Crypto risks and mitigation opportunities in Russia

Larisa V. Sannikova
Head of Centre for Legal Research of Digital Technologies, State Academic University for the Humanities, Russian Federation, Moscow

Abstract

The position of national financial regulators in relation to cryptocurrencies is largely determined by the presence of risks of their use. Historically, the development of the crypto market has proved that fears seem to be well founded. Both internationally and nationally, there are mainly four types of risks associated with the use of cryptocurrencies: risks of violation of consumer rights; risks of money laundering and terrorist financing; environmental risks; risks to financial stability. Despite the risks being objective in nature and recognised by all financial regulators in the world, when forming a national legal regulation, each country should assess these risks based on its ability to manage them. The study showed that the risks of public costs in the circulation and use of cryptocurrencies are not destructive for the Russian financial market. Russia needs to adhere more strictly to a risk-based approach to regulating the crypto asset market. To manage risks, it is necessary to legalise the crypto asset market in Russia and create an appropriate market infrastructure. Only the legalisation of the turnover of crypto assets will ensure proper control over it, and, consequently, minimise the existing risks.

Keywords list (en): cryptocurrencies, cryptoassets, crypto market, cryptoasset risks, Ce-Fi, De-Fi

Publication date: 05.07.2023

Acknowledgment:

This research was supported by the Russian Foundation for Basic Research via grant 21-511-93004 КАОН а “The rule of law in the digital economy in China and Russia: current state, challenges and future development”.

Citation link:


INTRODUCTION

The rapid development of the crypto market in recent years shows the futility of attempts to marginalise cryptocurrencies in general and bitcoin in particular. According to the head of the US Securities and Exchange Commission (SEC) Hester Peirce, the cryptocurrency market is ripe for institutional investors. The crypto market, like the stock market, has recently been rapidly falling due to problems in the global economy, thereby demonstrating an inextricable connection with the real economy. In the current circumstances, the decline in the activity of crypto investors (the predicted onset of the “crypto winter”) gives national financial regulators time to develop balanced approaches to the regulation of crypto assets.

In the report of the Bank of Russia (2022) "Cryptocurrencies: Trends, Risks, Measures", the main emphasis was placed on the existing risks of using cryptocurrencies in connection with their spread in Russia. The regulator's decisions were tied to the need to tighten supervision over transactions using cryptocurrencies by creating a system for monitoring the risks associated with investments in cryptocurrencies. It is difficult to agree with this approach, since it does not imply the use of the potential of cryptocurrencies for the development of the digital economy in Russia, taking into account the opportunities available in the country to reduce the risks of their use.

In addition, in Russia, the change in policy in the field of legalisation of cryptocurrencies is actualised in connection with the introduction of financial sanctions by unfriendly countries. Many foreign crypto exchanges have suspended services for users with Russian accounts. At the same time, in 2021 the volume of transactions of Russians with cryptocurrencies, according to the Bank of Russia (2022), reached $5 billion (about 350 billion rubles). It is obvious that Russians consider cryptocurrencies as an alternative investment tool, despite its high-risk nature. The need for such a tool is obvious against the backdrop of restrictions and instability in the domestic foreign exchange market, which greatly narrows the possibilities for Russian citizens to use traditional instruments for savings, which in recent decades have been the euro and the dollar. Interest in the use of cryptocurrencies is also demonstrated by businesses focused on imports and exports, as medium and small businesses can make payments in cryptocurrencies to circumvent various restrictions caused by financial sanctions.
The interest of citizens and businesses in cryptocurrencies cannot be ignored by the monetary authorities. In the context of sanctions against Russia, cryptocurrencies can become an important driver for the development of the digital economy, acting as a financial investment tool for citizens, a way to attract investment for high-tech start-ups, and a tool for settlements with importers and exporters from unfriendly countries.

