International Cooperation in the Investigation of Economic Crimes Related to Cryptocurrency Circulation

OLEH KREMINSKY1, OLENA KUZMENKO2, ANASTASIIA ANTONIUK3, OLHA SMAHALO4
1,3Department of Criminal Procedure and Criminology, UNIVERSITY OF THE STATE FISCAL SERVICE OF UKRAINE, UKRAINE
2Department of Criminal Procedure and Forensic Science, UNIVERSITY OF THE STATE FISCAL SERVICE OF UKRAINE, UKRAINE
4Department of Finance, VINNYTSIA INSTITUTE OF TRADE AND ECONOMICS OF THE KYIV NATIONAL UNIVERSITY OF TRADE AND ECONOMICS, UKRAINE

ABSTRACT

The cross-border nature of transactions with virtual currencies and the use of anonymity technologies exacerbates the difficulties in investigating economic crimes. The purpose of the article was to study the effects of international cooperation in the investigation of economic crimes related to the circulation of cryptocurrency. The research methodology is based on the method of content analysis of reports, recommendations and standards of the FATF (Financial Action Task Force) for 2012-2020, as a leading international organization for the prevention and development of policies for the regulation of economic crimes related to the circulation of cryptocurrencies. The results demonstrate the following effects of international cooperation in the investigation of economic crimes related to cryptocurrency: 1) the need to use a risk-oriented approach of the international community at the global level, coordination of government efforts to prevent economic crimes; 2) formation of a network of organizations that provides an effective balance between existing threats and opportunities for cryptocurrency circulation; 3) the development of free, decentralized management networks at the global level, which is an innovative and effective way to combat criminal activity, compared to traditional centralized forms of coercion in an era of rapid and unpredictable technological change. The considered experience of the absence of regulatory acts of cryptocurrency circulation and taxation of virtual assets on the principle of traditional assets indicates the absence of concern about illegal activities and possible economic crimes in this area. At the same time, decentralized and quasi-autonomous virtual assets could potentially threaten years of global anti-money laundering efforts. There is a “race” in the international community for leadership in combating economic crime. However, such efforts to establish legitimate jurisdictions that meet the requirements of the AML (Anti-Money Laundering) provide few measures in practice to counter and limit the opportunities for money laundering in other jurisdictions.

Keywords: Counteraction to economic crimes; Virtual assets; International counteraction to cryptocurrency; Illegal circulation; Money laundering schemes.

JEL Classification: B17, F02, F38.

Received: May 07, 2021
Accepted: June 02, 2021
Cooperación Internacional en la Investigación de Delitos Económicos Relacionados con la Circulación de Criptomonedas

OLEH KREMINSKYI1, OLENA KUZMENKO2, ANASTASIIA ANTONIUK3, OLHA SMAHLO4
1,3Department of Criminal Procedure and Criminology, UNIVERSITY OF THE STATE FISCAL SERVICE OF UKRAINE, UKRAINE
2Department of Criminal Procedure and Forensic Science, UNIVERSITY OF THE STATE FISCAL SERVICE OF UKRAINE, UKRAINE
4Department of Finance, VINNYTSIA INSTITUTE OF TRADE AND ECONOMICS OF THE KYIV NATIONAL UNIVERSITY OF TRADE AND ECONOMICS, UKRAINE

