REICE
Revista Electrónica de Investigación en Ciencias Económicas
Abriendo Camino al Conocimiento
Facultad de Ciencias Económicas, UNAN-Managua

Vol. 10, No. 19, Enero - Junio 2022 REICE ISSN: 2308-782X
http://revistacienciaseconomicas.unan.edu.ni/index.php/REICE
revistacienciaseconomicas@gmail.com

Managing The Investigation of Cryptocurrency Crimes in The Russian Federation

Gestión de la investigación de delitos relacionados con criptomonedas en la Federación de Rusia

Fecha recepción: enero 01 del 2022
Fecha aceptación: enero 19 del 2022

Viktor Victorovich Pushkarev
Plekhanov Russian University of Economics, Moscow, Russia.
Email: pushkarev.v.v@bk.ru
ORCID: https://orcid.org/0000-0002-3536-6497
Anna Vladilenovna Skachko
Management Academy of the Ministry of Internal Affairs of Russia, Moscow, Russia.
Email: skachko.a.v@yandex.ru
ORCID: https://orcid.org/0000-0002-2878-8413
Alexander Ivanovich Gaevoy
North Caucasian branch of the Russian Academy of Justice, Krasnodar, Russia.
Email: gaevoy.a.i@bk.ru
ORCID: https://orcid.org/0000-0002-4134-3101
Vitaliy Fedorovich Vasyukov
Moscow State Institute of International Relations (University) of the Ministry of Foreign Affairs of the Russian Federation (MGIMO-University), Moscow, Russia.
Email: vvf0109@yandex.ru
ORCID: https://orcid.org/0000-0003-0743-5616
Elmir Nizamievich Alimamedov
Finance University under the Government of the Russian Federation, Moscow, Russia.
Email: alimamedov.e.n@mail.ru
ORCID: https://orcid.org/0000-0003-2477-3166

esumen

El análisis de datos estadísticos y otras cifras sobre casos penales particulares en Rusia indican que los recursos del sistema financiero atraen a los delincuentes. Anualmente, el número de tales delitos crece mientras que las criptomonedas y otros activos o derechos digitales se convierten en un objeto o medio para cometer un delito. El riesgo de tales delitos aumenta, así como el número de personas involucradas y su nivel de competencia en la materia. Es más, se mejoran los medios para cometer estos delitos y se desarrollan otros nuevos que suponen un peligro para la sociedad. Existe una infraestructura criminal emergente que aumenta la criminalización de la economía digital y fomenta una imagen negativa del entorno de las criptomonedas entre las personas, la sociedad y el Estado. Tal situación justifica la relevancia de este trabajo que aborda el tema de incrementar la calidad y eficiencia de la investigación de delitos de criptomonedas.

Palabras clave: Criptomoneda, Fiscalía, Investigador, Economía digital, Sistema financiero, Delito

Abstract

The analysis of statistical data and other figures on particular criminal cases in Russia indicate that the resources of the financial system attract criminals. Annually, the number of such crimes grows while cryptocurrency and other digital assets or rights become an object or means for committing a crime. The risk of such crimes increases as well as the number of people engaged and the level of their proficiency in the matter. What is more, means of committing such crimes improve and new ones are developed what entails danger to society. There is an emergent criminal infrastructure that increases the criminalization of the digital economy and fosters a negative image of the cryptocurrency environment among people, society, and the State. Such a situation justifies the relevance of this paper that covers the issue of increasing the quality and efficiency of the investigation of cryptocurrency crime.

Keywords: Cryptocurrency, Prosecution, Investigator, Digital Economy, Financial System, Crime.

Introduction

In Russia, the current state of combatting cryptocurrency crime reveals a number of interrelated and intrinsically linked problems. The solution to these problems lies in cooperation during identification, disclosure, and investigation as well as criminal prosecution. However, the officials responsible for these processes lack special knowledge.

