Journal of Management & Technology
e-ISSN: 2177-6652

CRYPTOCURRENCY AS A PRIORITY MEANS OF TERRORISM FINANCING IN THE DIGITAL ECONOMY

A CRIPTOMOEDA COMO MEIO PRIORITÁRIO DE FINANCIAMENTO DO TERRORISMO NA ECONOMIA DIGITAL

LAS CRIPTOMONEDAS COMO MEDIO PRIORITARIO DE FINANCIACIÓN DEL TERRORISMO EN LA ECONOMÍA DIGITAL

Svetlana Muradyan
http://orcid.org/0000-0002-1366-5074
Moscow University of the Ministry of Internal Affairs of Russia named by V.Ya. Kikot
Russian Federation

Nikolay Pcholovsky
http://orcid.org/0000-0001-7506-5448
St. Petersburg University of the Ministry of Internal Affairs of Russia, Russian Federation

Grigory Sarbaev
http://orcid.org/0000-0002-0876-2486
Russian Orthodox Religious Institution – the Institution for professional religious education of the Russian Orthodox Church Postgraduate and doctoral courses, named after Holy and Equal-to-the-Apostles Cyril and Methodius

Kristina Vinogradova
http://orcid.org/0000-0002-7500-9996
Moscow University of the Ministry of Internal Affairs of Russia named by V.Ya. Kikot, Russian Federation

Vitaliy Vasyukov
http://orcid.org/0000-0003-0743-5616
Moscow State Institute of International Relations (University) of the Ministry of Foreign Affairs of the Russian Federation (MGIMO-University), Russian Federation

Scientific Editor: José Edson Lara
Organization Scientific Committee
Double Blind Review by SEER/OJS
Received on 02/05/2022
Approved on 07/19/2022

ABSTRACT

International terrorist organizations, while maintaining a significant financial potential, are increasingly looking for new sources of funding, following the trend of high rates of informatization of society. To date, the use of the Internet is one of the most effective means of managing forces and financial resources. To finance their activities, terrorists, in addition to actively using international Muslim humanitarian funds, speculating on stock exchanges, investing in real estate, in a number of legal sectors of the economy, as well as participating in the criminal business of a number of countries, began to actively use cryptocurrency. These funds are used to create new and finance sleeping cells, fundraising is organized to carry out specific terrorist attacks, the formation of their own cyber units, which, vice versa, are able to extract financial resources through hacker attacks using remote theft, extortion, the sale of weapons and drugs as predicate crimes, the means of committing which is often the use of cryptocurrencies.

Key words: cryptocurrency, bitcoin, terrorist financing, al-Qaeda, peer-to-peer networks, computer attacks, social engineering.

RESUMO

As organizações terroristas internacionais, embora mantenham um potencial financeiro significativo, procuram cada vez mais novas fontes de financiamento, acompanhando a tendência de elevados índices de informatização da sociedade. Até à data, a utilização da Internet é um dos meios mais eficazes de gestão de forças e recursos financeiros. Para financiar suas atividades, os terroristas, além de usarem ativamente fundos humanitários muçulmanos internacionais, especularem nas bolsas de valores, investirem em imóveis, em vários setores jurídicos da economia, além de participarem do negócio criminoso de vários países , começou a usar ativamente a criptomoeda. Esses fundos são usados para criar novas células adormecidas e financiar, a captação de recursos é organizada para realizar ataques terroristas específicos, a formação de suas próprias unidades cibernéticas, que, vice-versa, são capazes de extrair recursos financeiros por meio de ataques de hackers usando roubo remoto, extorsão, a venda de armas e drogas como crimes antecedentes, o meio de cometer que muitas vezes é o uso de criptomoedas.

Palavras-chave: criptomoeda, bitcoin, financiamento do terrorismo, al-Qaeda, redes peer-to-peer, ataques a computadores, engenharia social.

