Is it easy to hide money in the crypto economy? The case of Russia

Armin Ahari, Johannes Duong, Jakob Hanzl, Elsa Maria Lichtenegger, Lukas Lobnik, Andreas Timel[1]

Russia's stance on crypto assets has clearly changed since its invasion of Ukraine. Throughout 2021, the Bank of Russia was set on strictly regulating crypto activities, maybe even close to all-out banning them from Russian territory in an attempt to protect investors and to close down on criminal activities. Since the invasion of Ukraine, this has clearly changed, even drastically so. Russia is now considering permitting crypto mining, investment and also payment to some extent. To shed light on possible reasons for this paradigm change, our study examines the potential for sanction evasion through the crypto economy. We show examples of countries that have already developed methods of using the crypto economy to circumvent sanctions more or less successfully. In our work, we distinguish between wealth preservation and the search for alternative payment channels for trade as two central motivations for the circumvention of sanctions, taking a deeper look into the EU sanctions regime as well as crypto market liquidity. Based on real world examples, we derive three hypothetical methods for circumventing sanctions through the crypto economy, i.e. the direct peer-to-peer system, the intermediary model and the escrow model. All these methods have major weaknesses though, and especially in light of low crypto market liquidity, we come to the conclusion that, for the time being, the crypto economy does not seem to offer sufficient potential to governments or major oligarchs for circumventing sanctions on a large scale.

JEL classification: F51, G15, O30, O38
Keywords: sanctions, cryptocurrency, crypto assets, crypto economy, Russia

Russia counts as one of the leading crypto nations. The crypto economy enjoys exceptionally high acceptance and strong adoption rates among individuals and firms. 46% of Russian internet users regularly pay for online trades and services with e-money. Globally, Russian users move around USD 16.8 billion in cryptocurrencies per year. Next to notoriously low trust in Russian banks and institutions, this may explain why Russia consistently leads the Global Crypto Adoption Index[2] (Allinger et al., 2022; Chainalysis, 2020). There have been strong efforts, though, especially by the Bank of Russia (CBR), to follow China's example and largely ban the crypto economy in Russia. The CBR sees a lot of similarities between crypto assets and financial instruments, as well as between stablecoins and money market funds. It has great concerns regarding money laundering, terrorism financing, systemic threats and proper payment function viability (CBR, 2022). That said, the internal political debate following the invasion of Ukraine in February 2022 and

[1] *Oesterreichische Nationalbank, Legal Division, armin.ahari@oenb.at, lukas.lobnik@oenb.at; Treasury – Back Office, johannes.duong@oenb.at; Supervision Policy, Regulation and Strategy Division, jakob.hanzl@oenb.at, elsa.maria.lichtenegger@s.wu.ac.at, andreas.timel@oenb.at.* *Opinions expressed by the authors of the study do not necessarily reflect the official viewpoint of the OeNB or the Eurosystem. The authors would like to thank Katharina Allinger, Elisabeth Beckmann, Katharina Ederer and Konrad Richter (all OeNB) for helpful comments and valuable suggestions. The cut-off date for this study was end-June 2022. However, selected, important developments that have occurred since then were included during the revision process (including the 8th EU sanctions package in October 2022).*

[2] *Chainalysis aggregates a number of weighted key indicators, with a particular focus on long-term behavior and tendencies, to evaluate adoption rates and usage patterns in the crypto economy across 154 countries.*

subsequent sanctions against Russia has since brought a dawn of more crypto-friendly sentiments on the part of Russian governmental institutions.

Against this backdrop, the question arises if this newly awakened interest in the crypto economy may have a deeper purpose. Could the crypto economy, for instance, open up innovative ways of circumventing sanctions? Is such an idea even plausible on a large scale? And which possible forms of circumvention could be deduced from known illegitimate practices in recent history?

In an attempt to answer a number of these questions, this paper is structured as follows: Section 1 discusses Russia's recently turbulent history in crypto policy and sheds light on crypto market developments around the Ukrainian invasion. Section 2 provides an overview of the current sanctions regime as it relates to the crypto economy. Section 3 takes a deeper look into potential motivations and methods for circumventing sanctions, also taking into account crypto market liquidity. And Section 4 offers concluding remarks on the main questions at hand.

1 The crypto economy and policy in Russia

In this section, we discuss recent developments in crypto asset regulation in Russia and the use of crypto assets since the start of the war against Ukraine.

1.1 Crypto policy in Russia

Russians are very active in crypto markets and generally share a rather appreciative public opinion of the crypto economy, regarding both mining and investments (Allinger et al., 2022). But despite this popularity, the course of future Russian regulation has been unclear for some time now. In January 2022, the CBR published a consultation paper addressed to industry and the broader public in which it suggested clear steps to reign in and even outright ban most crypto asset activities throughout Russia (CBR, 2022). With the invasion of Ukraine, this political debate took an unexpected turn again, this time toward some more flexibility but with tighter monitoring on Russian territory.

