DOI: https://doi.org/10.34069/AI/2021.45.09.25
How to Cite:
Voskobitova, L., Vilkova, T., Nasonov, S., Khokhryakov, M., & Reshetnikov, Y. (2021). Illegal circulation of digital currencies: features of criminal investigation. *Amazonia Investiga*, *10*(45), 252-264. https://doi.org/10.34069/AI/2021.45.09.25

Illegal circulation of digital currencies: features of criminal investigation

Незаконный оборот цифровых валют: особенности расследования уголовных дел

Received: July 27, 2021 Accepted: September 12, 2021

Written by:
Lydiya Voskobitova[98]
https://orcid.org/0000-0002-6676-0120
SPIN-code of the registry of elibrary.ru: 1160-1718
AuthorID: 291675
Tatyana Vilkova[99]
https://orcid.org/0000-0003-3436-1288
SPIN-code of the registry of elibrary.ru: 1063-9047
AuthorID: 396777
Sergey Nasonov[100]
https://orcid.org/0000-0002-2433-9426
SPIN-code of the registry of elibrary.ru: 8037-6330
AuthorID: 664873
Maxim Khokhryakov[101]
https://orcid.org/0000-0003-3382-3399
SPIN-code of the registry of elibrary.ru: 9061-6768
AuthorID: 732762
Yuri Reshetnikov[102]
https://orcid.org/0000-0002-7798-6504
SPIN-code of the registry of elibrary.ru: 4511-1782
AuthorID: 1120916

Abstract

The purpose of the study is to analyze the international and national legal regulation of the digital currencies circulation at the present stage, to assess the state of crime with the illegal use of these assets, to identify the features of the investigating such crimes and to substantiate proposals aimed at improving legislation and law enforcement practice.
The following methods were used in the research: normative and comparative legal – in the analysis of legislation and practice of seizure and confiscation of digital currencies in different states, to identify the strengths and weaknesses of national approaches, to assess the possibility of their unification and harmonization; phenomenological – in considering the criminal

Аннотация

Цель исследования состоит в анализе международного и национального правового регулирования обращения цифровых валют на современном этапе, оценке состояния преступности с незаконным использованием этих активов, выявлении особенностей расследования таких преступлений и обосновании предложений, направленных на совершенствование законодательства и правоприменительной практики.
При проведении исследования применялись методы: сравнительно-правовой – при анализе законодательства и практики наложения ареста и конфискации цифровых валют в различных государствах, для выявления достоинств и недостатков

[98] PhD in Law, Head of the Department of Criminal Procedure Law at Kutafin Moscow State Law University, Moscow, Russia.
[99] PhD in Law, Associate Professor of the Department of Criminal Procedure Law at Kutafin Moscow State Law University, Moscow, Russia.
[100] PhD in Law, Associate Professor of the Department of Criminal Procedure Law at Kutafin Moscow State Law University, Moscow, Russia.
[101] PhD in Law, Associate Professor at the Department of Criminal Procedure Law and Deputy Director of the Institute of Public Law and Management at Kutafin Moscow State Law University, Moscow, Russia.
[102] The 4-year Student of the International Law Institute at Kutafin Moscow State Law University, Moscow, Russia.

trafficking in digital currency as a phenomenon that requires special methods of detection and investigation; general logical methods of analysis and synthesis, induction and deduction, methods of empirical research and analysis.
It was shown that with the rapid growth of crime involving cryptocurrencies, the legislation of various states is at the stage of formation of legal regulation of the fight against its illicit trafficking: only some countries have established the status of digital currency as property, provided for the specifics of seizure, storage and sale of digital currency in criminal cases.
The need to recognize digital currencies as property has been substantiated. It is shown that the seizure and confiscation of cryptocurrencies should be carried out only by court decision. The lack of special knowledge in the field of digital technology among the investigator, prosecutor and the court requires the mandatory involvement of a specialist in the proceedings on cases of crimes committed with the use of digital currency.

Keywords: seizure, confiscation, cryptocurrency, digital currency, bitcoin, property, criminal proceedings, auction.

национальных подходов, оценки возможностей их унификации и гармонизации; феноменологический – при рассмотрении преступного оборота цифровой валюты как явления, которое требует особых способов выявления и расследования; общелогических методов анализа и синтеза, индукции и дедукции, методов эмпирических исследований.
Показано, что в условиях быстрого роста преступности с использованием криптовалют законодательство различных государств находится на этапе становления правового регулирования борьбы с ее незаконным оборотом: лишь в некоторых странах установлен статус цифровой валюты как имущества, предусмотрены особенности ареста, хранения и реализации цифровой валюты по уголовным делам.
Обоснована необходимость признания цифровых валют имуществом. Показано, что арест и конфискация криптовалют должны производиться только по судебному решению. Отсутствие специальных знаний в области цифровых технологий у следователя, прокурора и суда требуют обязательного привлечения специалиста к производству по делам о преступлениях, совершаемых с использованием цифровой валюты.

Ключевые слова: наложение ареста, конфискация, криптовалюта, цифровая валюта, биткоин, имущество, уголовное судопроизводство, аукцион.

Introduction

The growing interest of society and government agencies in digital currencies is due to the fact that cryptocurrency is a new financial instrument that has both positive and negative potential (in this article, the terms "digital currency" and "cryptocurrency" are used as synonyms).

The new promising opportunities opened up by the introduction of digital currency include not only everyday economic transactions, including those for investment purposes, but also, for example, the anonymous payment of remuneration by the state to persons who report information about crimes and criminals known to them on the condition of anonymity (Wang, He, Liu & Guo, 2020; Saiedi, Broström, & Ruiz, 2020).

At the same time, practice shows a steady increase in crimes committed with the use of digital technologies, including the use of various digital currencies – Bitcoin, Ethereum, Monero – which are becoming a means of payment in the criminal activities of terrorist organizations, drug dealers, as well as a subject of theft, extortion, tax evasion, money laundering, Ponzi schemes and other crimes (Albrecht, Duffin, Hawkins, & Rocha, 2019; Custers, Pool, & Cornelisse, 2019; Lee & Choi, 2021; Kethineni & Cao, 2020).

Anonymity and the complete absence of an administrative center in the cryptocurrency circulation are an obstacle to the regulation and control of this area. Cryptocurrency is used for fast anonymous remote payments without being linked to any bank account. And this is what attracts representatives of the shadow economy to the cryptocurrency.

