Conference Paper

Regulating cryptocurrencies: new challenges to economic security and problems created by individuals involved in the schemes of laundering cryptocurrencies-generated profits

Kadyrov R. E. and Prokhorov I. V.

National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Kashirskoe shosse 31, Moscow, 115409, Russia

Corresponding Author:
Kadyrov R. E.
kra_@inbox.ru

Received: 11 December 2017
Accepted: 20 January 2018
Published: 13 February 2018

Publishing services provided by Knowledge E

Selection and Peer-review under the responsibility of the FinTech and RegTech: Possibilities, Threats and Risks of Financial Technologies Conference Committee.

Abstract

This article explores the mechanisms of the organization and operation of virtual payment systems. The appearance of such payment systems is associated with the development of Internet technologies in the field of mutual settlements for goods (works and services). The study aims at analyzing the classification, types of emission of cryptocurrencies, the mechanism of functioning of cryptocurrency systems; evaluating their impact on the monetary system and the involvement of individuals in the laundering of illegal incomes using cryptocurrencies; estimating prospects for the development of virtual payment systems in Russia and abroad, and defining mechanisms to counteract illegal activities. As a result, the current status of virtual cryptocurrency systems is estimated, their distinctive features and advantages are considered. The study also identifies drawbacks in the use of cryptocurrency with the involvement of individuals in the system of non-cash settlements. The results of the analysis of cryptocurrency systems can be useful for the improvement of the state monetary policy.

Keywords: electronic money, bitcoin, cryptocurrency, blockchain, money laundering.

1. Introduction

A brief history of blockchain technology. Key stages and basic terms. Theoretical approaches to the study of the legalization of illegal cryptocurrencies-generated profits in the financial and banking system

Methodology. Classification, forms and types of crypto-currencies have been studied. The use of methods of comparative analysis, logical cognition and methods based

How to cite this article: Kadyrov R. E. and Prokhorov I. V., (2018), “Regulating cryptocurrencies: new challenges to economic security and problems created by individuals involved in the schemes of laundering cryptocurrencies-generated profits” in *III Network AML/CFT Institute International Scientific and Research Conference “FinTech and RegTech: Possibilities, Threats and Risks of Financial Technologies”*, KnE Social Sciences, pages 383–393. DOI 10.18502/kss.v3i2.1568

on the principles of reasoning, made it possible to identify the key problems in the development of virtual payment systems based on modern IT technologies.

The invention of cryptocurrencies is a new type of E-money, which was made possible due to the development of the Internet, innovative technologies and modern encryption tools based on blockchain technology. Actual generation of virtual money (issuing or emission of cryptocurrencies) requires a complicated technology and processes.

All crypto-currencies are generated by using the so-called mining process. Typically, the miners (creators of a cryptocurrency in question) use super-powerful computers or servers with special video cards and chips. Crypto-currencies are called ”electronic gold”.

By 2017 over 1500 cryptocurrencies have been created. The most widely used is Bitcoin, but there are hundreds of alt-coins like Litecoin, Peercoin, Namecoin, Worldcoin, Hobonickel, Gridcoin, Fireflycoin, Zeuscoin, etc. [1]

As defined by FATF (Financial Action Task Force), virtual currency is a measure of value that can be traded digitally, but does not have a legal tender status in any jurisdiction. However, crypto currency can be exchanged for fiat money (dollar, euro, ruble) and vice versa. These transactions take place on virtual exchanges.

Many governments believe that Bitcoin and other crypto-currencies must be regulated in the same manner as the fiat money, because there is a risk that bitcoin and alt-coins are used or will be used to launder illegal profits and for other illegal financial transactions. Some countries (Germany, USA) already regulate cryptocurrencies, but because it is very difficult to build an efficient regulatory system, many countries (Thailand, Iceland, Russia etc) completely or partially prohibit the use of crypto-currency. [2]

Consequently, both governments and individuals need regulatory and monitoring structures for anonymous payment systems. The main problem of modern blockchain-based payment systems is the emergence of new schemes for the legalization of illegal profits, despite liberalization of the movement of funds.