Materials and Methods

The purpose of the study justifies its methodology and implies the use of special legal methods. The formal legal method helped characterize the current situation as it regards certain questions that arise during the initiation, implementation, and termination of prosecution of economic crimes in the pre-trial proceedings. It also helped analyze the identified problems, classify them, and suggest a solution.

The comparative legal method helped review international legal standards and foreign practices of prosecution of economic criminals. The synthesis and analysis helped obtain real data on the effectiveness of criminal prosecution as a means of criminal proceedings.

The sociological method helped obtain empirical data as well as analyze, systemize, and generalize the obtained information. This methodology helped obtain new insights on the procedures of criminal prosecution, tendencies and prospects for its further improvement as it regards the performance of officials responsible for preliminary investigation of economic crimes.

The empirical basis consists of the results of 85 criminal cases; questionnaire results among 38 investigators and detectives, 43 members of the teaching group of the Ministry of Internal Affairs of the Russian Federation, Moscow University of the Ministry of Internal Affairs. Based on the study of the law enforcement practice of investigators of territorial internal affairs bodies investigating crimes in the sphere of banking, expressed in the materials of specific criminal cases; obtained and processed data from a sociological

study on the state of practice in investigating cryptocurrency crimes in the Russian Federation; corrective data from the Investigative Department of the Ministry of internal Affairs of Russia was received and studied. The analytical research method has enabled us to draw several essential conclusions that resolve the question which serves as the hypothesis for this study.

Result and discussion

The investigation into allegations of cryptocurrency crimes should be assigned to the most qualified and experienced investigators. It should also be carried out with the use of investigative and procedural activities that are stipulated in Art. 144 Para. 1 of the Criminal Procedure Code of the Russian Federation. In addition, it should include detective work conducted by the investigative body as requested by the investigator. In order to ensure a complete gathering of reports, it is necessary to organize cooperative discussions among representatives of operational units.

At the initial phase of an inquiry, criminal investigation police officers who investigate such cases should focus on checking the evidence of the offense as stipulated in Art. 174, 174.1, 210 of the Criminal Code of the Russian Federation, and if it is classified as an offense, criminal investigation police officers should review the aforementioned articles additionally.

In the investigation into allegations of cryptocurrency fraud, it is important to make procedural decisions according to the peculiarities of instituting criminal proceedings of semi-public prosecution procedure. According to Art. 20 Para. 2 of the Criminal Procedure Code, it regards crimes that are stipulated in Art. 159 of the Criminal Code of the Russian Federation.

In cooperation with the Federal Financial Monitoring Service of the Russian Federation (Rosfinmonitoring), it is crucial to conduct an in-depth financial investigation. For instance,

in the case of the illicit manufacture and sale of drugs through cryptocurrency, the provisional amount of $2 million was estimated.

In another criminal case, the investigators of the Russian Federation Investigative Department in cooperation with the operational staff of GUKON and Rosfinmonitoring detected more than 1000 third-party electronic wallets that were used by the organizers of the international drug syndicate ‘KhimProm’. The suspects consistently transferred illegal proceeds making them difficult to trace or monitor. In such a way, they legalized more than $35 million.

In the investigation into allegations of cryptocurrency crimes, there is a cooperation between the investigator and officials conducting the initial inquiry who are responsible for the supporting documentation. They identify people who may possess information relevant to the case and people who have been involved in the offense.

According to Art. 38 Part 2 Para. 4 of the Criminal Procedure Code of the Russian Federation, the investigator supplies the operational staff with written requests on searches aimed at identifying the whereabouts of the stolen property, cryptocurrency transactions, and looted funds transactions as well as on other actions depending on the case (Ivanov et al., 2020a, p. 753-759).

In the preliminary check, to identify the property status of the individuals, their vehicles, money held in bank accounts, stakes in the authorized capital of legal units, the presence of affiliate organizations, and individuals involved in cryptocurrency fraud, the internal affairs officers file corresponding requests to public authorities, credit and financial institutions, banks, interregional units of Rosfinmonitoring.