So, 1,1 million bitcoins were stolen for the period of 2013-2017, which corresponded to a monetary loss of the equivalent of $8,9 billion at the prices of 2018 (Grobys, 2021).

The conviction of Ross Ulbricht, the founder of the Silk Road black market site, which sold drugs, fake identity cards, and other illegal goods using bitcoin for payment, became widely known (Thompson, 2015).

In this regard, states have a need to combat a qualitatively new way of carrying out criminal activities and a need for legal regulation and technical support of criminal proceedings on crimes related to the illegal circulation of cryptocurrencies (Markaryan, 2018). At the same time, there is a certain lag in the legal regulation and practice of combating the criminal use of cryptocurrency from the criminal activity development pace (Covolo, 2020).

The need to adopt regulations in this area and train specialists to carry out legal actions in relation to digital currencies is also increasing due to the fact that about 70 states are currently developing projects for national digital currencies. National digital currencies, like other technologies, are vulnerable from the point of view of information security. Cyber-attacks and security breaches can lead to the theft of funds and personal data, and even lead to the shutdown of economic activity.

The above circumstances determine the need to study the state of legal regulation of the digital currencies circulation at the present stage, assess the state of crime with the illegal use of these assets, identify the features of such crimes investigation, substantiate proposals aimed at developing legislation and law enforcement practice in the field of seizing cryptocurrency in criminal cases, its storage, confiscation and further implementation.

Theoretical Framework

Legal regulation of digital currency circulation at the present stage

The lack of legal regulation of the digital currencies circulation is observed both at the international and national levels. Even the status of a cryptocurrency itself often remains uncertain: whether it can be recognized as money, property, whether transactions with it should be taxed, whether it can be confiscated, etc.

In the context of insufficient legal regulation, the legal positions of international and national judicial authorities on certain aspects of cryptocurrency transactions are important, for example, the decision of the Court of Justice of the European Union dated 22 October 2015 No. C-264/14 in the case of Skatteverket v David Hedqvist (Court of Justice of the European Union, 2015), which recognized that transactions for the exchange of fiat money for bitcoins and vice versa qualify as services and are exempt from value added tax, resolution of the Ninth Arbitration Court of Appeal of Russia dated May 15, 2018 in case No. A40-124668/2017 (Database of arbitration cases of the Russian electronic justice system, 2018) on the attribution of cryptocurrency to property and its inclusion in the bankruptcy estate for the subsequent full satisfaction of creditors' claims (the debtor was obliged to transfer the password from the crypto wallet to the financial manager to replenish the bankruptcy estate).

The first international act regulating virtual currencies was the 5th Anti-Money Laundering Directive 2018/843, adopted by the European Union (hereinafter referred to as the EU), which distributed international standards against money laundering over virtual assets' markets.

The European Union (EU) regulation exists not only at the Pan-European level, but is also included in the national legislation of the participating countries. As of July 2020, 35 of the 54 reporting jurisdictions reported that they have now implemented the revised FATF standards, with 32 of them regulating the virtual currencies circulation and the activities of virtual asset service providers ("VASPs", which include exchanges, custodians and hedge funds), and 3 prohibiting their operation.

As for the national laws, we would like to note the Liechtenstein law on blockchain, which is proposed for use as a basis for the development of an international standard for regulating blockchain and cryptocurrency (Teichmann & Falker, 2020).

In Russia, Federal Law No. 259-FZ dated July 31, 2020 "On Digital Financial Assets, Digital Currency and on Amendments to Certain Legislative Acts of the Russian Federation" (hereinafter referred to as Law No. 259-FZ) (Federal Law No. 259-FZ, 2020) entered into force on January, 1 2021, which regulates relations arising from the issuance, accounting and circulation of digital assets.

This federal law defines that a digital currency is a set of electronic data (digital code or designation) contained in an information system that is offered and (or) can be accepted as a means of payment that is not a monetary unit of

the Russian Federation, a monetary unit of a foreign state and (or) an international monetary or settlement unit, and (or) as an investment, and in respect of which there is no person obligated to each owner of such electronic data, except for the operator and (or) nodes of the information system, that are only obliged to ensure that the procedure for the release of these electronic data and the implementation of actions in relation to them to make (change) records in such an information system complies with its rules. Besides, the rules for the legitimate circulation of digital currency are established. In particular, it is prohibited to accept payment for goods, works and services in digital currency. Russian legal entities and individuals who have actually been in Russia for at least 183 days during the year, will be able to defend the claims related to the possession of digital currency in court only if they have reported that they have such a currency and they have made transactions with it. A number of other Russian laws ("On Insolvency (Bankruptcy)" (Federal Law No. 127-FZ, 2002), "On Enforcement proceedings" (Federal Law No. 229-FZ, 2007)) recognize digital currency as property.

Along with this, a number of states – Algeria, Bolivia, Morocco, Nepal, Pakistan and Vietnam – have established a complete ban on any actions related to the cryptocurrencies turnover.

Practice of seizing digital currencies and confiscating them in criminal cases

An important place among the measures taken to prevent and deter crimes related to cryptocurrency payments is occupied by the seizure of it in criminal proceedings and its further confiscation.

The legal regulation of the application of these measures in criminal proceedings, as well as the legal regulation of the digital currencies circulation in general, is at the stage of its formation, which creates obstacles to combating crimes related to the illegal circulation of cryptocurrencies.

Besides, the seizure and confiscation process is largely complicated by the "decentralization" nature of cryptocurrencies, i.e., the absence of a central authority that performs the functions of an administrator in relation to such assets. Currently, there are 3 main types of cryptocurrency exchange platforms: 1) trading platforms, i.e. the websites where you can buy and sell cryptocurrencies; at the same time, buyers and sellers only access the platform and do not interact with each other; the service charges a commission fee for each concluded transaction; 2) peer-to-peer platforms, which connect buyers and sellers directly; the exchange rate is set by agreement of the parties; 3) crypto brokers, operating as forex brokers and setting the value of cryptocurrencies.

Despite the incompleteness of legal regulation, cryptocurrencies seizure, confiscation and sale are widely used in practice, and the high effectiveness of these measures in the fight against corruption and money laundering is noted in doctrinal studies (Vandezande, 2017).