This chart clearly shows a trend towards an increase in the outflow of capital from the national financial systems. In 2013, capital outflows exceeded 60 billion USD. In 2014, it reached US$ 150 million – an increase of 2.5 times. The outflow of capital from the Russian Federation is 30-40%.

This trend demonstrates – loud and clear - the need for systems that will identify money laundering risks and threats and protect our financial and economic systems.

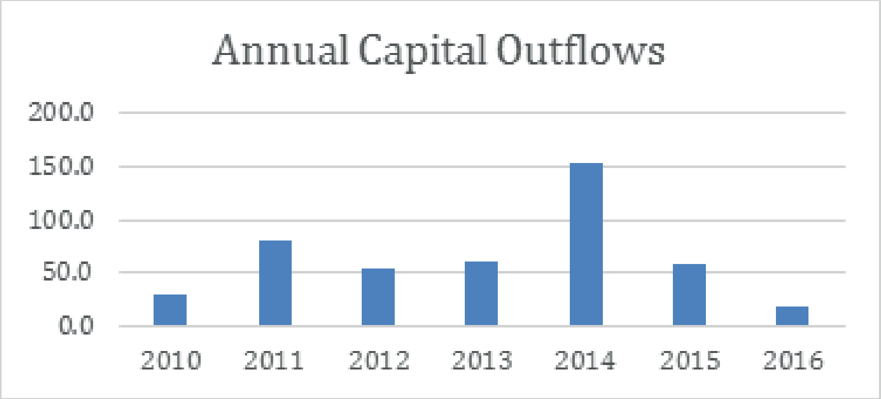


Figure 1: Annual Capital Outflows.

In 2008 Satoshi Nakamoto published the Internet article entitled ”Bitcoin: A Peer-to-Peer Electronic Cash System” [3] where he described methods for creating a peer-to-peer payment system that allows its members to make electronic transactions without any regulatory oversight. The author proved that this objective could be achieved by using a digital signature. However, one must take into account that the digital signature system requires an authorized individual, which essentially doubles its costs and deprives the system of its advantages.

2. Main part

1) Analyzing the basic conditions for emergence of risk of the banking system participation and individuals in the process of laundering of illegal profits

As we have already noted, the crypto-currency system is an innovative equivalent of a global payment system based on a public collective register of transactions. Some even believe that crypto currency is capable of replacing the existing financial systems. Why? Because unlike the fiat money issued (emitted) by central banks, Bitcoin and altcoins are based on the trust of participants in the payment system.

Based on a comprehensive analysis of cryptocurrencies and their circulation, we can identify their key features as follows:

- Anonymity of transactions;
- Weak control over transfers;
- Decentralized emission/issuing process;
- Absence of any regulator [4]

The main source of risks in using e-money is that it is practically impossible to control cryptocurrency transactions. Third-party control is practically impossible because transactions are made electronically (via Internet) directly between parties and are encrypted using modern encryption tools [1].

On the one hand, anonymity of payments and emission/issuing process is attractive to users seeking tax evasion tools (e.g., from shadow economy). On the other hand, exactly this anonymity significantly increases the risks of financial losses for currency owners due to the bankruptcy of cryptocurrency stock exchanges or hacking.

The fundamental principle of anonymity, on which all cryptocurrencies are based, does not make them attractive to the government authorities because the anonymity of payments is hampering the regulation of the national economy by financial authorities of the economy and does not comply with the internationally accepted standards of disclosing information by participants in financial markets [1]

Recently, cryptocurrency-based lending has been introduced. An individual requests the necessary loan amount. In response he/she receives offers that include both the loan amount and the interest rate. Thus, parties enter in loan contracts bypassing banks and other lending institutions. [5]

Cryptocurrencies are either centralized (i.e. have a single issuer) or decentralized (i.e., have multiple issuers).

By the end of 2008, the decentralized Bitcoin crypto currency had been created. Bitcoin made it possible to build a multiple-issuer cryptocurrency system without compromising the trust of the participants. A common feature of new payment methods is the absence of a direct personal contact between parties, - and of the customer identification. According to FATF Recommendation 8, the absence of such contact represents a "specific" risk of money laundering because it allows criminals to act anonymously.