The materials of financial intelligence are exploratory and require further investigation, that is why they are used for planning police operations and further procedural actions. One of the problems in cooperation between investigators of the Department of Internal Affairs and Rosfinmonitoring units is the declaration of official secrecy of the obtained

information which is why it cannot be appended to case files and requires filing additional requests to the corresponding units and institutions.

In the vast majority of cases, the information from Rosfinmonitoring is not used in the criminal investigations due to a long execution of queries on financial audit and invalidity of information on the receipt of results. It takes place due to the fact that the necessary information has been already obtained by investigators from registration authorities and credit organizations during a preliminary investigation through filing requests (in some cases, the criminal case is filed to court).

Information gathering is conducted by information systems of entities engaged in financial and economic activity, the Ministry of Internal Affairs' databank as well as through confidential data from the Ministry of Internal Affairs' Bureaus.

In execution of an order of the investigator, the requests are filed to the regional offices of the Ministry of Internal Affairs, Directorates of economic security and combating the corruption, and regional Departments for criminal investigation to locate the stolen property and stolen stock allocation, to specify the criminal origin of funds, property, and other valuable objects.

Moreover, it is necessary to identify the property status of the offender's relatives. At this stage, the cooperation between the investigator and operational units is crucial and can take the following forms:

– obtaining information on the relationships the suspects and their relatives have;

– identifying the periodicity of traveling abroad and within the country as well as the purposes of those trips;

– identifying the income obtained legally and comparing it to the spending and the possessed property.

If there is any discrepancy, further verification activities are organized.

In interviewing and interrogating the relatives and friends of the suspect, it is important to verify what property is owned by them. Investigators file requests to different organizations (the Main Directorate for Traffic Safety of the Ministry of Internal Affairs, the State Inspection for Small Vessels, the State Technical Supervision Body, the Russian State Register, the Federal Service for State Registration, Cadastre and Cartography, the Federal Taxation Service (on the participation in legal entities), the Pension Fund of the Russian Federation, credit organizations, etc.) in order to identify whether the suspect (the accused) possesses movable and immovable property, money in bank accounts, money deposits, etc.

On receiving and assessing the information, the investigator should file a motion to court under Art. 115 of the Criminal Procedure Code of the Russian Federation to arrest the property of the suspects (the accused) to enforce a sentence relating to a civil suit or other legal action (e.g. imposing a fine) involving property as stated in Art. 104.1 Part 1 of the Criminal Code of the Russian Federation (Ivanov et al., 2020b, p. 47).

It is important to consider the measures taken by the body of inquiry aimed at compensation for damage caused by an offense.

It is necessary to request information from the cryptocurrency market on the registered individuals whose activity is checked under the investigation. Moreover, it is important to request the IP address of the computer or smartphone which was used by an individual to access the Internet to register or file an electronic application as well as their contact phone number, email address, and application time.

Given the fraudster's IP address and time of filing an electronic application, it is possible to locate where the fraudster was at that time. Using such websites as https://whoer.net/ru/checkwhois or www.2ip.ru it is possible to identify the Internet provider, e.g. IP: 31.173.80.241; Provider: PJSC MegaFon; Host:N/A; Operating system:Win7; Browser:Chrome 80.0; DNS 85.26.158.1852 Russian Federation.

If possible, it is advised to file a written request to the Internet provider to obtain an electronic document containing connection logs for the past three months before the money was stolen.

In addition, it is advised to file a motion to the court regarding the cash recipient indicating the reported details of the recipient on the collection of the unjustified wealth transfer and interest for the money used (Chapter 60 of the Civil Code of the Russian Federation). Also, it is necessary to file a motion for the court to implement measures to seize the money in the amount of the unjustified wealth transfer. It is necessary to attach a copy of a motion to initiate criminal proceedings or a copy of a ticket with a serial number from the crime record (Ivanov et al., 2021, p. 417-422).

