

Digital Ruble: Assessing the Criminological Risks of the Proposed Model

Submitted: 15 October 2021

Revised: 22 November 2021

Accepted: 2 December 2021

Article submitted to peer blind review

Licensed under a Creative Commons Attribution 4.0 International

Elina L. Sidorenko*

<https://orcid.org/0000-0002-4741-0184>

Zarina I. Khisamova**

<https://orcid.org/0000-0003-0561-8718>

Maxim I. Inozemtsev***

<https://orcid.org/0000-0003-1845-1363>

Pierre von Arx****

<https://orcid.org/0000-0003-2312-1940>

DOI: <https://doi.org/10.26512/istr.v14i1.40388>

Abstract

[Purpose] The article deals with the prospects of introducing the digital ruble within the territory of the Russian Federation.

[Methodology/Approach/Design] The methodological basis of this study is a set of methods of scientific knowledge, among which the main place is taken by the methods of historicism, consistency, analysis and comparative law. Having conducted a detailed review of global trends in this area, authors identified the main reference points that are relevant for most countries where pilot CBDC projects are being implemented.

[Findings] The analysis of the key report, issued by the Central Bank of Russia, on the prospects for introducing the digital ruble allowed us to assess the architecture of the models proposed by the Central Securities Market, their advantages, and their disadvantages.

* Elina Sidorenko is a professor at the Department of criminal law, criminal procedure and criminalistics, director of the Center for Digital Economy and Financial Innovation MGIMO (U). She is the Head of the working group on risk assessment of turnover of the cryptocurrency State Duma of the Federal Assembly of the Russian Federation. E-mail: 12011979@list.ru.

** Zarina Khisamova is a head of scientific department of Krasnodar University of the Ministry of interior of Russia. She is a participant of international research conferences and forums, constantly reports her scientific developments and posts her articles in lead world publications. E-mail: alise89@inbox.ru.

*** Maxim I. Inozemtsev is an associate professor of the Department of Private International and Civil Law, Head of Dissertation Council Department, MGIMO-University, Editor-in-Chief of Digital Law Journal. He has worked at MGIMO-University giving lectures on Corporate Law of Foreign Countries, Civil Law and International Private Law. Dr. Inozemtsev also worked as an Associate for Baker Mckenzie. E-mail: inozemtsev@inno.mgimo.ru.

**** Ambassador von Arx entered the Swiss Federal Department of Foreign Affairs in 2009 as Deputy Head of Delegation for Security Policy Issues of the Permanent Mission of Switzerland to the OSCE and United Nations in Vienna. Ambassador von Arx holds a PhD in Natural Sciences from the Swiss Federal Institute of Technology in Zürich (ETH) with a specialization in genetics and molecular biology. E-mail: pierre.vonarx@osce.org.

[Practical Implications] Taking into account the assessment of statistical indicators on the Russian crime rate, the state of Russian criminal legislation, the concerns of institutional market participants, and the positions of mega regulators around the world, a criminological analysis of the potential risks of introducing the digital ruble was made.

[Originality] The results of the study will be useful to both legal scholars who deal with issues of comparative law, and for practical specialists. The article provides detailed explanations about the theoretical and applied aspects of the introduction of the digital ruble. For the first time, the authors gave a theoretical justification for the risks associated with the introduction of a digital currency.

Keywords: Digital Currencies of Central Banks. Digital Ruble. Regulation. Criminological Risks. Digital Law.

INTRODUCTION

For many countries around the world, the mega-regulator's agenda is currently focused on the issue of their central bank's digital currency. The catalyst for such prioritization was digital corporations creating stablecoins that can compete with national currencies.

Central banks have said that Facebook's potentially huge reach of cross-border payments will instantly make it a systemic competitor to traditional currencies. For example, the G7 countries claim that "global stablecoins pose a threat to the global financial system and they cannot be launched until the legal, regulatory and supervisory risks are resolved" (Financial Stability Board, 2019). These are operational risks, concentration risks, risks of monopolizing the payment market, and risks of reducing the effectiveness of the transmission of the monetary policy and the policies to maintain financial stability (Central Bank of Russia, 2020).

Most countries expressed sharp criticism of Facebook for trying to create its own digital currency, Libra; threats of sanctions were subsequently leveled against the companies that acted as Libra's co-founders, which included payment giants like Visa, MasterCard, Stripe, and eBay. The net result was that they quit the project due to the "blurring boundaries of stablecoin regulation". In turn, the ECB banned the circulation of Libra-type stablecoins until an effective regulatory mechanism for their circulation would be created (Filipenok, 2019).

In these conditions, characterized by corporations' private stablecoins being artificially "contained", central banks around the world moved to considering and implementing the central securities market.

ARCHITECTURE AND MODELS OF CBDC IMPLEMENTATION

The Financial Stability Board and the Bank for International Settlements have expressed serious concerns about the risks of launching a CBDC – in particular,

about how fundamental the impact of CBDC on the existing financial ecosystem will be, which ultimately calls into question the role of banks in financing economic activities and makes their widespread issuance unlikely in the short term (Barontini, 2019).