RESUMEN

Las organizaciones terroristas internacionales, si bien mantienen un importante potencial financiero, buscan cada vez más nuevas fuentes de financiación, siguiendo la tendencia de los altos índices de informatización de la sociedad. Hasta la fecha, el uso de Internet es uno de los medios más efectivos para administrar fuerzas y recursos financieros. Para financiar sus actividades, los terroristas, además de utilizar activamente fondos humanitarios musulmanes internacionales, especulan en bolsas de valores, invierten en bienes raíces, en una serie de sectores legales de la economía, así como participan en el negocio criminal de una serie de países. , comenzó a usar criptomonedas activamente. Estos fondos se utilizan para crear nuevas y financiar células durmientes, la recaudación de fondos se organiza para llevar a cabo

ataques terroristas específicos, la formación de sus propias unidades cibernéticas que, viceversa, pueden extraer recursos financieros a través de ataques de piratas informáticos mediante robo remoto, extorsión, la venta de armas y drogas como delitos determinantes, cuyo medio de comisión suele ser el uso de criptomonedas.

Palabras clave: criptomoneda, bitcoin, financiación del terrorismo, al-Qaeda, redes peer-to-peer, ataques informáticos, ingeniería social.

1. INTRODUCTION

The financing of terrorism has been recognized as a threat to the world community for a long time. At the international level, this is confirmed by the adoption of resolution 54/109 of the UN General Assembly, approving the International Convention for the Suppression of the Financing of Terrorism (December 9, 1999) and more UN Security Council Resolutions in this area. The regional level is represented by the activities of such organizations as the Financial Action Task Force on Money Laundering (FATF), the Eurasian Group on Combating Money Laundering and the Financing of Terrorism (EAG), the Committee of Experts on the Evaluation of Measures to Combat Money Laundering and the Financing of Terrorism (MONEYVAL) and others.

In the context of the global digitalization of the economy, the emergence of digital currencies, such cooperation had to be extended to combat the illegal use of cryptocurrencies for criminal purposes (Pushkarev et al., 2021, pp. 395-406), including for the financing of terrorism. Thus, according to Chainalysis , in 2020, law enforcement agencies around the world have identified and investigated more terrorist financing schemes using cryptocurrencies than in previous years (The Chainalysis Crypto Crime Report, February 16, 2021).

For example, in 2020, French law enforcement authorities investigated a criminal case under a cryptocurrency financing scheme for terrorism, arresting 29 French citizens. The scheme involved dozens of people in France buying "cryptocurrency coupons" in small denominations ranging from $11 to $165. The indicated amounts were credited to accounts opened abroad for persons marked in adherence to jihadism, who converted them into cryptocurrency. According to French law enforcement agencies, hundreds of thousands of

euros were transferred in this way to the accounts of Al-Qaeda and the Islamic State group (The Chainalysis Crypto Crime Report, February 16, 2021).

Cryptocurrencies as a tool for financing terrorism, compared to sources that have long been used, are still in their infancy. The attractiveness of the characteristics of this tool has no alternatives today: anonymity; lack of effective and coordinated regulation, both at the international, regional, and domestic levels (Muradyan, 2020. pp. 110-118; Tien et al., 2021); high speed and irreversibility of transactions; decentralized registries. The only thing that stops terrorists from choosing cryptocurrencies as a profiling means of generating their financial resources is their high volatility, which means price instability, which is essential when we talk about large amounts of funds that are at the disposal of terrorist organizations every day. However, recently, authoritative researchers have stated that the use of stablecoins is a very effective means of solving the problem of the volatility of the cryptocurrency exchange rate (Pushkarev et al., 2020, p. 332-335). The second limiting factor is not the universal recognition of cryptocurrencies as a means of payment. However, as the experience of law enforcement agencies in most states shows, terrorists find ways to implement their plans, regardless of the difficulties.

2. METHODS

The philosophical and ideological basis of the study was the dialectical method of cognition applied to various legal phenomena, which allows us to consider them in constant development, close interconnection and interdependence. Using the dialectical method, the authors managed to describe the objective dependence of the transformation of economic and legal processes associated with the spread of digital currencies under the influence of the digitalization of the economy and law in general.

Of the general scientific methods of scientific knowledge, such as analysis, synthesis, deduction, induction, classification and others were used.

Among the theoretical and empirical methods, the authors used: systemic, comparative legal, statistical methods, as well as a generalization of the investigative and judicial practice

of Russia and foreign countries in the field of using cryptocurrencies as a means and subject of a crime in order to form sources of financing terrorism.