RESUMEN

El carácter transfronterizo de las transacciones con monedas virtuales y el uso de tecnologías de anonimato agravan las dificultades para investigar los delitos económicos. El objetivo del artículo es estudiar los efectos de la cooperación internacional en la investigación de los delitos económicos relacionados con la circulación de criptodivisas. La metodología de la investigación se basa en el método de análisis de contenido de los informes, recomendaciones y normas del GAFI (Grupo de Acción Financiera Internacional) para el período 2012-2020, como organización internacional líder en la prevención y desarrollo de políticas para la regulación de los delitos económicos relacionados con la circulación de criptodivisas. Los resultados demuestran los siguientes efectos de la cooperación internacional en la investigación de los delitos económicos relacionados con las criptodivisas: 1) la necesidad de utilizar un enfoque orientado al riesgo de la comunidad internacional a nivel mundial, la coordinación de los esfuerzos gubernamentales para prevenir los delitos económicos; 2) la formación de una red de organizaciones que proporcione un equilibrio eficaz entre las amenazas existentes y las oportunidades para la circulación de cryptocurrency; 3) el desarrollo de redes de gestión libre y descentralizada a nivel mundial, que es una forma innovadora y eficaz para combatir la actividad criminal, en comparación con las formas centralizadas tradicionales de coerción en una era de cambio tecnológico rápido e impredecible. La experiencia considerada de la ausencia de actos de regulación de la circulación de criptodivisas y la imposición de activos virtuales sobre el principio de los activos tradicionales indica la ausencia de preocupación por las actividades ilegales y los posibles delitos económicos en este ámbito. Al mismo tiempo, los activos virtuales descentralizados y casi autónomos podrían poner en peligro años de esfuerzos mundiales contra el blanqueo de dinero. Existe una "carrera" en la comunidad internacional por el liderazgo en la lucha contra los delitos económicos. Sin embargo, estos esfuerzos por establecer jurisdicciones legítimas que cumplan los requisitos de la Lucha contra el Blanqueo de Capitales (AML, por sus siglas en inglés) proporcionan pocas medidas en la práctica para contrarrestar y limitar las oportunidades de blanqueo de capitales en otras jurisdicciones.

Palabras clave: Lucha contra los delitos económicos; Activos virtuales; Lucha internacional contra las criptomonedas; Circulación ilegal; Esquemas de blanqueo de dinero.

Clasificación JEL: B17, F02, F38.

Recibido: 07 de Mayo de 2021
Aceptado: 02 de Junio de 2021
1. Introduction

Law enforcement information systems are developing at a slower pace than innovative technologies, in particular in the field of payment systems development (Barone and Masiandaro, 2019), which are related to the circulation of cryptocurrency. This makes it difficult to investigate economic crimes and money laundering schemes using cryptocurrency. The cross-border nature of virtual currency transactions and the use of anonymity technologies exacerbate difficulties in investigating economic crimes (Kethineni and Cao, 2020; Burova et al., 2020). While the ecosystem of virtual currency circulation is developing dynamically, the legal system cannot be applied to its effective regulation (Cumming et al., 2019). At the same time, interest in the potential of blockchain technologies as the basis for cryptocurrency circulation is growing among both governments and cybercriminals (Oxford Analytica, 2017).

The main motive for economic crimes using cryptocurrency is convenience, financial gain for the company, personal purposes of use (Nolasco Braaten and Vaughn, 2019). Since the beginning of 2008, the role of cryptocurrency in money laundering has been growing, in particular due to dynamic innovations in payment systems (Barone and Masiandaro, 2019; Zelisko et al., 2018). It provides a reduction in time and a wider scale of criminal activity (Kamps and Kleinberg, 2018; Burova and Kabakov, 2020). Bitcoin as the most common virtual currency can provide users with laundering of 76 billion dollars annually due to illegal activities (46% of bitcoin transactions) (Barone and Masiandaro, 2019). All mentioned above trends in the growth of economic crimes are related to the circulation of virtual currencies; the purpose of the article is to study the effects of international cooperation in the investigation of economic crimes related to the circulation of cryptocurrencies. Cryptocurrency is a convertible decentralized virtual currency based on cryptographic operations (Brenig and Müller, 2015; Vasylieva et al., 2018). “Cryptocurrencies are private supplies of payment means that are produced and distributed using a decentralized, peer-to-peer transfer system, which is known as the blockchain technology (or distributed ledger technology, DLT)” (Huberman et al., 2017; Abadi and Brunnermeier 2018; Casey et al. 2018). Decentralization and anonymity are the basic principles of cryptocurrency circulation (Dyntu and Dykyi, 2018; Khamzin et al., 2016).