Despite this, over the past 5-7 years, the discussion has moved from completely rejecting pilot projects to implementing them. According to a survey conducted by the Bank for International Settlements (BIS) in January 2020, across 21 advanced economies and 45 advanced economies (covering 75% of the world's population and 90% of all economic production), 80% of central banks were conducting certain types of work on CBDC – from capacity studies to pilot projects – constituting 90% of such projects (Boar, 2020). At least 36 central banks have published analytical papers on their research on the Central Securities Market, including the Central Bank of Russia (2020). Three countries have already tested national digital currencies (Uruguay, Ukraine, Ecuador), and six more, including China, South Korea, and Sweden, are implementing pilot projects.

The interest banks have in the central securities market is also growing, since the number of non-cash payments has sharply increased during the pandemic, and the transition to a "remote" economy has forced regulators to look for fundamentally new models of mutual settlements while maintaining state control over monetary policy and ensuring the security of settlements. We will also make an assessment that the CBDC cannot be categorized as cryptocurrencies, as there can be no fork (no new currency can appear), it is free to purchase/sell, it must be anonymous, and so on. Note that such a characteristic of the network as decentralization is also not mandatory for the central securities, which distinguishes them from the stablecoins (Khisamova, 2020).

Pointing out the security and stability of payments, financial stability, the efficiency of cross-border payments, and their increasing availability among the advantages of the CBDC, most central banks have not come to a decision on what economic model can be used as the basis for CBDC.

Most of the designed CBDCs are intended for general use, although some of them serve exclusively for wholesale payments and settlements between central banks (Central Bank Digital Currency. <https://cbdc.ru>).

Three main models can be proposed:

- **Direct Settlement Model** (*quasi-commercial bank model*). CBDCs are issued and managed by the central bank. In this case, the central bank, contrary to the two-tier financial system, enters into direct communication with economic agents (both individuals and legal entities), serves retail payments, and maintains a register of all

transactions; that is, it performs the settlement functions of a commercial bank;

- **Hybrid Service Model.** It assumes that retail payments are handled by a commercial bank, and the central bank maintains a register of transactions and provides technical security for making payments. With this approach, the two-tier financial system suffers less, but the question arises in which cases the wallets of consumers are managed by the central bank, and in which cases by a commercial bank; and
- **Intermediary Model** (*quasi-cash settlement model*). According to this theory, the digital currency of central banks is considered as a new means of transporting money, a kind of alternative to non-cash payments. In this case, commercial banks retain all the advantages of non-cash funds: both the transfer mechanism through the registers of a commercial bank and the ability to track payments. In this model, the binding of the currency to the central bank is more of a marketing nature and is aimed at increasing public confidence in the new payment instrument.

Depending on the characteristics of the users, there are two main options for implementing CBDC:

- Retail CBDC is a currency available to a wide range of users, including in retail sales; and
- Wholesale CBDC is a currency available to a limited number of users (professional market participants and credit organizations).

In this regard, it is important to mention the Bank of England's Digital Currency Report of March 12, 2020. The bank has clearly defined that when talking about CBDC, it means retail CBDC (that is, available for use by ordinary citizens). On the contrary, the existing "digital money of the central bank", or the reserves available to commercial banks, cannot be called CBDC. All in all, there is no such question of this currency becoming a digital analogue of non-cash payments.

Besides, the Bank of England proposes linking the central bank to the fiat currency and then to consider them as an analogue of cash. This means that the regulator has removed another important issue in the architecture of the digital currency – the question of whether one can regulate and preserve its value by charging interest or differentiated remuneration depending on the number of funds in the digital wallet.

Among the advantages of the digital currency, the Bank of England notes the speed and reliability of payments and competitiveness to stablecoins. The obvious

risks for commercial organizations should be minimised by refusing to pay interest rates on deposits. This will save the deposit holders and prevent their massive outflow into digital currencies secured by the mega-regulator.

The Bank of England proposes creating a CBDC and a digital platform for payments in CBDC. Payment Interface Providers (PIP) should give average people the opportunity to use CBDC. Besides the actual payments, PIP should create additional systems, such as programmed money, micropayments, smart contracts, etc. PIP should be bound by regulations that will reduce possible risks.