The main obstacle to the creation of a crypto market in Russia today is the negative attitude of the Bank of Russia towards crypto assets. It seems that this attitude is due to the fact that the Bank of Russia, as a mega-regulator of the financial market, will be responsible for supervising this new, emerging, and therefore unpredictable, market. Therefore, the Bank of Russia sees major risks in the development of the crypto market. Other departments, such as the Ministry of Finance of Russia, the Ministry of Energy of Russia and the Ministry of Industry and Trade of Russia, see not only risks, but also opportunities for the development of the Russian economy, especially in the face of sanctions pressure. They advocate for a more balanced approach to the regulation of crypto assets. To create and develop the crypto market in Russia, various Russian departments need to objectively assess the existing risks and develop a unified position on the regulation of cryptocurrencies.

**CONSUMER RISKS**

Since the emergence of Bitcoin, market participants have been predominantly crypto enthusiasts who had the necessary technical knowledge of the new technology and could manage the risks of using cryptocurrencies. As the crypto asset market expands, so does the diversity of its participants. This is happening not only at the expense of institutional investors, but also ordinary consumers who use cryptocurrencies both as an investment tool and as a payment method in the virtual space or in the real economy (if this is allowed in a particular country). In the context of legal uncertainty associated with the unwillingness of financial regulators to offer comprehensive regulation of crypto markets, risks for consumers of crypto assets are increasing.

Financial regulators point out high risks for consumers associated with the following factors: high volatility of crypto assets; information asymmetry in the crypto market; cybercrime; lack of legal consumer protection mechanisms (EBA 2021; Bank of Russia 2022).

The high volatility of crypto assets raises concerns among economists (Doumenis et al. 2021; Dong et al. 2020; Caporale and Zekokh 2019; Liu & Serletis 2019), as it indicates a lack of maturity of the cryptocurrency market. The price of crypto assets is formed solely on the speculative expectations of investors, so the cryptoasset market is prone to the formation of "bubbles" (Diniz et al. 2022; Bianchetti et al. 2018; Corbet et al. 2018; Fry and Cheah 2016). Accordingly, consumers have increased risks of financial losses when investing money in crypto assets.

Informational asymmetry in the crypto market arises due to both the lack of financial literacy of consumers and the specifics of informing them. Many consumers do not understand the technological features of various types of crypto assets, which are described in the White Paper of crypto projects, cannot evaluate them and make a rational forecast about their investment potential. At the same time, a considerable number of new financial products based on crypto assets have recently emerged, including derivative financial instruments – crypto derivatives. For example, in the UK, the Financial Conduct Authority (2020) banned crypto exchanges subject to its regulation from selling derivatives and exchange-traded index bonds (ETNs) backed by cryptocurrencies to retail consumers.

When making a choice, consumers are forced to focus on the information posted on media, which is often insufficient in terms of risk assessment. Despite the requirement that consumers are to be informed about the high-risk nature of the cryptoassets, when advertising cryptoassets or financial products based on them, the providers mainly focus on the potential benefits, and not on the existing risks. Engaging popular media influencers of crypto projects encourages consumers to make emotional decisions that can cause financial losses.

Cybercrime poses a real threat to the functioning of the crypto market. The most common crimes in the crypto asset market include: fraud, phishing, hacker attacks.

According to Chainalysis, 54% of illegal crypto-related activity is fraud. Most of all, confidence in the crypto market is undermined by cases of ICO fraud. However, Liebau and Schueffel (2019) do not agree with this assessment, claiming that those crypto projects that simply turned out to be unviable for various reasons also fell under the signs of fraud.

Another common method is phishing. The attackers send fake emails with instructions to users, redirecting them to a specially crafted website that asks them to enter their secret key information. With this information, hackers can steal the cryptocurrency contained in these wallets.

Another specific method of fraud in DeFi (decentralised finance) projects is "rug pull". When liquidity is stolen ("hard mat"), developers remove liquidity from pools or vaults on decentralised exchanges and disappear along with the participants' funds. In dumping ("soft mat"), developers first accelerate the value of their tokens, usually with an aggressive social media campaign, and then quickly sell off their supply of tokens at a bargain price. This significantly reduces the price of the token, and as a result, investors are left with depreciated tokens.