2. Literature Review

The scientific literature considers schemes of money laundering through the mechanisms of cryptographic operations such as investing, new instruments and methods of payment, substitutes for state currencies. Nolasco Braaten and Vaughn (2019) identified the several mechanisms of criminal activity: 1) the creation of operational front companies; 2) building relationships with criminals; 3) revaluation of the value of cryptocurrencies by criminals to encourage investment; 4) violation of fiduciary duties through misappropriation of company profits; 5) conducting transactions anonymously in the network. Barone and Masiandaro (2019) also provides a credit mechanism for money laundering through initial coin offering (ICO), which is a financing instrument. Bloomberg (2017) reported the four major forms of cryptocurrency-related crimes: money laundering, contraband transactions, tax evasion and extortion.

The lack of legal status and basis of cryptocurrencies causes difficulties in the investigation of criminal offenses associated with this tool of money laundering (identification, the fact of the crime) (Nahorniak et al., 2016; Dyntu and Dykyi, 2018). The European Union (EU) is actively discussing the need to regulate cryptocurrency as a potential type of financial instrument for money laundering. Kamps and Kleinberg (2018) note the lack of state regulation of the cryptocurrency market and the detection of potential criminal activity is possible through abnormal trading data on exchanges, which allows detecting signals of the real situation of money laundering. Stroukal (2016) proves the active intervention of governments in the functioning of the cryptocurrency market. The government must ensure the functioning of a secure financial system by regulating the requirements of circulation and cooperation at various levels (Spithoven, 2019; Haydanka, 2019). At the same time, regulation of cryptocurrency requires adjustment of monetary, trade and state security policy, in particular in
cyberspace (Nath, 2020). However, there is still not only a common understanding of cryptocurrency, but also a single approach to taxation policy and regulation of their circulation (Solodan, 2019; Buribayev et al., 2015). Thus, regulation of cryptocurrency circulation at the state level is insufficient to prevent economic crimes related to virtual currencies (Dumchikov et al., 2020; Atabekova and Radic, 2020). International cooperation is a potential way to address the threats of criminal activity in the study area.

At the Group of Twenty (G20) meeting in 2018, the European Union recommended that its member states should develop rules for the circulation of cryptocurrencies, noting the future growing interest in virtual assets. The main challenge is for governments was to support the fight against tax fraud, money laundering and other crimes and the dynamic development of a legal framework for the circulation of decentralized cryptocurrencies that can ensure security, confidentiality and anonymity. For example, Thailand has developed a state-sponsored cryptocurrency to prevent money laundering and other criminal activities related to decentralized cryptocurrencies (Emmanuel, 2018; Abu and Karim, 2021; Haydanka, 2018). The policy of curbing the circulation of cryptocurrency leads to a reduction in the level of profitability of virtual assets for criminal organizations.

3. Materials and Methods

In the scientific literature, there are three groups of countries, which pursue different policies for the regulation of cryptocurrencies: 1) countries with an absolute ban; 2) countries with no specially designed regulatory policy; 3) countries that regulate virtual currencies as a national currency. The first group of countries includes South Korea, China, Thailand and Russia, which ban or impose strict restrictions on virtual currencies. In 2018, South Korean regulators planned to close all virtual currency exchanges and ban cryptocurrency trading, use anonymous bank accounts, but they decided to abandon this plan. The Chinese central bank has rejected the status of legal tender for bitcoin (BTC) (Riley and Dayu, 2013; Apakhayev et al., 2018). In September 2017, the Chinese government suspended all virtual currency exchange operations and banned fundraising through the initial offering of cryptocurrencies. In July 2013, the Bank of Thailand ruled that BTC was illegal. Russia has pursued a moderate policy on virtual currencies; however, in 2019 it planned to ban completely the BTC.