3. DISCUSSIONS

Technological progress, digitalization of all spheres of society's life naturally extends to its criminal component. Among the entire spectrum of “digital” threats, financial crimes committed in connection with or with the help of digital currencies are of particular concern. Thus, during the operation "HAECHI-II", conducted under the auspices of Interpol, in just four months (from June to September 2021), the police of 20 states participating in the above program arrested more than 1,000 people and seized digital currencies in the equivalent of 27 million US dollars (More than 1,000 arrests and USD 27 million intercepted…, 2021).

The U.S. Internal Revenue Service managed to seize $3.5 billion worth of cryptocurrencies in fiscal year 2021. This represents 93% of all funds seized by the State Criminal Investigation Department during the same time period (IRS: CI Annual Report 2021, 2022).

In these cases, digital currencies were either the subject or means of committing crimes such as drug or weapons trafficking, remote fraud, theft, extortion and were used as a source of terrorist financing, sometimes directly, sometimes after the commission of ordinary crimes, as predicates, when funds already legalized by transferring them into cryptocurrency were transferred to the accounts of terrorist organizations.

The organization “Rosfinmonitoring” notes that facts of financing terrorism using cryptocurrencies are also recorded in Russia. Bitcoin, Ethereum and Monero are especially popular (Rosfinmonitoring records the facts of terrorist financing using cryptocurrencies…, 2021). In October 2021, the head of “Rosfinmonitoring” stated that they had suppressed the financial activities in the digital environment of more than 15,000 terrorists, of which about 850 were foreign citizens (Meeting of the President of Russia V.V. Putin…, 2021).

However, the issues of legislative regulation of the processes of arrest and confiscation of cryptocurrencies in Russia are still open. First of all, taking into account the experience of

the world practice of investigating cybercrimes, for their positive resolution it is necessary to establish interaction between law enforcement agencies, which will be empowered to arrest and confiscate cryptocurrencies, with the owners of crypto platforms for the exchange of cryptoassets (exchanges, mixers).

It is quite understandable that in the context of universal digitalization, terrorist organizations also saw the benefits of raising funds through a decentralized digital currency, given its circulation outside the traditional banking system.

The reasons for the high attractiveness of cryptocurrencies for use in the framework of terrorist financing and money laundering are:

- the proper level of anonymity of most cryptocurrencies, when the systems do not require the necessary identification, as when opening and using standard bank accounts;
- global availability. The system solves the problem of seamless transfer of any amount of money from any place and at any time;
- speed, when the speed of a transaction complicates the ability to intercept and block it;
- irreversibility. In the process of making transactions with cryptocurrencies, no additional checks or validation are required, after which the operation can be suspended or canceled;
- low cost of use. The exception is crypto exchangers that set interest rates for converting cryptocurrencies to fiat money;
- ease of use due to special applications with a user-friendly interface;
- difficulty in tracking transactions;
- gaps in legal regulation. The lack of a clear legal framework for cryptocurrencies, their free use in a number of states allows them to accumulate funds directed to charity, under the auspices of which resources are often collected for the needs of terrorist organizations.

Of course, the use of physical money is even more anonymous and more difficult to track than the use of cryptocurrencies, but this is where their competitive advantages end. The limited amount of physical money in circulation, the difficulty of anonymously transporting

and converting it, especially if we talk about large amounts, all these factors do not allow it to be used as a preferred source of terrorist financing.

However, the desire, for example, of Bitcoin to the generally accepted principles of client fame KYC (Know Your Customer - know your client) and AML CFT CWMDF (Anti-money laundering and counter-terrorist financing and counter-weapons of mass destruction financing - countering money laundering obtained by criminal means, countering the financing of terrorism and the financing of weapons of mass destruction) makes the ability to track and match transactions and their network more realistic with the right level of training. In addition, the bitcoin distributed ledger is public.

