ISSN: 2776-0960 Volume 2, Issue 6 June, 2021

ResearchJet Journal of Analysis and Inventions
https://reserchjet.academiascience.org

IMPROVING CONTROL OVER THE CIRCULATION OF CRYPTO ACTIVITY IN THE FIGHT AGAINST MONEY LAUNDERING AND TERRORIST FINANCING

Achilov Alisher Temirovich
Associate Professor of the Department of Special Legal Disciplines of the Customs Institute of the State Customs Committee of the Republic of Uzbekistan, Lieutenant Colonel of the Customs Service

Rasulov Shokhjakhon Shukhrat ugli
Master's degree student at the Customs Institute of the State Customs Committee of the Republic of Uzbekistan,
Senior Lieutenant of the Customs Service

Annotation

The article discusses the issues of improving the control of the circulation of crypto activity in the fight against money laundering and terrorist financing, the threats and risks of financing crime using cryptocurrencies, as well as proposals for improving the law enforcement activities of state bodies against money laundering and terrorist financing.

Keywords: cryptocurrency, blockchain, transactions, risks, regulatory legal regulation, AML/CFT, identification.

The impact of innovation on modern human activities is constantly growing and, along with its advantages, brings certain threats. The emergence of such a phenomenon as cryptocurrency creates new, poorly understood, confusing money laundering schemes and expands the possibilities for criminal activity.

An assessment of the national risks of money laundering carried out by the National Agency for Project Management under the President of the Republic of Uzbekistan classified the risk of using virtual currencies in money laundering schemes as a high-risk group, while noting that the anonymity of settlements using cryptocurrencies ensures the popularity of this method when committing crimes, and, besides addition complicates the investigation process. All this confirms the relevance of conducting scientific research on this topic.

As noted in the report of The Financial Action Task Force (FATF): “Virtual currency refers to a digital medium of expression of value that acts as a medium of exchange, either a currency of account or a medium of storage. cost and at the

ResearchJet Journal of Analysis and Inventions
https://reserchjet.academiascience.org

same time not falling under the concept of legal tender, i.e. which is not an officially valid legal tender in settlements with creditors ".

Cryptocurrencies differ from electronic money in that in order to use electronic money as a means of non-cash payment, it is necessary to replenish the account, from which the operation will subsequently be performed. And when using cryptocurrency, there is no need to deposit money, since it is issued on the network.

According to the FATF report, the most popular type of cryptocurrency is currently Bitcoin, developed by a programmer (or a group of programmers) unknown to the general public under the pseudonym Satoshi Nakamoto, under whose authorship a White Paper was published in November 2008 describing how Bitcoin works. and its protocol.

For the first time, the term cryptocurrency was applied in 2009 to describe the first decentralized means of payment - Bitcoin. The real cryptocurrency boom happened after the release of Ethereum. Smart contracts have significantly simplified the creation of blockchain projects and cryptocurrencies, as a result of which the market began to develop actively.

As of April 05, 2021, there are 2,322 cryptocurrencies in the world, and the total market capitalization was 2.01 trillion. US dollars. More than half of the total volume is Bitcoin capitalization - 1.1 trillion. US dollars. In second place is Ethereum ($ 245 billion). The third position is taken by Binance Coin with a capitalization of $ 58 billion US dollars. To represent the scale of this market, it can be noted that the volume of world GDP in 2020 amounted to 83,844.99 billion US dollars, and the GDP of the Republic of Uzbekistan in 2019 amounted to 57.92 billion US dollars.

Before investigating the main threats associated with cryptocurrencies, you should consider their inherent properties, which in the first place make it difficult to conduct a financial investigation if they are used in criminal activities:

1. Fast and non-refundable transactions.

From the point of view of money laundering, it is important to pay attention to factors such as the speed and the possibility of canceling transactions with cryptocurrencies.

The speed of transactions with cryptocurrencies is indicated as a risk factor for committing criminal activity. In particular, funds can be withdrawn or converted much faster than traditional methods. The high speed of transactions makes it difficult to monitor and freeze funds.

ResearchJet Journal of Analysis and Inventions
https://reserchjet.academiascience.org

2. Anonymity.

Some of the cryptocurrencies were specifically created to ensure the anonymity of transactions. The most prominent example is Bitcoin.

The peculiarity of the anonymity offered by cryptocurrencies is that, while it is not difficult to trace the flow of values transmitted through the Bitcoin network, it is extremely difficult to understand how this flow relates to the transfer of values between different parties in the real world.

3. Difficulties in establishing the facts of the use of cryptocurrencies.

The relatively poor knowledge of virtual currencies (compared to cash, payment cards or other forms of online payments) can become a problem for establishing the facts of using cryptocurrencies to launder dirty money.

4. Complex, convoluted transaction models.

The lack of communication between accounts in virtual currencies and real people, combined with the ability to have an unlimited number of accounts, creates fertile ground for the creation of new complex models aimed at concealing the criminal origin of funds.

For example, consider the fact that any user of the Bitcoin network can create any number of addresses. Transactions between two addresses, both of which are controlled by the same person, are no different from transactions in which different people control these addresses. Thus, in theory, attackers could conduct, for example, 100,000 Bitcoin transactions between addresses that they control, before converting Bitcoin into another form. Restoring such a chain of operations, especially if done manually, would take at least a very long time, if it were possible at all. This can be part of a complex money laundering scheme involving multiple persons, virtual currencies, etc.