The second group of countries includes countries without specific regulatory policies: 27 countries, including Alderney, Argentina, Belgium, Canada, Chile, Croatia, Cyprus, Denmark, Estonia, France, Greece, Hong Kong, India, Indonesia, Ireland, Italy, Japan, Malaysia, Malta, the Netherlands, New Zealand, Nicaragua, Poland, Portugal, Singapore, Taiwan and Turkey. The European Union also has no specific provisions on the circulation of virtual currencies. Despite the lack of regulations, virtual currencies can be regulated as an object of taxation or a commodity. In 2017, the Australian government declared BTC and other cryptocurrencies with similar characteristics to be assets subject to capital gains (Government of Australia, 2017; Boeva-Omelechko et al., 2019). Similarly, the Canadian Review Agency requires BTC users to pay tax on any transactions involving the circulation of digital currency. In addition, the Financial Transactions and Reports Analysis Center of Canada has sent messages to companies operating on BTC exchanges stating that they are not covered by the Law on Proceeds from Crime and Terrorist Financing and its provisions (Library of Congress, 2014; Onishchenko and Suniehin, 2018). The Hong Kong Secretary for Financial Services and the Treasury has stated that there is no need to develop rules for the circulation of BTC (Weese, 2018; Shah et al., 2021), as Organized and Serious Crimes Ordinance can be applied to any criminal activity related to BTC, such as money laundering or fraud. Similarly, India applies the Foreign Exchange Management Act to counter virtual currency traders (Library of Congress, 2014; Oxford Analytica, 2017).

The tax regime of virtual currencies has been introduced in the United Kingdom (UK), Spain, Finland, Slovenia and Israel, which consider virtual currencies as taxable. In the UK, BTC is classified as a single-purpose voucher and the sale of BTC is subject to value added tax. The Finnish tax authorities have issued specific guidelines on the taxation of virtual currencies (Library of Congress, 2014). Brazil and Germany belong to the third group of countries that regulate cryptocurrency as a real currency (Tu
and Meredith, 2015; Serebrennikova et al., 2020). For example, in Germany, BTC is considered a currency substitute and is classified as a foreign currency in the German Banking Act, although cryptocurrency is not considered a form of legal tender (Library of Congress, 2014). In Brazil, BTC is classified as electronic currency under Law No. 12.865 (Library of Congress, 2014). In October 2018, the Brazilian Supreme Court ruled in favor of Itau for closing Brazil’s largest BTC account, arguing that banks “have the right to close any cryptocurrency-related accounts without any justification” (Kethineni and Cao, 2020; Voyarenko et al., 2021; Bulatov et al., 2020). Thus, different countries have different models of regulating the circulation of virtual currencies. Regulatory policies are often limited to traditional regulations that identify a cryptocurrency as an object of taxation and a quoted financial instrument. Such restrictions indicate a lack of joint action by governments in international cooperation on possible economic crimes related to the circulation of cryptocurrencies.

This study is based on a qualitative methodology of content analysis of reports, recommendations and standards of the Financial Action Task Force (FATF) for 2012-2020, as a leading international organization for the prevention and development of policies to regulate economic crimes related to the circulation of cryptocurrencies. The FATF Anti-Money Laundering Development Team is an intergovernmental organization that officially includes thirty-five Member States and two regional organizations. About 170 countries work with the FATF as associate members or observer members, members of regional bodies such as the FATF, which provide international cooperation within the requirements and standards of AML. The following FATF reports, guidelines and standards were used for content analysis: 1) 12-month Review Virtual Assets and VASPs (Virtual Asset Service Providers), FATF, Paris, France; 2) FATF Report to the G20, FATF, France; 3) International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation; 4) Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF, Paris.

4. Results and Discussion

The main consequences of cryptocurrency trafficking in the context of combating global economic crimes are the capabilities of blockchain technologies. Second, the FATF's risk-based approach, used globally to coordinate governments' efforts to prevent economic crime, provides an effective balance between existing threats and cryptocurrency opportunities. The development of FATF free, decentralized management networks can be seen as an innovative and more effective way of combating criminal activity than traditional centralized forms of coercion in an era of rapid and unpredictable technological change.