A study by Auer, Cornelli, and Frost (Auer,2020) summarizes the prevalence of each of the CBDC models:

Australia	E-AUD	Finland	Digital-euro
Brazil	Digital Fiat Currency	France	Digital-euro
Bahamas	Sand Dollar	United Kingdom	E-pound
Canada	E-dollar	Ghana	E-cedi
Curacao and Sint Maarten Gulden	Digital Curaçao and Sint Maarten Guilder	Indonesia	E-rupiah*
Switzerland	E-franc	Israel	E-shekel
China	E-CNY	India	Digital-rupee*
Denmark	E-krona	Iceland	Rafkróna
Euro Area (ECB)	Digital-euro	Jamaica	Digital Jamaican dollar*
Ecuador	Dinero Electrónico	Japan	Digital-Yen*
Eastern Caribbean	DCash	Korea	E-won*
Estonia	Digital-euro	Kuwait	Digital Dinar
Spain	Digital-euro	Lithuania	Digital-euro
Malaysia	E-ringgit*	Madagascar	eAriary
Netherlands	Digital-euro*	Sweden	E-krona
Norway	E-krona*	Swaziland	E-lilangeni*
New Zealand	CBDC series	Tunisia	E-dinar*
Philippines	Digital peso*	Trinidad and Tobago	E-dollar*
Russia	Digital-rouble	Ukraine	E-hryvnia
Uruguay	Billete Digital	United States	Digital-dollar*
South Africa	Electronic legal tender		

Table 1 – CBDCs Developed according to the "Retail" Model.

United Arab Emirates	Project Aber
Australia	E-AUD
Canada	Project Jasper
Switzerland	Project Helvetia
Euro Area (ECB)	Project Stella
France	Digital-euro
United Kingdom of Great Britain and Northern Ireland	Cross-border interbank payments and settlements
Hong Kong	Inthanon-Lion Rock
Indonesia	E-rupiah
India	Digital-rupee
Japan	Project Stella
Saudi Arabia	Project Aber
Singapore	Project Ubin
Swaziland	E-lilangeni
Thailand	Inthanon-Lion Rock
South Africa	Project Khokha

Table 2 – CBDCs Developed according to the "Wholesale" Model.

According to the architecture, we can conditionally distinguish a model built on a centralized database and the distributed registry technology (blockchain). The Bank of England, in its study, indicates that its prospective CBDC will not necessarily be based on blockchain, although it recognizes the convenience of blockchain in several aspects, such as decentralization and cyber resilience (Bank of Canada, Bank of England, 2018). Of course, even in the case of introducing the distributed registry technology, the system is unlikely to be built on open access (DLT). In this case, the differences between the banks' digital currencies and private cryptocurrencies will be smoothed out (Sidorenko, 2020).

Experts distinguish the following global trends in implementing CBDCs:

The rapid growth of the exchange rate and the popularity of alternative means of payment, such as cryptocurrencies, encourages central banks to "keep up with the times" and offer decent alternatives.

The analysis of the implemented models shows that no more than 1-2 months pass from publishing the research report to testing the first pilot, which is a confirmation of the central bank's high interest in releasing CBDCs.

The vast majority of central banks have not yet decided on the model of their national digital currency, although many countries are leaning towards the

RETAIL model. The report of the Central Bank of Russia identified 4 models (A, B, C, D) (Central Bank of Russia, 2020). The choice of the distribution model is largely determined by the goals and motives that guide the central bank when creating CBDC. Many authors (Barrdear, Kumhof, 2016), (Kiyutsevskaya, 2019) identify the following motives for creating CBDC: political (early involvement in the creation of an international system of digital currency settlements, increasing national security); economic (increased competition, increased sustainability, increased GDP and increased transparency while reducing the share of the shadow economy); social (increased welfare, creating the products that do not have direct commercial benefits).

No country has yet got things working well. China has moved the furthest on this issue. At the same time, market participants are very optimistic about the prospects for the digital yuan. According to a report by Goldman Sachs (Goldman Sachs, 2020), the digital yuan, China's planned national virtual currency, will account for 15% of total consumer payments in 10 years, helping commercial banks to gain more positions from fintech companies.

At the same time, the central banks of some countries, such as Denmark and Switzerland, have concluded that the current costs of implementing a "general purpose" CBDCs and the potential risks outweigh the possible benefits.

DIGITAL RUBLE: THE PROPOSED MODEL OF THE CBDC AND ITS ADVANTAGES

It is obvious that the digital ruble is a popular solution for the Russian economy. Since 2020, the stable coin sector has expanded by a staggering 500%, increasing from a total market capitalization of about \$20 billion to over \$125 billion. According to the Central Bank of Russia, Russian users are among the most active participants in the digital currency market. "Russia is among the leaders in the number of visits to the Binance digital currency exchange. According to estimates of large banks surveyed by the Bank of Russia in July 2021, the volume of transactions of the Russian population with digital currencies annually amounts to about 5 billion US dollars (about 350 billion rubles).

On October 13, 2020, the Central Bank of Russia released a report for public discussion on the digital ruble. Bringing the issue to public discussion caused a wide response in the banking community, experts, and other market participants. The proposed model highlighted the main aspects of the digital ruble, alongside the associated risks.

The document defined the "digital ruble" as an additional form of the Russian national currency, to be issued by the Bank of Russia in digital form, combining the properties of cash and non-cash rubles (Central Bank of Russia, 2020). It proposed to give the digital ruble the ability to make remote payments and

settlements online (as with non-cash funds), and at the same time the ability to make payments offline (as with cash). The Bank of Russia, when introducing the issue for discussion, cited the following advantages of the digital ruble: free transfer of money from one form to another, reducing the cost of settlements, increasing financial accessibility, improving payment technologies, and recovering funds in the event of losing an offline wallet (Central Bank of Russia, 2020).

