thanks to the internet resource Blockchair, the possibilities of tracking transactions in the blockchains supported by it, primarily in the Bitcoin, Ethereum, Bitcoin Cash, Solana, Tron, etc. networks have been investigated.

Studying the technical capabilities of such a resource as the Internet Archive proved its possibility and expediency for obtaining electronic digital evidence files.

The possibility of using the Wayback Machine when searching for pages on the internet that were deleted or altered to conceal traces of criminal activity was also considered. The technical capabilities and features of working with the Crystal and Chainalysis software to analyse and track transactions in the blockchains of specific cryptocurrencies were examined during the study. The technical capabilities and features of recording electronic evidence in criminal proceedings for the studied category of programmes, such as Mozilla Firefox with the Easy YouTube Video Downloader Express extension and the MediaInfo and RapidCRC Unicode programmes were also investigated.

Also, in the process of research, the practice of Ukrainian courts on this issue was studied, namely, the monitoring of the Unified State Register of Court Decisions, in which 140 guilty verdicts and decisions of investigating judges in criminal proceedings about crimes committed were processed using cryptocurrency (virtual assets). This made it possible to establish that in this category of proceedings, without the use of electronic (digital) evidence, it is impossible to form an evidence base.

Also, in the process of research, the practice of Ukrainian courts on this issue was studied, namely, the monitoring of the Unified State Register of Court Decisions, in which 140 guilty verdicts and decisions of investigating judges in criminal proceedings regarding crimes committed were processed using cryptocurrency (virtual assets). This made it possible to establish that in this category

of proceedings, without electronic (digital) evidence, it is impossible to form a reliable evidence base.

2. Evidence in proceedings regarding crimes committed using cryptocurrencies

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

Movchan and Kozii (2022) include the main types of crimes in this area:

1) hacking of cryptocurrency exchanges and electronic wallets;

2) theft of cryptocurrency by the exchanges themselves;

3) various fraudulent schemes,

as a result of which, individuals who have purchased cryptocurrencies may lose them. Such fraudulent schemes may include: the voluntary transfer of cryptocurrencies to a fraudulent platform; loss of cryptocurrencies due to phishing, computer or smartphone hacking, where information about cryptocurrency wallets and their private keys is sent to attackers as a result of malicious software aimed at stealing them; a scam, i.e. the sale of a new cryptocurrency or token, the value of which is deliberately "inflated" by criminals who receive the excess profits, leaving buyers with a worthless cryptocurrency or token that no one needs; and the creation of cryptocurrency clones with no value.

Fraud in the exchange of cryptocurrencies, as described in the work of Pengcheng *et al*. (2020), is becoming increasingly widespread.

Cryptocurrency "network fraud" is also common, which is the subject of a scientific study by Swartz (2022).

In many cases, crimes of this category have a high latency; their investigation is extremely difficult, and law enforcement agencies in Ukraine are increasingly encountering cases in the field. According to the Economic Security Bureau of Ukraine report, detectives exposed a financial company through which virtual assets were converted into hryvnias and funds were withdrawn in cash. Detectives conducted 11 searches, during which they seized unaccounted cash in hryvnias and foreign currency equivalent to approximately 13 million hryvnias, as well as five cold keys for crypto wallets, mobile phones, laptops, and draft documentation confirming illegal activities. The court ordered the seizure of virtual assets valued at almost UAH 28.5 million, stored on one of the well-known crypto exchanges. The pre-trial investigation is ongoing (Economic Security Bureau of Ukraine, 2024).

At the same time, in other countries recently, there have also been significant cases of people brought to justice for committing crimes in the field of cryptocurrencies. According to a Reuters report dated 1 May 2024, Changpeng Zhao, the founder of the world's largest crypto exchange, Binance, was sentenced to four months in prison in the USA. According to the indictment, Binance management was aware of transactions related to the financing of terrorism, child pornography, and other illegal activities, but the platform did not inform law enforcement agencies. In March 2024, a court in the USA sentenced Sam Bankman-Fried, the founder of the bankrupt crypto exchange FTX, to 25 years in prison for stealing money from clients. Before the bankruptcy, this exchange was one of Binance's main competitors (Bloom & Stempel, 2024).