The network approach to controlling the movement of virtual assets has been actively implemented in 34 countries out of 54 that follow FATF standards and global recommendations for 2019-2020 (Financial Action Task Force, 2020c; Oxford Analytica, 2017). Progress in this area is being achieved in particular through the integration of technologies that make it possible to implement a 'travel rule' for 'virtual asset service provider' (VASPs), which strengthens public-private cooperation in combating economic crime (Virtual assets is the term of the FATF uses to refer to crypto-assets and other digital assets” (Financial Action Task Force, 2020c). Public-private partnership primarily involves monitoring and control over the movement of virtual assets. At the same time, FATF standards need to be revised due to the problems of implementing the ‘travel rule’, anonymous one-time transactions. The FATF is expanding its international cooperation agenda, but the priority of other revenue laundering mechanisms has a lagging effect in policy development and implementation worldwide. At the same time, the space of virtual assets is evolving and include a number of products, business models, transactions of virtual assets due to new technologies, which enhances such a lagged effect in international cooperation (Abdramanova et al., 2019; Onishchenko and Bobrovnyk, 2019).

The FATF provides the development of a cybercrime repository as a component of the Global Cybercrime Program and a central repository of cybercrime legislation, international cooperation to facilitate ongoing assessment of the needs and capabilities of criminal justice, the provision and coordination of technical assistance to governments. Despite the limited practice of using
International cooperation in the investigation of economic crimes related to cryptocurrency circulation

cryptocurrencies in money laundering compared to traditional methods, the FATF calls on governments to implement international recommendations to combat the illicit trafficking of virtual assets. This is due to illegal transactions and financial flows, which must be included in the circulation within the legal financial system. In addition, there are new ways to conduct, verify transactions and cryptocurrency transactions outside political borders. In this case, the question of the illusory fairness of the government’s activities in the field of combating money laundering arises.

Governments in different countries concerned about cryptocurrency trafficking due to limited regulation. Considered experience of the absence of regulatory acts of cryptocurrency circulation and taxation of virtual assets on the principle of traditional assets shows the absence of concern about illegal activities and possible economic crimes in this area (Bulatov et al., 2019). At the same time, decentralized and quasi-autonomous virtual assets could potentially threaten years of global anti-money laundering efforts. National regulators use existing and new measures to combat economic crimes with cryptocurrencies. The most aggressive country in combating money laundering is the United States, where current regulations are an example for different countries in combating economic crimes. In the United States, there are law enforcement practices and cases of lawsuits related to the circulation of cryptocurrency (Abdulla, 2020; Piddubnyi et al., 2019).

For example, the American Department of Justice (DoJ) used the Money Laundering Control Act of 1986 in violation of the prosecution of Bitinstant CEO (Chief Executive Officer) Charlie Schrem, who pleaded guilty to aiding and abetting the transfer of unlicensed virtual money in 2014. In 2015, the US Financial Crimes Enforcement Network (FinCEN) of the US Treasury Department applied the Bank Secrecy Act of 1970 in its first-ever civil lawsuit against a cryptocurrency exchange. San Francisco-based Ripple Labs was fined $700,000 for failing to implement effective anti-money laundering programs within two years of the implementation of the 2013 FinCEN guidelines. A similar example is the case of the Department of Justice against the management of the cryptocurrency exchange Coin.mx, which used a credit union to launder proceeds from ransom attacks against large financial institutions such as JP Morgan Chase, as well as the media, the Dow Jones.

Outside the United States, various formal efforts have been made to reduce the use of cryptocurrencies. Altcoins are banned in several countries, including Bangladesh, Bolivia and Ecuador, while their legal status remains in question in other countries, such as Russia and Thailand. In 2013 and 2014, the People’s Bank of China and the State Bank of Vietnam, respectively, issued laws prohibiting financial services companies and their employees from processing and conducting any cryptocurrency transactions. The Central Bank of Iceland in its decision from 2014 stated that the purchase of cryptocurrencies is a violation of the Law on Foreign Currency. The Central Bank of Indonesia has also stated that Bitcoin and other virtual currencies are not currency or legal payments. While the European Central Bank warned that regional authorities are trying not to encourage the use of digital currencies, the European Banking Authority has recommended that regional authorities prevent lending to organizations operating cryptocurrencies. European countries, such as the Netherlands, have filed several lawsuits against people suspected of money laundering through cryptocurrencies (Figure 1).