In one of the cases, the court indicated that around January 2019, the defendant paid 25,000 rubles via the Internet, transferring the indicated funds to the untraceable Bitcoin cryptocurrency, transferred the indicated means of payment to the Rutor website by placing an order for weapons. Then, acting deliberately and illegally, he acquired a pistol by picking up a “cache-bookmark” in an unspecified place near the Nagatinskaya metro station in Moscow, which was converted by a home-made method from an MP-371 flare pistol. Also, having criminal intent, at an unspecified time, but no later than March 07, 2019, in an unspecified place in the city of Moscow, he acquired ammunition: 66 cartridges of 9 mm caliber. Without a license to purchase weapons, their main parts and ammunition, acting in violation of the Federal Law of the Russian Federation No. 150 FZ “On Weapons” dated December 13, 1996, and knowing that criminal liability has been established for illegal circulation of weapons, their main parts and ammunition, he turned the gun and cartridges into his illegal possession by placing them in his apartment (The verdict of the Perovsky District Court of Moscow No. 01-0603/2019, June 17, 2019).

So, monitoring the sources of receipt of digital currencies for the purposes of financing terrorism showed that they include, first of all:

- accumulated financial resources in digital assets obtained through profitable investments or trading, in the form of short-term speculations, when a trader directly from the members of a terrorist organization or a specialist involved in the interests of this organization conducts many transactions with cryptocurrency and

achieves profit in a fairly short period of time;

- donations, for example, through charitable foundations, or in other ways, as in our example of France through the purchase of coupons;
- funds received from the commission of predicate crimes, in the form of illicit trafficking in narcotic drugs, psychotropic substances or their analogues, illicit trafficking in weapons; committing theft in the form of fraud using information and telecommunication technologies (Pushkarev et al., 2019, p. 2563-2566), etc.

As part of the analysis of the last paragraph, with regard to money laundering schemes for the purposes of financing terrorism, where the predicate crimes are crimes related to the contactless sale of substances and objects prohibited in circulation, then, in essence, the scheme for implementing the objective side is quite standard here. The difference is manifested only in the peculiarities of the circulation of instruments for committing such crimes. As a rule, transactions of this kind are made on the expanses of the Darknet. Money from buyers goes directly to Qiwi e-wallets of direct sellers or pawnbrokers, and then converted into cryptocurrency. In Russia, these are more often bitcoins, which are subsequently withdrawn through electronic exchanges to the accounts of members of a criminal group. Cryptocurrency is converted into rubles. In this case, we can talk about the commission of a crime under Art. 1741 of the Criminal Code of the Russian Federation "Legalization (laundering) of funds acquired by a person as a result of committing a crime". Similarly, these acts will be qualified in other states, since such an approach was approved in the framework of the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism of May 16, 2005 (Council of Europe Convention on Laundering, Search, Seizure and Confiscation…, May 16, 2005) and taking into account Recommendation 15 FATF (Virtual assets and virtual asset service providers…, 2019).

As for the fraudulent actions of terrorists in relation to cryptocurrencies, depending on the method used, they can be divided into two large groups: these are thefts committed using social engineering methods and thefts carried out by computer attacks.

Crimes committed with the use of social engineering are aimed either at a trading

counterparty or at the layman. Fraudsters use deceit and breach of trust to get hold of funds or personal data. The attacker pretends to be a real trader interested in buying or selling Bitcoin or other cryptocurrencies on a P2P platform. He can post his own trade ad or respond to an existing one. An alternative technique widely used on centralized marketplaces is to imitate a help desk. In this case, the attacker, having contacted the potential victim, pretends to be an employee of the trading platform and, as a rule, tries to obtain personal information or payment details from him.

As of today, fraudulent schemes are actively used when buying cryptocurrencies, such as Bitcoin on Binance P2P. The seller asks to cancel the transaction after payment by the buyer. If the buyer agrees, then the escrow service returns the cryptocurrency back to the seller's wallet. The seller asks the buyer to complete the transaction outside the P2P platform, that is, in the absence of access to the escrow service, and therefore without guarantees of receiving cryptocurrency after payment. And the third most common option is when the seller asks to pay an additional commission in addition to the commission declared by the marketplace, that is, he tries to illegally receive a reward from the buyer.

Among the fraudulent schemes used in the sale of cryptocurrencies, one can single out the blocking of coins, when the counterparty marks the transaction as “paid”, even if he did not send the payment. And when you try to contact him, he usually does not answer. This type of scam is usually aimed at beginners, who are more prone to such errors due to their lack of experience. The most banal way is when the counterparty asks for a loan with a promise to repay the debt with high interest. Sometimes, the buyer requires to transfer the coins before the payment is completed. Such a transfer deprives the participant of the transaction of the guarantee for sending funds from the side of the buyer.