Note that allocating similar advantages is common to all central banks in developing countries. At the same time, the only motivation for advanced economies rated as very important is payment security (Boar, 2020); the second most important motivation is to improve the efficiency of cross-border payments (Bech & Boar, 2019).

The report of Skorobogatova, the Deputy Chairman of Sberbank of Russia, also indicates the possibility of using smart contracts and assigning attributes to the digital ruble that allow it to be spent only on certain social programs, which is undoubtedly very valuable for controlling the targeted use of budget funds.

It is obvious that the digital ruble's competitive advantages will directly depend on the design of the digital currency. Here, however, it is important to answer the question of which of the advantages should be a priority for the state: preserving value, ensuring the anonymity of payments, improving control over operations by commercial banks, which consider CBDC as an analogue of non-cash funds.

It is obvious that each of these issues needs a detailed analysis, including based on a review of the already tested CBDCs.

The abovementioned report only stated the problem of the architecture of the digital ruble system. It should be noted that in contrast to emerging economies, the central banks of developed countries, including the US Federal Reserve, the Bank of Japan, the European Central Bank, and the Swiss National Bank, have not yet developed an unambiguous position on the architecture of the "general purpose" CBDC and the prospects for its practical implementation. The report of the Central Bank of Russia suggested 4 possible distribution models: two indirect and two direct.

- Model A corresponds to the traditional two-tier financial model. The Central Bank of Russia issues a digital ruble, opening wallets to banks for interbank settlements and transactions. This model does not make it possible to consider the digital ruble as a retail tool and does not give additional advantages to banks and users. For this reason, it was rejected by the central bank;

- Model B implies that the Bank of Russia opens and maintains electronic wallets of users (companies and individuals). Besides monitoring the security of wallets, it takes over control and cash management. This system excludes commercial banks from settlements and places a heavy burden on the mega-regulator in terms of servicing the wallets of individuals. At the same time, though, this model has one undoubted advantage – most payments between individuals will be carried out under the strict control of the Bank of Russia. In addition, the operationally introduced support for the digital ruble (for example, by charging interest for use, etc.) will ensure a controlled balance of digital cash and non-cash funds;
- Model C has commercial banks acting as intermediaries between the central bank (the issuer of money) and the users. It is they who initiate opening e-wallets by customers and implementing payments on them. The problem, however, is that this model assumes a detailed and complete delineation of the competencies and responsibilities of the central bank and commercial banks for opening accounts, maintaining them, ensuring the security of settlements, and controlling AML/CFT; and
- Model D assumes that the central bank creates and maintains the wallets of commercial banks, and the banks themselves open the wallets of customers and make payments on them. In this case, it is the commercial ones who are responsible for the security of payments, AML/CFT, the quality of payment applications, etc. This model is much more beneficial for banks than Model C, since they are assigned fairly clear and transparent functions of financial control over users. Nevertheless, introducing this system will inevitably cause a drastic redistribution of forces in the financial market: small and medium-sized banks will not be able to compete with technologically strong credit institutions in the fight for the digital wallet market, nor with the central bank for the market of cashless retail payments.

Meanwhile, there is every reason to say that shortly the Bank of Russia will start implementing either Model C or Model D: that is, the model of indirect development with the involvement of the banking sector. This position is based on both the global practice of developing pilot CBDC projects (mainly in large countries with a large number of banks and other financial intermediaries) and the sharp rejection of direct distribution models by the banking community. This is also since the modern Russian banking system simply cannot afford to bring down

the market of non-cash payments and bank deposits due to some stagnation of the market and a decrease in the volume of cash flows.

It is worth noting that the banking community – regarding the shortcomings of direct distribution models, besides such purely economic factors as reduced liquidity or the risk for deposits (Gleeson, 2020) – was also concerned about the hypothetical exclusion of credit institutions from the digital ruble settlement chain, since the central bank's building its architecture could provoke such a situation when settlement and cash services would be provided by the central bank directly, bypassing intermediaries.

Considering the pandemic, users are much more interested in the reliability of the bank than in the profitability of their accounts receivable. Regarding this, if a digital ruble secured by the obligations of the central bank emerges, commercial banks risk being left without cash deposits and losing large volumes of non-cash payments and their servicing. In this case, there is a great risk of bringing down the economy of commercial banks and significantly reducing the volume of profit received from servicing the accounts of individuals and legal entities, issuing loans, etc.

It is quite logical that, anticipating possible threats to their business, credit institutions have simultaneously begun to search for vulnerabilities and shortcomings of the direct distribution model (the most common model). For example, Sberbank of Russia estimated that creating the infrastructure to ensure the cyber-stability of the digital ruble will cost at least 20-25 billion rubles (Chernyshova, 2020); also, Association of Banks of Russia, based on the results of an express survey of 17 credit institutions (which account for 59.5% of the total assets of the banking system) completely doubted the feasibility of introducing the digital ruble. According to the survey, "47.1% of respondents believe that the digital ruble cannot provide significant advantages over the existing forms of payments and settlements. The overwhelming majority of credit institutions (64.7%) spoke in favour of model D, according to which The Bank of Russia opens and maintains the wallets of banks and financial intermediaries, and they open and maintain the wallets of customers and make payments on them" (Association of Banks of Russia, 2020).