Hacker attacks on the digital platforms of centralized crypto exchanges, DeFi projects, gaming platforms, etc., also pose risks to consumers. Consumers need to know how to use technical means to protect their crypto assets, for example, using non-custodial (cold) crypto wallets.

The risks of consumers of crypto assets are exacerbated by the lack of legal mechanisms to protect their rights. Even in countries where the free circulation of crypto assets, including cryptocurrencies as a means of payment, is allowed, cryptocurrency owners are not subject to the rules applicable to consumers of financial services (Parsons 2016). Regulators are limited to the requirement to indicate when advertising crypto assets and financial products based on them as high-risk. As a result, owners of crypto assets cannot count on the protection of their rights in case of their violation due to the lack of adequate effective remedies.

It should be emphasised that due to the transnational nature of crypto assets, the consumer risks of their use does not depend on the jurisdiction in which the consumer is located. Therefore, the regulator, creating a comfortable and secure infrastructure for the circulation of crypto assets, also protects the rights of consumers of these assets.
Since the inception of Bitcoin, anonymity has been seen as one of the advantages of cryptocurrencies, which made them attractive for use as a means to launder the proceeds of crime. Therefore, attention to cryptocurrencies was shown by both the criminal community and law enforcement agencies. In the course of using cryptocurrencies, it turned out that the traceability of cryptocurrency transactions in the blockchain allows users to be identified, despite the fact that they do not disclose their personal data, acting under fictitious names (nicknames). Accordingly, most cryptocurrencies are inherently pseudonymous and do not pose much threat. Along with them, there are cryptocurrencies with a higher degree of anonymity of transactions: Monero (XMR), Dash (DASH), Zcash (ZEC), etc. Some countries completely prohibit their use, for example, such a ban was legally established in Japan in 2018.

However, the transnational nature of cryptoassets necessitates the joint efforts of states to counter the use of cryptoassets for the purpose of laundering proceeds of crime and financing terrorism. After the G20 summit held in Buenos Aires in 2018, the leaders of the participating countries decided to "regulate crypto assets to combat money laundering and counter the financing of terrorism in accordance with FATF standards" (G20 Summit Argentina 2018).

Financial Action Task Force (FATF) for the first time assessed the potential risks of cryptocurrencies in its Report "Virtual Currencies – Key Definitions and Potential Risks in the AML/CFT Area" (FATF 2014). Subsequently, a number of documents were developed, combined in the Targeted Update on Implementation of FATF's Standards on VAs and VASPs (2022). The FATF recommends a risk-based approach to virtual assets, which means not avoiding risks by banning such assets, but properly evaluating and managing them. The extraterritorial nature of cryptocurrencies makes their ban ineffective, as it only drives crypto market participants into a gray, unregulated and uncontrolled zone.

It should also be noted that the FATF combines both cryptocurrencies and other crypto assets into a single category – virtual assets. In this regard, the attempts of the Russian monetary authorities to distinguish between the concepts of "digital currencies" and "digital financial assets" seem inappropriate.

According to the FATF, the main risks of using virtual assets for money laundering and terrorist financing (AML/CFT) arise when making transactions for the exchange of virtual currencies for fiat money, as well as when making transactions for the exchange of various virtual assets among themselves. In order to supervise such activities, the concept of a "virtual asset service provider" has been introduced and requirements for their regulation, supervision and monitoring have been established. In particular, the activities of providers are subject to mandatory licensing or registration in the jurisdiction in which they are created, in order to apply to them AML/CFT legislation. They are obliged to comply with the principle of "know your customer" (KYC), as well as transfer customer information to each other when they make transfers of funds between exchanges. Supervision and control over the activities of providers should be carried out by competent state bodies (national financial regulators), and not by self-regulatory organisations.

The FATF also recommends taking into account the risks of reducing the ability of virtual asset service providers to implement the "know your customer" principle arising from the use of: crypto assets that provide an increased degree of anonymity; built-in "mixers" and "mixers" of crypto assets; anonymisers to hide IP addresses, such as the anonymous TOR (Onion Router) network or a network called the Invisible Internet Project.