Such bans and restrictions on the use of virtual currencies have been criticized. For example, lawyer Singh (2015) argues that rigid approaches are ineffective in preventing economic crimes involving the circulation of cryptocurrencies and other clandestine transactions by restricting the more legal use of virtual assets. However, the "despotic" categorization is widely used in research. Singh implicitly refers to tactics that could undermine the benefits of cryptocurrencies like requirements for key centralized points in the cryptocurrency ecosystem, such as exchanges, for transactions with other operators and users that meet anti-money laundering (AML) requirements. The main problem in the pursuit of exchanges is that their location is easy to identify, however, such operators may relocate their own jurisdictions with weaker anti-money laundering requirements and countermeasures. AML’s high standards and requirements may prompt CC operators to exercise regulatory arbitrage when relocating to less stringent jurisdictions and darker areas of the "shadow financial system" where weak
AML rules apply. Thus, the decentralized nature of digital currency circulation schemes means that there are difficulties in imposing restrictions on cryptocurrency transactions.

Figure 1 Scheme of international cooperation in the investigation of economic crimes related to the circulation of cryptocurrency

There is a "race" in the international community for leadership in combating economic crime. For example, New York State and other jurisdictions have tried to stand out as legitimate centers to combat cryptocurrency trafficking. Since 2014, Singapore has made it mandatory to exchange virtual currency to verify the identity of customers and report suspicious transactions to the suspicious transaction-reporting department. English Channel island of Alderney has created a cluster of AML-compatible cryptocurrency services to position itself as a leading international cryptocurrency transaction center. For the title of Bitcoin Isle competes the neighboring island of Isle of Man, which amended the basic legislation to combat money laundering, including the circulation of cryptocurrencies, and developed similar innovative schemes for regulating and financing virtual assets.

However, such efforts to establish legitimate jurisdictions that meet AML requirements do little to counteract and limit the spread of money laundering in other jurisdictions. National authorities also seek to impose AML's own requirements on transactions with bank accounts outside their jurisdiction. In May 2013, the US Department of Homeland Security issued an arrest warrant for a US firm that translated the once-dominant Tokyo cryptocurrency exchange Mt. Gox, who complied with the requirements and received a license to service the money business just a few months before filing for bankruptcy protection after the devastating break-in. However, apart from this well-known case and the assumptions of scholars about the leadership of American policy to combat economic crimes in this area, the extraterritorial application of US laws goes so far as to ensure legitimate global rather than unilateral AML standards for cryptocurrencies. This means that governments must choose to regulate using US jurisdictions and U.S. law or impose bans to mitigate the use of cryptocurrencies to interact with countries globally.

Limited regulation and governance at the sectoral and national levels require a coordinated global effort to reduce the potential illicit use of cryptocurrencies for money laundering without limiting their more useful functions. Given the peculiarities of the circulation of digital currencies, which are not limited to national jurisdictions, a coordinated approach can be effective in regulating and investigating economic crimes at the global level. It is not possible to effectively regulate cryptocurrency at the international level without the mutual cooperation and assistance between states that allow its use. Such global problems of collective action are certainly not new, as in the past they have negatively
affected the management of a number of new technologies. International organizations have sought to ensure the implementation of standards, which coordinate national laws and regulations in the field of AML relating to the circulation of virtual assets. In 2014, the United Nations Office on Drugs and Crime (UNODC) issued a detailed guide to detecting and seizing cryptocurrencies used in money laundering, and together with the Organization for Security and Cooperation in Europe (OSCE) is training officials in investigating crimes related with money laundering through cryptocurrencies. In 2015, the International Organization of Securities Commissioners (IOSCO) established the Blockchain working group, while the Commonwealth convened a ten-member working group to regulate the circulation of virtual currencies, while trying to coordinate approaches to AML. Similarly, Interpol and Europol have established a joint partnership.