Such actions in all cases must be qualified under Article 159 of the Criminal Code of the Russian Federation as fraud. If, subsequently, the funds received using social engineering methods are used to finance terrorism and extremist activities, then additional qualifications will be required under Part 1^1 of Art. 205^1 of the Criminal Code of the Russian Federation.

Computer attacks are most often associated with hacking wallets (How are Bitcoins stolen…, 2019). This rather simple and not requiring large financial investments method

allows terrorists to receive financial resources, for example, immediately before the commission of a terrorist act, when law enforcement agencies will obviously not have enough time to track their receipts and the purposes of their use.

Until new methods become known to law enforcement agencies, including the financial intelligence of states, and it is not possible to prevent them, criminals, having tried them once, begin to actively use them everywhere. That is, the new schemes of cybergroups of terrorist organizations act as a kind of best practice for “colleagues”.

Recently, the following most effective criminal cyberattacks can be distinguished as follows:

- receiving updates. For example, the real Electrum application (Bitcoin wallet) during users' transactions, if any of the malicious servers was reached, it would display an error message. The message form looked formal by presenting the information as rich text. Then the message indicated the only possible way out of the situation, this is the need to download updates. After accepting the offer, the message sent the user to another GitHub repository and the person downloaded another wallet that was stealing data for the scammers. If it was possible to immediately continue the transaction, then the “update process” required two-factor identification, which in reality is used only to confirm transactions. However, users did not see anything wrong with this, they entered all the required data and the funds were transferred to the wallets of scammers;
- interception on third-party services. Coinomi, written in Java, is rendered through the built-in Chromium-based browser with the function of automatically spell-checking all text fields. This feature has been preserved for wallets on the Coinomi platform. This means that with the help of MitM “man in the middle” attacks, it was not difficult for hackers, for example, through public wi-fi, to intercept phrases from wallets;
- Trojan in Chrome extension. Trojan.Win32.Razy.gen was distributed through ads and could work in Google Chrome, Mozilla Firefox, and Yandex. Installed extensions were disabled from integrity checks and automatic updates, and were entirely aimed at finding addresses of cryptocurrency wallets and replacing them.

The capabilities of the malware were so high that it could also forge images of wallets and their QR codes; change to phishing pages of crypto-exchanges in order to force the user to transfer their credentials;

- Docker attacks. Analysts managed to find quite a lot of such vulnerabilities. The use of Docker containers with an open control mechanism is possible in the following areas: hidden mining of Monero, connecting to a botnet in order to steal personal data, or use it to create host services in phishing.

Such actions with the aim of raising funds for the needs of terrorist organizations will be qualified, depending on the specifics of the implementation of the objective side for the relevant offenses provided for by the norms of Chapter 28 of the Criminal Code of the Russian Federation "Crimes in the field of computer information". And, if necessary, also in conjunction with Part 1^1 of Art. 205^1 of the Criminal Code of the Russian Federation.

As part of the analysis of the sources of financing of terrorism through the collection of donations through charitable foundations, the experience of the United States is very interesting. Consider one illustrative criminal case involving the Federal Bureau of Investigation, the Department of Justice, and the Criminal Investigation Division of the U.S. Internal Revenue Service. As a result of the coordinated actions of these entities, several different charitable campaigns controlled by terrorist groups and their financial intermediaries were identified. As a result, the US Department of Justice managed to seize more than $1 million worth of bitcoins from wallets controlled by these organizations (Chainalysis in Action…, 2019).

During the investigation, it was possible to establish that al-Qaeda has created its own deployed infrastructure for accepting donations for the purposes of financing terrorism. Al-Qaeda, along with affiliated terrorist groups operating mainly in Syria, used multi-layered transactions to hide the movement of these donations to a central address hub, from where the funds were then redistributed to individual groups. With the help of blockchain analysis, US law enforcement agencies were able to identify the central node of this infrastructure "BitcoinTransfer", located in Idlib (Syria). "BitcoinTransfer" posed as a cryptocurrency exchange, but was involved in several terrorist financing schemes and, according to US law

enforcement, was completely controlled by terrorist groups. Since the start of the service at the end of December 2018, more than 280,000 US dollars in bitcoins have passed through “BitcoinTransfer”, most of which was related to the financing of terrorism.

In order to enable the US Department of Justice to seize all cryptocurrency funds associated with al-Qaeda controlled addresses passing through "BitcoinTransfer", it was kept active even after discovery. This made it possible to study all past transactions for terrorist susceptibility and to track organizations and transactions, the funds from which in the future could be used for terrorist financing purposes.

While many terrorist groups have launched their own customized donation services, almost all of them have followed a similar strategy. The groups posed as charities operating in Syria and asked for bitcoin donations through social media and messaging platforms - mainly Telegram and Facebook. However, despite the pretext of charitable organizations, these groups often published messages indicating that the donations would be used to purchase weapons for the militants, for example. In May 2019, law enforcement monitoring the Telegram page of one such group, Tawheed & Jihad Media, saw administrators promoting a "bullets and missiles for the Mujahideen" funding campaign with a single Bitcoin address listed. Monitoring the transactions associated with this address as donations came in indicated that the group admins eventually transferred all funds received to the address hosted on “BitcoinTransfer”.

In the spring of 2020, individuals associated with terrorist groups began touting “BitcoinTransfer” in English, Arabic, Turkish, French, and German as an “anonymous and secure way” to transfer money. The essence of the advertisement was clearly intended to reassure potential "donors" who otherwise would never use cryptocurrencies as a tool for financing terrorism.

Using similar methods of analysis, law enforcement continued to monitor terrorist financing campaigns run by other al-Qaeda-affiliated groups, most of which collected donations in a similar fashion - pretending to be charities, actually funding terrorist activities - and then sending the proceeds funds to the addresses of the same “BitcoinTransfer” (Chainalysis in Action…, 2020). After receiving data on all transactions and their subjects, law enforcement agencies stopped the activities of all BitcoinTransfer participants.

4. CONCLUSIONS

Money is always the most important pillar of every terrorist group, providing everything from media production to real-life attacks. The emergence of digital currency in the financial sector of the economy is associated with the development of information technologies and their active use. Despite all the advantages, the digital currency allows you to get away from the control of the law enforcement system, providing opportunities for the legalization of proceeds from crime and the financing of terrorism.

These developments should come as no surprise given terrorists' experience of using social media, messengers and other technologies to recruit and plan attacks. It took a lot of time for law enforcement agencies to stop such activities, in this regard, it is necessary to intensify their activities in countering crimes committed using cryptocurrencies and related to the financing of terrorism, so as not to see a similar scenario in the financial sector.

In fact, the use by terrorist groups of such new technologies as cryptocurrency has made it possible to neutralize all the results of the progress of the cohesive actions of the world community to counter the financing of terrorism. The exception was the adoption of the 15th FATF Recommendation. “New technologies”, which requires countries and financial institutions to identify and assess the money laundering or terrorist financing risks that may arise from the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies as new as well as existing products.

In accordance with Resolution 73/187 of the UN General Assembly, entitled “Countering the use of information and communication technologies for criminal purposes”, the Secretary-General prepared a report in 2019 based on the information requested from Member States on the difficulties they face in countering the use of information and communication technologies for criminal purposes. As the expert notes, in one form or another, almost all the states that provided information pointed to the lack of mechanisms for

international cooperation in this area. This is also confirmed by the European Union Agency for Law Enforcement Cooperation (Europol) Internet Crime Threat Assessment (IOCTA).

In this regard, the initiative of the Russian Federation to adopt a universal convention on combating cybercrime to replace the outdated Budapest Convention on Computer Crime of 2001 has become a significant step. As part of the proposed initiative, the possibility of creating new structures and mechanisms for interaction, both nationally (round-the-clock centers) and at the international level (international technical commission). Such measures should definitely help to improve the indicators for detecting, disclosing and investigating crimes in the field of information and telecommunications technologies, including those related to the financing of terrorism.

The main focus of the work of law enforcement agencies should be the identification of such crimes, the identification and suppression of the movement of digital assets for criminal purposes and compensation for property damage caused by such crimes.

The examples given in the article highlight the global threat of financial crimes using cyber technologies. In this regard, the issues of restricting the freedoms of citizens, argued by the auspices of protection against terrorism, remain relevant. A similar statement, of course, should also apply to the regulation of the circulation of cryptocurrencies.

REFERENCES

Chainalysis in Action: Department of Justice Announces Takedown of Two Terrorism Financing Campaigns with Help from Blockchain Analysis. (August 13, 2020). Retrieved from: https://blog.chainalysis.com/reports/cryptocurrency-terrorism-financing-al-qaeda-al-qassam-brigades-bitcointransfer

Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism. (May 16, 2005). Council of Europe. Retrieved from: https://rm.coe.int/168008371f

How are Bitcoins stolen? Schemes that even experienced users fall for. (April 16, 2019). Retrieved from: https://crypto-fox.ru/article/kak-voruyut-bitkoiny-shemy/

International Convention for the Suppression of the Financing of Terrorism. (December 9, 1999). Retrieved from: https://www.un.org/ru/documents/decl_conv/conventions/terfin.shtml

IRS: CI Annual Report 2021. (2022). Retrieved from: https://www.irs.gov/pub/irs-pdf/p3583.pdf

Meeting of the President of Russia V.V. Putin with the Director of the Federal Financial Monitoring Service Yuri Chikhanchin. (October 29, 2021). Official website of the President of Russia. Retrieved from: http://kremlin.ru/events/president/news/67034

More than 1,000 arrests and USD 27 million intercepted in massive financial crime crackdown. (November 26, 2021). Interpole. Retrieved from: https://www.interpol.int/News-and-Events/News/2021/More-than-1-000-arrests-and-USD-27-million-intercepted-in-massive-financial-crime-crackdown

Muradyan, S.V. (2020). Actual problems of countering the financing of terrorism using cryptocurrencies (scientific article), in: Collection of articles on the results of the International Scientific and Practical Conference dedicated to the 20th anniversary of the adoption of the UN Convention against Transnational Organized Crime, pp. 110-118. "Actual problems of international cooperation in the fight against crime". Moscow: Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikot.

Pushkarev, V. V., Gaevoy, A., Skachko, A. V., Kolchurin, A., & Lozovsky, D. N. (2019). Criminal prosecution and qualification of cybercrime in the digital economy. Journal of Advanced Research in Dynamical and Control Systems, 11(8 Special Issue), 2563–2566.

Pushkarev, V. V., Poselskaya, L. N., Skachko, A. V., Tarasov, A. V., & Mutalieva, L. S. (2021). Criminal Prosecution of Persons Who Have Committed Crimes in The Banking Sector. Cuestiones Políticas, 39(69), 395–406. https://doi.org/10.46398/cuestpol.3969.25

Pushkarev, V.V., Artemova, V.V., Ermakov, S.V., Alimamedov, E.N., Popenkov, A.V. (2020). Criminal Prosecution of Persons, Who Committed Criminal, Acts Using the Cryptocurrency in the Russian Federation. Revista San Gregorio, 42, 330-335.

Rosfinmonitoring records the facts of terrorist financing using cryptocurrencies. (March 21, 2021). Interview with Deputy Head of Rosfinmonitoring Herman Neglyad. Retrieved from: https://tass-ru.turbopages.org/tass.ru/s/ekonomika/10978989.

The Chainalysis Crypto Crime Report. (February 16, 2021). Retrieved from: https://go.chainalysis.com/2021-Crypto-Crime-Report.html

The verdict of the Perovsky District Court of Moscow No. 01-0603/2019. (June 17, 2019). Retrieved from: https://mos-gorsud.ru/rs/perovskij/services/cases/civil/details/e21eb234-7bae-438e-bc99-9945210a7360

Tien, N. V., Pushkarev, V. V., Tokareva, E. V., Makeev, A. V., & Shepeleva, O. R. (2021). Compensation for Damage Caused by a Crime in the Socialist Republic of Vietnam and the Russian Federation. Jurnal Cita Hukum, 9(2), 211–220. https://doi.org/10.15408/jch.v9i2.21738

Virtual assets and virtual asset service providers: Guidelines for the application of a risk-based approach. (June, 2019). FATF official websit: https://www.fatf-gafi.org/media/fatf/documents/recommendations/MUMCFM-FATF-Guidance-RBA-VA-VASPs.pdf