Taking into account these circumstances, the Bank of Russia does not consider it possible to completely exclude commercial banks from the digital ruble circulation system. In the framework of Model C, their functionality is seen in providing technical functions, and in the framework of model D in giving them the status of an active participant in this turnover. It is not clear, however, how the responsibility will be distributed among the participants of this market, and what final benefits the digital ruble will give to commercial banks. Today, the Bank of Russia does not provide answers to these questions. Nevertheless, it is

obvious that the key functionality of commercial banks in this area is still official: they provide operational support for the turnover of the digital ruble. Introducing this new feature will undoubtedly stimulate the development of fintech and increase competition between technologically advanced banks. However, it is not yet clear what economic effect this work will have for the banks themselves, creating competition for their services.

Meanwhile, the Bank of Russia has prepared an analytical note to mitigate potential risks to the banking system. The document notes that it is not so much the digital ruble that will have a greater impact on changing the structure of bank income, but rather competition with digital corporations: "increased competition with fintech and bigtech companies will contribute to the redistribution of bank income from such liabilities (bank deposits) in favour of households, regardless of whether a digital ruble will appear or not"(Grishchenko, 2020).

In turn, we note that the model of indirect distribution of the digital ruble, in contrast to the direct one, carries the least advantages of the digital form, which are so valuable in digital currencies. At the same time, its implementation creates even greater risks both in the field of data privacy, the digital and financial security of the state, and the ensuring private interests.

THE MAIN LEGAL RISKS OF INTRODUCING THE DIGITAL RUBLE

We will focus on the main criminological risks that need to be resolved first when building and implementing this model:

Potential increase in the number of economic encroachments due to the lack of a legal basis for the digital ruble and potential gaps

Researchers at the International Monetary Fund (IMF) studied the laws of the 174 IMF members' central banks to answer the question of whether a digital currency is real money. The study found that of all the central banks studied, only about 23%, or 40 central banks, "have the legal right to issue digital currencies". All in all, thus, the digital ruble should cause a deep legal transformation. According to experts, without giving the status of a legal tender, acquiring a full-fledged digital currency can be a difficult task.

Among the most pressing issues that will arise when creating the digital currencies of central banks will be "laws on taxes, property, contracts and insolvency; payment systems; privacy and data protection; most importantly, preventing money laundering and terrorist financing"(Helms, 2021).

Immaturity and novelty of the specified payment instrument can provoke a potential increase in the number of thefts of "digital rubles".

Since 2013, the crime rate in the field of information and communication technologies or using IT technologies has increased more than 20 times. At the

end of 2020, the number of such crimes amounted to more than 510,000. Compared to 2019, this had grown by 73%.

According to the Prosecutor General's Office of the Russian Federation, in January-August of this year, the number of thefts from bank accounts amounted to 107,200, which is twice as many as in the same period of 2019. Every fourth crime committed in Russia falls into this category. In particular, it includes crimes with the use of settlement plastic cards (from 34,000 to 190,000 – +453 %), computer equipment (from 18,000 to 28,000 – +57%), the Internet (from 157,000 to 300,000 – +91.3%), and mobile communications (from 116,000 to 218,000 – +88.3%).

It has become twice as likely, or more so, that such incidents be recorded in certain constituent entities (35 such entities). Over eight months of 2020, the number of fraud cases committed using electronic means of payment doubled. Growth to varying degrees is observed in 90% of the regions. In absolute terms, most of them happen in the Saratov (2,200) and Omsk (1,700) regions (Almakunova, 2020).

There is also a lack of transparent KYC (know your customer) and AML/CFT (countering the legalization (laundering) of proceeds from crime and financing terrorism) procedures, and as a result, there is the possibility of laundering criminal proceeds and financing terrorism through the digital ruble.

Despite the very strict and well-regulated standards in the field of AML/CFT, cases of laundering criminal proceeds through the financial system are far from isolated. In particular, the unique technical features that a central bank currency will add to paper money – such as microtransactions and wallet programmability – may contribute to the creation of more sophisticated money laundering schemes (Gutbrod, 2020).

Legalizing criminal assets is often disguised as legal transactions. Every year, there are more and more new ways to legalize criminal proceeds, which forces lawmakers and law enforcement agencies to solve the emerging problems promptly – for example, to recognize exchange operations with cryptocurrencies as money laundering by amending the thematic resolution of the Plenum of the Russian Supreme Court.

Such risks remain when making cross-border payments; they are not always obvious, since they often occur under the guise of legitimate transactions.