The Federal Bureau of Investigation investigates cybercrimes, including crimes committed using cryptocurrency, in the USA. Under U.S. federal law, the government has the power to seize and hold – and then ultimately sell, with the proceeds going to the state treasury – "any property, real or personal, involved in a transaction or attempted transaction" that violates certain federal laws. At the moment, virtual currency is recognized as property in the United States.

The confiscation of cryptocurrency was made in 2013 for the first time: the US Federal Bureau of Investigation confiscated 144,000 bitcoins from the well-known DarkNet marketplace – the "Silk Road" company, which carried out bitcoin transactions in exchange for drugs, stolen property, fake documents and hacking services. "Silk Road" was the most popular and extensive criminal market on the Internet before it was discovered by the FBI. The US government estimates that the site earned about 600,000 bitcoins during this period. About 175,000 of them were seized when the head of the marketplace was arrested and the site was shut down. The Federal Prosecutor for the Southern District of New York noted during the trial in the Silk Road case that the seized cryptocurrency should be treated in the same way as any other currency obtained as part of illegal transactions (Manhattan, 2014). The Justice Department seized the contents of an electronic wallet belonging to the company, as part of a civil case, in the amount of 69,000 bitcoins worth more than a billion dollars in November 2020.

Europol (2018), with the support of the Spanish Civil Guard, confiscated more than $4,5 million in bitcoins and other cryptocurrencies, as well as 800 thousand doses of LSD from drug traffickers from the DarkNet in 2018. This seizure was made possible due to obtaining access to computer information contained on electronic media found during searches.

In Australia, there is also a practice that confirms the right of authorized bodies to confiscate virtual currency as property. The Australian High-Tech Crime Centre (AHTCC) is located at the Australian Federal Police (AFP) headquarters in Canberra. Under the auspices of the AFP, the AHTCC is a party to a formal joint operation agreement concluded between the AFP, the Australian Security and Intelligence Organization, and the Australian Signals Directorate's Computer Network Vulnerability Group. Australia has developed a special law on combating money laundering and the financing of terrorism, which regulates illegal activities carried out with the help of cryptocurrency.

The authority issuing crypto licenses in Australia is AUSTRAC. A joint official release was issued in 2019 by the Australian Federal Police (AFP) and AUSTRAC in connection with the case against Bullin during the second phase of the Australian Federal Police (AFP) investigation into the activities of an organized crime syndicate. He played a key role in leading the operations of a criminal syndicate that used various dark web sites, bitcoin accounts, and legitimate businesses to find, pay for, and distribute illicit drugs. The AFP officers executed search warrants in Melbourne's suburbs, seizing Australian currency and cryptocurrency-related items. Bullin was subsequently arrested and charged with importing, trafficking and possessing a total of about 30 kilograms of drugs. The Criminal Assets Confiscation Task Force (CACT) successfully sought the confiscation of assets related to the investigation in a separate special operation. Orders were obtained from the District Court of Victoria to seize property worth more than $2 million, including cryptocurrency. The orders were issued in accordance with the Anti-Money Laundering and Counter Terrorism Financing Act 2006 No. 169, 2006. (Federal Register of Legislation of Australian Government, 2018)

On May 30, 2018, the Supreme Court of the Republic of Korea ruled that cryptocurrencies can be confiscated if their use was detected in illegal activities. This decision overturned the decision of the district court, which indicated that it was impossible to withdraw bitcoins from a person accused of distributing child pornography due to the lack of a physical embodiment and an objective standard value. However, the Supreme Court of the Republic of Korea did not agree with this opinion, noting that "Korean law provides that hidden assets subject to confiscation include cash, deposits, shares and other forms of tangible and intangible objects that have a standard value. Bitcoin is intangible and comes in the form of digitized files, but it is sold on an exchange and can be used to buy goods. Thus, getting bitcoins is profit-taking" (Kim, 2018).

Legal regulation of the seizure of digital currencies and their confiscation in criminal cases

The regulation of the cryptocurrencies seizure is necessary in order to ensure the execution of a sentence in terms of a civil claim, the collection of a fine, other property penalties or their possible confiscation. However, at present, only some states have developed rules for the seizure, storage, exchange and further circulation of cryptocurrencies in the state's income.

For example, the Finnish government adopted instructions on the storage of confiscated cryptocurrencies in 2018: cryptocurrencies themselves are considered as an asset, not a currency; law enforcement agencies should not store them on exchanges, but keep them offline without access to the Internet (in cold storage); after a court ruling that the seized funds will not be returned to the owner, it becomes possible to exchange them for euros at public auctions, and not on cryptocurrency exchanges (Palmer, 2018).

In the Republic of Belarus, a Decree on the development of the digital economy was issued in 2017, legalizing cryptocurrency exchanges, cryptocurrency exchange operators, mining, smart contracts, blockchain, tokens, etc. (Decree No. 8, 2017), and the first cryptocurrency exchange in Belarus was opened on the Internet in 2019, and Article 132 of the Criminal Procedure Code of the Republic of Belarus (Criminal Procedure Code of the Republic of Belarus No. 295-Z, 1999) provides for the possibility of seizing cryptocurrencies as a type of property in criminal proceedings since January 2021.

However, in general, the grounds, procedure and conditions for the cryptocurrencies seizure in criminal cases and their further confiscation in many states remain unresolved.

Thus, in the Russian Federation, the mechanisms for the recovery of "digital rights", "digital financial assets" and "digital currency", the seizure of such property or its confiscation in accordance with Articles 115, 230 of the Criminal Procedure Code of the Russian Federation (hereinafter – the Criminal Procedure Code of the Russian Federation) and Chapter 15[1]

of the Criminal Code of the Russian Federation (hereinafter – the Criminal Code of the Russian Federation) (Criminal Procedure code of the Russian Federation No. 174-FZ, 2001, Art. 15[1], 115, 230) remain unsettled, and in practice, the cryptocurrencies seizure, the forensic examination that determines their sale from computer equipment, and confiscation are not applied, although there are criminal cases of crimes, the subject of which was the cryptocurrency.

Law No. 259-FZ (Federal Law No. 259-FZ, 2020) recognizes digital currency as property for the purposes of Federal Law No. 115-FZ dated July 7, 2001 "On Countering the Legalization (Laundering) of Proceeds from Crime and the Financing of Terrorism" (Federal Law No. 115-FZ, 2001), No. 127-FZ dated October 26, 2002 "On Insolvency (Bankruptcy)" FZ (Federal Law No. 127-FZ, 2002), No. 229-FZ dated October 2, 2007 "On Enforcement Proceedings" (Federal Law No. 229-FZ, 2007), and No. 273-FZ dated December 25, 2008 "On Combating Corruption" (Federal Law No. 273-FZ, 2008), but this is not mentioned in the Criminal Procedure Code of the Russian Federation.