Assessing risks for AML/CFT purposes, it is important to consider the business model of the virtual asset service provider, which can be centralised or decentralised. The requirements for traditional financial institutions are applicable to participants in the centralised finance market (Ce-Fi). Therefore, the FATF recommendations are focused mainly on the Ce-Fi market.

The growing decentralised finance (De-Fi) market, in which DApps provide financial services related to crypto assets, is also under the scrutiny of the FATF. Decentralised applications (DApps) are software that runs on the basis of blockchain or other distributed ledger technologies. Despite the fact that the DApp is controlled by an algorithm, the FATF indicates that the functioning of such an application is impossible without some participation or control from some center, for example, when creating and issuing virtual assets, developing DApp functions and user interfaces for accounts, storing an administrative "key" or collecting fees. In cases where it is possible to identify persons involved in the management and control of a De-Fi application, it is proposed to apply the same requirements to them as to virtual asset providers.

With the growing popularity of De-Fi applications, many owners of crypto assets began to withdraw their digital assets from centralised crypto exchanges to non-custodial (cold) wallets. For owners of non-custodial wallets, it is impossible to carry out KYC and AML procedures. This increases the risks of their use when conducting illegal transactions. Therefore, it was suggested to ban such wallets, which provokes an active discussion in the community with most experts pointing out the technological difficulties to implement the total ban as well as the effect this ban may have on the development of crypto industry. In the proposals developed by the EU "on information accompanying the transfer of funds and individual crypto assets," only anonymous wallets remained banned.

Association of Banks of Russia proposed to introduce criminal liability for the use of non-custodial wallets, which also did not receive support in the Russian expert community.

In addition to identifying participants in the crypto-asset market, tracking crypto-asset transactions is becoming another trend in countering money laundering and terrorist financing. In 2019, the FATF extended the Travel Rule, proposed in Recommendation 16, to virtual asset service providers. According to it, crypto companies, like traditional financial institutions, are required to collect data on participants in transactions in excess of 1000 US dollars or euros. When carrying out transactions, banks and/or service providers in the field of virtual assets must exchange the data of the sender and recipient, hence the name "Travel Rule", since the data of the parties "travel" along with crypto.

In Russia, the Federal Financial Monitoring Service has developed the Transparent Blockchain service to track cryptocurrency transactions. This service allows you to determine the parameters of "normal", suspicious and high-risk transactions; trace the chains of movement of digital financial assets; create a database of cryptocurrency wallets related to the implementation of illegal activities and the financing of terrorism.
Thus, the risk-based approach to the use of cryptocurrencies in order to counter the legalisation of proceeds from crime and the financing of terrorism provides for the implementation of measures in the following main areas:

- licensing, supervision and monitoring of virtual asset service providers;
- identification of clients of service providers in the field of virtual assets;
- tracking transactions using crypto assets.

The implementation of these measures in Russia requires the creation of an appropriate legal framework for the legalisation of Russian participants in the crypto market.

**ENVIRONMENTAL RISKS**

The third type of risk, ignored by the Bank of Russia in the report, but highlighted by European financial regulators, is related to environmental consequences. Environmental risks arise from the high level of energy consumption in the production of those cryptocurrencies that use the Proof-of-Work (PoW) consensus algorithms.

Special participants in the network, the miners, solve a mathematical problem using an algorithm contained in the code of a cryptocurrency (for example, bitcoin). The miner who is the first to solve this problem receives a reward that encourages them to make similar calculations in the future and maintain the working condition of the network. However, such competition of miners leads to the fact that most of them waste electricity.

According to the Cambridge Bitcoin Electricity Consumption Index (CBECI), the energy consumption of bitcoin mining accounts for 0.4% of the total energy consumption in the world. At the same time, the share of other cryptocurrencies using PoW is at least 1/3 of the total electricity consumption during mining (Gallersdörfer et al. 2020).

The main risks of high electricity consumption when mining cryptocurrencies:

1) The high carbon footprint of cryptocurrencies due to the use of fossil fuels. Thus, studies show that bitcoin has a significant impact on the environment and contributes to global warming (Calvo-Pardo et al. 2021; Qin et al. 2020; Stoll et al. 2019; Houy 2019; Foteinis 2018).