On April 14, 2020, the Financial Stability Board presented general recommendations for the stablecoin regulation. For example, digital currencies must meet the same requirements that are met by other organizations and institutions that carry similar risks, regardless of the technologies used. That is, Due Diligence and KYC/AML procedures must be strictly applied to them, which will allow them to at least partially eliminate the risks. At the same time, it is

noted that the control over them, when used for making international payments, is complicated by differences in the financial regulation of different countries.

States are encouraged to show flexibility and develop a single standard for regulating digital currencies so that their issuers need not "move" from one jurisdiction to another. If necessary, the competent authorities should specify the regulation and eliminate possible gaps in the domestic legal system to effectively minimize risks (John & Wilson, 2020). Regardless of a particular model of using the digital ruble, it should include clear control mechanisms on the part of entities that provide access to the central bank's digital currency.

The requirements of AML (anti-money laundering) and KYC (know your customer) require mandatory disclosure of information about transactions exceeding a certain amount to avoid their use for criminal purposes. Blockchain technology is currently advanced enough to program transactions, making them confidential to certain parties on the network, and still leaving control to regulators (Inozemtsev, 2021). Smart contracts help automate information disclosure and compliance in a previously impossible way.

There is a lack of mechanisms for returning illegally debited funds and compliance with the personal property interests.

This mechanism is not yet fully effective for the system of non-cash payments, and in the context of the theft of the new digital aspect of the ruble, people are very likely to remain "one on one" with their problem. So, according to the report of the central bank's FinCERT, in 2019, attackers stole almost 6.5 billion rubles from cards, yet at the same time, the banks reimbursed the victims only 15% of the stolen funds, or 1 billion rubles (Almakunova, 2020).

The problem of the responsibility distribution.

The specified risk is directly related to the previous one. Introducing the new digital ruble will require a detailed study of the responsibility of the digital ruble issuer, users, and providers/system operators. This issue is particularly relevant for the following potential cases: the central bank's digital currency stored in the wallet was stolen due to 1) the vulnerabilities in the digital currency system; 2) a system failure or technical failure; 3) imperfections of the algorithms used.

Given that the federal law "On the National Payment System" of 27.06.2011 No. 161 has been amended 27 times over the past 10 years, and the issues of supervision in the national payment system still cause complaints, it is difficult to imagine how long it will take the central bank and the participants of the digital ruble system to reach a consensus on the distribution of responsibility.

The lack of a time limit for the "offline" wallet, failures, and the possible "loss" of the digital ruble when switching from offline payments to online can provoke a surge in fraudulent requests for unauthorized debiting, which credit organizations may face.

The issue of opening and maintaining a digital wallet is not considered in detail in the Report of the Central Bank; however, the analogy with digital assets (which, in our opinion, is quite appropriate in this aspect) suggests that digital wallets are one of the most sensitive points in the system.

The recommendations of the Financial Stability Board place special emphasis on the CBDC operators. Operators are required to take measures to effectively manage risks and ensure the system's sustainability. For example, they are required to protect against cyberattacks, prevent money laundering, and counter terrorist financing (John & Wilson, 2020).

In our opinion, the use of the wallet in online and offline mode can allow unscrupulous people to report that their access to the wallet was lost during the specified period due to the theft of a mobile device or suchlike. The repeated use of digital currency in offline payments, as well as the theft in the event of losing the devices with installed software, is very risky.

There are insufficient mechanisms of criminal legal influence on malicious users in the event of attacks on the digital ruble infrastructure and the theft of funds due to the unpreparedness of criminal legislation for such novelties.

Speaking about the potential vulnerabilities of the digital ruble infrastructure, we cannot ignore the possible interference from the inside, nor can we ignore the theft of the user's profile through remotely hacking the personal account or through the errors that occur when identifying the client, including those provoked intentionally using malicious software.

Given the traditional "lag" between criminal legislation and regulatory measures in terms of responding to criminal encroachments in the banking sector, the lack of corpus delicti can sometimes act preventatively when holding the offender liable for theft. In this aspect, it is seen as extremely necessary, even when piloting a model, to approach this issue comprehensively.

The law enforcement system's unreadiness to prevent illegal activities in the digital ruble's infrastructure.

The lack of training and "shortage of personnel" in law enforcement agencies dealing with the investigation of high-tech crimes is among the main reasons for the low detection of theft in the digital sphere.

Fraud with the use of social engineering will become more widespread with the introduction and distribution of the digital ruble, as was the case with cryptocurrencies.

Social engineering remains the main method used by fraudsters when stealing money from accounts. 90% of cases prevented by VTB Bank in 2020 (totaling 3.8 billion rubles) fell on fraud using social engineering techniques. According to the Russian Ministry of Internal Affairs, in 2020, the amount of fraud using electronic

means of payment increased by more than 60 % (from 15,000 to 26,000) (Almakunova, 2020).

Such indicators are largely due to the faster transformation of cybercrime, in contrast to the existing security systems and legal regulation, which creates the prerequisites for the malicious use of telecommunications networks and Internet services in the absence of any punishment.