Article 115 and other provisions of the Criminal Procedure Code of the Russian Federation regulate the property seizure (Criminal Procedure code of the Russian Federation No. 174-FZ, 2001, Art. 115). At the same time, the property seizure in criminal proceedings also includes the seizure of funds and other valuables held in an account, in a deposit or in storage in banks and other credit organizations: operations on this account are terminated in full or in part within the limits of funds and other valuables that are seized; the heads of banks and other credit institutions are obliged to provide information about these funds and other valuables at the request of the court, as well as the investigator or inquirer based on a court decision.

The significance of the property seizure increases due to the increase in the amount of damage caused by crimes. So, it amounted to 512.8 billion rubles in Russia in 2020. During 2015-2019, the Russian preliminary investigation authorities applied to the court with the requests for the property seizure in 35-45 thousand criminal cases. The majority of such requests were granted by the courts: in 2015 – 87,1%, in 2016 – 88,1%, in 2017 – 87,4%, in 2018 – 86,7%, in 2019 – 86,3%.

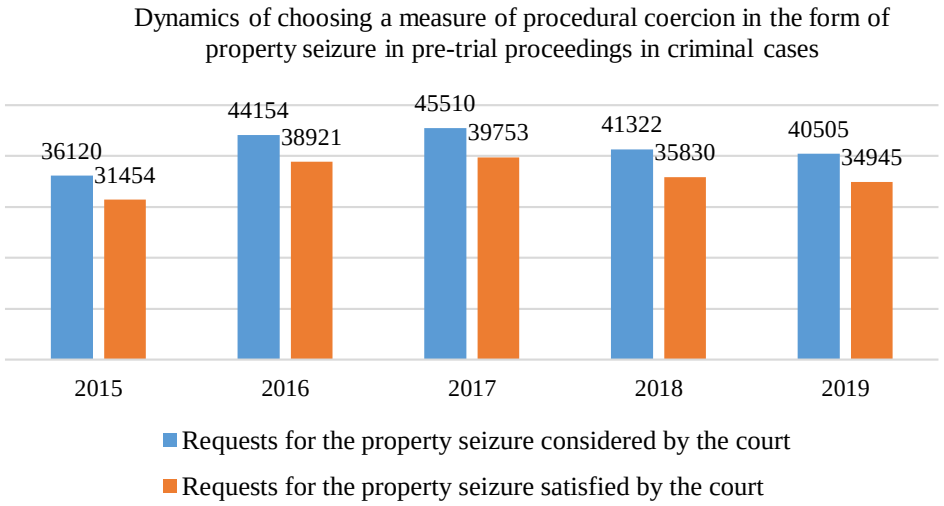

Figure 1. Dynamics of choosing a measure of procedural coercion in the form of property seizure in pre-trial proceedings in criminal cases. We have independently compiled this graph based on statistical information from the site indicated above Summary statistical data on the activities of federal courts of general jurisdiction and justices of the peace for 2015-2019, form 1, section 4. Official website of the Judicial Department at the Supreme Court of the Russian Federation (2015, 2016, 2017, 2018, 2019).

Meanwhile, the potential of this enforcement measure is not exhausted, since at present the Criminal Procedure Code of the Russian Federation does not disclose whether the seizure of cryptocurrency is allowed, and it is not applied in practice.

In order to introduce legal certainty, it seems necessary to make additions to Article 5 of the Criminal Procedure Code of the Russian Federation (Criminal Procedure code of the Russian Federation No. 174-FZ, 2001,Art. 5), explicitly providing that for the purposes of the Criminal Procedure Code of the Russian

Federation, digital currency is recognized as property, by analogy with the amendments made by Law No. 259-FZ to a number of other federal laws (Federal Law No. 259-FZ, 2020).

It is also necessary to establish the rule in the Criminal Procedure Code of the Russian Federation (in part 2 of Article 29) that the seizure of such a type of property as cryptocurrency and its subsequent confiscation are possible only by a court decision (Criminal Procedure code of the Russian Federation No. 174-FZ, 2001, Art. 29). This is due to the fact that the court order is an additional and important guarantee of the legality of any actions and decisions in criminal proceedings that restrict the property inviolability. When making a court decision on the cryptocurrency seizure, a balance must be observed between privacy, on the one hand, and the state's duty to detect, suppress and solve crimes, on the other (Lloyd, 2020).

If there is a court decision, the seizure must be carried out with the mandatory participation of a specialist, which should also be reflected in the law.

The procedure for seizing digital currency should be described in a separate article due to the peculiarities of this type of property, by analogy with the norm of Article 116 of the Criminal Procedure Code (Criminal Procedure code of the Russian Federation No. 174-FZ, 2001, Art. 116).

Moreover, Articles 81-82 of the Criminal Procedure Code of the Russian Federation (Criminal Procedure code of the Russian Federation No. 174-FZ, 2001, Art. 81-82) on material evidence and Article 230 of the Criminal Procedure Code of the Russian Federation (Criminal Procedure code of the Russian Federation No. 174-FZ, 2001, Art. 230) on interim measures are subject to addition.

The Criminal Procedure Code of the Russian Federation does not contain special rules governing the seizure and confiscation of digital currencies at the request of the competent authorities of a foreign state for mutual legal assistance in criminal matters. This gap should also be eliminated.

It should be noted that the Criminal Code of the Russian Federation does not provide for the elements of crimes the subject of which is digital currency.

In 2019, amendments were made to the Resolution of the Plenum of the Supreme Court of the Russian Federation No. 32, 2015 "On judicial practice in cases of legalization (laundering) of money or other property acquired by criminal means, and on the acquisition or sale of property knowingly obtained by criminal means" (Resolution of the Plenum of the Supreme Court of the Russian Federation No.1, 2019). In accordance with these additions made due to the FATF recommendations, Articles 174 and 174^1 of the Criminal Code on the legalization of criminal proceeds should also apply to cryptocurrency (Criminal Code of the Russian Federation No. 63-FZ, 1996, Art. 174-174^1).