2) Shortage of electricity for industry and the population. This is evidenced by the experience of China and Kazakhstan. In May 2021, at a meeting of the Committee on Financial Stability and Development of the State Council of the People's Republic of China, he called for measures against bitcoin mining. As a result, most of China's provinces have imposed tough measures against miners, which have led to a massive exodus of mining-related businesses to other countries. Many miners have chosen Kazakhstan for relocation. As a result, the demand for electricity in Kazakhstan by the end of November 2021 increased by about 8% compared to January instead of the usual 1-2% (Muir 2021), which led to energy shortages in a number of areas and a tightening of the authorities' positions on miners.

Russia ranks third in the world in bitcoin mining, its share is 11.23% of the global hashrate. According to data center operator BitRiver, there are 300,000 bitcoin miners in the country. Their activities bring in an average of $1.5 billion a year, and producers of other cryptocurrencies earn about $2.5 billion a year. In the production of electricity in Russia, mainly sources belonging to the category of "green" are used: natural gas, nuclear energy, hydropower. Therefore, the legalisation of cryptocurrency mining will not harm the country's ecology.

In Russia, there is no threat of energy shortages. As a result of the refusal of unfriendly countries to supply Russian electricity in a number of regions, a surplus of electricity is formed. The current tariff policy in the field of electric power solves the problems with household mining and provides an opportunity for the development of industrial mining. The Ministry of Energy of the Russian Federation considers mining as an effective way to eliminate the surplus of generated electricity and as a driver for the development of territories (mainly Siberia).

**FINANCIAL STABILITY RISKS**

In the IMF's (2021) Global Financial Stability Report "COVID-19, Crypto, and Climate: Navigating Challenging Transitions", a separate section was devoted to the cryptocurrency ecosystem and financial stability issues. Much of the report's focus was on emerging market and developing economies. First, it was noted that the introduction of cryptoassets and stablecoins can accelerate the growth of cryptoisation risks and weaken the effectiveness of existing currency restrictions and capital controls. Secondly, it was pointed out that the expansion of the purchase and sale of crypto assets by users in emerging markets could cause destabilising capital flows.

However, the main emphasis was placed on the emergence of global risks due to the rapidly developing process of integrating the crypto ecosystem into the financial system, both globally and in individual countries. This is evidenced by a number of factors, such as, trading of crypto assets by traditional exchanges; provision of services related to crypto assets, large payment networks and banking institutions; the interest of institutional investors in investing in crypto assets. Both the IMF and the European Central Bank point out that the widespread use of cryptocurrencies by banks and other financial institutions could put their capital at risk and undermine investor confidence, credit and financial markets.

As general recommendations, the IMF calls on national regulators to implement global standards applicable to crypto assets, to control and monitor the risks of using crypto assets, and to coordinate among national regulators to promote effective enforcement.

The IMF is also concerned about new sources of risk, such as De-Fi and stablecoins. The growing market for centralised finance has led to the emergence of new De-Fi finance financial products that are even more complex and less transparent to consumers. In addition, they are exposed to great technological and management risks that can arise due to incorrect computer code. Liquidity risks and cyber attack risks are highlighted. The problems of regulating the De-Fi market are due to the lack of financial regulators of any technological capabilities for this. The IMF report (2022) on global financial stability proposes two main areas of regulation of crypto markets to reduce the risks associated with De-Fi finance.
The first direction is related to the creation of comfortable conditions for the development of the centralised finance market (Ce-Fi), by providing legal certainty for centralised market participants, such as stablecoin issuers, centralised crypto exchanges, hosting wallet service providers, reserve managers, network administrators and market makers. According to the IMF, these crypto market participants will benefit if they act on the basis of a reliable and comprehensive national regulatory framework developed in accordance with global standards. In turn, this will restrain the growth of the De-Fi market.