The possible risks are the following: first, the public is not ready for the mass use of such new technologies, which, in turn, naturally makes people lack confidence in the digital currency. If people know nothing about the architecture of the digital ruble, then they are easy to deceive and for the funds available in non-cash form to be stolen; this can create a vulnerability that will be used by those who want to steal other people's money by deceiving or abusing their trust.

The state can increase control over the people's expenses and block a lot of amounts of funds (at first, potentially unlimited amounts) for purposes that do not correspond to the interests of the user.

Article 101 of the federal law " On Enforcement Proceedings " of 02.10.2007 No. 229 provides for a ban on foreclosing on certain types of income, and provides for their return to the owner, in case of repayment at the expense of these funds of debts under the enforcement order. Meanwhile, Russians often face unjustified recovery of funds by the bailiff service (Gosteva, 2020).

The need to ensure information security in the field of lending, due to the hackers using the digital ruble.

Russian figures of crimes related to credit fraud remain consistently high. For 12 months of 2019, 2,178 people were convicted under this article. Of these, only 1 accused was acquitted. However, against the background of the pandemic, fraudsters have become more likely to steal money from bank customers, tricking them into issuing loans and then withdrawing these funds. As a result, the victim is left with a debt to the bank, which is almost impossible to challenge. It is quite obvious that a new form of money will provoke a new wave of such encroachments.

CONCLUSIONS

The questions outlined above allow us to determine the starting points on which the concept of the digital ruble should be built. First of all, though, it is important to determine what advantages Russia sees for itself in this tool. Undoubtedly, introducing the digital ruble is associated, initially, with risks to the financial security and economic stability of the state. However, in our opinion, the issues of legal regulation and risks associated with them should be considered first.

The introduction of the digital ruble will undoubtedly require amendments to Russian legislation. According to our estimate, changes will be required in 25 federal laws. Their development is planned in 2022 after a successful experiment on the introduction of the digital ruble. Amendments will be made to the Civil Code, the Tax Code, the Budget Code, as well as to the Criminal Code and the Code of Administrative Offenses:

1. The powers of the Central Bank of Russia to organize monetary circulation based on the digital ruble and the rights of the regulator to carry out banking operations with its use will also be expanded by law.
2. In the Civil Code, it will be necessary to add the digital ruble to the list of objects of civil rights, as well as legalize it as a means of payment, he said. In addition, security measures should be fixed for settlements using the digital ruble (those used for bank accounts and cards can be taken as a basis), as well as mandatory requirements for processes, devices, software for the circulation of a new form of money.
3. In the law on digital financial assets (CFA), it is necessary to differentiate the concepts of digital currencies, digital ruble and stablecoins, and strengthen guarantees of judicial protection.
4. The system of legal protection of owners of digital rubles will require amendments to criminal legislation and the Administrative Code. It will be necessary to provide for liability for violation of the provisions of the CFA law, regulate the process of collecting property from debtors in the form of digital currency and the procedure for exchanging digital assets for fiat money.

REFERENCES

- ALMAKUNOVA R. (IN PRESS) **The conclusion is made: the theft of money from accounts in 2020 doubled.** 13 Oct. 2020 Available at: <https://iz.ru/1072799/roza-almakunova/vyvod-sdelan-krazhi-deneg-so-schetov-v-2020-m-vyrosli-vdvoe>. (in Russian).
- AUER R. et al. (2020) Rise of the central bank digital currencies: drivers, approaches and technologies. **BIS Working Papers.** 880 Available at: <https://www.bis.org/publ/work880.htm>.
- BANK OF CANADA, BANK OF ENGLAND, MONETARY AUTHORITY OF SINGAPORE. (2018) **Cross-Border Interbank Payments and Settlements: Emerging opportunities for digital transformation. Emerging opportunities for digital transformation.** November 2018. 68 p. Available at: <https://www.mas.gov.sg/>

/media/MAS/ProjectUbin/Cross-Border-Interbank-Payments-and-Settlements.pdf?la=en&hash=5472F1876CFA9439591F06CE3C7E522F01F47EB6.