According to Bitcoin Magazine, dated 30 May 2024, well-known investor and businessman Roger Ver was arrested in Spain on criminal charges by the US Department of Justice for tax evasion and filing false tax returns. The indictment alleges that from 2011 to 2014, Ver bought bitcoins for himself and his companies, amassing about 131,000 BTC worth approximately $240 million at the time. In 2014, Ver received citizenship of the island nation of St. Kitts and Nevis and soon renounced his US citizenship in a process known as expatriation. As a result, he became subject to US tax laws, including having to report capital gains from the sale of his assets around the world, including bitcoins, and pay the corresponding tax (Hoffman, 2024).

According to the press service of the US Department of Justice, a court in Texas sentenced Ukrainian hacker

Yaroslav Vasinsky to 13.5 years in prison and a fine of $16 million for cybercrimes. It is noted that Vasinsky was in the Revil group and participated in more than 2,500 attacks using ransomware. Together with accomplices, they hacked thousands of computers worldwide and demanded a ransom of more than $700 million for not disclosing the personal data of the victims (Office of Public Affairs, U.S. Department of Justice, 2024)

All these cases of investigations, prosecutions, and convictions of individuals for committing crimes in the field of cryptocurrencies have in common that the basis of the evidence is primarily not the testimony of witnesses or suspects and accused individuals, but rather electronic evidence.

3. Search and recording of evidence in proceedings regarding crimes committed using cryptocurrencies: recommendations and algorithms

In the Ukrainian scientific doctrine, electronic evidence is considered to be information that is stored electronically in any type of electronic media, in electronic devices, or in electronic information systems, and that meets the requirements of Art. 84 of the Criminal Procedure Code of Ukraine.

The study of the concept of electronic evidence in criminal proceedings allowed Kozytska (2020) to conclude that electronic evidence is essentially a digital object that serves as proof that some criminal offence has been committed, preserves electronic digital traces of a criminal offence, is a subject or object of a criminal offence, or contains other information that may be used as evidence of a fact or circumstance established during criminal proceedings.

In criminal proceedings concerning crimes committed using cryptocurrencies, depending on the specific case, evidence can include information from the blockchains of various virtual assets, data provided by exchanges, as well as various exchange resources, and information contained in open sources on the Internet. Such evidence may consist of malicious software to be removed, electronic correspondence between suspects and victims, and software found on the electronic devices of suspects – such as multi-currency cryptocurrency wallets like Via Wallet, Trust Wallet, Komodo, Coinomi, etc. – or cold cryptocurrency wallets such as Ledger Nano and Trezor etc.

When committing crimes in the field of cryptocurrencies, electronic digital traces are left, which, in particular, can include correspondence on the Internet, posts, photos, and videos contained in social media (for example, in applications such as Telegram, Viber, Signal, WhatsApp, etc.). This can consist of content in social networks (YouTube, Facebook, TikTok, etc.), as well as links to Internet resources and various types of malicious links, including messages with transaction confirmation codes sent to the email of persons who initiated and carried out such transactions out.

In many cases, such electronic (digital) evidence is quickly deleted or altered by criminals to make it untraceable. Therefore, in this category of criminal proceedings, in order to establish an appropriate evidence base regarding the relevant criminal activity, it is necessary to promptly capture electronic (digital) information using the available procedural and technical tools

When searching for and recording evidence in cryptocurrency crime proceedings, it is important to observe both the procedural and technical aspects, which are quite extensive and, therefore, require research and structuring to develop appropriate guidelines and algorithms.

First of all, we will consider the procedural aspect of this process, which for Ukraine consists of:

1) Ukrainian criminal procedural legislation, which primarily includes the Criminal Procedural Code of Ukraine, and specific laws regulating the work of electronic documents, such as, for example, the Law of Ukraine "On Electronic Documents and Electronic Document Management" as well as the Law of Ukraine "On Electronic Trust Services";

2) international legislation regulating the field of search, collection and recording of electronic evidence, the most important of which are the Berkeley Protocol and the Budapest Convention.

In the Ukrainian context, the procedural aspect includes choosing the correct form of recording electronic evidence. The investigative (search) action, which must be promptly undertaken in such cases, is the review of elec-

tronic documents and computer data, under Art. 237 of the CPC of Ukraine.