However, such explanations are not enough: firstly, they are advisory in nature, and secondly, the question of whether transactions with cryptocurrency are covered by other crimes remains unresolved.

Thus, in our opinion, in order to solve this problem, it is necessary to expand the objective side of the elements of crimes provided for in the articles 159^3, 159^6, 171, 172^1-172^3, 174, 175, 183, 185-185^6, 187, 195, 199^2 of the Criminal Code of the Russian Federation (Criminal Code of the Russian Federation No. 63-FZ, 1996, Art. 159^3, 159^6, 171, 172^1-172^3, 174, 175, 183, 185-185^6, 187, 195, 199^2), extending them to cryptocurrency.

The development of legal regulation of the fight against crimes related to the illegal circulation of digital currency should be comprehensive and cover not only criminal procedure and criminal legislation, but also regulatory acts regulating operational search and banking activities, establishing guarantees for the protection of the rights of bona fide buyers and cryptocurrency sellers, etc.

Organizational and technical aspects of the digital currencies seizure and confiscation in criminal cases

The organizational and technical aspects of the digital currencies seizure, their subsequent storage and sale remain unresolved.

In Russia, the algorithm of investigative actions in relation to the cryptocurrency (its inspection, seizure, etc.), the cryptocurrencies seizure and confiscation is under development. The relevant proposals should be prepared by the Ministry of Internal Affairs of the Russian Federation together with the Federal Financial Monitoring Service, the Prosecutor General's Office of the

Russian Federation, the Investigative Committee of the Russian Federation, the Ministry of Justice of the Russian Federation, the Federal Security Service of the Russian Federation, the Federal Customs Service and the Federal Bailiff Service with the participation of the Supreme Court of the Russian Federation by December 31, 2021.

The greatest difficulties arise when it is necessary to gain access to digital currencies for seizure and subsequent confiscation, if law enforcement agencies have to deal with cryptocurrencies that have built-in anonymity and privacy features, which make it very difficult to track funds to a specific user or successfully seize funds available in a cryptocurrency wallet (Koerhuis, Kechadi, & Le-Khac, 2020). But the most well-researched and transparent cryptocurrencies, including Bitcoin, also require the development of special methods to seize them.

However, current global trends in the fight against cybercrime refute the idea that digital currencies and the blockchain network are invulnerable to unauthorized access through code modification, use of malware, and invulnerability to theft or other property crimes against users or third parties (Mkrtchian, 2020; Turner, McCombie, & Uhlmann, 2019).

There are already special software tools created for tracking and controlling transactions that link public encryption keys to certain individuals identified on the network in the United States and Europe (Dolgieva, 2018), although until recently it was believed that the technical possibility of hacking a crypto wallet when a suspect or accused refuses to cooperate with the investigation is not feasible.

However, not all states have the necessary software yet, so the methods of the digital currencies seizure and confiscation, the implementation of which is possible if the suspect, the accused or a third party voluntarily discloses the password required for authorization and use of the crypto wallet, are more widely used in practice in foreign countries.

So, in February 2021, German prosecutors confiscated more than 50 million euros ($60 million) worth of bitcoin from a fraudster, but they can't unlock the money because he won't give them the password (O'Donnell, 2021).

In the "Basic Manual on the Detection and Investigation of the Laundering of Crime Proceeds Using Virtual Currencies", published by the UN Office on Drugs and Crime in June 2014, it is stated that crypto wallets contain information about private keys that provide individual control over digital assets, taking possession of these keys is tantamount to confiscating these crypto assets.

In general, there are 2 methods to seize cryptocurrencies and confiscate them.

The first is to leave the cryptomonets in the wallet of the suspect, accused or convicted, but with the mandatory replacement of the access code (password) required for authorization and use of such a wallet.

The second method involves the transfer of digital currencies from the crypto wallet of the suspect, accused or convicted person to a crypto wallet specially opened for this purpose under the control of a law enforcement officer to store the seized property in the form of digital rights.

The cryptocurrency wallets for storing confiscated digital assets are just being created in some states, while in others they have already been created. As an example, we can cite the Police Instructions of the State of Indiana of the United States on the standard procedure for the confiscation of cryptocurrencies and virtual currencies.

The cryptocurrency is stored in a wallet, i.e. a program that contains one or more private keys. There are "cold" and "hot" wallets. In the first case, the data is stored offline on a hard disk, electronic media, in the second – on the network and is in some way connected to the Internet. You can access the wallet using a key that can be private (a complex form of encryption that allows the user to access their cryptocurrency) or public (a cryptographic code that allows the user to receive cryptocurrency to their account).

The seizure and confiscation of digital currencies ("transparent" bitcoins) can also be carried out without the consent of the suspect, accused or convicted in cases where users store encryption keys on personal computers or accessible USB devices.

In the United States, obtaining passwords from crypto wallets from suspects, accused persons, or third parties on a voluntary basis is additionally stimulated in several ways. The U.S. Secretary of the Treasury, in consultation with the U.S. Attorney General, establishes a fund to pay a reward of no more than $450,000 to any person who provides information that leads to the conviction of an individual who has used digital

currency for terrorist activities (Financial Technology Protection Act Art. 4, 2019).

Thus, there is information in the public domain that the US Department of Justice was assisted in gaining access to the electronic wallet of the "Silk Road" online service in the amount of more than 1 billion US dollars in exchange for the removal of all charges in the criminal case by a person whose identity was not disclosed.

The question of the fate of the confiscated cryptocurrency often remains unresolved.

As a rule, the confiscated cryptocurrency is sold at auctions, and the received fiat money is converted into state revenue.

For example, the cryptocurrency was confiscated from the "Lesen und Lauschen" online platform, which sold counterfeit copies of various content – audiobooks, films, software – without the knowledge and consent of the copyright holders during the trial in Bavaria in 2017. In total, the German police confiscated 1,312 bitcoins, 1,399 Bitcoin Cash (bitcoin fork) and 200 Ethers, which was equivalent to 12 million euros ($13,9 million). The seized cryptocurrency was sold through 1,600 separate transactions within two months (Voß, 2018).

The sale of confiscated cryptocurrency at auction has also spread in the United States of America, as evidenced by the announcement of the auction on the website of the US Marshals Service (a division of the Ministry of Justice). On January 22, 2018, 3,813 bitcoins were offered for sale, divided into 11 blocks (since the cryptocurrency was seized in eleven separate proceedings), with a total value of $53,38 million at the time of publication.