Moreover, obviously, it creates new attractive opportunities for organized crime that needs money-laundering schemes for legalizing enormous amounts of cash generated by their illegal activities. According to estimates by IMF and World Bank, the total amount of laundered funds in the world reaches 3-5% of world GDP, (i.e. US$ 2-3 trillion) [7]

Such enormous amounts of laundered proceeds from criminal activities significantly decrease the efficiency of social and economic reforms initiated by the governments and create obstacles to attractive private investments into national economies. It must also be taken into account that organized crime always tries to expand its operations, often resorting to violence. [8]

2) International regulatory practices in combating money laundering operations

Understanding the consequences of the uncontrolled growth of the international money laundering activities forced the global community to develop and implement efficient measures for minimizing (and ideally, eliminating altogether) these highly dangerous endeavors.

More specifically, the international community created an organization called FATF - Financial Action Task Force on Money Laundering. FATF develops and implements international recommendations and standards aimed at preventing, curtailing (and, ideally, eliminating) money laundering activities.

International cooperation in combatting money laundering is based on bilateral and multilateral treaties and is implemented as joint activities under the auspices of international organizations. [7].

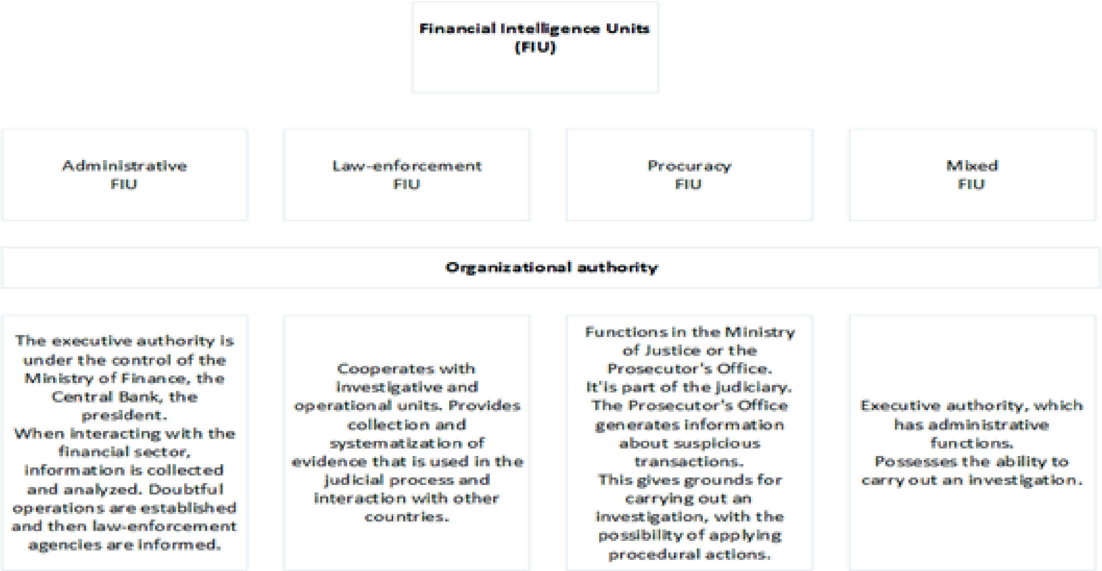
Each of the 189 nations (as of 19 September 2017) that ratified the 2000 Palermo Convention (The United Nations Convention against Transnational Organized Crime - UNTOC) committed themselves to taking a series of measures against transnational organized crime, including the creation of domestic criminal offences (participation in an organized criminal group, money laundering, corruption and obstruction of justice); the adoption of new and sweeping frameworks for extradition, mutual legal assistance and law enforcement cooperation; and the promotion of training and technical assistance for building or upgrading the necessary capacity of national authorities. Most (156) of these nations established financial intelligence units which became members of another international organization - the Egmont Group of Financial Intelligence Units. Egmont Group also issues recommendations and guidelines which must be adhered to by each member agency.

Figure 2 presents four different categories (by core competencies and authority) of specialized government entities – financial intelligence units (FIU). The key element of an FIU is the process of identification of parties conducting financial transactions.

3) Examples of crypto-currency fraud in the Russian Federation.

