Advances in Economics, Business and Management Research, volume 71
4th International Conference on Economics, Management, Law and Education (EMLE 2018)

Risks of Unregulated Use of Blockchain Technology in the Financial Markets

Nataliya Amosova
Financial University under the Government of the Russian Federation
Moscow, Russia
E-mail: NAAmosova@fa.ru

Anna Yu. Kosobutskaya
Voronezh State University
Voronezh, Russia
E-mail: kosobutskaya@econ.vsu.ru

Olga Rudakova
Financial University under the Government of the Russian Federation
Moscow, Russia
E-mail: OSRudakova@fa.ru

***Abstract*—The article is devoted to the analyses of the risks of civil society, financial organizations, regulators, law enforcement agencies that are associated with the unregulated use of blockchain technologies. The authors proceed from the fact that new technologies applied in the financial markets produce not only new business opportunities, but also threats of a new type. Special attention is paid to the risks of anti-money laundering via the blockchain technology.**

Keywords—anonymity of operations; regulation; risks; risk profile; new technologies; blockchain technology; financial markets; digital space; anti-money laundering (AML)

I. INTRODUCTION

The problem of blockchain technology abuse is discussed in the most general terms in different literature sources [6], [9], [17], [18], [20], [21], [24]. At the same time governments of many countries, international regulators and financial institutions work at a problem of AML-risks mitigation [8], [11], [12], [16], [22], [23]. Progress is being made also in the Russian Federation [1], [2], [3], [4], [5], [13], [14], [15], [19]. In accordance with the FATF Recommendations and the Methodology [11], countries should continuously assess the risks of money laundering (ML) and terrorist financing (TF) with the aim of creating an adequate understanding at the national level of risks and threats to the financial system and the economy as well as the negative consequences that these acts pose. Countries should also develop adequate mitigating measures.

II. THE TECHNOLOGICAL AND ECONOMIC NATURE OF RISKS OF MONEY LAUNDERING BY USE OF BLOCKCHAIN DERIVATIVES

Risks of anti-money laundering via blockchain derivatives are not defined either in the legislation, or in government rules and regulations. Meanwhile, it is evident that emerging market and non-market relations with digital financial assets carry within them not only the enormous potential to transform the world economy, the society, but also generate new risks to the functioning of national economies, the states, civil societies, business structures and individuals.

By FATF recognition, convertible virtual currencies that can be exchanged back-and-forth for real money or other virtual currencies are potential vulnerable to money laundering and terrorist financing abuse for many of the reasons. They may allow greater anonymity than traditional noncash payment methods and permit anonymous transfers, if sender and recipient are not adequately identified. For example:

- by design, Bitcoin addresses, which function as accounts, have no names or other customer identification attached;
- the Bitcoin protocol does not require or provide identification and verification of participants or generate historical records of transactions that are necessarily associated with real world identity; furthermore, there is no central oversight body;
- nowadays AML software currently available to monitor and identify suspicious transaction patterns is being tested; states' regulatory framework around cryptocurrencies and blockchain technologies is still under development [12].

Virtual currency systems can be accessed via the Internet (including via mobile phones) and can be used to make cross-border payments and funds transfers. In addition, virtual currencies commonly rely on complex infrastructures that involve several entities, often spread across several countries, to transfer funds or execute payments.

This segmentation of services means that responsibility for AML/CFT compliance and supervision/enforcement may be unclear. Moreover, customer and transaction records may be held by different entities, often in different

jurisdictions, making it more difficult for law enforcement and regulators to access them.

And importantly, components of a virtual currency system may be located in jurisdictions that do not have adequate AML/CFT controls. Centralized virtual currency systems could be complicit in money laundering and could deliberately seek out jurisdictions with weak AML/CFT regimes. Decentralized convertible virtual currencies allowing anonymous person-to-person transactions may seem to exist in a digital universe entirely outside the reach of any particular country [12].

According to a report released by Cipher Trace in "Fig. 1" [7], in the first half of 2018 $ 761 million was laundered through cryptocurrency channels that is three times more than all of 2017 ($266 million). It is expected that the amount of money laundered via crypto will exceed $1, 5 billion this year, based on trends.

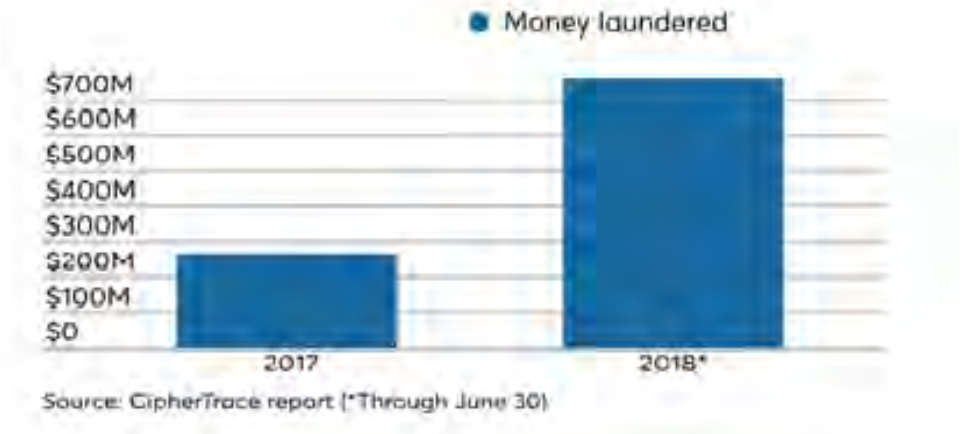

Fig. 1. The amount of money laundered through cryptocurrency channels in 2017 and in the first half of 2018.

According to the Europol, three to four billion pounds ($4.1 to $5.5 billion) of criminal money is being laundered using cryptocurrency in Europe alone. It is thought in the Agency that the process of laundering money via Bitcoin would involve purchasing the cryptocurrency, breaking into its smallest values (Satoshis) and distributing it to various addresses and e-wallets. This process “erases any trail that the criminal money might ordinarily leave behind” [10].

The consequences of the AML risks occurrence, including legal risks, based on the use of the blockchain technology include since 2014 unregulated functioning of digital infrastructure and institutions (shown in "Table I").

TABLE I. INSTITUTIONS AND TOOLS OF DIGITAL INFRASTRUCTURE (SUPPORT SERVICES) THAT CAN BE COMPLICIT IN MONEY LAUNDERING [12]

№ п/п	Name of institution or tool of crypto support services	Content of the activities	Examples
1.	Anonymizer	A complex of tools and services, designed to obscure the source of a Bitcoin transaction and facilitate anonymity (such as darknets and mixers)	Tor (darknet); Dark Wallet (darknet); Bitcoin Laundry (mixer)).
2.	Mixer (laundryservice, tumbler)	a type of anonymizer that obscures the chain of transactions on the blockchain by linking all transactions in the same bitcoin address and sending them together in a way that makes them look as if they were sent from another address; It sends transactions through a complex, semi-random series of dummy transactions that makes it extremely difficult to link specific virtual coins (addresses) with a particular transaction; It operates by receiving instructions from a user to send funds to a particular bitcoin address; then it “mixes” this transaction with other user transactions, and it becomes unclear to whom the user intended the funds to be directed..	Bitmixer.io; Shared Coin; Blockchain.info; Bitcoin Laundery; Bitlaunder; Easycoin
3.	Tor (originally, The Onion Router)	an underground distributed network of computers on the Internet that conceals the true IP addresses, and therefore the identities of the network’s users, by routing communications / transactions through multiple computers around the world and wrapping them in numerous layers of encryption; makes it extremely difficult to physically locate computers hosting or accessing websites on the network; it uses an additional tumblers or anonymizers on its network; it is one of several underground distributed computer networks, often referred to as darknets, cypherspace, the Deep web, or anonymous networks, which individuals use to access content in a manner designed to obscure their identity and associated Internet activity.	

№ п/п	Name of institution or tool of crypto support services	Content of the activities	Examples
4.	Dark Wallet	a browser-based extension wallet, currently available on Chrome (and potentially on Firefox), that seeks to ensure the anonymity of Bitcoin transactions by incorporating the following features: auto-anonymizer (mixer); decentralized trading; uncensorable crowd funding platforms; stock platforms and information black markets; and decentralized market places	Silk Road
5.	Cold Storage	refers to an offline Bitcoin wallet (a Bitcoin wallet that is not connected to the Internet); is intended to help protect the stored virtual currency against hacking and theft.	
6.	Hot Storage	refers to an online bitcoin wallet; is more vulnerable to hacking/theft than cold storage, as it is connected to the Internet.	
7.	Local Exchange Trading System (LETS)	a locally organized economic organization that allows members to exchange goods and services with others in the group; a locally created currency is used to denominate units of value that can be traded or bartered in exchange for goods or services;	Ithica Dollars и Mazacoin)

Capabilities of artificial intelligence were put to work in money laundering control. In particular, American cyber security company CipherTrace has got some success with regard to this. It created the CipherTrace AML platform, that helps to identify potential sources of AML risks using cloud technologies and neuro-analysis. The developers offered a visual interface that can trace financial flows and show attribute data concerning the current location of the currency, including the country and the exchanges used. But, according to experts, the lack of legislative control of crypto economies generates and realizes the risks of legalization (laundering) of proceeds from crime by means of derivative products of blockchain technology faster than counteraction to these attempts manages to work. That is why an adequate understanding and management of the money laundering risks generated by appliance of the blockchain derivatives is vitally important in modern conditions.

Investigation of risks at all levels of the economy, business entities with regard to application of distributed ledger technology (with chains of blocks) is conducted in all countries, discussed by theorists and practitioners of various fields of activity (economists, lawyers, risk takers, marketing specialists, security officials, strategists, IT specialists, etc.).

This issue is studied actively by the institutions of state security and financial intelligence, legislators, regulators and supervisory authorities of all countries of the world. There are no clearly defined conceptual frameworks of the regulation of emerging crypto-economy and crypto-crime. There are no agreed-upon definitions, methods of such risk identification and assessment. Not only their classification is lucking, but also distinct specifications.

All this, in addition, generates legal risks of legalization of money and tools on the basis of the blockchain technology.

The G-20 summit in the summer of 2018 discussed the feasibility of creation of the uniform regulatory rules and recommendations for their application to new cryptocurrency exchanges and the nature of cooperation with countries that prohibit cryptocurrency trading. [16]

The Financial Stability Board (FSB) evaded the creation of an international legal base for cryptocurrency market control, and confined itself to special metrics, enable to assess the threats. The metrics are, as an example, a scope of the cryptocurrency market, influence of financial institutions and quantity of financial cryptocurrency based products. FATF announced its intention to complete revision and to publish new Recommendations and in October, 2018 adopted amendments to the FATF Standards to respond to the increasing use of virtual assets for money laundering and terrorist financing.

In contrast to the previous guidelines, that did not entail legal obligations, the new recommendations assume control of legalization of funds and tools via the blockchain technology. Exchanges and wallet providers will be required to implement AML/CFT controls, to report of suspicious transactions and to be licensed or registered and supervised or monitored by national authorities. Strengthening the standards is part of a comprehensive approach that the FATF has developed to prevent the misuse of virtual asset activities for money laundering and terrorist financing. All countries are encouraged to swiftly take the necessary steps to prevent the misuse of virtual assets. Previously countries solved these issues differently.

III. AML Risks Produced by Blockchain Derivatives in Russian Federation

A paradoxical situation has developed in the Russian Federation: after four years of passive surveillance over the development of crypto-market and its infrastructure (though in 2014, the Bank of Russia and the Federal Financial Monitoring Service in the known Letters warned about a potential danger of cryptocurrencies and operations with them), in 2018 projects of digital legislation formation were presented by Bank of Russia [2], [4], Ministry of Finance [19], Ministry of Communications and Mass Media.

After that, it became obvious that in four years the situation with formation of the foundations of digital legislation remained almost unchanged — there is no a statutory act regulating this sphere. The study of the drafts of legislation and the comments of their developers, experts,

allow us to conclude that various ministries and departments, regulators and legislators have no common glossary yet. Even when they use the same terms, they interpret them differently.

Values of the players involved in AML risks are not designated in any way, but also it is not always clear whose particular values we are talking about. Whose values and interests should protect the law in regard to AML risks mitigation and combating money laundering?

Study of theoretical and legal sources, generalization and systematization of international and domestic experience allow to divide into groups the risks of the parties which are actively involved in or regulate processes of the emerging legal and illegal cryptoeconomy.

We believe that the range of interested parties is very wide.

It is advisable to speak about risks of legalization of money and tools on the basis of blockchain technology with respect to (at least and first of all):

- individuals;
- financial organizations;
- regulators;
- law enforcement agencies responsible for AML/CFT;
- civil society.

Risks Relevant to Individuals

Cryptocurrency and other blockchain derivatives, in accordance with current Russian legislation, are not objects of civil law rights; that means that they cannot be the subject of criminal encroachment in the form of fraud, extortion, theft, etc.

In this context, at present, in the Russian Federation, due to the lack of digital legislation, the certain legal risks are accumulated. These risks render legal protection of the following bona fide persons impossible. These persons are:

- owners of cryptocurrency (i.e. persons, who already own cryptocurrency and other blockchain derivatives (digital financial assets));
- those wishing to become owners of cryptocurrency (i.e. potential owners who are willing to exchange real currency for cryptocurrency);
- those wishing to get out of cryptocurrency (through a legal entity) they own (for speculative or other purposes).

Risks Relevant to Financial Organizations

Due to delays with digital legislation development, the clusters of financial institutions' risks are formed. The risks aggravate the current situation; in particular, probability of occurrence of the following problems increases:

- to be deeply involved in ML/FT;
- not to have relevant internal regulatory framework in the field of AML / CFT;
- not to manage to provide training of personnel capable to prevent attempts of ML / FT;
- be significantly late with software updates;
- not to start timely processing of smart contracts with due protection, etc.

Risks Relevant to Regulators

As concerns the Bank of Russia, it generates legal risk associated with relatively low-tech and lagging financial institutions supervision in terms of AML / CFT. Besides, there is a real legal risk based on incoherence. Inadequacy of the legal framework regulating financial organizations in the field of AML/CFT, to the current and prospective objectives also produces legal risks.

Risks Relevant to the Law Enforcement Agencies Responsible for AML/CFT

The risk of money legalization is reinforced by impossibility to coordinate efforts with foreign colleagues and international organizations as there are legislative lacunas in Russia. A legal risk of inefficient and unsatisfactory work is increasing due to existence of unregulated crypto-economic zones. A legal risk of money legalization via blockchain technology extends the time when it is impossible to repress illegal activities as it is impossible to prove the existence of a legally defined crime under current legislation. Widely discussed Article 128 of the Civil Code of the Russian Federation and Articles 174 and 174.1 of the Criminal Code are still the most problematic.

Risks Relevant to Civil Society

Inadequate digital legislation, including AML / CFT sphere, creates a legal risk of loss of economic processes control. A risk of irreversible lagging behind the world leaders in terms of application of blockchain technology is conceivable due to criminalization and discrediting of a country segment of crypto-economy.

IV. CONCLUSION

Risks of anti-money laundering via blockchain derivatives are not defined either in the legislation, or in government rules and regulations. Meanwhile, it is evident that emerging market and non-market relations with digital financial assets generate new risks to the functioning of national economies, the states, civil societies, business structures and individuals.

The consequences of the AML risks occurrence, including legal risks, based on the use of the blockchain technology include since 2014 unregulated functioning of digital infrastructure and institutions. Such institutions or tools of crypto support services as anonymizer, mixer (laundry service, tumbler), Tor (originally, The Onion Router), Dark Wallet, Cold Storage, Hot Storage and Local

Exchange Trading System (LETS) are described in the article.

Absence of agreed-upon definitions, methods of such risk identification and assessment, classification and distinct specification of risks generates legal risks of legalization of money and tools on the basis of the blockchain technology. The risks of the parties which are actively involved in or regulate processes of the emerging legal and illegal cryptoeconomy in Russian Federation are divided by the authors into groups with respect to (at least and first of all): individuals; financial organizations; regulators; law enforcement agencies responsible for AML/CFT; civil society.

REFERENCES

[1] AML/CFT Law.Federal Law of August 7, 2001 No. 115-FZ – «On Combating Legalization (Laundering) of Proceeds from Crime and Financing of Terrorism» (last updated: April, 18 2018)

[2] Bank of Russia Methodological Recommendations No. 5-MR, dated 16 February 2018 'On approaches to the management of the risk of legalization (laundering) of criminally obtained incomes and financing of terrorism by credit institutions'

[3] Bank of Russia Methodological Recommendations No. 9-MR, dated 2 April 2015, 'On Scrutinizing Certain Customer Transactions by Credit Institutions'

[4] Bank of Russia Ordinance No.4758-U,dated 30March 2018, 'On Amending Bank ofRussia Regulation No. 375-P,dated2 March 2012, 'On the Requirements for aCredit Institution's Internal Control Rules Designed to Counter the Legalization (Laundering) ofCriminally Obtained Incomes and the Financing ofTerrorism'

[5] Bank ofRussia Regulation No. 375-P,dated2 March 2012, 'On the Requirements for aCredit Institution's Internal Control Rules Designed toCounter the Legalization (Laundering) ofCriminally Obtained Incomes and the Financing ofTerrorism'

[6] Chris Skinner. ValueWeb: How Fintech Firms Are Using Mobile and Blockchain Technologies to Create the Internet of Value. Moscow: Mann, Ivanov and Ferber Publisher. 2017. 416 p.

[7] Crypto money laundering up threefold in 2018: Report. American Banker.03 July 2018.Available at https://www.americanbanker.com/news/crypto-money-laundering-rose-3x-in-first-half-2018-report

[8] Crypto-assets Report to the G20 on work by the FSB and standard-setting bodies. Financial Stability Board (FSB). 16 July 2018. Available athttp://www.fsb.org/wp-content/uploads/P160718-1.pdf

[9] Don Tapscott, Alex Tapscott. Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. New York, Penguin Random House LLC. 2016. 348 p.

[10] Europol Claims $5.5 billion Laundered Using Cryptocurrency. Available at https://forklog.com/evropol-do-5-5-mlrd-byli-otmyty-s-pomoshhyu-kriptovalyut/

[11] FATF Member countries Mutual Evaluation Reports 2017. Available at https://index.baselgovernance.org/sites/index/documents/Basel_AML_Index_Report_2017.pdf

[12] FATF report. Virtual Currencies. Key Definitions and Potential AML/CFT Risks. Available at http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

[13] Federal Financial Monitoring Service. National money laundering risk assessment. 2017 – 2018: Key findings. Public report. Moscow, 2018. Available at http://www.fedsfm.ru/content/files/documents/2018/%D0%BE%D1%86%D0%B5%D0%BD%D0%BA%D0%B0%20%D1%80%D0%B8%D1%81%D0%BA%D0%BE%D0%B2%20%D0%BE%D0%B4_5.pdf

[14] Federal Financial Monitoring Service. Ros Fin Monitoring Activity Report, 2017. Moscow, 2018. Available at http://www.fedsfm.ru/content/files/documents/2018/%D0%BF%D1%83%D0%B1%D0%BB%D0%B8%D1%87%D0%BD%D1%8B%D0%B9%20%D0%BE%D1%82%D1%87%D0%B5%D1%82%202017.pdf

[15] Federal Law No. 173-FZ of June 28, 2014 «Concerning the specifics of conducting financial transactions with foreign nationals and legal entities, amendments to the Russian Code of Administrative Offences and invalidation of certain provisions of Russian legislative acts» (last updated: December 30, 2015). Available at http://www.fedsfm.ru/documents/federal-laws/1838

[16] G20: Digital Economy Ministerial Declaration. Salta, Argentina, 23–24 August 2018. Available at https://g20.org/sites/default/files/media/g20_detf_ministerial_declaration_salta.pdf

[17] Genkin A., Miheev A. Blockchain. How Das It Work and What Comes Next. Moscow, Alpina Publisher. 2018. 592 p.

[18] Kariappa Bheemaiah. The Blockchain Alternative – Rethinking Macroeconomic Policy and Economic Theory. Publisher Apress. 2017.- 248 p.

[19] MinFin. Draft Federal Law "About digital finance", published January 25, 2018. Available at https://www.minfin.ru/ru/document/?group_type=&q_4=%D0%9E+%D1%86%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D1%8B%D1%85+%D1%84%D0%B8%D0%BD%D0%B0%D0%BD%D1%81%D0%BE%D0%B2%D1%8B%D1%85+%D0%B0%D0%BA%D1%82%D0%B8%D0%B2%D0%B0%D1%85&DOCUMENT_NUMER_4=&M_DATE_from_4=&M_DATE_to_4=&P_DATE_from_4=&P_DATE_to_4=&t_4=1217268127&order_4=P_DATE&dir_4=DESC

[20] Paul Vigna, Michael J. Casey. The Truth Machine: The Blockchain and the Future of Everything Hardcover. St. Martin's Press. 2018. 320 p.

[21] Roger Wattenhofer. The Science of the Blockchain. CreateSpace Independent Publishing Platform. 2016, 124 p.

[22] Solutions report study on Financial institutions across six markets in Asia. Available at https://www.lexisnexis.com/risk/intl/en/resources/research/true-cost-of-aml-compliance-apac-survey-report.pdf

[23] Time to regulate bitcoin, says Treasury committee report. The Guardian.. Angela Monaghan. Wed 19 Sep 2018 Available at https://www.theguardian.com/technology/2018/sep/19/time-to-regulate-bitcoin-says-treasury-committee-report

[24] William Mougayar. The Business Blockchain. Promise, Practice, and Application of the New Internet Technology. Foreword by Vitalik Buterin. Moscow: Ecsmo, 2018. 224 p.