In 2017, the Bulgarian authorities seized cryptocurrency from an organized criminal group accused of corruption. The subsequent sale of 213,519 confiscated bitcoins brought about $3,3 billion to the state treasury and helped pay off 20% of Bulgaria's public debt (Campbell, 2017).

Auctions for the sale of confiscated cryptocurrencies are very popular among investors due to the fact that the initial value of digital assets is much lower than if they were purchased at the existing exchange rate at the time of sale.

Thus, there is already a successful experience in solving crimes related to the illegal circulation of cryptocurrency, which can be used in legislative and law enforcement activities.

Methodology

The analysis of the procedural activity features in cases of crimes related to the illegal circulation of cryptocurrencies is interdisciplinary. This determines the need to study the same object – the seizure of digital currencies and their confiscation – from the positions of various scientific disciplines: legal, information and economic ones. The science of criminal procedure law acts as the main discipline and allows us to study the legislative regulation of the specifics of the proceedings in such cases and law enforcement practice. Information science, which studies the analysis, collection, storage, search, classification and protection of information, allows us to develop a method for seizing, storing and selling such a specific object as digital currencies. Economic science provides an opportunity to determine what part of the contents of the crypto wallet should be seized, how the exchange rate of the cryptocurrency unit should be calculated in relation to the official national monetary unit.

The present study uses general scientific, interdisciplinary and specific methods.

The regulatory approach was shown in the analysis of international and national legislation in the field of legal regulation of digital currency turnover and the specifics of criminal proceedings in the seizure and subsequent confiscation of this type of asset.

The comparative legal method made it possible to compare the regulations and law enforcement practice of various states on the procedure for applying interim measures in criminal proceedings in relation to digital currencies.

The study widely applies a systematic approach, which is necessary in cognition of such categories as procedural actions and decision-making in relation to cryptocurrencies within criminal proceedings in the new digital reality.

The use of normative-value, functional, structural-functional approaches, as well as general logical methods (analysis and synthesis, induction and deduction, abstraction and ascent from the abstract to the concrete, etc.) and methods of empirical research allowed us to form a methodology for research on the seizure of digital currencies, their storage in criminal

proceedings, further confiscation and sale in this paper.

Results

The number of crimes involving cryptocurrencies, including those of a cross-border nature, is currently increasing rapidly. The amount of damage caused by these crimes is impressive. The increase in crime is accompanied with the large amount of confiscation of cryptocurrencies in criminal cases.

Meanwhile, the legal regulation of digital currencies, both internationally and nationally, is in its infancy. The status of cryptocurrencies remains unclear and there are no unified rules for their seizure, confiscation and disposal in criminal cases. At the same time, traditional criminal procedure legislation does not consider the specifics of digital currencies. The insufficiency and incompleteness of legal regulation creates difficulties for fighting crimes related to the illegal use of cryptocurrencies.

In these circumstances, the importance of acts of international organizations and judicial decisions to develop common approaches of different states to the prevention, investigation and detection of crimes committed with illicit trafficking in cryptocurrencies increases, as does the importance of studying the extensive experience of different states, is increasing.

Organizational and technical aspects of seizure of digital currencies, their subsequent storage and realization remain unresolved. However, current experience in the fight against cybercrime refutes the thesis that digital currencies are invulnerable and cannot be seized.

However, not all states have the necessary software yet. There are not enough competent professionals to assist investigative authorities and courts. That is why the most widely used method of seizing cryptocurrencies today is to obtain cryptocurrency wallet passwords from suspects or defendants.

The further fate of confiscated cryptocurrency remains largely unresolved. In practice, confiscated cryptocurrencies are usually successfully sold at auctions, generating great interest among investors, and the fiat money received is converted into state revenue.

Conclusion

This research leads to the conclusion that further improvement of international and national legal regulation of the status of digital currencies and the rules of their legal circulation, as well as the establishment of conditions and procedures for their seizure in criminal (and not only) legal proceedings, their storage, confiscation and sale is necessary.

Harmonisation and unification of national legislation is particularly necessary since this category of offences often has a cross-border nature and only similar legal regulation will allow to effectively combine the efforts of different states in combating them.

Legislative classification of cryptocurrencies as property would provide an opportunity for various investigative actions in criminal cases of crimes related to their illicit trafficking, application of procedural coercive measures, including seizure of this type of assets and their conversion into the income of the state. The legality and validity of such actions and decisions should be guaranteed by a court decision, as seizure of digital currencies restricts the inviolability of property. Criminal proceedings in relation to cryptocurrencies at the present stage are not possible without the involvement of a specialist.

The procedure for seizure of property should not only provide for the powers of the criminal justice authorities, but also enshrine the rights of the accused due to the privilege against self-incrimination. This is particularly important in the current context where the seizure of digital currencies in the absence of cooperation by the defendant is extremely difficult and the temptation for criminal justice authorities to seek such cooperation by various methods is high.

In this regard, it is necessary to complete Article 5 of the Criminal Procedure Code of the Russian Federation (Criminal Procedure Code of the Russian Federation No. 174-FZ, 2001, Art. 5) with a provision stating that in criminal proceedings, digital currency is recognised as property.

It is also necessary to establish in the Criminal Procedural Code of the Russian Federation (Criminal Procedure Code of the Russian Federation No. 174-FZ, 2001, Art. 29) a provision stating that seizure of such type of property as cryptocurrency and its subsequent confiscation is possible only under a court

decision. If there is a court decision, seizure should be carried out with the obligatory participation of a specialist, what should also be reflected in article 58 and article 115 of the Criminal Procedural Code of the Russian Federation (Criminal Procedure Code of the Russian Federation No. 174-FZ, 2001, Art. 58, 115).

In addition, articles 81-82 on material evidences, article 230 on interim measures, chapter 53 on seizure and confiscation of digital currencies at the request of the competent authorities of a foreign state on mutual legal assistance in criminal cases should also be supplemented.

The Criminal Code of the Russian Federation should provide for criminal liability for crimes involving digital currency, including the extension of articles 159^3, 159^6, 171, 172^1-172^3, 174, 175, 183, 185-185^6, 187, 195, 199^2 of the Criminal Code to cryptocurrency (Criminal Code of the Russian Federation No. 63-FZ, 1996, Art. 159^3, 159^6, 171, 172^1-172^3, 174, 175, 183, 185-185^6, 187, 195, 199^2).