The FATF has developed 40 recommendations since its inception in 1989, which are recognized as global AML standards (Financial Action Task Force, 2012). Since 2003, the FATF has used a risk-based approach to develop measures to prevent and detect economic crimes. In contrast to the more traditional “rule-based approach”, the “risk-based approach” gives national regulators considerable leeway in taking action to achieve the common goal of reducing money laundering. This more flexible and decentralized approach, combined with the organization of forums for mutual learning and evaluation, demonstrates the use of a networked and experimental approach in modern global economic crime management.

The FATF recommendations and the “risk-based approach” are used to regulate the circulation of cryptocurrencies and virtual assets. Management of the circulation of virtual currencies is characterized by a lag effect: five years after the emergence of bitcoins, a general assessment of payment systems over the Internet has been developed. A study of the prospects of FATF cryptocurrencies has shown the legitimate potential of their circulation in the financial system. At the same time, the complexity and segmentation of the technical infrastructure underlying cryptocurrencies due to the lack of control over organizations and jurisdictions cause difficulties in regulating the circulation of virtual assets. The 2014 FATF report noted the inaccessibility of the cryptocurrency ecosystem in the digital environment for any country and government, leading to uncertainty of responsibility for compliance with AML requirements, inability to monitor and control, law enforcement. These challenges have led to the development of FATF recommendations for the management of the cryptocurrency ecosystem. In 2015, the FATF developed guidelines to help identify threats to money laundering, which are related to cryptocurrency circulation, and to develop standards, regulations and guidelines for national authorities to support global efforts to combat economic crime (Financial Action Task Force, 2012).

The FATF invites national authorities to establish coordination mechanisms for the active exchange of information in ways that contribute to a deeper understanding of the risks of money laundering in the cryptocurrency ecosystem. The risk-based approach assumes that national authorities target specific “nodes” that are likely to be in revenue laundering jurisdictions that intersect with the regulated financial system in paper currency. The FATF proposes that countries regulate the institutions most at risk of participating in money laundering because they send, receive, and store certificates, not individuals. The 2015 FATF guidelines state that exchanges and circulation should be aimed at enhanced monitoring. Nevertheless, the FATF calls for comprehensive customer due diligence when establishing business relationships or when conducting random transactions using reliable, independent source documents, data or information. The forty-fourth paragraph of the FATF Recommendation provides for the exchange of cryptocurrencies using user credentials using national identification numbers or Internet Protocol addresses, as well as conducting online customer searches to verify activity information that matches the customer’s transaction profile.

In the presence of violations on cryptocurrency exchanges, the FATF offers the authorities to take comprehensive measures to combat and prevent criminal activity. For example, the government may impose a direct ban or a series of effective, proportionate and dissuasive sanctions (criminal, civil or administrative). At the same time, such measures should take into account the impact of the ban on the local and global level of money laundering / terrorist financing. In other words, the FATF is urging
national authorities to recognize that a total ban on cryptocurrencies may further exacerbate regulatory arbitrage and cross-border differences in the governance of exchanges, which act as key nodes in financial transactions with cryptocurrencies. The value of virtual assets involved in most identified cases of income laundering is still compared relatively less to cases, which use more traditional financial services and products. However, this does not preclude the need for continuous monitoring of any potential threats and risks. In most cases, only one type of virtual asset was used. In cases where criminals did use more than one type of virtual asset, such use was made mainly for the distribution of illicit proceeds.

While cases filed by jurisdictions typically involved money laundering or predicate offenses, criminals did use virtual assets to evade financial sanctions and to raise funds to support terrorism (Financial Action Task Force, 2012). In general, the use of virtual assets as a method of division by level is the most prominent typology. This typology is observed due to the simplicity of rapid transfer and distribution of income. Professional machine learning networks use virtual assets as a means of laundering illicit proceeds. The main types of economic crimes related to virtual assets, the FATF includes money laundering, sale of controlled substances and other illegal items (including firearms), fraud, tax evasion, evasion of sanctions, computer crimes (e.g., cyber-attacks, leading to theft), child exploitation, human trafficking. Among them, the most common are drug-related crimes and fraud (e.g., investment fraud, blackmail and extortion) (Financial Action Task Force, 2020d). Jurisdictions that have implemented the regime of counteraction to economic crimes related to virtual assets,