The next element consists of compliance by the investigator and prosecutor with the requirements of part 4 of Article 99 of the Criminal Code of Ukraine regarding the need to involve a specialist. In this aspect, the formal fulfilment of the requirement of the Criminal Procedure Code of Ukraine regarding the involvement of a specialist does not guarantee the identity of the copy of the original information. The specialist engaged by the prosecution must possess the necessary knowledge and skills in the field of information technology and be able to correctly copy electronic data, which must include verifying (checking) the integrity and authenticity with the provision of appropriate guarantees. In some cases, the formal involvement of a specialist when copying electronic data, with non-compliance with technical aspects to guarantee the integrity and authenticity of this data, can discredit the produced copy (Kalancha & Harkusha, 2021).

Since proper fixation requires special knowledge and skills, before carrying out such an investigative (search) action as specialists, under the requirements of Art. 71 of the CCP of Ukraine it is necessary to attract specialists in the field of computer technologies, programming, and information security. They can also be specialists who work on cryptocurrency exchanges, if necessary, programmers. Specially trained and authorized investigators and prosecutors should ensure the investigation process.

Making a copy of computer data is mandatory because, according to Part 4 of Art. 99 of the Criminal Procedure Code of Ukraine, it must be recognized by the court as the original document. Creating such copies (which are actually identical to the original, i.e. duplicates) will allow them to be presented as evidence in court, and in the case of damage or loss of the originals of the corresponding electronic (digital) evidence, the court will recognize the duplicates as the original and, accordingly, proper and admissible evidence.

When conducting reviews of electronic information that may be contained in electronic documents, video recordings, and computer data, it is important to consistently and fully indicate exactly what actions are taken, which information, files, or programs are reviewed, on which gadgets, sites, social networks, or messengers they are located, by which links they are accessed, with which software they are used, and what their content is.

Another important element of the procedural aspect that we are investigating is compliance with the requirements of clause 3 part 3 p. 104 of the Criminal Procedure Code of Ukraine, which indicates the requirements for the final part of the protocol of the investigative (search) action. This must contain information about the duplicate documents produced, as well as copies of information, including computer data, and the method of their identification. This aspect is extremely important because it aims to ensure the possibility of confirming the integrity and immutability of electronic evidence, while preventing the risks of their change.

The Berkeley Protocol provides international requirements for certain aspects of electronic evidence capture that must be followed, including data archiving. This requirement, in our opinion, although not a legally established requirement, plays an important role in ensuring the storage of a backup copy of electronic evidence on a recognized electronic archival resource.

In the context of the Budapest Convention, it should be noted that compliance with its norms is important when using its mechanisms for obtaining electronic evidence and is not mandatory in all cases.

In addition to compliance with procedural norms, the need to comply with the technical aspects of the process of finding and recording evidence in proceedings regarding crimes committed using cryptocurrencies is obvious, the importance of which is difficult to overestimate.

The technical aspect of the investigated process has:

1) a technical component – rules and actions of a non-procedural nature that must be done with electronic evidence;

2) software component – technical software products that must be used for searching and recording electronic evidence.

In the Ukrainian context, to ensure the technical aspect of the process of copying information, it is advisable to apply SSTC ISO/IES 27037:2017 (ISO/IES 27037:2012, IDT) "Information technologies. Protection methods. Guidelines for

identification, collection, acquisition and preservation of digital evidence" (SSTC ISO/IEC 27037:2017, 2019).

The standard distinguishes between the processes of making a physical or bit-by-bit copy (image) of electronic media and a copy of a separate electronic file. A specific block of electronic information with a specified name, size, and attributes is copied when copying a specific file. In the case of making a physical copy of an electronic data carrier, all information blocks of the data carrier intended for data storage (from the first to the last bit) are copied sequentially. The creation of such a copy represents the creation of an image of information from an electronic information carrier that is identical to the original. During the subsequent examination of the physical copy of the electronic information carrier, it is possible to restore deleted electronic data that were not detected by the initial review of the electronic information carrier, which was conducted only in part of the existing files (Kalancha & Harkusha, 2021).

SSTC ISO/IES 27037:2017 describes in detail the conditions under which the copying of information for use in legal procedures can be considered reliable and permissible from a technical point of view. In general, it is worth highlighting two requirements:

1) the inadmissibility of making changes to the primary information that is the object of copying, before the beginning of copying, during and after it is carried out;

2) verification (checking) of a copy of the information by hashing the primary information, a copy of the information, and comparing the received hash values.

This provides an opportunity to mathematically check and confirm the integrity and authenticity of a copy of the information recorded on the target electronic media (SSTC ISO/IEC 27037:2017, 2019). In this context, we can see a connection between the requirement for hashing from the SSTC ISO/IES 27037:2017 and the need to reflect the method of identification of electronic data in the protocol of investigative (search) actions from clause 3, part 3, p. 104 of the Criminal Procedure Code of Ukraine. The uniqueness of hash values (hashes) can be a highly effective method of identifying electronic data.

According to the results of hashing, file hashes are indicated in the protocol, which allows us to check their authenticity at any time and confirm that no changes have been made to the files after they were saved. If, in court, the defence questions the authenticity of the electronic evidence being examined or indicates that changes were made to it after it was secured and archived, thus constituting falsification of evidence, then checking the hashes of the relevant files enables one to refute or confirm.

It is important to note that DSTU ISO/IEC 27037:2017 is not a unique work of Ukrainian specialists but was created based on the international standard ISO/IEC 27037:2012 Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. That is, in this aspect, Ukrainian requirements for collecting, obtaining and preserving digital evidence meet international standards.

As rightly noted by Jaromir Weber and Zdenek Smutny (2015) in the article Standard ISO 27037:2012 and Collection of Digital Evidence: Experience in the Czech Republic, the ISO/IEC 27037:2012 standard in several places notes the need to calculate checksums to verify data integrity, but it is not sufficiently emphasized that these values obtained during hashing should be recorded directly in the protocol of the procedural action. Fulfilment of this requirement can ensure verification of the collected evidence for integrity and authenticity. In our opinion, the mass introduction by Ukrainian bodies of pre-trial investigation of the European experience, which involves the hashing of electronic evidence, will have a positive effect on the criminal process of Ukraine.

The software component of the technical aspect of the process of recording evidence in proceedings regarding crimes committed using cryptocurrencies is very important because it acts as a tool by which this process is carried out. It includes various software products.

When reviewing, it is recommended to use programmes such as Mozilla Firefox with the Easy YouTube Video Downloader Express extension, as well as MediaInfo and RapidCRC Unicode. At the same time, 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 onto the data carrier. In the future, you need to copy the photo or video files using the software. It is important to fix the metadata of the copied files. For this, it is advisable to use the MediaInfo programme. Hashing, that is, the calculation of file hash codes, is carried out using the

RapidCRC Unicode programme. File hash codes are to be specified in the protocol. Web resources can be archived using the Internet Archive service (digital library). Using the Wayback Machine resource at the specified link is also possible, which can help if the content is selected or changed in pages on the internet (Movchan *et al*. 2023).

It is also necessary to record cryptocurrency transactions in this category of proceedings. In the case of access to cryptocurrency wallets, all transactions that have taken place must be sequentially recorded in the review protocol. Usually, this should be done in chronological order; however, if the subject of proof is a specific transaction or multiple transactions, then only one or those separate transactions should be recorded and described. At the same time, the hash of each transaction, the addresses of the wallets (both the one from which the transfer was made and the one to which it was made), the name and number of cryptocurrencies in each transaction, as well as other relevant data, should be indicated. If the wallet was accessed using the seed phrase, then this must also be indicated. In this case, the protocol must consistently reflect the process of creating a new wallet, which the investigator, the prosecutor, the pre-trial investigation body, or the prosecutor's office control, and consistently describe the process of transferring cryptocurrency to the new wallet. At the same time, the mnemonic (seed) phrase belonging to the newly created wallet cannot be indicated in the protocol. It should be kept separately in the criminal proceedings in a sealed form, preventing unauthorized access.

If the subject of proof is individual transactions, they can also be recorded in electronic form by examining the relevant cryptocurrency wallets, if accessible, and by examining blockchains. A resource such as Blockchair may be sufficient for this.

However, if we are talking about thousands or tens of thousands of transactions, as well as the use of bridges and cross-chains, as well as decentralized exchangers and mixers to make the traces more confusing, then special software from companies such as Crystal, Chainalysis, Global Vision, etc., must be used to track transactions. Thanks to such special programmes, it is possible to establish connections between cryptocurrency wallets and identify them as belonging to specific exchanges. Subsequently, one can receive personal data and block cryptocurrency by submitting requests to the compliance service of these exchanges (if the user is verified). Quite a lot of other technical information can be obtained situationally. For example, it can include data on the complete trading history of a certain account, methods of replenishing the exchange account with bank cards, if such replenishment took place, IP addresses from which the account was accessed, etc. All this data can be used as evidence in specific criminal proceedings. However, it should be noted that access to such programmes is paid and can amount to tens of thousands of US dollars per year.

Therefore, the results of the conducted research indicate the need to develop and implement in Ukraine unified algorithms for recording electronic evidence in criminal proceedings regarding crimes committed using cryptocurrencies. This state of affairs is due to the insufficiency of legal regulation in this sphere of social relations, as well as the lack of established practices and approaches for investigating criminal proceedings of this category.

Conclusions

The study of scientific sources, legislation, and practical cases related to the recording of electronic evidence in criminal proceedings concerning crimes committed using cryptocurrencies allowed us to formulate the following guidelines for the investigation of these crimes:

a) the investigation process must be ensured by specially trained and authorized investigators and prosecutors;

b) must follow the requirements of part 4 of Article 99 of the Criminal Code of Ukraine regarding the need to involve a specialist. This specialist must have knowledge and skills in the field of information technology and be able to correctly copy electronic data, verify the integrity and authenticity with the provision of appropriate guarantees;

c) the process of searching for and recording evidence in the technical aspect must meet the requirements of the SSTC ISO/IES 27037:2017;

d) creation of a bit-by-bit copy of computer data discovered during a search or inspection is mandatory;

e) according to the hashing results of electronic data, hashes of these files must be specified in the protocol;

f) during a search or inspection, need to use programs such as Mozilla Firefox with the Easy YouTube Video Downloader Express extension, as well as MediaInfo and RapidCRC Unicode;

g) all cryptocurrency transactions that have taken place must be sequentially recorded in the review protocol. This should be done in chronological order, collecting the hash of each transaction, the addresses of the wallets, the name and number of cryptocurrencies in each transaction, as well as other data;

h) the protocol must consistently reflect the process of creating a new wallet, which the investigator or the prosecutor controls, and consistently describe the process of transferring cryptocurrency to the new wallet. The mnemonic (seed) phrase belonging to the newly created wallet should be kept separately in the criminal proceedings in a sealed form, preventing unauthorized access.

The acquired results are of great practical significance, as they form the basis for creating and applying successful cybersecurity systems at different scales. The software tools and methods developed can help states and organisations improve their cybersecurity posture and lower cyberattack risks. In light of this study's findings, it is advised to conduct more thorough research on contemporary trends in cyberterrorism and constantly enhance strategies for thwarting cyber threats. Additionally, it's critical to keep creating and enhancing software tools for network monitoring and cyberattack defence.

References

BLOOM, D.; STEMPEL, J. (2024, May). "Binance crypto founder Zhao sentenced to four months in prison". *Reuters*, [online]. Available at: https://www.reuters.com/legal/binances-ceo-zhao-faces-sentencing-over-money-laundering-violations-2024-04-30

COINMARKETCAP (2024). "Today's Cryptocurrency Prices by Market Cap". *CoinMarketCap* [online]. Available at: https://coinmarketcap.com

ECONOMIC SECURITY BUREAU OF UKRAINE (2024, May). "The Bureau of Economic Security in the Lviv region exposed a financial company illegally exchanging cryptocurrency". *Economic Security Bureau of Ukrain*e [online]. Available at: https://esbu.gov.ua/news/biuro-ekonomichnoi-bezpeky-u-lvivskii-oblasti-vykrylo-finkompaniiu-shcho-nelehalno-obminiuvala-kryptovaliutu

EU (2018). 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. *Eur-Lex* [online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018L0843

EU (2023). REGULATION (EU) 2023/1114 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937. *Official Journal of the European Union*. L 150/41, 9.6.2023 [online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R1114

HOFFMAN, N. (2024, April). "Doj arrests early bitcoin investor Roger Ver, 'bitcoin jesus,' on charges of tax fraud". *Bitcoin Magazine* [online]. Available at: https://bitcoinmagazine.com/legal/doj-arrests-early-bitcoin-investor-roger-ver-bitcoin-jesus-on-charges-of-tax-fraud

KALANCHA, I. H.; HARKUSHA, A. M. (2021). "Copy of electronic information as evidence in criminal proceedings: procedural and technical aspects". *Juridical scientific and electronic journal*, no. 8, pp. 336-339. DOI: https://doi.org/10.32782/2524-0374/2021-8/77

KIM, D.; IHM, S.-Y.; SON, Y. (2021). "Two-Level Blockchain System for Digital Crime Evidence Management". *Sensors*, vol. 21, no. 9. DOI: https://doi.org/10.3390/s21093051

KOZYTSKA, O. H. (2020). "Regarding the concept of electronic evidence in criminal proceedings". *Legal scientific electronic journal*, no. 8. pp. 418-421. DOI https://doi.org/10.32782/2524-0374/2020-8/103

KREMINSKY, O. V. (2022). "Investigating the legalization (laundering) of proceeds obtained by crime in the context of the use of virtual currencies". Diss. for obtaining sciences. degree of Doctor of Philosophy. Irpin. 218 p, [online]. Available at: https://dpu.edu.ua/zdobuvachi-stupenia-doktora-filosofii?view=article&id=1989&catid=2

MADHAVAN, B.; KALABASKAR, N. (2022). "Digital Forensic Investigation on Ponzi Schemes". *International Conference on Information Security, Privacy, and Digital Forensics*, Goa. DOI: https://doi.org/10.1007/978-981-99-5091-1_14

MANDELA, N.; MAHMOUD, N.; SHAKER, A. (2023). "Implications of Forensic Investigation in Dark Web". *Communications in Computer and Information Science*, vol. 1893, pp. 103-115. DOI: http://dx.doi.org/10.1007/978-3-031-43140-1_10

MAURUSHAT, A.; HALPIN, D. (2022) "Investigation of Cryptocurrency Enabled and Dependent Crimes". *Financial Technology and the Law: Combating Financial Crime*, vol. 47. pp. 235-267. DOI: https://doi.org/10.1007/978-3-030-88036-1_10

MOVCHAN, A.; SHLIAKHOVSKYI, O.; KOZII, V.; FEDCHAK, I. (2023). "Investigating cryptocurrency financing crimes terrorism and armed aggression". *Social and Legal Studios*, vol. 6, no. 4, pp. 123-131. DOI: https://doi.org/10.32518/sals4.2023.123

MOVCHAN, A; KOZII, V. (2022). "Fundamentals of Investigation Crimes Regarding Illegal Possession of Cryptocurrency". *Science and law enforcement*, vol. 4, no. 58, pp. 178-189. DOI: https://doi.org/10.36486/np.2022.4(58)

OFFICE OF PUBLIC AFFAIRS U.S. DEPARTMENT OF JUSTICE (2024, May). "Sodinokibi/REvil Affiliate Sentenced for Role in $700M Ransomware Scheme". *Justice.gov*, [online]. Available at: https://www.justice.gov/opa/pr/sodinokibirevil-affiliate-sentenced-role-700m-ransomware-scheme

PENGCHENG XIA; HAOYU WANG; BOWEN ZHANG; RU JI; BINGYU GAO; LEI WU; XIAPU LUO; GUOAI XU (2020). "Characterizing cryptocurrency exchange scams". *Computers and Security*, vol. 98, no. 101993. DOI: https://doi.org/10.1016/j.cose.2020.101993

RUECKERT, C. (2019). "Cryptocurrencies and fundamental rights". *Journal of Cybersecurity*, vol. 5, no. 11. DOI: https://doi.org/10.1093/cybsec/tyz004

SCHMIDT, A. (2021). "Virtual assets: compelling a new anti-money laundering and counter-terrorism financing regulatory model". *International Journal of Law and Information Technology*, vol. 29, no. 4. pp. 332-363. DOI: https://doi.org/10.1093/ijlit/eaac001

SIU, G. A.; HUTCHINGS, A.; VASEK, C; MOORE, T. (2022). "'Invest in crypto!': An analysis of investment scam advertisements found in Bitcointalk". *APWG Symposium on Electronic Crime Research (eCrime)*, Boston, Massachusetts, USA, pp. 1-12. DOI: https://doi.org/10.1109/eCrime57793.2022.10142100

SPAIN (2021). Ley 11/2021, de 9 de julio, de medidas de prevención y lucha contra el fraude fiscal, de transposición de la Directiva (UE) 2016/1164, del Consejo, de 12 de julio de 2016, *BOE*, no. 164 [online]. Available at: https://www.boe.es/buscar/doc.php?id=BOE-A-2021-11473

SWARTZ, L. (2022). "Theorizing the 2017 blockchain ICO bubble as a network scam". *New Media and Society*, vol. 24, no. 7, pp. 1695-1713. DOI: https://doi.org/10.1177/14614448221099224

UKRAINE (2001, April). Law of Ukraine No. 2341-III "Criminal Code of Ukraine". *Rada* [online]. Available at: https://zakon.rada.gov.ua/laws/show/2341

UKRAINE (2019). SSTC ISO/IEC 27037:2017 (ISO/IEC 27037:2012, IDT) "Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence". Valid from 2019.01.01. Kyiv. UkrSRTC, 2018. VI, 31 p.

UKRAINE (2022, February). Law of Ukraine No. 2074-IX "On virtual assets". *Rada* [online]. Available at: https://zakon.rada.gov.ua/laws/show/2074-20

VEBER, J.; SMUTNY, Z. (2015). "Standard ISO 27037:2012 and Collection of Digital Evidence: Experience in the Czech Republic". *14th European Conference on Cyber Warfare & Security*, Hatfield, UK, 2-3 July 2015, p. 294-299 [online]. Available at: https://www.researchgate.net/profile/Zdenek-Smutny/publication/283226153_Standard_ISO_270372012_and_Collection_of_Digital_Evidence_Experience_in_the_Czech_Republic/links/569a87dd08ae6169e55b844f/Standard-ISO-270372012-and-Collection-of-Digital-Evidence-Experience-in-the-Czech-Republic.pdf

Recommended citation

KOZII, Vasyl; KALANCHA, Inha; VLASOVA, Hanna; ORLEAN, Andriy (2024). "Peculiarities of recording electronic evidence in criminal proceedings regarding crimes committed in Ukraine using cryptocurrencies". *IDP. Internet, Law and Politics Journal*, no. 42. UOC [Accessed: dd/mm/yy]. DOI: http://dx.doi.org/10.7238/idp.v0i42.429924

About the authors

Vasyl Kozii
Prosecutors Training centre of Ukraine
k_vasilisk@ukr.net
ORCID: https://orcid.org/0000-0001-8181-1857

PhD in Law, expert in the Prosecutors Training centre of Ukraine.

Inha Kalancha
Borys Grinchenko Kyiv Metropolitan University
inga.kalancha@gmail.com
ORCID: https://orcid.org/0000-0002-5246-7337

Candidate of Sciences of Law, Associate Professor of the Public Law Department of the Borys Grinchenko Kyiv Metropolitan University, Faculty of Law and International Relations.

Hanna Vlasova
Borys Grinchenko Kyiv Metropolitan University
ganna.vlasova78@gmail.com
ORCID: https://orcid.org/0000-0002-5616-3904

Doctor of Legal Sciences, Professor, Honored Worker of Science and Technology of Ukraine. Head of the Public Law Department of the Borys Grinchenko Kyiv Metropolitan University, Faculty of Law and International Relations.

Andriy Orlean
National Academy of Internal Affairs
balansandrey@gmail.com
ORCID: https://orcid.org/0000-0002-7439-5311

Doctor of Legal Sciences, Professor of the Department of Criminal Law of the National Academy of Internal Affairs, Ukraine.