The development of legal regulation of combating offences related to illicit digital currency circulation should be comprehensive and cover not only criminal procedural and criminal legislation, but also acts regulating operational and investigative activities, banking activities, establishing guarantees of protection of rights of bona fide buyers and sellers of cryptocurrency, etc.

A promising way to sell the confiscated cryptocurrency should be recognized as its sale at auctions, the procedure for conducting which also requires the development of special rules, including notifying the public about the auction.

The best way to overcome the negative factors in the spread of criminal manifestations in the economy is to continue progressive work on the development of the legal framework (both international and national) regarding the creation of a wide range of conditions to prevent the turnover of assets obtained by criminal means, including their digital expression, with the simultaneous comprehensive implementation of generally recognized financial security standards in national legislative systems.

Acknowledgements

Publication prepared within the state task 075-00998-21-00 dated 22.12.2020 "Transformation of Russian Law in the Conditions of Big Challenges: Theoretical and Applied Foundations". The topic number is FSMW-2020-0030.

Bibliographic references

Albrecht, C., Duffin, K. M., Hawkins, S., & Rocha, V. M. M. (2019). The use of cryptocurrencies in the money laundering process. Journal of Money Laundering Control, 22(2), 210-216.

Campbell, S. (2017). Bitcoins Bulgarian police seized from an 'organised crime gang' would now pay off a FIFTH of the country's national debt after value rises by 600% in six months. Dailymail, December 9, 2017. Retrieved from https://www.dailymail.co.uk/news/article-5163209/Bulgaria-Bitcoins-pay-FIFTH-debt.html

Court of Justice of the European Union (2015) Judgment of the court (Fifth Chamber) in case C-264/14 «Skatteverket v David Hedqvist». October 22, 2015. Retrieved from https://curia.europa.eu/juris/document/document.jsf?text=&docid=170305&doclang=EN

Covolo, V. (2020). The EU Response to Criminal Misuse of Cryptocurrencies: The Young, already Outdated 5th Anti-Money Laundering Directive. European Journal of Crime Criminal Law and Criminal Justice, 28(3), 217-251. DOI: https://doi.org/10.1163/15718174-bja10003

Criminal Code of the Russian Federation No. 63-FZ. IMOLIN: site, June 13, 1996, adopted by the Federation Council on June 5, 1996. Retrieved from http://www.imolin.org/doc/amlid/Russian_Federation_Criminal_Code.pdf

Criminal Procedure Code of the Republic of Belarus No. 295-Z. Nuclear Security Legislation Database by VERTIC Organisation, July 16, 1999. Retrieved from https://www.vertic.org/media/National%20Legislation/Belarus/BY_Criminal_Procedure_Code.pdf

Criminal Procedure Code of the Russian Federation No. 174-FZ. IMOLIN: site, December 18, 2001, approved by the Federation Council December 5, 2001. Retrieved from https://www.imolin.org/doc/amlid/Russian_Federation_Criminal_Procedure_Code.pdf

Custers, B. H. M., Pool, R. L. D., & Cornelisse, R. (2019). Banking malware and the laundering of its profits. European Journal of Criminology, 16(6), 728-745. DOI: https://doi.org/10.1177/1477370818788007

Database of arbitration cases of the Russian electronic justice system (2018). Decision of the Ninth Court of Arbitration Appeals of Russia in the case A40-124668-2017, May 15, 2018. Retrieved from https://kad.arbitr.ru/Document/Pdf/3e155cd1-6bce-478a-bb76- 1146d2e61a4a / 58af451a-

bfa3-4723-ab0d-d149aafecd88 /A40-124668-2017_20180515_Postanovlenie_apelljacionnoj_instancii.pdfDolgieva, M. M. (2018). Cryptocurrency confiscation. Legality, 11(1009), 45-49.

Decree No. 8. On the development of the digital economy, Press service of the President of the Republic of Belarus, December 21, 2017. Retrieved from https://president.gov.by/ru/documents/dekret-8-ot-21-dekabrja-2017-g-17716

Europol. (2018). Police seize more than EUR 4.5 million in cryptocurrencies in Europe's biggest ever LSD bust. European Union Agency for Law Enforcement Cooperation: official site, June 28, 2018. Retrieved from https://www.europol.europa.eu/newsroom/news/police-seize-more-eur-45-million-in-cryptocurrencies-in-europe%E2%80%99s-biggest-ever-lsd-bust

Federal Law No. 115-FZ. On Countering the Legalization (Laundering) of Proceeds from Crime and Financing of Terrorism. Garant: Legal Information Portal, August 7, 2001. Retrieved from https://base.garant.ru/12123862

Federal Law No. 127-FZ. On Insolvency (Bankruptcy) (as amended). Garant: Legal Information Portal, October 26, 2002. Retrieved from https://base.garant.ru/185181

Federal Law No. 229-FZ. On enforcement proceedings. Garant: Legal Information Portal, October 2, 2007. Retrieved from https://base.garant.ru/12156199

Federal Law No. 259-FZ. On Digital Financial Assets, Digital Currency and on Amendments to Certain Legislative Acts of the Russian Federation. Garant: Legal Information Portal, July 31, 2020. Retrieved from https://www.garant.ru/products/ipo/prime/doc/74351466

Federal Law No. 273-FZ. On Counteracting Corruption. Garant: Legal Information Portal, December 25, 2008. Retrieved from https://base.garant.ru/12164203

Federal Register of Legislation of Australian Government (2018) Anti-Money Laundering and Counter-Terrorism Financing Act 2006. Retrieved from https://www.legislation.gov.au/Details/C2019C00011

Financial Technology Protection Act, H.R.56 – 116th Congress. Library of Congress: official site, 2019. Retrieved from https://www.congress.gov/bill/116th-congress/house-bill/56

Grobys, K. (2021). When the blockchain does not block: on hackings and uncertainty in the cryptocurrency market. Quantitative Finance, 21(8). DOI: https://doi.org/10.1080/14697688.2020.1849779

Judicial Department at the Supreme Court of the Russian Federation (2015). Report on the work of courts of general jurisdiction on the consideration of criminal cases at first instance for the 12 months of 2015. Retrieved from https://www.cdep.ru/userimages/sudebnaya_statistika/2015/F1-ug_pr-vo_1_inst-2015.xls