The results of the study prove the convenience of cryptocurrency as a tool for laundering income due to the relative autonomy of the currency owner, the lack of requirements for providing personal information about the user and his location (Dyntu and Dykyi, 2018). As a result, law enforcement agencies are less likely to track criminal activity. The release of cryptocurrency transactions from the control of governments due to the lack of need for their confirmation by third parties is the main reason for failures in the investigation of such crimes (Dyntu and Dykyi, 2018). In addition, the lack of a policy to regulate the circulation of cryptocurrencies and non-compliance with FATF international recommendations entails additional risks of economic crime. The FATF uses the risk-based approach and provides a balance of opportunities and threats of virtual currency circulation (Campbell-Verduyn, 2018). This comprehensive approach aims to organize regulatory measures to enable the legal circulation of cryptocurrencies while reducing the risk of economic crimes. Governments that stay away from international action to implement FATF standards will increase the risks of relocating illegal jurisdictions to their own country.

In response, the identified challenges in the fight against economic crime Zhang and Xu (2019) offer a decentralized blockchain network for the exchange of global information flows at low transaction costs for services to ensure the effectiveness of international cooperation. Such a conceptual network provides tracking and early warning, identification of cross-border economic crimes, capital flows and information. “Distributed ledger technology, also known as the blockchain, is gaining traction globally. Blockchain offers a secure validation mechanism and decentralized mass collaboration” (Cumming et al., 2019). Nath (2020) argues for the need to develop an international control policy for independent governments in the context of the use of virtual currencies: “There is a need for comprehensive global Crypto regulations of controlling the Cryptocurrency crimes”. S. De Vido (2014) proposes network regulation of cross-border crime based on standards and recommendations that are integrated at the state level. The FATF uses a networked approach, disseminating its own recommendations through a network of regional bodies in more than 200 jurisdictions worldwide (Financial Action Task Force, 2020a). In June 2019, the FATF (2020a) adopted the first standards for reducing the risk of money laundering associated with virtual assets – Interpretive Note to Recommendation 15 (INR.15). Among the main risks is the mass integration of virtual assets. “However, as yet, the majority of countries have not taken any action. These gaps in the global regulatory system have created significant loopholes for criminals and terrorists to abuse” (FATF).
5. Conclusion

The illicit circulation of cryptocurrency in the context of combating global economic crimes has necessitated the use of a risk-oriented approach of the international community at the global level, coordination of governments’ efforts to prevent economic crimes. As a result, a network of organizations has been formed that provides an effective balance between existing threats and opportunities for cryptocurrency circulation. The development of FATF free and decentralized management networks at the global level can be seen as an innovative and more effective way of combating criminal activity than traditional centralized forms of coercion in an era of rapid and unpredictable technological change.

The considered experience of the absence of regulatory acts of cryptocurrency circulation and taxation of virtual assets on the principle of traditional assets shows the absence of concern about illegal activities and possible economic crimes in this area. At the same time, decentralized and quasi-autonomous virtual assets could potentially threaten years of global anti-money laundering efforts. National regulators use existing and new measures to combat economic crimes with cryptocurrencies. The most aggressive country in combating money laundering is the United States, where current regulations are an example for various countries in combating economic crime. Outside the United States, various formal efforts have been made to reduce the use of cryptocurrencies. Such bans and restrictions on the use of virtual currencies have been criticized for the potential ineffectiveness of rigid approaches of preventing economic crimes, involving cryptocurrencies and other clandestine transactions, by restricting the more legal use of virtual assets. There is a "race" in the international community for leadership in combating economic crime. National authorities also seek to impose AML’s own requirements on transactions with bank accounts outside their jurisdiction. However, such efforts to establish legitimate jurisdictions that meet the requirements of the AML provide few measures in practice to counter and limit the opportunities for money laundering in other jurisdictions.

References