The second direction involves supporting the development of self-regulation of the decentralised market, which includes through the development of industry codes or the creation of self-regulatory organisations. However, even in this case, the IMF allows the introduction of restrictions for regulated companies to interact with De-Fi. Thus, it is supposed to slow down the growth rate of the De-Fi market and eliminate the risks of strengthening the relationship and interdependence between regulated financial markets and the De-Fi market.

It seems that the IMF's attempts to slow down the De-Fi market are counterproductive. It is the possibilities of decentralisation that have attracted the attention of the whole world to bitcoin and other crypto assets. Increased regulatory pressure on the centralised finance market may lead to the opposite effect – a sharp expansion of the decentralised finance market.

The emerging De-Fi market is also a concern for the Bank of Russia (2022a), which has prepared an information and analytical report "Decentralised Finance". The report identifies three possible regulatory approaches to the decentralised finance market, but the position of the national regulator on this issue remained undisclosed. It seems clear that the Bank of Russia is not yet ready to respond to the challenges caused by the growth of this segment of the crypto market.

Following the recommendations of the IMF, the Bank of Russia also analysed the risks to the country's financial stability when using cryptocurrencies. The main risks in the report on cryptocurrencies were identified as the following:

- undermining of monetary circulation and loss of sovereignty of the national currency;
- a possible decrease in the volume of financing of the real sector of the economy;
- capital outflow from the country and the weakening of the ruble;
- the flow of funds from bank deposits, which may lead to a decrease in the financial stability of banks.

The report of the Bank of Russia was prepared based on the IMF report (2021) on global financial stability, which, as mentioned above, focused on the risks of cryptoisation for emerging markets and developing economies. IMF experts directly link the processes of cryptoisation with dollarisation. Factors such as low levels of trust in central banks, inefficient payment systems and/or limited access to them and financial services are forcing the population to use reserve currencies more actively, primarily the US dollar, as a store of value. The same effect can occur with the wider use of cryptocurrencies, thereby undermining the efforts of central banks to implement monetary policy, causing liquidity risks and destabilising the economy.

However, the risk of cryptoisation depends on the degree of adoption of crypto assets in the national financial system. Therefore, it is highest in countries like El Salvador, that have decided to allow the circulation of cryptocurrency as legal tender along with the national currency. With a limited degree of adoption of crypto assets, in particular, even if the use of crypto assets for remittances is allowed in limited volumes, the impact on monetary policy will be negligible.

Accordingly, for Russia, the risk of cryptoisation is minimal, since attempts to use crypto assets as a means of payment from the very beginning of the spread of cryptocurrencies were severely suppressed by the Bank of Russia. In the development of this position, Federal Law No. 331-FZ of 14.07.2022 "On Amendments to Certain Legislative Acts of the Russian Federation and on the Suspension of Certain Provisions of Article 5-1 of the Federal Law "On Banks and Banking Activities" was adopted, which enshrines a direct ban on the use of digital financial assets and utilitarian digital rights as a means of payment for transferred goods, work performed, services provided, except as provided by law.

In the context of financial sanctions against Russia, the risk of capital outflow from the country and the weakening of the ruble exchange rate is significantly transformed. The world's leading crypto exchanges have blocked the accounts of Russian cryptocurrency owners in the execution of sanctions, which significantly reduces the possibility of withdrawing capital from the country. The functioning of the crypto exchange within the Russian jurisdiction would attract Russian crypto investors.

Tokenisation of the corporate sector can act as a preventive measure for a decrease in the volume of financing of the real sector of the economy. Equity tokens and debt tokens are able to attract investment, especially in IT start-ups, which is important for the development of high-tech business in Russia. In addition, stablecoins have great potential, the value of which is provided by pegging to liquid assets, in particular, to commodities. Russia is a producer of popular commodities, including but not limited to unique precious metals, grain, oil. Accordingly, in the context of the global economic crisis, commodity-backed stablecoins can be in demand not only by Russian, but also by foreign crypto investors.