The following documents may be withdrawn from the victim:

– the copy of the license for the PC operating system;

– the copy of the receipt for the purchase of the PC operating system;

– the description of the used software (the list of the licensed software used at work, the version of the operating system and recommended updates);

– the copy of the telematic service contract for the Internet connection;

– the description of the Internet access at work;

– the copy of the receipt for the Internet access on an hourly rate;

– the copy of the application to the law enforcement agencies;

– the copy of the license on anti-virus software;

– the copy of the receipt for anti-virus software;

– the description of the installed anti-virus software (the anti-virus software is installed on hard disk, its databases are updated; information on possible malware);

– the description of the information security system (presence of personal firewall; information on using the personal computer for purposes other than payment operations, e.g. to surf the Internet; information on data storage and media);

– agreements on opening and maintenance of bank accounts; agreements on distant banking service;

– information on the location where the bank account was opened;

– information on passport details of the individual (including the copy of the passport and other identity documents if available);

– data storage device with the security footage relating to the theft (before the original tape is withdrawn, it is important to ensure its preservation);

– documents with the statistics on the connection with online payment systems through distant banking service “client-bank” indicating accounts, external IP address, and exact time of connection at the time of unauthorized bank transfer;

– authentication logs on electronic means of payment at ATMs, information on telephone numbers and email addresses with notifications of incidents as well as telephone numbers and email addresses that were used by fraudsters to send messages (if available); data from fake websites (if available);

– data on bank notification services (text notifications, voice authorization, email notifications, IP address binding, etc.) and copies of the documents attached by the bank on these services;

The following information may be obtained if cryptocurrency deals are made through distant banking services:

– the date (year, month, day) and time (hour, minutes, seconds) of the client’s actions;

– the client’s identifier (identifiers);

– the identifier (code) of the client’s action;

– the identifier of the client’s device which is used to transfer money (e.g. IP address, MAC address, SIM card number, telephone number, and/or other identifiers);

– the browser used by the client;

– the operating system used by the client;

– the URL requested by the client;

– the page address entered by the client;

– the geographic location of the client;

– the HTTP header;

– the materials prepared by the security service of the bank based on internal audit.

In order to guarantee the optimum time frame of the investigation of criminal cases and rapid responses from the Internet providers, it is important to mention in the outgoing

request that in case of the failure to provide (or in case of delay) the requested information, the guilty party may be charged with an administrative offense according to Art. 17.7 of the Code of Administrative Offences of the Russian Federation.

Having obtained the information on the client and his or her address from the Internet provider, it is possible to plan police operations and investigative activities in the corresponding location. To substantiate the concurrence of the obtained IP address with the IP address of the alleged offender, it is necessary to conduct investigative activities such as inspection of electronic devices (computers, mobile phones, tablets, etc.). The detected fingerprints should be directed to fingerprint identification to identify the person.

In case of ATM withdrawals, it is necessary to request that the bank provides a video recording of the person who cashed the money (Artemova, Esina, Ivanov, 2020, p. 324-325).

The typical investigative and procedural actions of the initial stage of investigation are as follows:

– the detection, interviewing, and questioning of victims (or their representatives);

– the inspection of the scene in the premises (rooms) where the victim logged in to the computer or other portable device. It is crucial to note that contrary to an indoor theft when the whole location is inspected, in this case, only the device is to be examined. If it is a personal computer, it can be examined on-site but if it is a laptop, then there is no need to go to the place of residence since it can be delivered to the office and examined together with a specialist. Often, the inspection of the scene coincides with the place where the suspect was engaged in criminal activity;

– investigative work and investigatory actions aimed at identification of the guilty persons, their whereabouts, devices and other objects that were used in criminal activity;

– obtaining a court decision on receiving the information on connections between subscribers and (or) their devices (Art. 186.1 of the Criminal Procedure Code of the Russian Federation);

– obtaining the information on connections between subscribers and (or) their devices;

– the seizure of means of communication followed by their examination by a specialist;

– the search and seizure. If it is not possible to seize storage devices or there are other technical or procedural obstacles, the specialist generates a file system image or copies data sector-wise from electronic devices. In the seizure of mobile phones, it is sufficient to obtain the memory dump using special complexes “Mobilny Kriminalist” (“Mobile Criminalist”), “UFED”, or “XRY”. If it is not possible to withdraw the memory dump, it is important to turn on the airplane mode and deliver it to specialist units to withdraw information. Moreover, it is crucial to reveal the data used to log in to the system. i.e. passwords (Arestova, Artemova, Anisimova, 2019, pp. 298-299);

– the search that can be conducted on the computer in the investigator’s office. The research report describes the appearance of the website and all the actions taken by the investigator to follow the links and menu buttons. It is necessary to take into consideration the time of the research (since the information presented on the website is dynamic and can constantly change), i.e. every action taken to fix information should be timebound. It is important to record and indicate in the report the time zone or UTC time (Coordinated Universal Time) and the address of every frame of the website (as in the title bar of the web browser). To identify the IP address of the website, it is possible to use a special Internet service that withdraws the IP address using the domain name, e.g. the electronic source http://ipwhois.net/website_ip.php. The pages of the website are copied through the browser with the button “save as” or through specialized software to copy the entire contents of the website. The protocol should include the technical device (computer) and software that was used to examine and copy files. The copied files are downloaded into the non-rewritable media and are attached as an annex to the search record. It is important to take into account that videotapes are not usually stored on websites and social media pages but they contain links to download or watch videos. Videotapes are stored on servers of companies that provide such services. However, in legal terms, posting links on a user’s source equals posting the corresponding files since following the links leads to obtaining the information. To guarantee the validity of the copied information, it is necessary to perform investigatory actions in the presence of witnesses;

– the examination of memory storage of telecommunication facilities, computers and data processing machines, and electronic media that have been found during search and other investigative activities to obtain proof, reveal the connections that the detainee had, and other valuable information;

– the interview of possible witnesses. It is crucial to mention that such crimes are often committed without any evidence, and the testimony of the witnesses covers general details such as the personality of the suspect or occupation;

– when the suspect is identified, the search is conducted at the proposed location of criminal activity and the place of residence (in case those locations do not coincide) since other evidence can be traced apart from digital proof;

– the appointment and performance of all the necessary types of forensic examination (computer forensics, forensic radio survey, financial forensics, forensic fingerprinting, trace evidence, etc.). The choice of the type is made according to a particular situation of the investigation and material traces found during the search.

One of the issues in investigating cryptocurrency crimes is the difficulty of establishing the holder of a bitcoin wallet since when one registers the bitcoin account or another cryptocurrency account (e.g. Lightcoin, Livecoin, etc.), it is necessary to input an email address and the password (e.g. on the website www.blockchain.com) without any additional personal information. Also, the servers that store cryptocurrency accounts, are usually located outside the Russian Federation, consequently, it is not possible to retrieve information on the email address or the sender and the recipient of cryptocurrency.

To convert the bitcoin cryptocurrency, the sender who wants to exchange cryptocurrency to rubles offers a transfer to the bitcoin wallet of a “broker” who is now superseded by automated programs on exchange websites that have servers outside Russia.

Thus, such “brokers” play a bridging role in converting cryptocurrency into rubles. The location of these “brokers” or programs is impossible to trace since there is no information about the sender and the recipient of cryptocurrency as well as there are no servers in the

Russian Federation from which it is possible to request information about IP addresses used by cryptocurrency users to visit such websites.

In the preliminary investigation, there are obstacles in tracing bitcoin operations and transactions since the servers of cryptocurrency exchange websites are located outside the Russian Federation. However, it is possible to overcome this problem when the suspect (or the accused) is willing to cooperate in the proceedings. Then the suspect (or the accused) takes part in the examination of the Internet sources used in transactions.

In modern Russia, due to the fact that there is currently no official body authorized to estimate the time value of cryptocurrency, there are still problems in damage assessment. In the criminal case investigation, it is possible to calculate the value of one bitcoin using cryptocurrency markets, e.g. Exmo. This approach should be approved by the supervising procurator, and the procedure to calculate the cryptocurrency value should be stipulated in the request.

During the preliminary investigation, there are obstacles in identifying the holder of the domain that is registered in a foreign country as well as guilty parties that are in other subjects of the Russian Federation and dynamic IP addresses that spread information on cryptocurrency.

It is important to mention other typical problems that the investigator should take into account when planning the investigation of cryptocurrency crimes:

– the restricted access to information constituting bank secrecy (Ruchkina, Kurakin, Piskunova, 2020);

– a long waiting period to obtain data on request (in seizures ordered by the courts under the criminal case in question) since the responsible authorities are located in different subjects of the Russian Federation;

– a large amount of the obtained evidence and special procedures of examination;

– the number of necessary types of forensic examination, e.g. handwriting analysis, and the complexity of certain examinations that prolong them (Ivanov, 2021, p. 34).

It is crucial to highlight the productivity of cooperative material examination with operational units before the materials are registered in order to ensure the

comprehensiveness of material collection, the efficiency of procedural monitoring by the head of the investigative body and employees of methodology and control departments in cryptocurrency crime investigation.

It is prohibited not to initiate criminal proceedings as well as to refuse to extend the period of preliminary verification of crime report or to refuse to extend the period of preliminary investigation on the grounds that there is no information on operations in any organization to prove the payment (Esina, 2019, p. 50-51) since this means that the officials do not know the basics of the methodology of cryptocurrency crime investigation.

Conclusion

The authors provided arguments that prove the relevance of this topic.

After the material examination, it is necessary to take protective measures aimed to ensure crime compensation, to detect the property that can be arrested, and to locate criminal assets.

With the legal assistance of the responsible authorities of foreign countries, it is necessary to take measures aimed to identify, arrest, and return from abroad those assets that have been obtained as a result of criminal activity.

It is crucial to devise and improve programs of de-anonymization of criminal transactions and their beneficiaries.

It is crucial to devise effective measures of legal regulation for issues of freezing of cryptocurrency assets during the preliminary investigation of criminal cases.

Referencias Bibliográficas

1. Arestova, E.N., Artemova, V.V., Anisimova, N.V. (2019). Preliminary investigation: A textbook for university students studying in the direction of training "Jurisprudence". Moscow: LLC Publishing House "Unity-Dana".
2. Artemova, V.V., Esina, A.S., Ivanov, D.A. (2020). Preliminary investigation in the internal affairs bodies. Ensuring the rights of participants in criminal proceedings during the preliminary investigation: Problem solving. Moscow: IPR Media.
3. Esina, A.S. (2019). Activities of the investigator at the stage of the end of the preliminary investigation: a training manual. Moscow: Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikotya.
4. Ivanov, D.A., Ermakov, S.V., Alimamedov, E.N., Esina, A.S. (2021). Security for a Civil Claim in Criminal Proceedings. *Laplage Em Revista*, 7(1), 417-422.
5. Ivanov, D.A., Esina, A.S., Fadeev, P.V., Chasovnikova, O.G., Zorina, E.A. (2020a). Crime victim compensation. *Revista Gênero e Direito*, 9(4), 753-759.
6. Ivanov, D.A., Fadeev, P.V., Alimamedov, E.N., Dung, V.K. (2020b). Provision of the rights and legitimate interests of legal entities that have been victims of crimes. *Revista Turismo Estudos & Práticas*, S5, 47.
7. Ivanov, D.A. (2021). Investigation of fraud in the FOREX market: a tutorial. Moscow: Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikotya.
8. Ruchkina, G.F., Kurakin, A.V., Piskunova, N.K. (2020). Public legal means of the efficiency of economic and financial development. Moscow: Limited Liability Company "Publishing House" KnoRus".