Judicial Department at the Supreme Court of the Russian Federation (2016). Report on the work of courts of general jurisdiction on the consideration of criminal cases at first instance for the 12 months of 2016. Retrieved from http://www.cdep.ru/userimages/sudebnaya_statistika/2016/F1-svod-2016.xls

Judicial Department at the Supreme Court of the Russian Federation (201/). Report on the work of courts of general jurisdiction on the consideration of criminal cases at first instance for the 12 months of 2017. Retrieved from http://www.cdep.ru/userimages/sudebnaya_statistika/2017/F1-svod-2017.xls

Judicial Department at the Supreme Court of the Russian Federation (2018). Report on the work of courts of general jurisdiction on the consideration of criminal cases at first instance for the 12 months of 2018. Retrieved from http://www.cdep.ru/userimages/sudebnaya_statistika/2019/F1-svod_vse_sudy-2018.xls

Judicial Department at the Supreme Court of the Russian Federation (2019). Report on the work of courts of general jurisdiction on the consideration of criminal cases at first instance for the 12 months of 2019. Retrieved from http://www.cdep.ru/userimages/sudebnaya_statistika/2020/F1-svod_vse_sudy-2019.xls

Kethineni, S., & Cao, Y. (2020). The Rise in Popularity of Cryptocurrency and Associated Criminal Activity. International Criminal Justice Review, 30(3), 325-344. DOI: https://doi.org/10.1177/1057567719827051

Kim, H. (2018). Top South Korean court recognises cryptocurrency as asset. South China Morning Post: official site. Retrieved from https://www.scmp.com/news/asia/east-asia/article/2148616/top-south-korean-court-recognises-cryptocurrency-asset

Koerhuis, W., Kechadi, T., & Le-Khac, N. A. (2020). Forensic analysis of privacy-oriented cryptocurrencies. Forensic Science International-Digital Investigation, 33(200891). DOI: https://doi.org/10.1016/j.fsidi.2019.200891

Lee, H., & Choi, K. S. (2021). Interrelationship between Bitcoin, Ransomware, and Terrorist Activities: Criminal Opportunity Assessment via Cyber-Routine Activities Theoretical Framework. Victims & Offenders, 16(3), SI, 363-384. DOI: https://doi.org/10.1080/15564886.2020.1835764

Lloyd, C. (2020). The privacy revolution begins: Did carpenter just give bitcoin users a chance to

strike down the bank secrecy act? George Washington Law Review, 88(1), 204-238.

Manhattan, U. S. (2014). Attorney Announces Forfeiture of $28 Million Worth of Bitcoins Belonging to Silk Road. United States Departament of Justice. Retrieved from https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-forfeiture-28-million-worth-bitcoins-belonging-silk

Markaryan, E. S. (2018). Specificity of conducting a research examination in the investigation of crimes committed with the use of cryptocurrencies. Actual Problems of Russian Law, 6(91), 146-152. DOI: https://doi.org/10.17803/1994-1471.2018.91.6.146-152

Mkrtchian, S. M. (2020). Property Crimes in the Blockchain Sphere: New Criminal Schemes and Their Criminal Law Assessment. Russian Journal of Criminology, 14(6), 845-854. DOI: https://doi.org/10.17150/2500-4255.2020.14(6).845-854

O'Donnell, J. (2021). Police seize $60 million of bitcoin! Now, where's the password? Reuters. Retrieved from https://www.reuters.com/article/idUSL1N2KB0QK

Palmer, D. (2018). Finland Mandates Cold Storage, Public Auctions for Seized Bitcoins. Coindesk. Retrieved from https://www.coindesk.com/markets/2018/02/20/finland-mandates-cold-storage-public-auctions-for-seized-bitcoins/

Resolution of the Plenum of the Supreme Court of the Russian Federation No. 32 of July 7, 2015. «On judicial practice in cases of legalization (laundering) of funds or other property acquired by criminal means, and the acquisition or sale of property knowingly obtained by criminal means». Internet portal «Rossiyskaya Gazeta», July 13, 2015. Retrieved from https://rg.ru/2015/07/13/sud-dok.html

Resolution of the Plenum of the Supreme Court of the Russian Federation No.1 of February 26, 2019: «On Amending the Resolution of the Plenum of the Supreme Court of the Russian Federation of July 7, 2015 N 32 «On judicial practice in cases of legalization (laundering) of funds or other property acquired by criminal means, and the acquisition or sale of property knowingly obtained by criminal means». Internet portal «Rossiyskaya Gazeta», March 7, 2019. Retrieved from https://rg.ru/2019/03/07/postanovlenie-dok.html

Saiedi, E., Broström, A., & Ruiz, F. (2020). Global drivers of cryptocurrency infrastructure adoption. Small Bus Econ. DOI: https://doi.org/10.1007/s11187-019-00309-8

Teichmann, F. M. J., & Falker, M. C. (2020). Cryptocurrencies and financial crime: solutions from Liechtenstein. Journal of Money Laundering Control, Vol. ahead-of-print No. ahead-of-print. DOI: https://doi.org/10.1108/JMLC-05-2020-0060

Thompson, C. (2015). Silk Road website founder Ross Ulbricht found guilty on all counts. CNBC: official site. Retrieved from https://www.cnbc.com/2015/02/04/silk-road-website-founder-ross-ulbricht-found-guilty-on-all-counts.html

Turner, A. B., McCombie, S., & Uhlmann, A. J. (2019). A target-centric intelligence approach to WannaCry 2.0. Journal of Money Laundering Control, 22(4), 646-665. DOI: https://doi.org/10.1108/JMLC-01-2019-0005.

Vandezande, N. (2017). Virtual currencies under EU anti-money laundering law. Computer Law & Security Review, 33(3), 341-353. Retrieved from https://isiarticles.com/bundles/Article/pre/pdf/137977.pdf

Voß, O. (2018). Bavaria sells Bitcoin for 12 million euros. The daily mirror. Retrieved from https://www.tagesspiegel.de/wirtschaft/internet kriminalitaet-bayern-verkauft-bitcoin-fuer-12-millionen-euro/22611878.html

Wang, H., He, D., Liu, Z., & Guo, R. (2020). Blockchain-Based Anonymous Reporting Scheme with Anonymous Rewarding. IEEE Transactions on Engineering Management, 67(4), 1514-1524. DOI: https://doi.org/10.1109/TEM.2019.2909529.