- BARONTINI C., HOLDEN H. (2019) **Proceeding with caution – a survey on central bank digital currency**. January 2019. 24 p. Available at: <https://www.bis.org/publ/bppdf/bispap101.pdf>.
- BARRDEAR, J. & KUMHOF, M. (2016). The macroeconomics of Central Bank issued digital currencies. Bank of England. **Working Paper** 605 (2016). Available at: <https://www.bankofengland.co.uk/working-paper/2016/the-macroeconomics-of-central-bank-issued-digital-currencies>.
- BECH, M. & BOAR, C. (2019). Shaping the future of payments. Analysis of the 2018 **Red Book Statistics** Available at: https://www.bis.org/statistics/payment_stats/commentary1911.htm.
- BITCOIN.COM. **IMF Says Only 23% of Central Banks Can Legally Issue Digital Currencies**. (IN PRESS) 16 Jan. 2021 Available at: <https://news.bitcoin.com/digital-currency-money-imf-central-banks-legally-issue-digital-currencies/>.
- BOAR C., HOLDEN H., WADSWORTH A. (2020). Impending arrival – a sequel to the survey on central bank digital currency by Monetary and Economic Department. **BIS Papers No 107**. January 2020.
- CARSTENS A. (2020). Shaping the future of payments. **BIS Quarterly Review**. 17 Mar. 2020 Available at: https://www.bis.org/publ/qtrpdf/r_qt2003e.pdf.
- CENTRAL BANK OF RUSSIA. (2020). Digital ruble. **Report for public consultations**. Moscow, 2020.48 p.
- CHERNYSHOVA Y. (IN PRESS). Banks have warned of a surge in the theft of pre-approved loans. 31 Oct. 2020. Available at: <https://www.rbc.ru/finances/31/10/2020/5f9afd879a79470cfa72e8e7>. (In Russian).
- CHERNYSHOVA Y. (IN PRESS). **Sberbank estimated how much the stability of the digital ruble will cost protecting a new form of currency from fraudsters can cost more than 20 billion rubles**. 03 Dec 2020. Available at: <https://www.rbc.ru/finances/03/12/2020/5fc784d29a79478cbf802b14>. (In Russian).
- CLIFFORD CHANCE. (2020). **Central Bank Digital Currencies And Stablecoins – How Might They Work In Practice?** 21 September 2020. 10 p. Available at:

<https://www.cliffordchance.com/briefings/2020/09/central-bank-digital-currencies-and-stablecoins--how-might-they-.html>.

DIGITAL CURRENCY OF THE CENTRAL BANK. (2021). Available at: <https://cbdc.ru>.

INOZEMTSEV M.I. (2021). Taxonomy and typology of crypto-assets: approaches of international organizations in Engineering Economics: Decisions and Solutions from Eurasian Perspective, **139 Lecture Notes in Networks and Systems** (S Ashmarina et al. eds., 2021). Available at: https://doi.org/10.1007/978-3-030-53277-2_14.

FILIPENOK A. (IN PRESS) **The EU banned the circulation of the Facebook Libra cryptocurrency.** 06 Dec. 2019. Available at: <https://www.rbc.ru/economics/06/12/2019/5de984cc9a7947420136eb08>. (In Russian).

FINANCIAL STABILITY BOARD. (2019). **To G20 Finance Ministers and Central Bank Governors.** 13 Oct. 2019. Available at: <https://www.fsb.org/wp-content/uploads/PXX1019.pdf>.

GOLDMAN SACHS (2020) **Equity Research. Reinventing the Yuan for the Digital Age.** 2020. Available at: <https://www.goldmansachs.com/insights/series/goldman-sachs-research/>.

GOSTEVA E. (IN PRESS). **Double write-offs»: how bailiffs rob Russians.** 2019. Available at: <https://www.gazeta.ru/business/2019/06/21/12433093.shtml>. (In Russian).

GRISHCHENKO V., MOROZOV A., PETRENEVA E., SINYAKOV A. (IN PRESS). What will change for banks and their clients with the introduction of the digital ruble. **Analytical note of Central Bank of Russia.** January 2021. Available at: https://cbr.ru/Content/Document/File/118208/analytic_note_20210126_dip.pdf. (In Russian).

JOHN H., WILSON T. (2020). **G 20 sets ground rules before Facebook's Libra Stable Coin.** 14 Apr. 2020. Available at: <https://www.reuters.com/article/us-g20-regulator-stablecoins/g20-sets-ground-rules-ahead-of-facebooks-libra-stablecoin-idUSKCN21W0TU>.

KHISAMOVA Z.I. (2020). The Concept of Digital Currencies of Central Banks: The Main Risks in Terms of Compliance with the Requirements of AML ("Countering Money Laundering") and KYC ("Know Your Client"). **Actual Problems of Economics and Law.** 2020; 14(3): 508-515. (In Russian). Available at: <https://doi.org/10.21202/1993-047X.14.2020.3.508-515>.

- KIYUTSEVSKAYA A.M. Fintech: (2019). Current Trends and Challenges for Monetary Policy, (4) **Voprosy Ekonomiki**. 2019; (4): 137-151. (In Russian). Available at: <https://doi.org/10.32609/0042-8736-2019-4-137-151>.
- SIDORENKO, E.L. (2020). Stablecoin as a new financial instrument in Digital Age: Chances, Challenges and Future. ISCDTE 2019, 84 **Lecture Notes in Networks and Systems** (S Ashmarina et al. eds., 2020). Available at: https://doi.org/10.1007/978-3-030-27015-5_75.
- THE ASSOCIATION OF RUSSIAN BANKS. (IN PRESS). **The Association of Russian Banks discussed the report of the Bank of Russia on the digital ruble.** 2 December 2020. Available at: <https://asros.ru/news/asros/v-assotsiatsii-bankov-rossii-obsudili-doklad-banka-rossii-o-tsifrovom-ruble/>. (In Russian).