It is difficult not to recognise the validity of the Bank of Russia's concerns regarding the outflow of funds from bank deposits and, as a result, the decline in the financial stability of banks. Competition between the banking sector and the crypto industry will develop, and the flow of funds from banks to fintech companies, including cryptocurrency companies, is inevitable. The use of cryptocurrencies as financial instruments instead of traditional bank deposits will diversify financial risks for both individuals and legal entities. In this regard, the claim about the decrease in the financial stability of banks due to the circulation of cryptocurrencies looks like an attempt by the Bank of Russia to protect banks from market competition with the fintech sector. Such a protectionist policy of the regulator will help protect domestic banks, but may slow down the development of fintech, which will negatively affect the competitiveness of Russian financial institutions in the global financial market.

In addition, the experience of foreign countries shows that banks are interested in cooperation with the fintech sector and are ready to include services related to cryptocurrencies in their line of financial products. Therefore, the Bank of Russia should pay more attention to the risks to financial stability arising from the relationship between traditional financial institutions and the crypto industry, which the IMF also points out.

CONCLUSION
An analysis of existing risks shows that Russia has the technological and organisational potential to mitigate most of the risks associated with the use of crypto assets.

The greatest risk to financial stability is associated with the use of crypto assets as a means of payment. In this regard, the refusal to legalise crypto assets as a means of payment within the country seems to be quite reasonable. However, in order to overcome the sanctions pressure from unfriendly countries, it seems appropriate to allow the use of cryptocurrencies in cross-border payments.

The energy surplus in the regions of Russia allows for considering mining as a promising type of entrepreneurial activity that can become a driver for the development of the territories of Siberia. At the same time, the environmental risks from mining are minimal, since the country uses mainly "green" energy sources.

The strategic direction in regulating the use of crypto-assets should be recognised as ensuring control over transactions with them in order to minimise the risk of capital outflow, the risk of using them for the purpose of laundering proceeds from crime and financing terrorism. Russia has the technical capabilities to track cryptocurrency transactions using the Transparent Blockchain service. Nevertheless, according to the recommendations of international organisations such as the FATF and the IMF, an effective way to exercise such control is the legal regulation and supervision of the activities of professional participants in the crypto industry.

Legal regulation is also important to protect the rights of consumers using crypto assets. Creating an effective legal mechanism for the protection of consumer rights is possible only if the rights and obligations of all participants in the cryptoasset market are established. Russia has formed a legal framework for the creation and operation of the crypto market.

However, a regulated market for digital financial assets in Russia has not yet been created, and the existing cryptocurrency market is in a "gray" zone. Effectively, there is an imitation of a legislative process, which does not lead to the creation of an effective legal mechanism for regulating the crypto asset market, which clearly demonstrates the lack of national infrastructure for participants in the crypto industry. Such an approach seems to be counterproductive, as it does not contribute either to reducing the existing risks associated with crypto assets, or to obtaining advantages and benefits from their use.

References:

Crypto risks and mitigation opportunities in Russia

Санникова Лариса Владимировна
Руководитель Центра правовых исследований цифровых технологий, Государственный академический институт гуманитарных наук
Российская Федерация, Москва

Аннотация

The position of national financial regulators in relation to cryptocurrencies is largely determined by the presence of risks of their use. Historically, the development of the crypto market has proved that fears seem to be well founded. Both internationally and nationally, there are mainly four types of risks associated with the use of cryptocurrencies: risks of violation of consumer rights; risks of money laundering and terrorist financing; environmental risks; risks to financial stability. Despite the risks being objective in nature and recognised by all financial regulators in the world, when forming a national legal regulation, each country should assess these risks based on its ability to manage them. The study showed that the risks of public costs in the circulation and use of cryptocurrencies are not destructive for the Russian financial market. Russia needs to adhere more strictly to a risk-based approach to regulating the crypto asset market. To manage risks, it is necessary to legalise the crypto asset market in Russia and create an appropriate market infrastructure. Only the legalisation of the turnover of crypto assets will ensure proper control over it, and, consequently, minimise the existing risks.

Ключевые слова: cryptocurrencies, cryptoassets, crypto market, cryptoasset risks, Ce-Fi, De-Fi

Дата публикации: 05.07.2023

Ссылка для цитирования: