Critical analysis of the effectiveness of EU financial sanctions against the Russian Federation

ANGELA PACHOLCZAK

Independent author

https://orcid.org/0009-0000-4670-2364

Internal Security Review, 2024, no. 30: 353–383

https://doi.org/10.4467/20801335PBW.24.015.19617

ARTICLE

Abstract

The article focuses on the issue of international sanctions of a financial nature in the context of, in particular, the challenges to their effectiveness generated by the cryptocurrency market. An essential point of reference for this analysis is the current case of sanctions imposed by the Council of the European Union (supported by the application of complementary sanctions by part of the international community) on the Russian Federation in relation to that country's military aggression against Ukraine. The aim of this article is to show different perspectives on the assessment of the effectiveness of sanctions and, in particular, to identify the sources why, in a key number of cases, while weakening the economic potential of the sanctioned state, they nevertheless fail to achieve the original objective of their imposition, i.e. the deterrence of military action. In this subject, the axis of interest is the current and prospective impact of blockchain-based financial solutions on the creation of an important loophole in the sanctions regime to eliminate or marginalise the effects of international financial sanctions. The issue is also assessed through the prism of the crypto-asset market regulation entering into force in the European Union in the near future and the implementation of the so-called travel rule for cryptocurrency transactions.

Keywords

Russian Federation, financial international sanctions, crypto-assets, decentralised finance, DeFi, central bank digital currency, CBDC, MiCA regulation

War is merely the continuation of policy by other means.
Carl von Clausewitz, *On the Nature of War* (1832)

Engaging in military action by the international community in response to a violation of international law by one state can hardly be considered a good option when the overriding objective is to avoid an escalation of armed conflict. Consequently, a better, and sometimes the only choice for the international community becomes the use of sanctions, which are seen as a liberal alternative to war. However, in the context of achieving the main objective of the application of sanctions, i.e. deterring military aggression, they are more of a signal[1], rather than having a real impact on the party covered by them, especially its policy-makers and circles linked to the centres of power.

The concept of sanctions is primarily associated with the use of economic tools directly relating to the economic sphere, which involves the cessation or threat of cessation of existing trade or financial relations. Sanctions are more than a mere diplomatic declaration and their real effectiveness is conditional on causing a drastic impact on the economy of the sanctioned country.

The view should be shared that the effective enforcement of financial sanctions is far easier than the enforcement of trade sanctions[2], which is due to the fact that financial institutions and states are important providers or guarantors of financial flows. Moreover, there is far more supervision over the financial market than over the trade market. Financial activities should therefore, at least in principle, be easier to monitor and possibly identify violations of sanctions. In addition, studies have confirmed the greater effectiveness of financial sanctions compared to trade sanctions[3]. Indeed, it cannot be overlooked that, in an economic environment,

[1] This is due to the way in which the normative basis is understood, according to which it is assumed that through punishment and shaming it is possible to create moral motivations. This is related to the understanding of international sanctions as a negative reaction of the international community towards a state that violates its norms. See: R. Bierzanek, J. Symonides, *Prawo międzynarodowe publiczne* (Eng. Public international law), Warszawa 2003, p. 24.

[2] G.C. Hufbauer et al., *Economic Sanctions Reconsidered: Supplemental case histories*, Washington 2007, pp. 97–98.

[3] In a study by Gary C. Hufbauer, Jeffrey J. Schott and Kimberly A. Elliott conducted in 1985 (updated in 1990 and 2007), with regard to financial sanctions caseloads, 19 cases out of 53 involving the application of financial sanctions alone (36%), 32 cases out of 101 involving the application of financial and trade sanctions (32%) and 8 cases out of 21 involving the freezing of assets (38%) were considered successful. By contrast, in a situation involving the application of commercial sanctions only, a positive outcome was recorded in 10 cases out of 40 reviewed (25%). See: G.C. Hufbauer et al., *Economic Sanctions Reconsidered*…, p. 98.

trading activities require access to financial resources. Thus, financial sanctions have a complementary effect on trade flows as they avoid the problem of enforcement of sanctions against them[4]. However, counterintuitively, like other types of sanctions, financial sanctions can also be inhumane in nature and cause irreparable harm to the civilian population of the sanctioned country, but do not necessarily have a direct impact on the situation of its policy-makers.

This raises an important question about the impact of the developments in financial markets, globally observed for more than a decade (including innovative alternatives to traditional banking systems that increasingly interact with state monetary and currency systems), on undermining the effectiveness of international sanctions. Indeed, the question can be raised not only about the validity of the relevant laws, but also about the possibility of expressing in them norms that fully regulate the new solutions applied in the financial markets, which would indirectly ensure the enforcement effectiveness of the established sanctions. The aim of this article is to show the complexity of this issue in the context of access to and use of new financial instruments by state apparatuses. It is not limited to dogmatic research on this issue, but, due to the perception of law as a multifaceted cultural phenomenon[5], reference is made to the results of economic and political scientific research on the effectiveness of international sanctions, including a review of innovative financial instruments relevant to the EU sanctions imposed on the Russian Federation (RF) in connection with its military aggression against Ukraine.

The ineffectiveness of economic sanctions

There is a misconception associated with sanctions that enforcing an expected norm of behaviour will be triggered by mere concern about economic performance on the part of the covered state. Contrary to this assumption, economic research conducted in 1990 by Gary C. Hufbauer, Jeffrey J. Schott and Kimberly A. Elliott showed that the effectiveness of economic sanctions was relatively low at about 34%[6]. As a result of a critical analysis of these studies in political science terms,

[4] Ibid, pp. 47–48, 97.

[5] See: K. Opałek, J. Wróblewski, *Zagadnienia teorii prawa* (Eng. Issues in legal theory), Warszawa 1969; the same, *Prawo. Metodologia, filozofia, teoria prawa* (Eng. Law. Methodology, philosophy, theory of law), Warszawa 1991.

[6] The 1990 study included 116 cases in which sanctions were applied. In 40 cases, their application was found to have had a positive effect.

Robert A. Pape concluded that of the 40 cases identified in them, only five could be considered a real success of the application of sanctions[7].

The ineffectiveness of sanctions is influenced by a number of factors, primarily these are the inadequacy and insufficiency of the measures used. This makes it easier to avoid sanctions or at least minimise their negative implications. In this context, the basic condition for effectiveness is the unanimity of the international community on the imposition of sanctions on a country. The absence of this solidarity opens the door to the possibility of limiting and neutralising the effects of sanctions. For example, in terms of trade, this opens up new import destinations and changing markets for exports. At the same time, through new trade destinations, it becomes possible to 'smuggle' sanctioned goods to countries formally applying sanctions[8]. With regard to the financial system, on the other hand, it is possible to secure it through the so-called economy vaccination, which involves insulating it from the impact of sanctions by either securing a remedy to the sanctions or gaining easy access to alternatives[9].

Sanctions are also associated with the phenomenon of intensification of nationalist attitudes in the state against which they are applied. This is pointed out by Robert A. Pape, who unequivocally points out the ineffectiveness of sanctions when not only the state apparatus, but also citizens are willing to endure severe sanctions in the name of national interests. Such tendencies especially characterise autocratic systems, in which the authority can accept high costs in social terms if it enables it to achieve its own goals[10]. Thus, this phenomenon contradicts claims that striking at the economic interests of a country's citizens must involve their advocacy of political change.

In the current reality, the ineffectiveness of financial sanctions is also linked to the growing global importance of cryptocurrencies. They can play an important role in minimising sanctions both individually and involving a country's financial system.

---

[7] Pape corrected the number of cases examined - there were 115, not 116. He considered 5 cases to be repetitions, similarly, among the 40 cases classified as a success, he identified 1 repetition, in 18 cases the settlement actually resulted from the direct or indirect use of force, in 8 cases the sanctions had no effect, as the countries covered by them made no concessions, and 6 cases involved trade disputes, not strictly economic sanctions for political purposes. In 3 cases, evaluation for the effectiveness of sanctions is impossible. See: R.A. Pape, *Why Economic Sanctions Do Not Work*, "International Security" 1997, vol. 22, no. 2, p. 93, 99.

[8] Naturally, this nevertheless entails negative consequences for the sanctioned country due to a drop in the price of exported raw materials and goods.

[9] A. Demarais, *Backfire: How Sanctions Reshape the World Against U.S. Interests*, New York 2022, pp. 35–50.

[10] R.A. Pape, *Why Economic Sanctions*…, p. 106.

Russian case

In view of the hostilities against Ukraine and the illegal annexation of the Donetsk, Luhansk, Zaporozhye and Kherson regions (2022), and in view of the restrictive measures imposed on the Russian Federation in connection with the annexation of Crimea (2014), among others, the European Union (EU)[11] decided to impose further sanctions on the country. These were restrictive measures in the form of both individual sanctions as well as economic and visa sanctions. As of 5 March 2024, the EU Council had adopted 13 sanctions packages.

Focusing solely on the issue of direct impact on the Russian financial system, the following EU sanctions should be pointed out:

- A ban on financing the Russian government and the Central Bank of Russia, CBR (Russian: Центральный банк Российской Федерации or Банк России) and any transactions related to the management of its reserves and assets (foreign exchange reserve freeze), as well as bodies, entities or persons acting on behalf of or under its direction [e.g., the Russian National Wealth Fund (Фонд национального благосостояния)];
- A ban on the export of banknotes and the sale of negotiable securities[12] to Russia denominated in euros and other official EU currencies[13];
- A ban on investing in projects co-financed by the Russian Direct Investment Fund (Российский фонд прямых инвестиций), as well as participating in or making other contributions to projects[14];
- A ban on all transactions with certain Russian state-owned enterprises in various sectors that make up the Kremlin's military-industrial complex[15],

[11] In addition to the EU sanctions (and its member states, which retained the ability to impose separate, additional sanctions), measures have also been imposed on Russia by: US, UK, Canada, Switzerland, Japan, Singapore, South Korea, Australia, New Zealand and Taiwan. The scope of these sanctions is not uniform in many cases. Singapore, for example, opted only to impose limited financial sanctions and export controls on weapons and items for offensive cyberoperations. See: *Sanctions and Restrictions Against Russia in Response to its Invasion of Ukraine*, Ministry of Foreign Affairs Singapore, 5 III 2022, https://www.mfa.gov.sg/Newsroom/Press-Statements-Transcripts-and-Photos/2022/03/20220305-sanctions [accessed: 5 III 2024].

[12] Linked to this ban is the prohibition on EU central securities depositories to hold accounts for Russian clients.

[13] Exceptions include funds necessary for the personal use of travellers to Russia or official purposes of diplomatic missions, consular missions, international organisations.

[14] In this respect, strict derogations are provided for contracts concluded before 2 March 2022.

[15] The complete list of the above-mentioned entities is set out in the list of Annex XIX of *Council Regulation (EU) No 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine*.

as well as a ban on holding positions in the governing bodies of these enterprises;
- A ban on the listing of shares of Russian state-owned entities on EU trading venues and the provision of related services;
- Prohibition of direct or indirect purchase, sale or provision of investment services or assistance in issuance and other activities with respect to marketable securities and money market instruments with respect to, among others, the Government of Russia and the CBR, legal persons, entities and bodies acting on their behalf, as well as entities identified in Annexes V and VI of *Council Regulation (EU) No. 833/2014 of July 31 2014 concerning restrictive measures in view of Russia's actions destabilizing the situation in Ukraine* (hereinafter: Regulation 833/2014);
- Prohibition on providing business services directly or indirectly, such as accounting, auditing, statutory auditing, bookkeeping and tax consulting, information technology consulting, legal consulting, architecture and engineering, management consulting, public relations, market and public opinion research, technical research and analysis, advertising and rating services;
- A ban on providing key Russian banks with specialised financial messaging services used to exchange financial data within the Society for Worldwide Interbank Financial Telecommunication (SWIFT)[16];
- A ban on providing public financing or financial assistance for trade with the Russian side or investment in the Russian Federation[17];
- A ban on the participation of Russian contractors in public contracts and concessions awarded in EU member states;
- A ban on EU Central Securities Depositories (CSDs) maintaining accounts for Russian clients and selling them euro-denominated securities;
- A ban on accepting deposits from citizens or Russian residents, legal persons, entities or bodies based in Russia, or legal persons, entities or bodies

[16] The sanctions under the third package of 2 March 2022 covered seven Russian banks, namely Банк Открытие (Bank Otkritie), Новикомбанк (Novikombank), Промсвязьбанк (Promsvyazbank), Банк "Россия" (Rossiya Bank), Совкомбанк (Sovcombank), Vnesheconombank (VEB, VEB.RF) and Банк ВТБ (WTB Bank), as well as all legal persons, entities or bodies established in Russia in which more than 50% of the ownership rights are directly or indirectly held by the above institutions. Subsequently, as part of the sixth package of 3 June 2022, the exemption from SWIFT was extended to Сбербанк России (Sberbank of Russia), Московский кредитный банк (Credit Bank of Moscow) and Российский сельскохозяйственный банк (Россельхозбанк) - (Russian Agricultural Bank).

[17] The exceptions are: the reservation to finalise contracts concluded before 26 February 2022 and special cases concerning trade in food products, agricultural, medical or humanitarian measures, and concerning EU programmes for small and medium-sized enterprises - up to a certain amount.

based outside the EU, where more than 50% of the ownership rights belong directly or indirectly to Russian citizens or natural persons residing in Russia, if the total value of their deposits per credit institution exceeds the amount of EUR 100,000;
- A ban on the provision of financial planning advice and trusts as well as the acceptance of large deposits by EU banks;
- A ban on the provision of cryptographic services initially of high value (i.e. EUR 10,000) and then regardless of value.

At the same time, following the introduction of the thirteenth package of sanctions against Russia, a total of 2,177 individuals and entities[18] were subjected to individual sanctions involving, among other things, the freezing of assets and the prohibition of funds or economic resources. New sanctions were also established against Belarus (due to actions undermining the territorial integrity, sovereignty and independence of Ukraine) and Iran (in connection with its military support in the form of the delivery of unmanned aerial vehicles). As for individual sanctions imposed on Belarus, they were applied to 271 individuals and entities[19], and on Iran - to 280 individuals and entities[20].

The enforcement of sanctions adopted by the Council of the EU rests with member states, which are responsible for their implementation. In this regard, they are supported by the European Commission (EC), which is responsible for the uniformity of these measures and their international coordination[21].

EU sanctions targeting Russia and Belarus are supplemented in Poland by domestic sanctions. In this respect, the most important piece of legislation is the *Act of 13 April 2022 on special solutions to counter support for aggression against Ukraine*

---

[18] As set out in Annex I of *Council Regulation (EU) No 269/2014 of 17 March 2014 on restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine* - with 36 persons and entities having been removed from the list as at 5 March 2024, 2141 persons and entities therefore remain subject to sanctions.

[19] As set out in Annex I of *Council Regulation (EC) No 765/2006 of 18 May 2006 concerning restrictive measures in view of the situation in Belarus and in view of Belarus' involvement in Russia's aggression against Ukraine* - with 1 entity having been removed from the list as of 5 March 2024, 270 persons and entities remain subject to sanctions.

[20] As set out in Annex I of *Council Regulation (EU) No 359/2011 of 12 April 2011 concerning restrictive measures directed against certain persons, entities and bodies in view of the situation in Iran* - with 8 persons having been removed from the list as at 5 March 2024, 272 persons and entities therefore remain subject to sanctions.

[21] To this end, the EC has set up a Freeze and Seize task force to coordinate at EU level the implementation of individual sanctions against individuals. This group is also responsible for cooperation within the REPO (Russian Elites, Proxies, and Oligarchs) task force, which manages EU cooperation with the G7 (Group of Seven) countries and Australia.

and serving to protect national security, stipulating, inter alia, the establishment of an additional national sanctions list maintained by the minister responsible for internal affairs[22].

Pursuant to the provisions of this Act, a fine, imposed by the Head of the National Revenue Administration by way of an administrative decision, of up to PLN 20 million[23] shall be imposed on a person or entity who, with respect to a listed person or entity, fails to comply with: the obligation to freeze financial assets, funds or economic resources or the prohibition on making financial assets, funds or economic resources available, as set out in Article 2 (1) or (2) of *Council Regulation (EC) No 765/2006 of 18 May 2006 concerning restrictive measures in view of the situation in Belarus and Belarus' involvement in Russia's aggression against Ukraine* (hereinafter: Regulation 765/2006) or Article 2 of *Council Regulation (EU) No 269/2014 of 17 March 2014 on restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine* (hereinafter: Regulation 269/2014), or the obligation to communicate promptly the information required under Article 4(2) or 5 of Regulation 765/2006 or under Article 7(1) or 8 of Regulation 269/2014; or fail to comply with the prohibition on knowingly and intentionally participating in activities the object or effect of which is to circumvent the application of the measures set out in Article 2(1) or (2) of Regulation 765/2006 or Article 2 of Regulation 269/2014.

One has to agree with Pape that despite the comprehensiveness of the sanctions, their imposition on the Russian Federation has been a failure. They are undoubtedly harsh on the economy[24], but they do not actually force Russia to stop its

[22] The list is independent of the lists of persons and entities set out in Regulations 765/2006 and 269/2014, as the scope of measures applicable to persons and entities included in it may not duplicate the scope of measures laid down in respect of them in those Regulations (Article 2(2) of the aforementioned Act). As updated on 29 February 2024 by the Ministry of Internal Affairs, the list included 427 individuals and 82 entities. At the same time, 1 natural person and 8 entities were removed from the list between 2022 and 2023. As a result, 426 natural persons and 74 entities remained sanctioned as at the aforementioned date.

[23] Article 6 of the *Act on special solutions to prevent support for aggression against Ukraine and to protect national security*.

[24] This is confirmed, among other things, by the recorded decline in Russian gross domestic product (GDP). According to analyses by the World Bank, the International Monetary Fund and the Organisation for Economic Co-operation and Development, Russian GDP declined by 2.1% in 2022, with growth of 3% projected before the invasion by the Federal State Statistics Service, Rosstat (Федеральная служба государственной статистики, Росстат). See: *Wpływ sankcji na rosyjską gospodarkę* (Eng. The impact of sanctions on the Russian economy), Council of the EU, https://www.consilium.europa.eu/pl/infographics/impact-sanctions-russian-economy/ [accessed: 5 III 2024].

ongoing "military operation"[25]. The example of this country shows the full extent of the limitations on the effectiveness of the international sanctions regime.

The main factor determining the low effectiveness of the sanctions applied was, as mentioned above, the lack of unanimity of the international community on the subject, especially the negative attitude to the application of sanctions of China, India, Iran and the states of the former Soviet republics of Central Asia and the Caucasus or Turkey. Anticipation of the international community's lack of unanimity made it possible to inoculate the Russian economy and find alternatives to reduce the severity of the sanctions, as exemplified by the increase in the amount of foreign currency and gold reserves held in the years preceding the aggression against Ukraine[26]. Despite the freezing of part of Russia's foreign exchange reserves as a result of sanctions, their key reserves were preserved as a result of the CBR maintaining the highest level of reserves in gold (so-called monetary gold) deposited in vaults on the territory of the Russian Federation (21.7%), as well as placing approximately 13.8% of all reserves in China. It is also important to note that the foreign exchange reserves did not comprise only the euro and the dollar, but were successively invested primarily in the renminbi (yuan), as well as, for example, the yen and the rupee[27]. The CBR policy allowed, in the new environment, to preserve the necessary means to intervene in the foreign exchange and debt markets. Also, the loss of access to SWIFT did not turn out to be, as predicted, a 'financial nuclear weapon'[28]. Despite the application of this drastic sanction, Russian banks are still able to operate and raise cash resources to conduct business and interact with external markets. This is due to the availability of various alternatives to bypass

[25] R.A. Pape, entry on LinkedIn, https://www.linkedin.com/posts/robert-pape_someone-asked-my-view-on-how-sanctions-are-activity-6970475273985171456-6ora [accessed: 5 III 2024].

[26] *Annual value of international reserves of Russia from 2012 to 2022, by type*, Statista, https://www.statista.com/statistics/1049298/russia-international-reserves-value-by-type/ [accessed: 5 III 2024].

[27] *Bank of Russia foreign exchange and gold asset management report*, Bank of Russia, Moscow 2022, https://www.cbr.ru/Collection/Collection/File/39685/2022-01_res_en.pdf [accessed: 5 III 2024].

[28] French Finance Minister Bruno Le Maire, following a meeting of EU finance ministers on 25 February 2022, expressed the opinion that the exclusion of the FR from the SWIFT international payment system should be considered as a last resort. He stated that "SWIFT is a financial nuclear weapon. (...) The fact remains that when you have a nuclear weapon in your hands, you think before you use it. Some member countries have expressed reservations, we take them into account". Translations in the text are from the author - editor's note. See: G. Leali, *France not opposed in principle to cutting Russia from SWIFT: Bruno Le Maire*, Politico, 25 II 2022, https://www.politico.eu/article/frances-le-maire-not-against-cutting-russia-out-of-swift/ [accessed: 5 III 2024]. It should be noted that it was this sanction that was considered the most drastic, which, at the time of the Russian invasion of Crimea in 2014, resulted in the rejection of calls to exclude the Russian Federation from SWIFT already at that time, as this step was considered an excessive escalation of the conflict.

the sanctions. As a result of concerns about the exclusion of the Russian banking sector from SWIFT, the CBR had already started testing a financial message transmission system, the so-called SPFS (Система передачи финансовых сообщений), during the annexation of Crimea in 2014. According to a CBR statement, by July 2023, the system was already processing 70% of domestic financial transactions[29]. However, it is not exclusively for domestic settlements. As of January 2024, it is used by 557 entities, including 157 foreign entities from 20 countries[30]. An option for circumventing sanctions is also the use of the cross-border interbank payment system - CIPS (Chinese Cross-Border Interbank Payment System) - and its possible integration with the SPFS, especially for Sino-Russian cross-border settlements.

Despite the negative impact on the economy and social conditions, sanctions have also not triggered significant political changes, but on the contrary have unleashed a large adaptive potential that has facilitated the stabilisation of the economic situation. It is projected that in the long run, as a result of increasing control of the economy and the entrenchment of the model of state capitalism, this may also contribute to further empowerment of the authorities[31].

Cryptocurrency as an object of sanctions against the Russian Federation

In February 2022, Bloomberg, citing Russian government estimates[32], reported that Russian citizens held RUB 16.5 trillion (USD 214 billion) worth of crypto assets, which represented 12% of the global total. It was estimated that more than 17 million Russians held such assets[33]. According to the Cambridge Centre for Alternative Finance (CCAF)'s 2021/2022 assessments, Russia was also one of the top

[29] *В ЦБ сообщили о 70% внутрироссийского трафика у национального аналога SWIFT*, Известия, 3 VII 2023, https://iz.ru/1538263/2023-07-03/v-tcb-soobshchili-o-70-vnutrirossiiskogo-trafika-u-natcional nogo-analoga-swift [accessed: 5 III 2024].

[30] *Российский аналог SWIFT распространяется на Восток*, News.Ru, 27 I 2024, https://news.ru/economics/rossijskij-analog-swift-rasshiryaet-svoe-vliyanie [accessed: 5 III 2024].

[31] I. Wiśniewska, *Russian economy in 2022. Adaptation and a growing budget gap*, OSW, 16 II 2023, https://www.osw.waw.pl/en/publikacje/osw-commentary/2023-02-16/russian-economy-2022-adaptation-and-a-growing-budget-gap [accessed: 5 III 2024].

[32] The estimate was based, among other things, on an analysis of the IP addresses of the largest users of cryptocurrency exchanges.

[33] E. Pismennaya, *Russia Values Local Crypto at $200 Billion as Rules Near*, Bloomberg, 1 II 2022, https://www.bloomberg.com/news/articles/2022-02-01/russia-values-local-crypto-market-at-200-billion-as-rules-near#xj4y7vzkg [accessed: 5 III 2024].

five mining centres for bitcoin - providing 4.66% of its global production[34]. Confirming fears that cryptocurrencies could be a significant loophole in the financial sanctions regime targeting Russia and a way to limit their impact, there were reported increases in trading volumes between the rouble and the major cryptocurrencies[35]. In response to this threat, the so-called *Compliance package* of 9 March 2022 relating to Belarus clarified that the non-exhaustive definition of funds in Regulation 269/2014 also includes cryptocurrencies, and the definition of economic resources may also apply to certain cryptoassets. Accordingly, cryptoassets were to be subject to the asset-freezing provisions and the prohibition on making funds or economic resources available to persons on sanctions lists. It was also considered that, for the purposes of Regulation 833/2014, transferable securities include cryptoassets with the exception of payment instruments. In addition, it was emphasised that cryptoassets should not be used to circumvent any EU sanctions[36].

However, key restrictions in this area were only introduced as part of the fifth package of sanctions on 8 April 2022. At that time, it was decided to prohibit the provision of services involving the provision of crypto wallets, accounts or cryptoasset storage to Russian nationals or natural persons resident in Russia, or legal persons, entities or bodies based in Russia, if the total value of the cryptoassets of the natural or legal person, entity or body per wallet or account provider or per cryptoasset storage entity exceeds EUR 10,000[37]. This sanction has been tightened in the Eighth Package of 5 October 2022 by adopting a total ban on such services to the above-mentioned persons and entities, regardless of the value of the wallet amount[38].

---

[34] *Bitcoin Mining Map*, CCAF, https://ccaf.io/cbnsi/cbeci/mining_map [accessed: 5 III 2024].

[35] Following the introduction of the sanctions in February 2022, an increase in turnover was particularly observed on tether and bitcoin purchase transactions, which was primarily conditioned by the initial drastic fall in the value of the rouble. See: T. Wilson, *Rouble-crypto trading soars as sanctions hit Russian currency*, Reuters, 28 II 2022, https://www.reuters.com/markets/europe/rouble-crypto-trading-soars-sanctions-hit-russian-currency-2022-02-28/ [accessed: 5 III 2024].

[36] Press release from the European Commission: *Ukraine: EU agrees to extend the scope of sanctions on Russia and Belarus*, 9 III 2022, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1649 [accessed 5 III 2024]; *Crypto-assets. Relevant provision: Article 5b(2) of Council Regulation (EU) No 833/2014. Frequently asked question*s, UE, 21 III 2023, https://finance.ec.europa.eu/system/files/2023-03/faqs-sanctions-russia-crypto_en.pdf [accessed: 5 III 2024].

[37] Article 1(18) of *Council Regulation (EU) 2022/576 of 8 April 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine.*

[38] Article 1(10) of *Council Regulation (EU) 2022/1904 of 6 October 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine.*

Cryptocurrency as a source of vulnerability in the international financial sanctions regime

Some commentators[39] did not attribute much importance to the possibility of a loophole in the financial sanctions regime. They mainly pointed to the reduced liquidity of the cryptocurrency market, which could not meet the scale of Russian needs. Hence, it was considered that the Russian Federation more broadly would not be able to replicate the strategy of Iran, which legalised cryptocurrency payments on imports in the face of sanctions. However, it should be noted that in a situation of tightening Western sanctions, the Russian side was considering formalising the possibility of using cryptocurrencies in cross-border settlements[40].

It also highlighted the error of seeing decentralisation as a guarantee that users would remain fully anonymous[41]. Blockchain technology is a public ledger of activity, enabling the monitoring of fund flows between wallets. However, this argument was dismissed in the face of the indication that identification on blockchain is based on public key addresses, rather than real identity, potentially allowing for the avoidance of sanctions when a false identity is used. Sceptics considered such a threat to be marginal in view of the fact that the majority of cryptocurrency

[39] See: *Cryptocurrencies: a way to evade sanctions?*, BAFFI – Centre on Economics, Finance and Regulation, https://baffi.unibocconi.eu/research-units/mints-alternative-monies/newsletter/issue-0/cryptocurrencies-way-evade-sanctions [accessed: 5 III 2024].

[40] The main opponent of the implementation of such a solution is the CBR which is extremely sceptical of the cryptocurrency market itself. This institution also had the greatest influence on the content of Federal Law No. 331-FZ "On the amendment of 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»", amending Federal Law No. 259-FZ "On digital financial assets, digital currency and amendments to certain legislative acts of the Russian Federation", by adding in its Article 4(10) which reads: "It is forbidden to accept digital financial assets as a means of payment or other remuneration for donated goods, work performed, services rendered, as well as in any other way allowing payment for goods (work, service) with a digital financial asset, except in cases provided for by federal laws". However, in view of the Russian Ministry of Finance's articulation of the expectation that cryptocurrencies can be used as a means of cross-border settlement, the CBR promotes the use of the digital rouble in this regard. See: *ЦБ предложил дать зарубежным банкам доступ к цифровому рублю с 2025 года*, RBC.ru, 10 X 2023, https://www.rbc.ru/finances/10/10/2023/6523e87b9a7947b24f71b430 [accessed: 5 III 2024].

[41] See: C.S. Wright, *Bitcoin Is Anything BUT Anonymous*, Bitcoin & Blockchain Tech, 1 IX 2019, https://craigwright.net/blog/bitcoin-blockchain-tech/bitcoin-is-anything-but-anonymous/ [accessed: 5 III 2024]. The concept of anonymity should be distinguished from privacy and confidentiality. Complete anonymity may be an unnecessary and in most cases undesirable element, while it is possible to maintain privacy and confidentiality while accepting the requirement to prove one's identity. Thus, privacy hides the details of a transaction from the public at large, but not from those involved in the exchange, and not from those who are authorised by law to monitor exchanges.

trading takes place with intermediaries, such as cryptocurrency exchangers and exchanges or cryptocurrency wallet providers. Due to these factors, in most jurisdictions this trading is subject to anti-money laundering and anti-terrorist financing regulations. A large number of cryptocurrency exchanges also implement Know Your Customer, KYC, principles[42].

For example, in the Polish *Act of 1 March 2018 on the prevention of money laundering and terrorist financing*, due to the introduction of a legal definition of the virtual currency concept (Article 2(2)(26)), the catalogue of obliged institutions was expanded to include entities that are engaged in the business of providing the following services: exchange between virtual currencies and means of payment, exchange between virtual currencies themselves, intermediation in their exchange, as well as maintaining their accounts (so-called wallets)[43]. As a result, entities providing such services remain obliged to fulfil AML/CFT tasks[44].

However, cryptocurrency, as mentioned, can provide solutions to avoid financial sanctions, especially individual ones. These include, for example:

- chain-hopping - involving a rapid change of cryptographic assets to make a change to the blockchain that makes it difficult to trace the flow of funds[45],
- mixers, tumblers, foggers - services that mix potentially identifiable or tainted cryptocurrency funds with others in order to make it impossible to trace their true source,
- non-hosted wallets - which allow funds to be moved without being monitored by cryptocurrency exchanges, unlike the hosted wallets they provide; however, they require disclosure if one wishes to exchange cryptocurrency

[42] KYC is a mandatory process for financial institutions to identify and verify a customer's identity when they open an account and then re-evaluate that customer on a cyclical basis.

[43] Article 2(1)(12) of the Act on the prevention of money laundering and terrorist financing recognises the aforementioned entities as obliged institutions, which, inter alia, are obliged to apply security measures in the case of an occasional transaction using virtual currency of the equivalent of EUR 1,000 or more (Article 35(1)(2)(c) of the aforementioned Act). At the same time, the activity in the field of virtual currencies itself is a regulated activity within the meaning of the provisions of the Act of 6 March 2018 - Entrepreneurs' Law and may be performed after obtaining an entry in the register of activities in the field of virtual currencies made by the Minister of Finance. At the same time, it is necessary to meet the requirements of not having a criminal record and having relevant knowledge or experience when performing this type of activity (Articles 129m-129w of the Act).

[44] AML/CFT (*Anti Money Laundering/Counter Financing of Terrorism*) – a summary definition of the rules and principles that financial service providers are required to apply to prevent money laundering and terrorist financing.

[45] This technique has been used effectively by, among others, the North Korean group Lazarus to conceal the transfer path of funds stolen from cryptocurrency exchanges.

for fiat currency. Nevertheless, it is then possible to use exchanges in jurisdictions with low AML/CFT or KYC requirements,
– privacy-oriented cryptocurrencies, the so-called privacy tokens or private coins - their use is close to the implementation of the idea of anonymous transactions, because despite the visibility of the transaction itself in the public ledger (blockchain), the addresses of the wallets of the parties to the transaction remain invisible. An example of this is the cryptocurrency monero, which uses hidden addresses in transactions to protect the privacy of the recipient[46], but for the protection of the sender uses so-called ring signatures, which involve combining the user's account key with public keys from the blockchain,
– decentralised finance (DeFi) - based on peer-to-peer (P2P) exchange[47].

Despite the importance of Financial Intelligence Units (FIUs)[48] in relation to cryptocurrencies, the key role of financial sanctions enforcement falls to commercial financial institutions. These, subject to strict supervisory regulation by states, are forced to track the sources of money flows and verify that parties to transactions are not on sanction lists. When an entity is subject to financial sanctions, it becomes necessary for it to seek alternative solutions to preserve its ability to move capital. This is where the potential of cryptoassets as an instrument for circumventing sanctions lies. The existence of digital assets in the virtual space has the fundamental advantage that financial transactions can take place bypassing monitored markets, global payment networks or strictly regulated financial systems.

At the time of the introduction of EU sanctions, the market for payment tokens (bitcoin, altcoin and stablecoin) and investment and utility tokens remained effectively outside the regulation and supervision of the EU and its member states.

Pursuant to Polish regulations, the cryptocurrency market is not identified as a financial market segment within the meaning of the provisions of the *Act of 21 July 2006 on financial market supervision*. Thus, the Polish Financial Supervision Authority only supervises the activities of virtual currency exchanges and

[46] In order to avoid recording the recipient's wallet address on the blockchain, a Stealth Address system is used in which each transaction is sent to a unique, one-off address. The recipient has access to the funds sent to the stealth address, without revealing connections to the real public wallet and transaction history.

[47] Such a catalogue of possible solutions was pointed out, among others, in the document: K.E. Busch, P. Tierno, *Russian Sanctions and Cryptocurrency*, Congressional Research Service, 4 V 2022, https://crsreports.congress.gov/product/pdf/IN/IN11920 [accessed: 5 III 2024].

[48] In Poland, the main element of the anti-money laundering and terrorist financing system is the General Inspector of Financial Information, which performs its tasks through the Financial Information Department separated within the structure of the Ministry of Finance.

bureaux de change related to the provision of payment services by these entities on the basis of the stipulations of the *Act of 19 August 2011 on payment services*.

Cryptocurrency exchanges take place through encrypted transfers between wallets using a two-key mechanism: transfers require a public key, which is the address of the wallet, and a private key, which acts as a password. Both keys are alphanumeric codes. As mentioned earlier, wallets can be custodial (trusted, hosted), which involves the investor entrusting a third party with the management and protection of its wallet keys. This results in the custodian assuming responsibility for the investor's property. At the opposite extreme are so-called non-custodial (non-trustee, non-hosted) wallets. There are important differences between these types of wallets. First and foremost, custodian wallet owners entrust their private keys to crypto-asset service providers (CASPs), while both the private and public keys of non-custodian wallets are at the sole disposal of their owners, who make transfers via P2P transactions. Service providers, being the intermediary platform, will require at least bank account or credit card details to be disclosed in order to identify the customer. Non-trusted wallets, on the other hand, do not require a trusted intermediary in the form of an external institution to guarantee the security of the transaction. The second major difference is that transactions between custodial wallets are not stored on the blockchain until the funds are withdrawn from the CASP, whereas P2P transactions are immediately recorded.

CASPs, compared to the banking sector, have far fewer enforcement tools to identify customers, despite being formally bound by the same AML/CFT requirements that apply to financial institutions. This raises difficulties for non-custodial wallets, as only some transaction data on the blockchain is recorded by P2P transfers. As a result, establishing ownership of such wallets would require linking transaction details to the IP addresses of the parties to the transaction[49].

[49] A separate problem is that illicit money transfers are also facilitated by the vulnerability of blockchain and CASPs to cyberattacks, which involves secondary vulnerabilities. An example is taking control of 51% of the blockchain's computing power (hush rate) and, as a result, gaining the ability to modify or change details of transactions that have not yet been approved. Similarly, it is possible to exploit so-called cross-chain bridges, which are decentralised platforms that ensure the transfer of tokens between separate networks and guarantee the interoperability of cryptocurrency ecosystems. At the same time, attacks enable anonymity in P2P transactions. Normally, such transfers are encrypted but not anonymous, allowing payers to be identified through details and encrypted aliases stored on the blockchain by linking transactions to personal computers via IP addresses. As this information is masked or altered on the blockchain prior to validation, cyberattacks allow illegal transactions to take place without risk of identification. In the case of CASPs, the application of criminal procedures against them is made all the easier by the fact that these institutions are custodians for many wallets.

This situation will be changed, at least in part, by the entry into force of the provisions of *Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on cryptocurrency markets and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937* (the so-called MiCA Regulation). It establishes a legal framework for service providers for both cryptocurrency and consumer protection. These regulations are intended to strengthen the protection of purchasers and holders of cryptocurrencies and, as a consequence, affect not only the security of trading but, above all, its transparency. The regulation distinguishes between three types of cryptoassets, i.e. asset-linked tokens (ART), tokens that are electronic money (EMT) and utility tokens. The provision of a crypto-asset service will only be allowed by legal entities established in an EU Member State that have been authorised as a provider of such services[50]. With that said, the MiCA regulation makes it easier for entities such as credit institutions, brokerage houses, CSDs or e-money institutions to provide them, as it does not require them to obtain a licence to provide crypto services. Only the requirement to notify the competent supervisory authority is established[51].

The MiCA Regulation pays particular attention to money laundering and terrorist financing issues in relation to sanctions. In addition to the fact that CASPs will be included in the catalogue of obliged institutions under AML, at the same time the AML and privacy (anonymity) threads refer, inter alia, to the prohibition of the release of cryptoassets that have a built-in anonymisation function[52]. A CASP operating a cryptocurrency trading platform will have to have procedures in place to prevent its infrastructure from being used for money laundering or terrorist financing purposes, and the mere exposure of the activity

[50] The application for authorisation as a cryptoasset service provider will mainly have to include: a description of the procedure and system for detecting market abuse, a description of the principles of the cryptoasset trading platform, a description of the provider's IT systems and security solutions. A register of cryptoasset service providers will be maintained by the European Securities and Markets Authority (ESMA).

[51] At the same time, it is explicitly indicated in the MiCA Regulation that certain services can only be provided by certain entities. This includes making a public offering or applying for admission to trading of EMTs, which can only be done by a credit institution or an e-money institution that is also the issuer of such a token (Article 48(1) of the MiCA Regulation). Similarly, credit institutions will not be required to obtain a licence to offer to the public or apply for admission to trading of ART. As in the case of a CASP licence, in this respect the credit institution is required to draw up an information document, appropriate documentation and to notify the supervisory authority [paragraph (44) of the preamble and Article 17 of the MiCA Regulation].

[52] Except when the CASP running the trading platform will be able to identify crypto holders and transaction history.

by the CASP's governing body to the risk of money laundering is a mandatory ground for refusal of authorisation. The lack of effective internal AML procedures, on the other hand, will be an obligatory ground for revocation of the licence. In addition, the current obligation to apply KYC procedures starting at €1,000 in the absence of any suspicion of a customer carrying out a transaction in future will be reduced to €1. This will result in an obligation to verify every transaction and thus to use financial security measures. This will significantly affect anonymity, particularly in terms of exchanging cryptocurrencies for fiat currencies. Non-EU entities will in principle lose the possibility to offer cryptocurrency services within the Union. At this point in time, however, the MiCA Regulation does not refer to the situation of entities from the European Free Trade Association (EFTA) and the European Economic Area (EEA). The territorial scope of the MiCA Regulation is, however, limited as a result of allowing third-country firms to carry out the activities covered by its scope in a reverse solicitation model, i.e. on the sole initiative of the client[53].

The MiCA regulations, in an area where they introduce transparent regulation of the flow of cryptoassets, are seen as a source of increasing the effectiveness of sanctions. However, it should be taken into account that the EU regulation will only formally take effect from 30 December 2024, with a transitional period until even 1 July 2026 during which CASPs may continue to provide services in an unregulated manner. It is important to note that the MiCA Regulation did not cover a number of sensitive issues[54], including those related to international sanctions,

[53] Based on well-established interpretations under, inter alia, the regulations of *Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU* (the so-called Markets in Financial Instruments Directive, MiFID II), however, the model of providing a service at the sole initiative of the client should not apply in situations where: undertaking promotional campaigns targeting a particular market, creating a permanent business model based on reverse solicitation, actively soliciting service recipients from another country, having a website with a particular country domain, and initiating the publication of press releases in portals or magazines dedicated to a particular market.

[54] The MiCA does not, for example, address so-called security tokens, which can be considered as tradable securities, and other cryptoassets that constitute financial instruments within the meaning of MiFID II, as well as deposits, securitisation positions and insurance and pension products. Similarly, the MiCA Regulation does not cover the issue of unique (non-fungible tokens) - (NFTs) to the most important extent, unless they replicate a financial instrument or where the issuer creates a 'pool' of assets for purchase.

which is particularly true for decentralised finance (DeFi)[55] and Central Bank Digital Currency (CBDC)[56].

With the entry into force of the MiCA Regulation, the complementary *Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying funds transfers and certain cryptoassets and amending Directive (EU) 2015/849* (hereinafter: TFR Regulation) will become applicable. It implements the recommendations of the Financial Action Task Force (FATF) on the so-called travel rule. In this respect, there will be an extension of the obligations for EU payment service providers (including CASPs) to monitor transfers of both cash and crypto-assets, which will involve the obligation to provide detailed information on the payer (originator) and recipient of the transaction (beneficiary). However, the Travel Rule, as with the MiCA, will not apply where the initiator of the transaction and the beneficiary are PSPs or CASPs acting on their own behalf, as well as in transfers between persons carried out without the involvement of a CASP (Article 2(4) of the TFR Regulation)[57].

The sanction gap of decentralised finance

As signalled earlier, paragraph (22) of the preamble of the MiCA Regulation specifies that cryptocurrency-related services, as defined in the Regulation, do not fall within the scope of regulation when provided in a fully decentralised manner, without intermediaries. Despite this, the issue of DeFi raises quite a few questions under the MiCA Regulation. For example, a problem arises regarding the provision

[55] Recital (22) of the preamble to the MiCA Regulation stipulates the exclusion of the application of the Regulation provisions to crypto services provided in a fully decentralised manner without intermediaries. However, the MiCA Regulation contains review clauses under Articles 140(2)(t) and 142(2)(a) - insofar as they relate to decentralised finance - which mandate reporting on the assessment of the development of DeFi in crypto markets and the appropriate regulatory treatment of decentralised crypto systems, including an assessment of the necessity and feasibility of regulating decentralised finance.

[56] Recital (13) of the preamble to the MiCA Regulation specifies that it does not apply to digital assets issued by central banks acting as monetary authorities, which includes CBDCs. Similarly, related services provided by these central banks acting as monetary authorities are not subject to the EU framework.

[57] The first exception follows directly from the fact that the TFR Regulation does not apply to transfers of funds for which the payer and the payee are payment service providers acting on their own account (Article 2(4)(c) of the TFR Regulation). The second exception, on the other hand, stems from the scope of Article 2(1) of the TFR Regulation, i.e. the application only to payment service providers, crypto-asset service providers or intermediary payment service providers established in the EU.

of cryptocurrency exchange services or the operation of cryptocurrency trading platforms within decentralised exchanges (so-called DEX). This is because there are problems in deciding what full decentralisation is within the meaning of the regulation. This difficulty relates to the peculiarities of the construction of the blockchain network, which results in DeFi using a hierarchical layered architecture with different purposes[58]. Under the MiCA Regulation, it remains unresolved which aspect of decentralisation is at stake, as it can be referred to both in relation to the settlement layer[59], the way cryptocurrencies are stored, and the management of the organisation and ownership of the protocol. Due to the lack of clarity in the MiCA Regulation, the assessment of the degree of decentralisation is left to the sole discretion of the crypto service provider, who is expected to define their business model through this prism.

In the current environment of technological development, it is difficult to imagine the establishment of a regulatory framework over decentralised finance that would provide a real possibility of enforcement. This is supported by the problem of defining an appropriate legal order governing market access and supervision rules, due to the high geographical dispersion of users and the lack of central entities responsible for providing services. Given this, the real gap in the international sanctions regime in the future will be decentralised finance, as a new model for organising financial transfers without any intermediaries, with the automatic execution of transactions concluded through smart contracts, which are protocols that operate on the blockchain network.

As a kind of ecosystem of decentralised financial applications based on this technology, DeFi offers the possibility of a wide range of contracts. In essence, the system replicates existing financial service models bypassing their centralised intermediaries[60]. As a result, under DeFi, users retain full control of their assets

[58] A distinction is made between three essential layers, i.e. billing, protocol and interfaces. The billing layer (layer one) consists of the distributed ledger technology (DLT) and its native resource, containing the basic principles of the ecosystem. The protocol layer (layer two) includes the compiler, providing the ability to create application programming interfaces. An application programming interface (API) is a set of definitions and protocols for building and integrating application software. In the interface layer (layer three), user-oriented applications are developed, allowing interaction with the application via a web page. See: G. Maia, J. Vieira dos Santos, *MiCA and DeFi ("Proposal for a Regulation on Market in Cryptoassets" and "Decentralised Finance")*, "Revista Electrónica de Direito" 2022, vol. 28, no. 2, pp. 63–65.

[59] In this layer, a network of nodes not relying on a central server or central organisation consists of an unprivileged blockchain through P2P connections between unrelated and independent agents.

[60] E. Avgouleas, A. Seretakis, *How Should Crypto Lending Be Regulated Under EU Law?*, "European Business Organization Law Review" 2023, vol. 24, n. 3, pp. 423–424. https://doi.org/10.1007/s40804-023-00293-3.

through synergies with the ecosystem via decentralised P2P applications. These applications also do not need entities to settle possible disputes[61], as the predetermined code will do this on its own in predictable situations, as a so-called Lex Cryptographia[62], and thus according to rules governed by self-executing smart contracts and decentralised (autonomous) organisations[63]. However, with the acceptance of the 'code is law' idea comes the effect of technology displacing state legal systems[64].

When analysing the issue of smart contract, it is important to refer to the original definition of the term proposed by Nick Szabo, who described it as a computerised transactional protocol that automatically implements the terms of a contract. The design goals are to meet typical contractual conditions, minimise the occurrence of exceptions (both malicious and accidental) and eliminate any trusted intermediaries[65]. Indeed, the idea is based on the exclusion of the need for trust between the parties due to the increased certainty of performance of the contract, as designed, as a result of the guarantee of unalterability of the contract (code). Therefore, from an economic point of view, mental and computational additional costs are reduced, lowering the losses associated with potential fraud, arbitration and enforcement costs as well as transaction costs.

---

[61] Through a probabilistic approach, blockchain solved the reconciliation issue considered in game theory, cryptography and distributed systems theory, identified in 1980 by Marshall C. Pease, Leslie Lamport and Robert Shostak as the problem of Byzantine generals. See: M. Pease, L. Lamport, R. Shostak, *The Byzantine Generals Problem*, "ACM Transactions on Programming Languages and Systems" 1982, vol. 4, n. 3, pp. 382–401. https://doi.org/10.1145/357172.357176.

[62] Blockchain significantly changes the way law is understood by detaching it from the need for any cultural backing or legitimisation by state authority. According to Katrin Becker, blockchain decouples the concept of law from the three key dimensions of territory, language (and associated interpretation) and matter. See: K. Becker, *Blockchain Matters – Lex Cryptographia and the Displacement of Legal Symbolics and Imaginaries*, "Law and Critique" 2022, vol. 33, pp. 113–130. https://doi.org/10.1007/s10978-021-09317-8.

[63] A. Wright, P. De Filippi, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, SSRN, 12 III 2015, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664, p. 4 [accessed: 5 III 2024]. http://dx.doi.org/10.2139/ssrn.2580664.

[64] D.A. Zetzsche, D.W. Arner, R.P. Buckley, *Decentralized Finance*, "Journal of Financial Regulation" 2020, vol. 6, n. 2, p. 184. https://doi.org/10.1093/jfr/fjaa010.

[65] N. Szabo, *Smart Contracts*, 1994, https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html [accessed: 5 III 2024]; the same, *Smart Contracts: Building Blocks for Digital Markets*, 1996, https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_ contracts2.html [accessed: 5 III 2024].

Currently, the term 'smart contract' is defined as an implementation code running in a blockchain environment[66]. In this sense, it is algorithmic code in a computer program, typed and based on data in a blockchain[67]. All commitments in smart contracts remain in accordance with the classical Boolean logic[68], underlying all digital processing, i.e. 'if this then that' (IFTTT).

In the context of international sanctions, an important threat to their real effectiveness is the possibility of aggregating multiple contracts by creating applications with advanced functionalities. Examples include lending platforms[69], liquidity pools[70], social media platforms or distributed asset management systems (so-called decentralised autonomous organisations). It should be emphasised that smart contracts escape the legal regulation of the MiCA Regulation, nor are they defined in Polish legislation and other legal regimes. Of course, it can be assumed that the construction of these contracts resembles a specific type of automated deposit (escrow) or electronic bill of exchange. In legal terms, a smart contract could be regarded as a special form of contract, but only on the assumption that its conclusion is based on a conscious declaration of intent by the parties that they wish

[66] V. Buterin, *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform*, 2014, https://www.weusecoins.com/assets/pdf/library/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf [accessed: 5 III 2024].

[67] R. Wilkens, R. Falk, *Smart Contracts. Grundlagen, Anwendungsfelder und rechtliche Aspekte*, Wiesbaden 2019, pp. 3–4.

[68] George Boole in 1854 created the so-called Boolean algebra - a mathematical structure consisting of three binary operations: ∨ (or, or, alternative) - an action similar to addition; ∧ (i, and, conjunction) - equivalent to multiplication; ~ (no, not, logical negation) and the distinguished elements 0 (false), 1 (true). See: S. Givant, P. Halmos, *Introduction to Boolean Algebras (Undergraduate Texts in Mathematics)*, New York 2009, pp. 8–9.

[69] The funds lent on lending platforms by their users are provided by the users themselves, and consequently the provision of funds to such services is a *staking* within the same platform. An example is the MakerDAO project that allows Ethereum (ETH) holders to lend money between community members in the form of stablecoin DAI (trying to maintain a 1:1 value to the US dollar). The system involves locking up a certain amount of ETH in smart contracts, which allows investors to mint new DAI and thus establish collateral for loans. Once the debt is repaid with interest, ETH is unlocked. However, when the value of the ETH falls below the amount borrowed in the DAI, the loan is liquidated by selling the ETH to repay the borrowed DAI. The mere threat of liquidation deters excessive borrowing. Indeed, in the event that the price of ETH falls sharply, DAI loans are liquidated, in which case Maker Token Holders (MKR) are the lenders of last resort. MKRs are created and sold to repay the loans, and all MakerDAO fees are also paid in them. Liquidation penalties, on the other hand, are used to repurchase MKRs, which are then incinerated.

[70] Liquidity pools are a collection of funds locked into a smart contract, which are the basis of decentralised exchanges (DEXs) such as Uniswap, which use smart contracts to facilitate transactions.

to enter into a contract with a specific content between themselves[71]. This content could, in principle, be code placed on the blockchain. The call of a code function on the blockchain would constitute the submission of an instruction generating the execution of a contract. However, to consider a smart contract as a contract in the sense of civil law would imply assuming that a fully informed declaration of intent actually took place. Fulfilment of this condition would require the parties to the smart contract to have created the code themselves, or at least to have the ability to read it, i.e. to know the programming language in which the smart contract was encoded[72]. The question arises as to whether it is at all possible to attribute the value of a conscious declaration of intent as to the content of the contract when the declaration is made in the form of a code. Hypothetically, such a problem could be disregarded if the smart contract was the subject of prior negotiations, the arrangements of which would be written down in natural language and only subsequently encoded in the smart contract. In that case, the code could only be treated in terms of a tool to implement contractual obligations and not as the basis for the creation of those obligations. However, there is no requirement to draft the smart contract in natural language. Furthermore, defining all elements in the code itself automatically guarantees that the parties to the smart contract remain fully anonymous.

Digital rouble – centralised cryptocurrency

Another factor related to cryptocurrencies and blockchain technology that may affect the weakening of the financial sanctions regime is the development of Central Bank Digital Currency (CBDC). The Bank for International Settlements defines CBDC as (...) *a digital payment instrument denominated in a national unit of account, representing a direct obligation of the central bank*[73].

On 1 August 2023, the provisions of Federal Law No. 339-FZ "Amending Articles 128 and 140 of Part One, Part Two and Articles 1128 and 1174 of Part Three of the Civil Code of the Russian Federation" and Federal Law No. 340-FZ "Amending Certain Legal Acts of the Russian Federation" came into force. These regulations constituted the blockchain-based digital rouble as the new national currency of the Russian Federation. The regulations defined the rules for its introduction into

[71] Article 60 of the *Act of 23 April 1964 - Civil Code*.

[72] Currently, the most prominent platform for the implementation of smart contracts is Ethereum, which implements a complete Turing programming language called Solidity.

[73] *Central bank digital currencies: foundational principles and core features*, Bank for International Settlements, 2020, https://www.bis.org/publ/othp33.pdf, p. 3 [accessed: 5 III 2024].

circulation and the conditions for its use in settlements. It also specified the powers of the CBR as the operator of its platform, as well as the role of credit institutions in carrying out transactions by customers and the organisational basis for the use of the digital rouble by natural and legal persons as a new payment method, including in operations for foreigners.

By 31 December 2024, the Board of Directors of the CBR, together with the Federal Financial Monitoring Service of the Russian Federation (Федеральная служба по финансовому мониторингу, Rosfinmonitoring), must define the scope of users of the digital rouble platform who will be authorised to carry out digital rouble transactions on the platform, as well as the list of permissible types of transactions and the threshold amounts for such operations. As originally envisaged, the possibility to access the digital rouble platform creates the need to open a digital rouble account, which is a new type of bank account. The parties to the digital rouble account contract will be the user and the CBR, and the financial institution where the user has a classical bank account will be the intermediary representing the CBR in its relations with the user in order to use the digital rouble platform. Russia is therefore replicating in this respect the positive Chinese experience with the implementation of the digital yuan (e-CNY).

The difference between cryptocurrencies and digital national currencies is fundamental. CBDC may resemble what is known as stablecoin - a digital currency (payment token) whose value is linked to a stable reserve asset in circulation (e.g. fiat currency or gold). Above all, CBDC, like stablecoin, and unlike altcoin, is (at least in theory) subject to marginal fluctuations in value. The key difference is that CBDC is, unlike cryptocurrencies, legal tender in the country of issue, backed by the government[74]. However, centralised digital national currencies, managed by national central banks, cannot provide users with full anonymity. Indeed, while both parties to a transaction will remain anonymous externally, they will no longer be anonymous from the central bank's point of view, which will give the authorities the opportunity to fully monitor financial flows in real time[75].

[74] Due to their specific nature, stablecoins could, in principle, meet the definition of e-money established by the *Act on payment services*.

[75] Such a variant refers to an account-based model, where transaction approval by the principal and beneficiary is based on verification of the users' identities, as their transactions are assigned to identity-based accounts. Another solution is a token-based CBDC, where the transaction is approved by the originator and beneficiary based on a public-private key pair and digital signatures. Such a system does not require access to the user's identity, which provides a high level of privacy. See: *Central Bank Digital Currencies. Building Block of the Future of Value Transfer*, Deloitte, https://www2.deloitte.com/content/dam/Deloitte/in/Documents/financial-services/in-fs-cbdc-noexp.pdf [accessed: 5 III 2024].

From the perspective of the state, the CBDC provides new monetary policy tools and can be an effective instrument to influence, among other things, the dynamics of the money supply in the economy. The most important objective of implementing this instrument in the context of handling cross-border exchanges is the expectation of breaking the dominance of the dollar in trade settlements. It should be noted that the full implementation of the digital rouble includes plans to launch a platform for cross-border settlements within the post-Soviet space of the Eurasian Economic Union and the Commonwealth of Independent States, as well as with regard to the BRICS countries[76]. Consequently, the development of CBDCs from the perspective of these countries could significantly contribute to the marginalisation of the importance of Western international sanctions as these countries gain the ability to make payments without foreign commercial banks and financial infrastructure such as SWIFT[77]. It is the commercial banks that are the key link in the enforcement of Western sanctions, not only because of the powers of these banks, but also because they bear the responsibility for blocking transactions involving sanctioned entities. Because of US sanctions in particular, even institutions in countries formally not applying them, if there is a dollar element or other US link, must approach transactions with the Russian side with great caution for fear of secondary sanctions being imposed on these institutions.

In this context, a digital rouble in the future could enable cross-border payments without the need to use the banking system of other countries, by handling transactions exclusively through the CBR digital rouble platform.

[76] BRICS is a form of cooperation between countries of a political and economic nature. Originally, the group comprised Brazil, Russia, India and China and, since 2011, South Africa. As of January 2024, it was to expand its membership to include more countries, namely Argentina, Egypt, Ethiopia, Saudi Arabia, Iran and the United Arab Emirates. According to the official communication, Argentina eventually dropped its plan to join the group, while in the case of Saudi Arabia, its membership is still not officially confirmed. The main objective of this group is to create a new monetary system. See: BRICS Information Portal, http://infobrics.org/ [accessed: 5 III 2024]; K. Karwowski, *Jeden statek – różni kapitanowie. Grupa BRICS po rozszerzeniu* (Eng. One ship - different captains. The BRICS group after enlargement), Instytut Nowej Europy, 20 III 2024, https://ine.org.pl/jeden-statek-rozni-kapitanowie-grupa-brics-po-rozszerzeniu/ [accessed: 26 III 2024].

[77] K. Izenman, *The Other Side of the Digital Coin: Central Bank Digital Currencies and Sanctions*, RUSI, 26 V 2021, https://rusi.org/explore-our-research/publications/commentary/other-side-digital-coin-central-bank-digital-currencies-and-sanctions [accessed: 5 III 2024].

Conclusions

The Russian case illustrates well the problem of assessing the effectiveness of economic sanctions. Under the assumption that their purpose is to discipline and punish the countries[78] on which they are imposed, sanctions applied against the Russian Federation should be considered to have fulfilled their function. They undeniably have a negative impact on the Russian economy and its financial system, limiting the authorities' available economic and political choices, resulting in greater centralisation of the economy and dependence on available trading partners. However, from the perspective of the original and primary objective of getting the Russian Federation to abandon its military offensive in Ukraine, the sanctions applied have not had the desired effect. There is also the fundamental problem that the escalating impact of economic sanctions, negatively affecting the country's economic growth and investment capacity, is accompanied by a natural tendency to create resistance to them, as the capacity to effectively circumvent them takes shape.

The analysis presented confirms the doubt indicated at the outset regarding the real effectiveness of sanctions in view of the development of innovative financial instruments. In this context, it would be wrong to overlook the growing potential of digital assets, particularly the DeFi variant and their specific type in the form of central bank digital currencies. These instruments may, in the near future, allow for the creation of new alternative channels for financial flows, independent of the currently existing Western payment systems. Their further development could carve out a sanction-free financial transaction space and make the effects of any sanctions imposed, both financially and commercially, exclusively or predominantly negative for the countries using them. What is now a niche and marginal means of evading the enforcement of international sanctions could, in the not too distant future, become a powerful tool for shaping a new international order. This will become a challenge not only for financial market supervisory regimes, but also for those responsible for countering money laundering and terrorist financing.

Unfortunately, the question of what legal measures would fully eliminate the existence of loopholes in the international financial sanctions regime cannot be answered unequivocally, particularly with regard to the caseload of large global economies, and with a view to the further development of the possibilities of using blockchain technology. It is also utopian to expect to obtain international decision-making unanimity both on the inclusion of a country in preventive measures and on the identity of the scale and type of sanctions to be applied. Nevertheless,

[78] J. Field, *Sanctions, Russia and 'crypto crime'*, CoinGeek, 7 IV 2023, https://coingeek.com/sanctions-russia-and-crypto-crime/ [accessed: 5 III 2024].

for EU countries, the postulate should be the proper and smooth implementation of the MiCA Regulation, seeking to clearly specify the legal definition of the so-called full decentralisation concept. The aim is above all to avoid a situation in which decentralised activities unjustifiably escape the regulatory framework or room for discretion on the part of regulators as to their classification is created. Thus, with regard to decentralised finance, the *condicio sine qua non* remains the development of a basic classification mechanism (taxonomy) for this concept at the level of all member states and, more broadly, on a global scale[79].

Bibliography

Avgouleas E., Seretakis A., *How Should Crypto Lending Be Regulated Under EU Law?*, "European Business Organization Law Review" 2023, vol. 24, n. 3, pp. 421–438. https://doi.org/10.1007/s40804-023-00293-3.

Becker K., *Blockchain Matters – Lex Cryptographia and the Displacement of Legal Symbolics and Imaginaries*, "Law and Critique" 2022, vol. 33, pp. 113–130. https://doi.org/10.1007/s10978-021-09317-8.

Bierzanek R., Symonides J., *Prawo międzynarodowe publiczne* (Eng. Public international law), Warszawa 2003.

Demarais A., *Backfire: How Sanctions Reshape the World Against U.S. Interests*, New York 2022.

Givant S., Halmos P., *Introduction to Boolean Algebras (Undergraduate Texts in Mathematics)*, New York 2009.

Hufbauer G.C. et al., *Economic Sanctions Reconsidered: Supplemental case histories*, Washington 2007.

Maia G., Vieira dos Santos J., *MiCA and DeFi ("Proposal for a Regulation on Market in Cryptoassets" and "Decentralised Finance")*, "Revista Electrónica de Direito" 2022, vol. 28, no. 2, pp. 57–82.

Opałek K., Wróblewski J., *Prawo. Metodologia, filozofia, teoria prawa* (Eng. Law. Methodology, philosophy, theory of law), Warszawa 1991.

[79] The need for a unified systematics for DeFi and digital assets has been signalled, among others, in the document: *Decentralised Finance – Principles for building a robust digital economy*, AFME, 6 VI 2023, https://www.afme.eu/ Portals/0/DispatchFeaturedImages/AFME%20DeFi%20Whitepaper.pdf [accessed: 5 III 2024].

Opałek K., Wróblewski J., *Zagadnienia teorii prawa* (Eng. Issues in legal theory), Warszawa 1969.

Pape R.A., *Why Economic Sanctions Do Not Work*, "International Security" 1997, vol. 22, no. 2, pp. 90–136.

Pease M., Lamport L., Shostak R., *The Byzantine Generals Problem*, "ACM Transactions on Programming Languages and Systems" 1982, vol. 4, n. 3, pp. 382–401. https://doi.org/10.1145/357172.357176.

Wilkens R., Falk R., *Smart Contracts. Grundlagen, Anwendungsfelder und rechtliche Aspekte*, Wiesbaden 2019.

Zetzsche D.A., Arner D.W., Buckley R.P., *Decentralized Finance*, "Journal of Financial Regulation" 2020, vol. 6, n. 2, pp. 172–203. https://doi.org/10.1093/jfr/fjaa010.

Internet sources

Annual value of international reserves of Russia from 2012 to 2022, by type, Statista, https://www.statista.com/statistics/1049298/russia-international-reserves-value-by-type/ [accessed: 5 III 2024].

Bank of Russia foreign exchange and gold asset management report, Bank of Russia, Moscow 2022, https://www.cbr.ru/Collection/Collection/File/39685/2022-01_res_en.pdf [accessed: 5 III 2024].

Bitcoin Mining Map, Cambridge, CCAF, https://ccaf.io/cbnsi/cbeci/mining_map [accessed: 5 III 2024].

BRICS Information Portal, http://infobrics.org/ [accessed: 5 III 2024].

Busch K.E., Tierno P., *Russian Sanctions and Cryptocurrency*, Congressional Research Service, 4 V 2022, https://crsreports.congress.gov/product/pdf/IN/IN11920 [accessed: 5 III 2024].

Buterin V., *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform*, 2014, https://www.weusecoins.com/assets/pdf/library/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf [accessed: 5 III 2024].

Central Bank Digital Currencies. Building Block of the Future of Value Transfer, Deloitte, https://www2.deloitte.com/content/dam/Deloitte/in/Documents/financial-services/in-fs-cbdc-noexp.pdf [accessed: 5 III 2024].

Central bank digital currencies: foundational principles and core features, Bank for International Settlements, 2020, https://www.bis.org/publ/othp33.pdf [accessed: 5 III 2024].

Cryptocurrencies: a way to evade sanctions?, BAFFI – Centre on Economics, Finance and Regulation, https://baffi.unibocconi.eu/research-units/mints-alternative-monies/newsletter/issue-0/cryptocurrencies-way-eva de -sanctions [accessed: 5 III 2024].

Crypto-assets relevant pro-vision: Article 5b(2) of Council Regulation (EU) No 833/2014 – frequently asked questions, Council of the EU, 21 III 2023, https://finance.ec.europa.eu/system/files/2023-03/faqs-sanctions-russia-crypto_en.pdf [accessed: 5 III 2024].

Decentralised Finance. Principles for building a robust digital economy, AFME, 6 VI 2023, https://www.afme.eu/Portals/0/DispatchFeaturedImages/AFME%20DeFi%20Whitepaper.pdf [accessed: 5 III 2024].

Field J., *Sanctions, Russia and 'crypto crime'*, CoinGeek, 7 IV 2023, https://coingeek.com/sanctions-russia-and-crypto-crime/ [accessed: 5 III 2024].

Izenman K., *The Other Side of the Digital Coin: Central Bank Digital Currencies and Sanctions*, RUSI, 26 V 2021, https://rusi.org/explore-our-research/publications/commentary/other-side-digital-coin-central-bank-digital-currencies-and-sanctions [accessed: 5 III 2024].

Karwowski K., *Jeden statek - różni kapitanowie. Grupa BRICS po rozszerzeniu* (Eng. One ship - different captains. The BRICS group after enlargement), Instytut Nowej Europy, 20 III 2024, https://ine.org.pl/jeden-statek-rozni-kapitanowie-grupa-brics-po-rozszerzeniu/ [accessed: 26 III 2024].

Leali G., *France not opposed in principle to cutting Russia from SWIFT: Bruno Le Maire*, Politico, 25 II 2022, https://www.politico.eu/article/Frances-le-maire-not-against-cutting-russia-out-of-swift/ [accessed: 5 III 2024].

Pape R.A., entry on LinkedIn, https://uk.linkedin.com/posts/robert-pape_someone-asked-my-view-on-how-sanctions-are-activity-6970475273985171456-6ora [accessed: 5 III 2024].

Pismennaya E., *Russia Values Local Crypto at $200 Billion as Rules Near*, Bloomberg, 1 II 2022, https://www.bloomberg.com/news/articles/2022-02-01/russia-values-local-crypto-market-at-200-billion-as-rules-near#xj4y7vzkg [accessed: 5 III 2024].

Press release from the European Commission: *Ukraine: EU agrees to extend the scope of sanctions on Russia and Belarus*, 9 III 2022, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1649 [accessed: 5 III 2024].

Sanctions and Restrictions Against Russia in Response to its Invasion of Ukraine, Ministry of Foreign Affairs Singapore, 5 III 2022, https://www.mfa.gov.sg/Newsroom/Press-Statements-Transcripts-and-Photos/2022/03/20220305-sanctions/ [accessed: 5 III 2024].

Szabo N., *Smart Contracts*, 1994, https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html [accessed: 5 III 2024].

Szabo N., *Smart Contracts: Building Blocks for Digital Markets*, 1996, https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html [accessed: 5 III 2024].

Wilson T., *Rouble-crypto trading soars as sanctions hit Russian currency*, Reuters, 28 II 2022, https://www.reuters.com/markets/europe/rouble-crypto-trading-soars-sanctions-hit-russian-currency-2022-02-28/ [accessed: 5 III 2024].

Wiśniewska I., *Russian economy in 2022. Adaptation and a growing budget gap*, OSW, 16 II 2023, https://www.osw.waw.pl/en/publikacje/osw-commentary/2023-02-16/russian-economy-2022-adaptation-and-a-growing-budget-gap [accessed: 5 III 2024].

Wpływ sankcji na rosyjską gospodarkę (Eng. The impact of sanctions on the Russian economy), Rada UE, https://www.consilium.europa.eu/pl/infographics/impact-sanctions-russian-economy/ [accessed: 5 III 2024].

Wright A., De Filippi P., *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, preprint, SSRN, 12 III 2015, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664 [accessed: 5 III 2024]. http://dx.doi.org/10.2139/ssrn.2580664.

Wright C.S., *Bitcoin Is Anything BUT Anonymous*, Bitcoin & Blockchain Tech, 1 IX 2019, https://craigwright.net/blog/bitcoin-blockchain-tech/bitcoin-is-anything-but-anonymous/ [accessed: 5 III 2024].

Russian Internet sources

В ЦБ сообщили о 70% внутрироссийского трафика у национального аналога SWIFT, Известия, 3 VII 2023, https://iz.ru/1538263/2023-07-03/v-tcb-soobshchili-o-70-vnutrirossiiskogo-trafika-u-natcionalnogo-analoga-swift [accessed: 5 III 2024].

ЦБ предложил дать зарубежным банкам доступ к цифровому рублю с 2025 года, RBC.ru, 10 X 2023, https://www.rbc.ru/finances/10/10/2023/6523e87b9a7947b24f71b430 [accessed: 5 III 2024].

Российский аналог SWIFT распространяется на Восток, News.Ru, 27 I 2024, https://news.ru/economics/rossijskij-analog-swift-rasshiryaet-svoe-vliyanie [accessed: 5 III 2024].

Legal acts

Council Regulation (EU) 2024/745 of 23 February 2024 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine (Official Journal of the EU L of 23 February 2024).

Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on cryptocurrency markets and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (Official Journal of the EU L 150/40 of 9 June 2023).

Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying funds transfers and certain cryptoassets and amending Directive (EU) 2015/849 (Official Journal of the EU L 150/1 of 9 June 2023).

Council Regulation (EU) 2022/1904 of 6 October 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine (Official Journal of the EU LI 259/3 of 6 October 2022).

Council Regulation (EU) 2022/576 of 8 April 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's destabilising action in Ukraine (Official Journal of the EU L 111/1 of 8 April 2022, as amended).

Council Regulation (EU) No 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine (Official Journal of the EU L 229/1 of 31 July 2014, as amended).

Council Regulation (EU) No 269/2014 of 17 March 2014 on restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine (Official Journal of the EU L 78/6 of 17 March 2014, as amended).

Council Regulation (EU) No 359/2011 of 12 April 2011 concerning restrictive measures directed against certain persons, entities and bodies in view of the situation in Iran (Official Journal of the EU L 100/1 of 14 April 2011, as amended).

Council Regulation (EC) No 765/2006 of 18 May 2006 concerning restrictive measures in view of the situation in Belarus and its involvement in Russia's aggression against Ukraine (Official Journal of the EU L 134/1 of 20 May 2006, as amended).

Act of 13 April 2022 on special solutions to prevent support for aggression against Ukraine and to protect national security (consolidated text of Journal of Laws 2023, item 1497, as amended).

Act of 6 March 2018 - Entrepreneurs' Law (consolidated text of Journal of Laws 2023, item 221, as amended).

Act of 1 March 2018 on the prevention of money laundering and terrorist financing (consolidated text of Journal of Laws 2023, item 1124, as amended).

Act of 19 August 2011 on payment services (consolidated text of Journal of Laws 2022, item 2360, as amended).

Act of 21 July 2006 on financial market supervision (consolidated text of Journal of Laws 2023, item 753, as amended).

Act of 23 April 1964 - Civil Code (consolidated text of Journal of Laws 2023, item 1610, as amended).

Russian legal acts

Федеральный закон от 31.07.2020 N 259-ФЗ "О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации", Kremlin.ru, http://www.kremlin.ru/acts/bank/45766/page/1 [accessed: 5 III 2024].

Федеральный закон от 14.07.2022 № 331-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации и о приостановлении действия отдельных положений статьи 5.1 Федерального закона «О банках и банковской деятельности»", http://publication.pravo.gov.ru/Document/View/0001202207140083?index=1 [accessed: 5 III 2024].

Федеральный закон от 24.07.2023 № 339-ФЗ "О внесении изменений в статьи 128 и 140 части первой, часть вторую и статьи 1128 и 1174 части третьей Гражданского кодекса Российской Федерации", http://publication.pravo.gov.ru/document/0001202307240009 [accessed: 5 III 2024].

Федеральный закон от 24.07.2023 № 340-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации", http://publication.pravo.gov.ru/Document/View/0001202307240024 [accessed: 5 III 2024].

Angela Pacholczak

Graduate of doctoral studies at the Faculty of Law and Administration of the University of Warsaw.

Contact: angelapacholczak@gmail.com