4) Investigation of the crypto-currency risks of the financial and banking sector in the Russian Federation. Examples of crypto-currency fraud and crime

The existing prerequisites for rapidly developing progress in the field of technology and financial products have created favorable conditions for increasing the risks of the banking sector and individuals, as well as the emergence of such a form of investment attraction, as ICO. Over the past 10 years for various violations in the field of combating money laundering by the Bank of Russia for repeated violations of AML / CFT legislation and regulations from 2003 to 2011, more than 1500 fines were imposed on credit institutions and 137 licenses for banking operations were withdrawn. [12]



Financial Intelligence Units (FIU)

Administrative FIU	Law-enforcement FIU	Procuracy FIU	Mixed FIU
Organizational authority			
The executive authority is under the control of the Ministry of Finance, the Central Bank, the president. When interacting with the financial sector, information is collected and analyzed. Doubtful operations are established and then law-enforcement agencies are informed.	Cooperates with investigative and operational units. Provides collection and systematization of evidence that is used in the judicial process and interaction with other countries.	Functions in the Ministry of Justice or the Prosecutor's Office. It'is part of the judiciary. The Prosecutor's Office generates information about suspicious transactions. This gives grounds for carrying out an investigation, with the possibility of applying procedural actions.	Executive authority, which has administrative functions. Possesses the ability to carry out an investigation.

Figure 2: Types of Financial Intelligence Units.

This fact shows an increasing level of threats capable of inflicting potential damage or harm to effective economic activity. The threat in this context is understood as the conscious intention of participants in illegal schemes or an individual to use the opportunities of banking structures to implement illegal schemes in order to obtain profit and conceal the origin of money.

The most vulnerable to potential threats are credit institutions. Because the credit sector becomes an object of interest to organized crime for the purpose of laundering illegal income. On the one hand, criminal structures invest money in separate enterprises and control them. And on the other hand, banks, when necessary to repay debts on loans, turn to the criminal sector. [10]

The most rapidly developing form of financial and investment activity with very high risks was in the last 2017 ICO (”initial offering of coins, initial coin placement”). In fact, ICO is one of the forms of collective financing, crowdfinding. The peculiarity is that ICO is tightly connected with the technology of blocking and cryptocurrencies. However, the issuance of cryptocurrency is carried out outside mining. It is enough for the issuer to convince investors of the effectiveness of their own project and to provide the investor with a guarantee for the repurchase of its cryptocurrency. So, in 2017 the ”Kolionovo” farm was financed with the help of the ICO and 401 Bitcoin was earned [13].

At the moment, ICO in the Russian Federation does not have state regulation. In order to counteract the risks and potential threats to the involvement of banks and individuals in laundering illegal income system is a financial monitoring and state regulation.

According to "Kaspersky Lab", the number of cyberattacks on holders of cryptocurrency in Russia has increased dramatically. In some of these attacks, cyber-criminals used the CryptoShuffler to steal 23 bitcoins (at the time valued at about $150,000) by changing the address of the user's wallet during the transaction. [9]

Another type of fraud is browser mining: more and more sites are adding miners to JavaScript files. Mining occurs during the browsing of the site in question. Criminals use asm.js for mining (instead of the usual JavaScript used to implement hash algorithms). The names of frequently used scripts are as follows:

- scrypt.asm.js (Litecoin),
- cryptonight.asm.js (Monero),
- neoscrypt.asm.js (Feathercoin).

The address of the Feathercoin cryptocurrency wallet is the same for all transactions, while several different addresses are used for Monero cryptocurrency. Reducing risk is possible by either using script execution blockers or disabling JS altogether. Additional security extensions are currently being developed, e.g. NoCoin. Besides, AdBlock has released an extension/filter that does not allow the execution of malicious scripts. [10] However, experts estimate that, despite all these preventive measures, more than $ 200 million have been stolen from crypto-currency wallets this year alone. [9]

Based on the results of the study, you can draw up a list of potential risks associated with virtual currency. First of all, we should mention the improvement and further active use of various types of services and tools, allowing to ensure a high degree of anonymity, such as the service for washing "Mixer". Its essence lies in the fact that it ensures hiding the chain of operations in the chain of blocks by binding all operations to the same bitcoin address. Thus, the service sends all the blocks together, creating the impression that they are sent from a different address. Here, of note are the following services "mixers": Blockchain.info; Bitcoin Laundery; Bitlaunder; Easycoin [18].

The list of anonymizers and services can also include such tools as the network Tor (anonymous network), Dark Wallet (anonymous network service). These networks can hide the source of bitcoin operations and ensure anonymity. Special mention should be made of the service "Dark Wallet" associated with the hidden website "Silk Road". Drugs, weapons, goods and services prohibited by law were bought and sold anonymously through this site.

Among the possible risks of using crypto currency, we note:

- financing of terrorist organizations;
- penetration into information systems with unlawful purposes;
- unauthorized use of identification data;
- creation of viruses-extortionists (cryptolockers);
- drug trafficking, illegal trafficking in arms and people;
- blackmail;
- kidnapping;
- bribery of voters [1].

4) Instruments for financial monitoring and combatting illegal cryptocurrency activities in the Russian Federation

The officials of the Russian Central Bank (Bank of Russia) note that in the Russian Federation transactions with cryptocurrencies (and cryptocurrencies themselves) have no legal status. Consequently, government actions against illegal activities that involve cryptocurrencies, are regulated by the Federal Law #115-FZ dated 07.08.2001: "on Countering Legalization (Laundering) of Proceeds of Crime and Financing of Terrorism" (dubbed the "AML Law")

This law requires the development of a comprehensive system of measures for identification, evaluation and minimization of new threats originating from technological advances in the development and evolution of payment systems. [8].

Recently the ICOLab Holding and the "Rating Agency for the Evaluation of Digital Economy Projects" signed an agreement to jointly develop standards and methodologies for evaluating technology start-ups and creating professional ratings of projects and technologies that intend to raise money via ICO – Initial Coin Offering (an unregulated means by which funds are raised for a new cryptocurrency venture). [11]. These standards and ratings are necessary because cybercriminals are very interested in conducting fraudulent ICOs.

Also worth noting is the signed cooperation agreement between ICOLab Holding and the "Rating Agency for the Evaluation of Digital Economy Projects". The partners who sign the agreement plan to develop standards and methodologies for evaluating technological start-ups and creating professional ratings of projects and technologies [16], since attracting money through ICO often arouses the interest of scammers.

Suggested installation in Moscow of "cryptomats" for automated selling of digital currencies can also be considered a tool for financial monitoring of cryptocurrencies. Development of crypto currency in Russia, despite the existing risks, became possible due to the activities of Qiwi payment service, which proposed the creation of the specifically Russian crypto currency ”bitruble”. The Bank of Russia is ready to discuss the possibility of creating a new virtual payment system.

There are other factors in the Russian Federation that are creating the favorable conditions for the development and legalization of crypto-currency systems:

- Achievements of Russian cryptographers;
- Availability of a large number of competent IT professionals in the labor market
- Favorable climate for establishing large computing facilities
- Economic crisis that demands a radical reduction in operational and other expenses;
- Strained relations with the main regulators of global financial flows.

In addition to the above-mentioned mechanisms of counteraction, it is necessary to create an atmosphere of ideological intolerance for participating in schemes for the legalization of illegally obtained incomes, based on the principles of civic society [10].

3. Conclusion

Recommendations for the development of the algorithm for financial monitoring of risks of participation of financial and banking sector in money laundering schemes

This article presents the key issues in combatting money laundering schemes that involve cryptocurrencies. It also identifies and evaluates new global trends in development and evolution of cryptocurrencies and their influence on the transparency of financial flows.

The comparative analysis of various sources identified the following positive aspects of crypto-currency technologies:

- They reduce transaction costs,
- They verify authenticity and manage the reputation of the parties in the transaction,
- They ensure communication and trust between the participants of the system.

The unified digital blockchain-based platform helps professionals find customers and, under optimal and safe conditions, offers them financial and information services of high quality.

Blockchain technologies must be primarily used by the government entities, banking and innovative hi-tech sectors.

Obviously, there are different opinions regarding every aspect of cryptocurrency systems. However, the positions of digital currencies in the global economy are getting stronger because they can be successfully used for a variety of purposes.

References

[1] V. Bauer, Problems in the way of creating a unified digital platform for the digital economy, Rus. acad. of nature Sciences, 2017.

[2] D. Cochin, "Where to store data for decentralized applications on a blockbuster, 2-5-2017. [On the Internet]: https://habrahabr.ru/post/327836/.

[3] V. Pertsova, "Regulation of the Crypto-Currency: Will the State Lead the Process that Can not Be Stopped," 02 08 2017. [On the Internet]: http://www.forbes.ru/biznes/338503-regulirovanie-kriptovalyut-vozglavit-li-gosudarstvo-process-kotoryy-nelzya-ostanovit.

[4] "Import / export of capital by the private sector in 1994-2016 and January-September 2017," [On the Internet]. : https://www.cbr.ru/statistics/credit_statistics/bop/outflow.xlsx.

[5] S. Nakamoto, "System, Bitcoin: A Peer-to-Peer Electronic Cash," https://bitcoin.org/bitcoin.pdf, 24 5 2009.

[6] T.E. Nikolaeva, Modern types of money and trends in their development: monograph, Saarbrücken, LAP Lambert Academic Publishing, 2011. 108p.

[7] "Loans and microloans in bitcoins. Can I make money on this?, 8-04-2016. [On the Internet]: https://geektimes.ru/company/hashflare/blog/274028/.

[8] Ivolgina N.V., Financial Aspects of Intellectual Property Management,Intellectual Property Law. 2015. No 2. P. 33-37.

[9] "Recommendations of the FATF. International standards on combating money laundering, financing of terrorism and financing the proliferation of weapons of mass destruction, Trans. from English, Veche, 2012. - 176 p., "[OntheInternet]: http://www.fedsfm.ru/content/files/documents/fatf/%D1%80%D0%B5%D0%BA%D0%BE%D0%BC%D0%B5%D0%BD%D0%B4%D0%B0%D1%86%D0%B8%D0%B8%20%D1%84%D0%B0%D1%82%D1%84.pdf.

[10] N. Filchakova, Development of financial monitoring tools in the process of legalization of proceeds from crime, National interests: priorities and security, 2016, № 5(338).

[11] On combating the legalization of proceeds from crime and the financing of terrorism: Federal Law of 07.08.2001 No 115-FZ, Collection of legislation of the Russian Federation, 13.08.2001, No 33 (Part I).

[12] Karataev M.V., Karataev E.V., Risk-oriented approach in the field of AML / CFT: tasks, imperatives, trends, Internal control in a credit institution, 2012. #1.

[13] A. Krechetova,Kolionovo" farm in the Moscow Region attracted $ 500,000 on the "IPO on the blockchain, 02-05-2017. [On the Internet]:http://www.forbes.ru/tehnologii/343603-ferma-kolionovo-v-moskovskoy-oblasti-privlekla-na-ipo-na-blokcheyne-500-000.

[14] "CryptoShuffler, who stole 23 bitcoins, was identified by Kaspersky Lab," 2 10 2017. [On the Internet]: https://cryptorussia.ru/news/cryptoshuffler-ukravshiy-23-bitkoina-vyyavlen-laboratoriey-kasperskogo.

[15] "Mining in the browser," [On the Internet]: https://crypto-fox.ru/news/majning-v-brauzere/.

[16] "ICOLab and KICKICO will protect themselves from crypto-crooks, scum and investment projects-one-day", 2 10 2017, [On the Internet]: https://cryptorussia.ru/news/icolab-i-kickico-zashchityat-ot-kriptovalyutnyh-moshennikov-skama-i-investicionnyh-proektov.

[17] "100 crypts will appear in Moscow before the end of the year," 3 11 2017. [On the Internet]: https://cryptorussia.ru/news/100-kriptomatov-poyavyatsya-v-moskve-do-konca-goda.

[18] FATF Report, "Virtual currencies Key definitions and potential risks in AML / CFT", June 2014, https://www.cbr.ru/today/anti_legalisation/fatf/Virtualnye_valyuty_FATF_2014.pdf/