5. No restrictions on the amount.

Any amounts without restrictions or control can be transferred using cryptocurrencies. In the case of Bitcoin, for example, the transaction amount does not affect the transaction algorithm in any way. As long as the owner of a particular Bitcoin wallet can confirm his ownership of a certain amount of Bitcoin, he has the ability to transfer all coins to one or more Bitcoin wallets, regardless of the number of Bitcoin transferred.

Thus, based on the above, the main threats associated with the commission of crimes in the field of cryptocurrencies can be attributed to the modern threats:

1. Illegal transactions, money laundering.
2. Fraud, financial pyramids.

ResearchJet Journal of Analysis and Inventions
https://reserchjet.academiascience.org

3. Drug trafficking.
4. Financing of terrorism.

The risks associated with the use of cryptocurrencies include:

1. Current risks. Risks associated with the commission of predicate offenses: financing of illegal drug trafficking; export of funds abroad for the purpose of legalizing income; fraud (on the Internet); terrorist financing risk.
2. Economic risks: the risk of shifting foreign economic activity into the shadows in order to avoid paying taxes and customs duties; cryptocurrencies as a continuation of the shadow cash turnover.

Possible risks in the future:

1. Increase in existing and emergence of new threats in the financial system due to the emergence of new technologies for the circulation of financial instruments;
2. Hawala - Hi-tech, given that it is not under the control of state bodies and the chaotic nature of this settlement system, hawala is actively working for the drug market, terrorist financing, etc .;
3. Significant counterproductive impact on national economies by increasing capitalization and the number of cryptocurrencies;
4. Transition of various aggregates and marketplaces to cryptocurrency turnover.

One of the most prominent features of cybercrimes is their transnational nature, with elements of the crime, criminals, victims or evidence found in different jurisdictions. Thus, international cooperation in the investigation of money laundering committed with the use of cryptocurrencies often depends on the availability and competent use of mechanisms for international cooperation between the investigating authorities and other departments of the criminal justice system of the respective countries.

Considering the above, we offer the following recommendations for preventing and detecting illegal transactions using cryptocurrencies:

1. Implementation of the FATF Recommendations.

The recommendations set out the necessary measures that countries should have in order to: - identify risks, develop policies and coordinate within the country; - prosecute money laundering, terrorist financing and financing the proliferation of weapons of mass destruction; - apply preventive measures for the financial sector and other designated sectors; - establish the powers and responsibilities of competent authorities (for example, investigative, law enforcement and supervisory authorities) and other institutional measures; - strengthen the transparency and accessibility of information on beneficial ownership of legal

ResearchJet Journal of Analysis and Inventions
https://reserchjet.academiascience.org

entities and entities; - to ensure international cooperation. It should be noted that the FATF will begin publishing standards for the international regulation of cryptocurrencies in the near future.

2. Submission of reports of suspicious transactions.

Fraud and money laundering on the Internet often involves a large number of small transactions with the willful or unintentional involvement of money mules. This technique presents a challenge to the investigation, since each individual transaction is very minor and the understanding by the investigating authorities that such minor transactions may be part of a larger criminal scheme is often relatively weak. Even if suspicious transactions are identified, analyzing large volumes of small transactions and then investigating the true nature of the criminal activity can be extremely difficult.

4. Interdepartmental cooperation between government agencies.

Depending on the specifics in each specific country, responsibility for conducting financial investigations, forensics, confiscation of proceeds, measures to combat money laundering, cybercrime, and so on may be assigned to various government agencies and departments. Effective collaboration between these institutions to identify and investigate money laundering cases on the Internet is essential to success.

LITERATURE

1. Report on the results of the sectoral assessment of the risks of money laundering and terrorist financing in the field of turnover of crypto-assets in the Republic of Uzbekistan – NAPU 2021 й.

2. Interpol cyber research identifies malware threat to virtual currencies. [Электронный ресурс]. – Режим доступа: http://www.interpol.int/News-andmedia/News/2015/N2015-033

3. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. [Электронный ресурс]. Режим доступа: http://bitcoin.org/bitcoin.pdf

4. The EU Serious and Organized Crime Threat Assessment (SOCTA). – 2013. [Электронный ресурс]. – Режим доступа: https://www.europol.europa.eu

5. Ancerev R.S. Regulation of cryptocurrencies in the modern information economy // In the collection: "The state and the market in the context of the globalization of the world economic space." Collection of articles on the results of the International Scientific and Practical Conference. - 2018 .-- S. 11-14.

6. Batoev V.B., Semenchuk V.V. The use of cryptocurrency in criminal activity: problems of counteraction // journal "Proceedings of the Academy of Management of the Ministry of Internal Affairs of Russia". - 2017 - No. 2.
7. Journal "Financial Security" No. 20, April 2018 [Electronic resource]. - Access mode: http://www.fedsfm.ru/press/periodicals/fb.
8. Explanatory Note to Recommendation 30, “International Standards for Combating Money Laundering, Terrorist Financing and the Financing of the Proliferation of Weapons of Mass Destruction - FATF Recommendations,” FATF-GAFI, February 2012. [Electronic resource]. - Access mode: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf.
9. Korobeynikova O.M., Korobeynikov D.A., Nazarbayev O. Innovative payment instruments in payment systems // Actual problems of the humanities and socio-economic sciences. - 2017. - T. 5. - No. 11 (11). - S. 102-104. [Electronic resource]. - Access mode: https://elibrary.ru/item.asp?id=28938050.