In April and June, at last, and after a lot of public speculation, a number of drafts regulating digital token activities in great detail were sent to the Federation Council of the Russian parliament. They aim to introduce new rules regulating digital currencies[3] and amend basic law on digital financial assets from 2021 (Aksakov, 2020). With these draft bills, regulators seem to aim at more detailed, specific regulation but also for more liberties in digital investing (Aksakov, 2022), digital mining (Tkachev et al., 2022) and paying with crypto assets (Aksakov, 2022). They aim to introduce improvements, for instance, for those wishing to purchase crypto assets. This will open up investment into digital assets to all Russians on a limited scale and to professional investors on an unlimited scale. Non-fungible tokens (NFTs), on the other hand, do not seem to factor into the regulatory debate at all for the time being.

Cryptos with payment function are by far the most controversial topic among Russian regulators. The Russian Ministry of Finance supports more flexible regu-

[3] *Crypto tokens in Russia are broken down into three official categories: digital financial asset (DFA), utility digital right (UDR) and digital currency. Where DFA seems to be a rather generic and UDR a technical term, "digital currency" is a new term in Russian regulation whose distinct implications are not yet clear at the time of writing.*

lation on this issue while the CBR mostly opposes it. Although the CBR has recently expressed some leniency in its stance on cryptos that are only used for international payments and do not penetrate the Russian financial system, the debate is still ongoing (Tassev, 2022a). However, there seems to be general institutional consensus that digital financial assets should not be freely used for payment but could still be viable as substitutes for existing US dollar-based financial settlements, euro or other fiat currencies to some extent.

Regarding electronic platforms, their providers will be subject to the "national payment system," which most probably means that crypto exchanges will have to be registered, will be subject to an extensive record-keeping regime and also subject to CBR rulings in many areas of crypto service provision. Non-Russian exchanges will effectively have to partner up with Russian banks if they want to offer services on Russian territory.

The debate on crypto mining is still very young and there is a clear tendency toward recognizing crypto mining as a regular business activity. Natural persons and companies looking to engage in crypto mining will be expected to register and will be monitored but seem to be subject to special allowances for higher energy consumption and lower taxation as incentives. How far minted crypto tokens may also be allowed to freely circulate inside of Russia is being hotly debated.

In addition to all these currently very lively debates, a Duma representative, who was a central figure in these initiatives, was quoted to have said that the current collapse of the crypto economy is heavily influencing all discourses, too, naturally (Tassev, 2022b).

Because of the tough requirements on identification, recordkeeping and certification, the industry, especially fintechs, reacted critically and complained that regulation could overburden smaller players while favoring bigger players and banks (Kulikova, 2022).

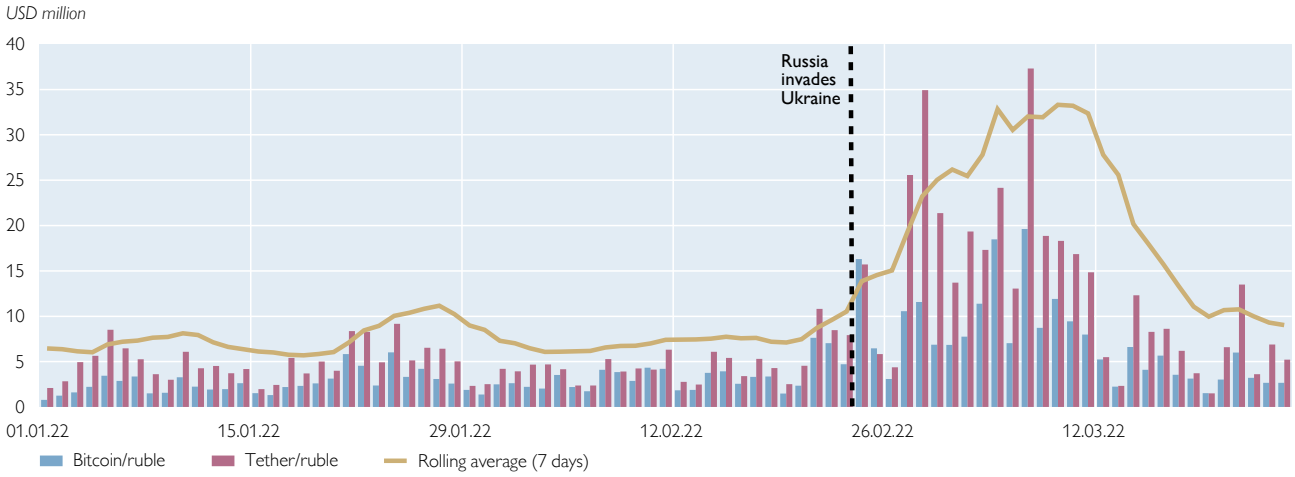
In mid-June, CBR Governor Elvira Nabiullina was quoted by the Russian newspaper Kommersant to have said that volatile crypto assets could be perfectly fine for usage in international settlements. This statement is seen as signal that the Russian government could be opening up to settlements in crypto assets with their global partners (Kolganowa, 2022). Remarkable comments similar to those of Pavel Zavalny, Chairman of the State Duma Committee on Energy, who already in March 2022 suggested accepting bitcoin as payment for Russian oil and gas exports, would fit into this line of thinking. It is still unclear if cooperative countries will be inclined to accept crypto assets as payment but if these ideas make their way into the upcoming regulation this could potentially prepare the legal ground for cryptos as money surrogate in international trade in due time (Liang, 2022).

1.2 Crypto markets in light of the invasion in Ukraine

Following the Russian attack on Ukraine, crypto assets seemed of heightened interest to both sides of the war. The Ukrainian government and companies raised crypto asset donations for various purposes and accumulated over USD 135 million by mid-May 2022 through these channels. From a Russian perspective, chart 1 shows very lively trading in crypto-ruble pairs for nearly a month before trading reverts back to normal levels.

Chart 1

Tether and bitcoin exchange for Russian ruble



Source: Kaiko.

With the beginning of the conflict, an unusually high increase in volumes of bitcoin-ruble and tether-ruble pairs can easily be observed. In an all-time high, ruble-crypto swaps with volumes as high as 37 million USD in tether and 20 million USD in bitcoin, respectively, were registered on March 7, 2022. It seems that the fears of ruble inflation dropped after the first months following the invasion, though. The crypto donations mentioned above, however, may have become a successful part of Ukraine's income model for the time being.

2 Sanctions

This section outlines sanctions passed by the EU and examines their implications for Russia as they are a central element in Russia's involvement in the crypto economy.

2.1 Definition and overview

Sanctions are targeted economic and fiscal measures imposed against a specific country in order to achieve a desired policy objective. Instead of actual warfare, sanctions attempt to create a political turnaround by increasing pressure on the relevant government. Sanctions surrounding Ukraine originally date back to the year 2014, when Russia was invading the Crimea. The European Union, besides other countries (e.g. UK, USA), introduced sanctions to change Russia's behavior against Ukraine. The sanctions imposed by the EU included asset freezes against certain persons which were involved in the Crimean politics (e.g. the "Prime Minister of Crimea").[4] Additionally, the EU introduced specific sanctions in the financial sector.[5] However, these sanctions did not lead to the intended outcome.

[4] *Council Regulation (EU) No. 269/2014 of 17 March 2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine, OJ L 2014/78, 6, as amended.*

[5] *Council Regulation (EU) No. 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilizing the situation in Ukraine, OJ L 2014/229, 1, as amended.*

In February 2022, Russian troops invaded Ukraine. As a response, far-reaching sanctions against Russia (and Belarus)[6] were introduced by the EU. Other countries like the UK, the USA and Switzerland also increased political pressure in a similar way. For the purposes of this study, we will, however, focus on EU-specific sanctions only.

Table 1

Applicability of EU sanctions by type of entity and location

	EU entities	Non-EU entities	EU citizens	Non-EU citizens
Inside EU	applicable	applicable	applicable	applicable
Outside EU	applicable	not applicable	applicable	not applicable

Source: Authors' compilation.

Regarding the applicability of EU sanctions, all citizens of EU member states and people living in the EU are subject to these measures since the sanctions regulations of the EU are directly applicable. This also covers companies inside or outside the territory of the EU that have been incorporated or constituted under the law of an EU member state as well as their representative offices in sanctioned areas and foreign companies that operate in the EU regardless of their origin. All EU companies operating in the crypto economy are therefore addressed by the sanctions regulations. On the other hand, companies and subsidiaries registered in Russia are seen as independent, liable Russian entities and are therefore not necessarily subject to the EU sanctions regulations (OeNB, 2022).

EU sanctions against Russia can be assigned to three different categories: personal sanctions (natural and legal persons), geographical sanctions (Crimea, Sevastopol, Donetsk and Luhansk) and sectoral sanctions (economic sanctions) (OeNB, 2022).

2.1.1 Personal sanctions

Personal or individual sanctions are the most severe sanctions in place. They prohibit any direct or indirect economic interaction (payment, provision of funds) with directly listed persons and with all companies that are owned or controlled by a sanctioned person.[7] Personal sanctions are also called "asset freezes" because they are aimed at freezing all funds and economic resources of the listed person. Also, no funds or economic resources shall be made available, directly or indirectly, to or for the benefit of listed persons.[8] However, sanctioned persons usually do not deal under their own name but make use of complicated corporate networks. Therefore, determining whether a company is under direct or indirect control by a sanctioned natural or legal person is of utmost importance. The European Commission has published a best practices paper in which the necessary factors for assessing ownership or control are described.[9]

As of the editorial closing date of this article, 1,262 natural persons and 118 entities were being targeted by the EU sanctions list concerning Russia.

[6] *Council Regulation (EC) No. 765/2006 of 18 May 2006 concerning restrictive measures against President Lukashenko and certain officials of Belarus, OJ L 2006/134, 1, as amended.*

[7] *E.g. if the direct or indirect ownership interest is 50% or more.*

[8] *Article 2 Council Regulation (EU) No. 269/2014.*

[9] *EU Best Practices Paper 8519/18, p. 22.*

2.1.2 Sectoral sanctions

Sectoral sanctions consist of a financial and an economic component, both specifically regulating the access to the European market.

Financial sanctions

The goal of financial sanctions is to severely restrict access to the European capital market with the intent of preventing any kind of financing via the EU. They cover transferable securities including crypto assets, money market instruments, loans and credits, stock exchanges, deposits, activities of the CBR, selective SWIFT exclusions and rating services (among other things). Additionally, it is prohibited to supply banknotes denominated in any official currency of an EU member state to Russia or to any natural or legal person, entity or body in Russia. One aspect is particularly interesting: the prohibition for EU credit institutions[10] to accept any deposits from Russian nationals or natural persons residing in Russia, or legal persons, entities or bodies established in Russia, if the total value of deposits at the credit institution exceeds EUR 100,000.[11] This prohibition was later also extended to crypto assets if a Russian natural[12] or legal person's crypto assets exceed EUR 10,000 per wallet, account or custody provider. In its latest update, the prohibition regarding crypto assets was replaced by an even more extensive provision: It is prohibited to provide any crypto asset wallet, account or custody services to Russian nationals or natural persons residing in Russia, or legal persons, entities or bodies established in Russia.[13]

Economic sanctions

Economic sanctions target different important areas of the Russian economy. The goal is to limit exports from and imports to Russia and therefore create pressure on the Russian economy. There are restrictions in the energy sector (e.g. the prohibition on importing crude oil from Russia except via pipeline which is to take effect at a later date), transport restrictions (e.g. a closure of EU airspace to all Russian-owned and Russian-registered aircrafts), restrictions on supplying Russia with goods that contribute to Russia's defense and security capabilities (e.g. dual-use goods or arms) and restrictions regarding imports of certain raw materials (e.g. iron, steel, wood, cement) from Russia into the EU as well as exports of luxury goods from the EU to Russia.

2.1.3 Regional sanctions

Although regional sanctions are an important element of the EU sanctions regime, they are mostly specific, regionalized instances of sectoral sanctions. For the purpose of analyzing the circumvention of sanctions we will therefore mainly focus on personal and sectoral sanctions.

[10] *As defined by Article 4 (1) (1) Capital Requirements Regulation – CRR (Regulation (EU) No. 575/2013 as amended).*

[11] *Article 5b Council Regulation (EU) No. 833/2014, as amended.*

[12] *As well as persons residing in Russia.*

[13] *Council Regulation (EU) 1904/2022 of 6 October 2022 which amended Article 5b Council Regulation (EU) No. 833/2014.*

2.2 Legal challenges with sanctions targeting crypto assets

To avoid the impact of the sanctions legislation, affected persons and corporations sometimes try to circumvent the rules and search for loopholes. EU legislators have found that especially crypto assets may be used to circumvent financial sanctions as well as personal sanctions. Therefore, some regulations have been extended to include the crypto market, however, often failing to target them properly.

Council Regulation (EU) No. 833/2014 for example defines that *"'transferable securities' means the following classes of securities, including in the form of crypto-assets […]."*[14] If crypto assets fulfill the requirements of *"transferable securities"* according to the MiFID[15] they are subject to the regulation regime of the MiFID anyway. However, the term *"crypto-assets"* itself lacks a clear definition. Without a conclusive definition, the legislative intention to ban crypto assets as a potential tool for circumventing sanctions regulations cannot be effectively fulfilled.

Example

The problem is illustrated by the following example: According to the sanctions regime in Council Regulation (EU) No. 833/2014, it is prohibited "to provide crypto-asset wallet, account or custody services to Russian nationals or natural persons residing in Russia, or legal persons, entities or bodies established in Russia."[16] However, the Council Regulation does not include any definition of crypto assets, wallet, account or custody provider. As long as the MiCAR[17] is not in force, the authorities as well as companies need to interpret these terms autonomously, which could potentially lead to legal uncertainty. The most sensible interpretation would be that the prohibition targets virtual asset service providers (VASPs)[18] (e.g. crypto exchanges), which need to comply with the sanctions regulations. But since the addressees of the prohibition are still not clearly defined, the provision lacks a clear scope of application.[19]

Also, Council Regulation (EU) No. 833/2014 – though it prohibits accepting deposits exceeding EUR 100,000 per EU credit institution – does not specify any reporting obligation for crypto asset wallet, account or custody services providers for crypto assets. Therefore, authorities are not able to monitor crypto stock effectively, which makes supervising these providers and monitoring compliance more difficult.

One main point of criticism has been clarified due to the latest amendment of Council Regulation (EU) No. 833/2014. In practice, compliance with the prohibition regarding crypto assets and its value threshold of EUR 10,000 was more complicated than the prohibition of accepting of deposits over EUR 100,000, since

[14] *Article 1 (f) Council Regulation (EU) No. 833/2014, as amended.*

[15] *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, OJ L 2014/173, 349, as amended.*

[16] *Article 5b (2) Council Regulation (EU) No. 833/2014 as amended.*

[17] *Proposal for a Regulation of the European Parliament and the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM(2020) 593 final 2020/0265(COD). The European Parliament and Council reached an agreement on this regulation on June 30, 2022, however, the legislative work is not yet finalized and the MiCAR is not yet in place.*

[18] *According to Article 47 AMLD (Directive (EU) No. 2015/849, as amended).*

[19] *Article 5g Council Regulation (EU) No. 833/2014 as amended.*

the value of crypto assets is highly volatile. The currently bearish market for crypto assets allowed a higher number of crypto tokens in e.g. a crypto asset account. However, if the value increased again, the value limit could have been exceeded quickly and exorbitantly.

To target crypto assets as part of the financial economy more effectively and to provide legal certainty, EU lawmakers could and should improve and *clarify the sanctions regulations* in the future. A clear and comprehensive definition of the term *"crypto-assets"* would lead to more legal certainty and support the target of preventing a possible circumvention of sanctions. A fragmentation of definitions under the MiCAR and the sanctions regulations should be avoided. Furthermore, if crypto assets are targeted by the sanctions regulations, a comprehensive reporting and monitoring system needs to be set up to be able to verify the compliance of VASPs with the regulations.

3 Circumventing sanctions: motives, models and limitations

Once we have taken a closer look at regulatory and geopolitical developments and implications, the actual motivations for circumventing current economic barriers become evident. But developing capacities for large-scale bypassing solutions is not easy. Based on observations in the global crypto economy, we found clear indications that some governments have already established a modus operandi for evading sanctions. Countries like North Korea and Iran, for instance, are successfully using or exploiting the crypto economy to markedly improve their financial situation. Later on, we will sketch the example of North Korea's systematic cyber-raids, which served as the model for our intermediary model concept.

3.1 Potential motives for circumventing sanctions

The current sanctions against Russia are supposed to hamper its business operations and relevant economic activities as much as possible. However, as the crypto market is still fairly unregulated, its continuing technical improvements could provide fruitful, discreet methods to bypass sanctions. Sanction evasion usually has clear motives, and we therefore differentiate between the motives of wealth preservation by influential individuals and keeping up sectoral trade and business by governmental parties.

3.1.1 Motive: individual wealth preservation

Personal sanctions may have the most immediate and severe impact on influential individuals. Such personalized sanctions address individuals with significant interest in preserving wealth, holdings and business contacts. Hence, high net worth individuals may find any form of effective circumvention attractive to prevent asset freezing and forced expropriation. The impact of personal sanctions becomes tangible when looking at examples of influential oligarchs cited by the media. In one representative example, speculations about frozen and lost assets since February range from 30% to 50% of individual net worth despite several early fire sale attempts (Robinson, 2022; Iain, 2022).

When seeking to evade sanctions, one of the main problems for Russian high net worth individuals is hiding their identity because of the "know your customer" (KYC) regimes most crypto exchanges enforce. Because of these regimes, most major crypto exchanges quickly were forced to put bans on Russian or even dubious

crypto accounts since they are bound by the asset freezes under the EU sanctions regulations (Bartenstein, 2022).

With these circumstances in mind, crypto assets may not be a very safe haven for wealth[20].

Two ways of crypto storage must generally be distinguished. The first one is having crypto assets stored in an *anonymous wallet*. This type of storage is accompanied by the question if asset transaction attempts from such accounts will be seen as dubious and blocked on principle. Tokens may safely and discreetly accrue in anonymous wallets but converting them into legal currency at gateways subject to KYC regimes has already become challenging and may become outright impossible in the near future.

KYC wallets (i.e. identifiable wallets) are a second option for crypto storage and trade. Identified portfolios are flexible and convenient to use. However, providers of crypto wallets and accounts in the EU and in many other countries are obliged to comply with personal identification regimes, which makes it easy to freeze assets of sanctioned persons.

3.1.2 Motive: governmental parties aiming to preserve sectoral trade

Sectoral sanctions may have a more indirect impact on Russian business capabilities than listings of natural or legal persons. They, nevertheless, could motivate ventures into rather unconventional means of payment or alternative avenues of income, at least more so than individual wealth preservation. In contrast to personalized sanctions, sectoral sanctions focus more on established import and export lines of industry and government. They therefore have a more structural and systemic impact, addressing whole sectors and groups of businesses.

However, would Russian trading partners even be willing and able to engage in crypto payment on a large enough scale? The example of Ukraine shows that manufacturers, even military grade manufacturers, are willing and able to accept crypto assets as payment (Singh, 2022). According to official statements, about 40% of Ukraine's international suppliers show willingness to accept payment against crypto assets, even NFTs (Kharif, 2022).

To better illustrate this case, we want to briefly outline two exemplary but very different sectoral business cases.

Example 1: Importing high-tech parts can be seen as vital for Russia and is naturally strictly sanctioned.[21] For goods this difficult to substitute, such as computer chips and complex software, most countries are dependent on reliable imports. Sympathetic trading partners, unmonitored trade channels und alternative payment options via the crypto economy would therefore understandably become interesting for building new, secure payment lines. Alternative payment methods aside, the challenge may still remain how to transport bespoke goods through customs checkpoints in exporting countries that have implemented sanction regimes against Russia.

Example 2: A very different business case and an example for alternative income would be the oil industry. Commodity trade often is essential for resource-rich,

[20] *The issue of asset recovery naturally affects all forms of digital tokens with value, from classic tokens like bitcoin and stablecoin to NFTs – non-fungible but tokens with inherent value nonetheless.*

[21] *E.g. Article 2a Council Regulation (EU) No. 833/2014, as amended.*

industry-focused countries, and export is a top priority. Nevertheless, import-export bans may entail an accumulation of in-country commodity supplies. Following Iran's example, there could also be an alternative use for raw materials: Oil can be utilized for cheap energy production. Iran has, for instance, generated new sources of income by subsidizing the crypto industry and crypto mining through cheap domestic energy, offering appealing licensing regimes for token mining and integrating economies of scale-oriented taxation (Reuters, 2021). Such subsidized licensing regimes seem to inspire Russia to follow suit with similar approaches, even more so if stored oil keeps piling up (Tkachev et al., 2022).

3.2 Potential models for circumventing sanctions

The essential question then is: How can sanctions realistically be circumvented? Might there already be models or concepts in place which would facilitate evasion? This paper identifies one basic system and two larger-scale models which we try to individually evaluate to determine their suitability for the aforementioned purposes (wealth preservation and governmental trade), i.e.:

- the *direct peer-to-peer system,* i.e. basic transactions between individuals who discreetly trade assets and goods;
- the *intermediary model,* which incorporates peer-to-peer trade into networks of inconspicuous middlemen of good standing;
- the *escrow model,* which incorporates payment facilitators and automates anonymous peer-to-peer trade on small to medium-scale transactions.

3.2.1 Direct peer-to-peer system

Direct peer-to-peer transactions can be seen as one of the most immediate and direct forms of trade. The concept of one wallet sending crypto assets to another wallet is as simple as it is sufficient for most regular economic activities. It can also be a viable business model for operations where discretion is of utmost importance, as the Russian ransomware industry impressively demonstrates. According to leading crypto crime analysts, Russia, as a high-risk jurisdiction, has brought forth several of the most experienced companies in the area of cybercrime, with as much as 74% of global ransomware revenue strains running straight into the business district of Moscow (Chainalysis, 2022). On top of that, unhosted wallets, anonymous accounts and bundled transaction methods (to name but a few ways of technical concealment) add a thick layer of obfuscation to such constructs. While, for instance, blockchain is a fully transparent architecture and can be analyzed thoroughly, anonymous wallets and untraceable accounts greatly reduce the informative value and impact of blockchain analyses.

Ransoms for clearing malware-infected computers are naturally payable in crypto assets and into anonymous wallets. So, quite obviously there already are professional and profitable business models that conduct their trade through opaque channels of the dark web (Ahmad et al., 2019).

The direct peer-to-peer system is the simplest basis for circumvention in that it may suffice for single or small bundle transactions even if bigger crypto volumes are involved. For systematic, ongoing or automatable trade and business, larger-scale models would be required in our opinion. These might incorporate parts of a peer-to-peer system but would need to be more reliable for large economies and

trade. In this regard, we perceive the next two models to be more fitting on a government level.

3.2.2 Intermediary model

The intermediary model rests on the idea that crypto assets will be bought, disguised, invested, further traded and sold via a network of business contacts like inconspicuous businesspeople, oligarchs, companies, crypto exchanges and public institutions (BAE Systems and SWIFT, 2020).

If we focus on the obfuscation of transactions, one of the most important components of this model is the complicit partner. Countries like the United Arab Emirates (UAE), which do not seem likely to participate in sanctions against Russia for the time being, could qualify for such a partnership. Shortly after the invasion of Ukraine, Russian wealth, including impressive crypto portfolios amounting to billions of US dollar, was shifted from sanctioning areas into other sympathizing countries without trouble. For instance, UAE-based crypto exchanges helped Russian and Belarusian clients relocate, rearrange or liquidate crypto stocks for further disposal (Alkousaa et al., 2022).

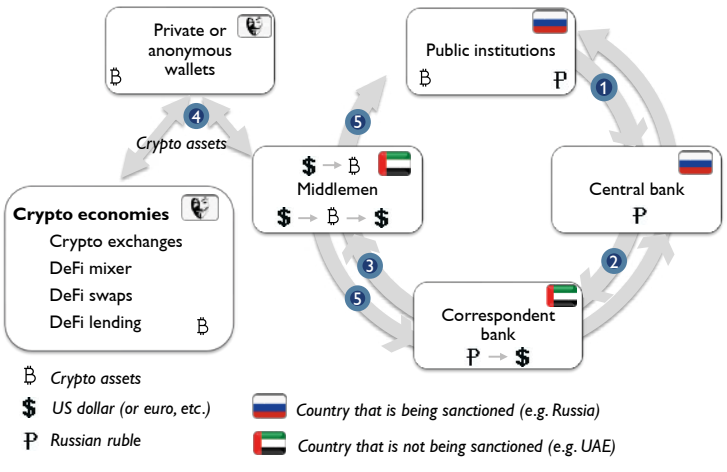
The intermediary model combines layers of middlemen that are used to cover large-scale Russian crypto activities. Looking at the process step by step, we begin in the sanctioned country, where state and state-related actors usually hold a sizable volume of assets in local currency (e.g. ruble in the case of Russia). State-related banks or central banks are then instructed to forward these funds to correspondent banks in a non-sanctioned, sympathetic country (e.g. the UAE). The correspondent bank exchanges the sanctioned country's local currency for USD or EUR, for example, and passes these funds on to intermediaries, i.e. individuals in good standing or inconspicuous enterprises, in non-sanctioned third countries. The middlemen layer changes the funds into crypto assets and moves them across multiple wallet addresses to disguise the origin of the funds and effectively tries to anonymize it. Then, the crypto asset flowback is either reconverted into fiat money (e.g. US dollar) and returned to the state bank via correspondent banks or left in the crypto economy for other purposes (e.g. crypto lending, peer-to-peer transactions or wallets of state actors for further investments).

From the perspective of a sanctioned country, the advantage of the intermediary model lies in the versatility of business opportunities and in its hypothetical potential for indirectly acquiring stable foreign cash reserves. We also see this model as the only one that is theoretically sufficiently powerful for state-level import-export requirements (the example of North Korea in box 1 validates this point).

However, the disadvantages for those seeking to evade sanctions include

Figure 1

Crypto cashflow in an intermediary model



Source: Authors' compilation.

Note: DeFi = decentralized finance.

the barrier of KYC regimes put in place in third countries to identify sanctioned actors, the potentially high complexity of such business networks and their inherent instability due to middlemen who may end up on sanctions lists themselves at any time. Although the intermediary model is freely scalable, its actual capacities depend on freely available crypto assets. If, for instance, not enough bitcoin are to be had on crypto exchanges, the amount of goods that can be bought or sold is limited as well. And as we will see in subsection 3.3, crypto market liquidity may only suffice for volumes interesting to smaller oligarchs at best.

Box 1

The intermediary model in action: cyberheists by the Democratic People's Republic of Korea

Within the last few years, the government of the Democratic People's Republic of Korea (DPRK) has consolidated its role as an advanced persistent threat (APT) to the crypto industry. Laundering crypto assets allows the state to circumvent international sanctions and finance its weapons programs. From 2017 to 2021, state-run hacker groups launched at least 32 cyber-attacks on crypto asset platforms, extracting approximately USD 1.45 billion worth of digital assets. These cybercriminals mainly target centralized exchanges and investment firms and steal funds from these institutions' internet-connected wallets by using malware, code exploits, phishing lures and advanced social engineering. The hacker groups transfer these stolen assets to DPRK-controlled wallets and further move them through multiple wallet addresses to disguise their origin – effectively using an intermediary model to mask illegal activities (Chainalysis, 2022).

A prominent example of the intermediary model in action emerged in April 2018: The Lazarus Group, a hacker group run by the DPRK, stole virtual assets worth USD 250 million from a crypto exchange (Reuters, 2022). Two Chinese citizens, acting as middlemen, received approximately USD 100 million of the stolen assets. To disguise the assets' origin, the middlemen moved the assets across addresses they held themselves. Furthermore, they transferred a portion of the assets through newly added bank accounts linked to their exchange accounts so that the crypto assets could be converted into fiat currency. Another portion of the stolen assets were transferred into Apple iTunes gift cards, which can be used to purchase additional crypto assets on certain exchanges. In March 2020, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned the two Chinese citizens (BAE Systems and SWIFT, 2020; U.S. Department of the Treasury, 2020).

Moreover, the process of laundering crypto assets, for example by sending them across different wallets, proves to be very time-consuming and may take several years. Thus, the DPRK holds large amounts of crypto assets which have not yet been converted into fiat currency. As a consequence, the current crypto crash[22] severely affects the crypto values held by the DPRK. According to analysts, unlaundered legacy crypto holdings from exchange raids between 2017 and 2021, which were worth approximately USD 170 million back then, have reduced their value to just USD 65 million as of spring 2022 (Smith, 2022).

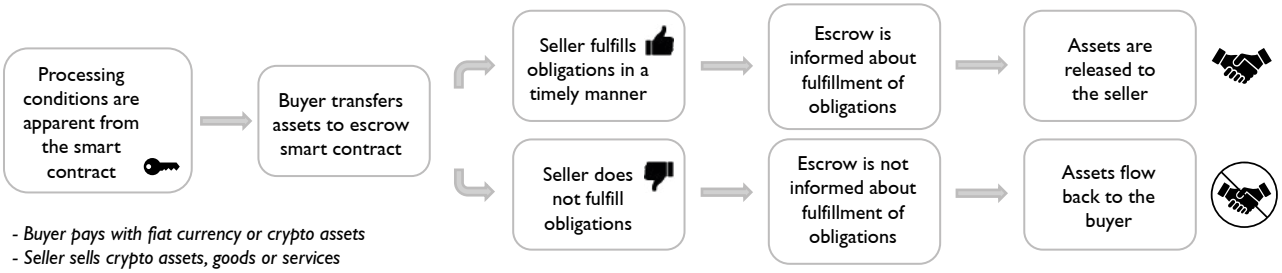
3.2.3 Escrow model

This model is derived from already existing online services that enjoy great popularity in Russia and are very advanced in their capabilities. The escrow model is established as a platform and can be seen as a partly automated, anonymized and

[22] *Amid a broader economic slowdown, crypto markets experienced a slump as a consequence of the Russian invasion in Ukraine.*

Figure 2

Escrow model process



Source: Authors' compilation.

smaller-scale variant of the intermediary model. It features an automated facilitation level and often involves trusted business partners for reputability. The model works with providers of cryptos, products or services who can place offers and, in turn, interested parties who may accept these offers. In that sense it is a marketplace that matches buyers and sellers, while escrows act as third-party intermediaries and help facilitate each trade.

The essential components of this model are anonymous buyers and sellers, and at least one internet trustee, the escrow, that acts as an intermediary in between. Terms and conditions for the transaction process are predefined by coded script or smart contract. Trading of goods and services can easily be automated. In order to complete a transaction, the predefined conditions must be met by both contracting parties, the buyer and the seller. The escrow holds the assets of the involved parties until all contracting parties fulfill their obligations (Hu et al., 2004). Escrow services are already widely used in the real estate industry: For example, Sberbank offers (classic) escrow accounts through which the purchase of real estate is processed (Mendentseva and Tokmakov, 2017; Confidus Solutions, 2022). This system could also be applied to the crypto economy and the exchange of service or goods for crypto assets (Bonneau et al., 2017).

Box 2

Example: Bitpapa

The online platform Bitpapa (bitpapa.org) presents itself as a peer-to-peer marketplace that matches buyers and sellers for the purpose of trading crypto assets. However, an escrow smart contract acts as an intermediary to settle deals and protect transactions. The website offers the opportunity to buy crypto assets like bitcoin, ether etc., offering more than 100 different payment forms. For example, Bitpapa also allows an exchange of Russian ruble for crypto assets by means of bank transfer via Sberbank or Tinkoff Bank. The deployment of a telegram bot to "connect" buyers and sellers directly (one-stop trading and settlement) allows for easy business automation. The site is currently operating in the UAE, Russia and Africa.

Bitpapa is incorporated under the laws of Ajman Media City Free Zone of the United Arab Emirates and effectively not subject to sanctions (Bitpapa, 2022).

Similar to the intermediary model, the escrow model is also versatile but less complex and easy to automate since it is based on smart contracts. KYC necessities

depend on national regulation and could, for example, be flexible in case of Russia. However, at the time of writing, we had the impression that volumes that are traded seem to be small-scale. The model could probably also have potential for larger-scale trade, but without existing examples to point to, we can only speculate. The findings presented in the next subsection regarding inferior crypto market liquidity also have large implications for the viability of this model.

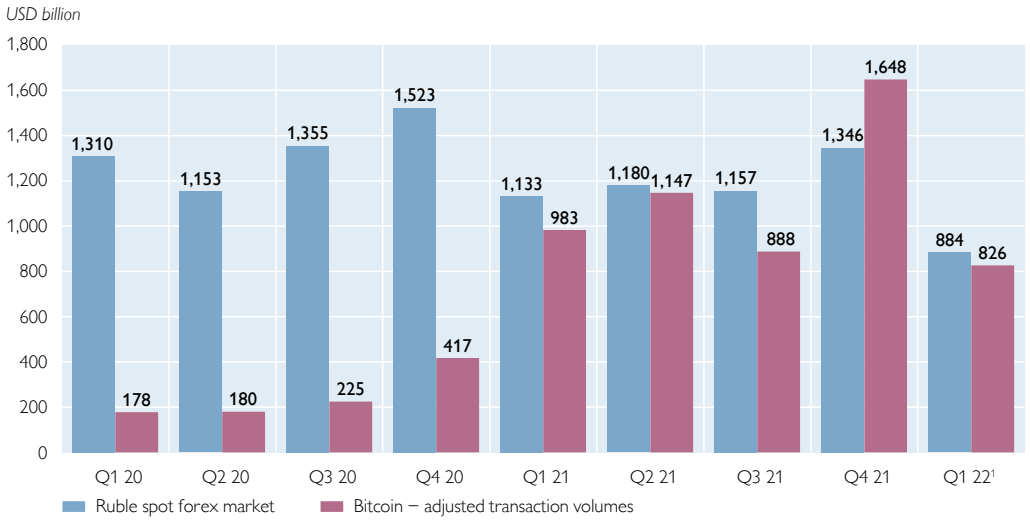
3.3 Crypto market liquidity

We have looked into potential motivations and models for circumventing sanctions, but one central question still remains unanswered: Does the crypto economy even have enough capacities available in the market for large-scale value transactions? We decided on a basic approach to this question and had a look at bitcoin transaction volumes as an indication of the available quantity of tradable tokens compared to ruble spot exchange trade volumes as a measure for capital required for Russian trade.

Based on data from Coin Metrics[23] as well as data from the CBR – and to gain a good measure for available free tokens of high value – we compared global adjusted bitcoin transaction volumes[24], as bitcoin is the crypto asset with the largest market share (about 40%) and the longest market history by far, with Russia's foreign exchange volumes.

Chart 2

Ruble spot exchange market vs. bitcoin transaction volumes



Source: Bank of Russia and Coin Metrics.

[1] Q1 22 only includes data for January and February.

[23] *https://charts.coinmetrics.io/network-data/ (accessed 12 July 2022).*

[24] *In our opinion, "transaction volumes" are a representative metric to identify non-staked, freely available and actively traded tokens on the market. Coinmetrics adjusts these transaction volumes by applying the early-spent output heuristic by Chator et al. (2017), were outputs spent within four blocks of their first expenditure are subtracted. This method reduces data distortion from e.g. wash trading or other dubious heuristics.*

This comparison reveals that, while the global bitcoin market volume rose impressively in the quarters preceding the Ukraine invasion[25], it is still not able to hold up to necessary Russian trade volumes, indicated by ruble foreign exchange volumes. In the time span from October to December 2021, when bitcoin volumes were at an extraordinary all-time high of USD 1,648 billion, the volume of all tradable bitcoins was just 22% higher than required by ruble forex trade. This means that forex compensation via, for instance, bitcoin tokens would have soaked up nearly all of bitcoin's liquidity, even in this very liquid phase. Therefore, we would not assume shifts into the crypto economy as a sustainable or even realistic perspective for ongoing large-scale business requirements. From 2020 to 2022, the average ratio of bitcoin to ruble volumes was only at 56% (44% lower than ruble spot forex demand), which shows even more clearly that it may still be a long way until bitcoin liquidity would reach any levels necessary.

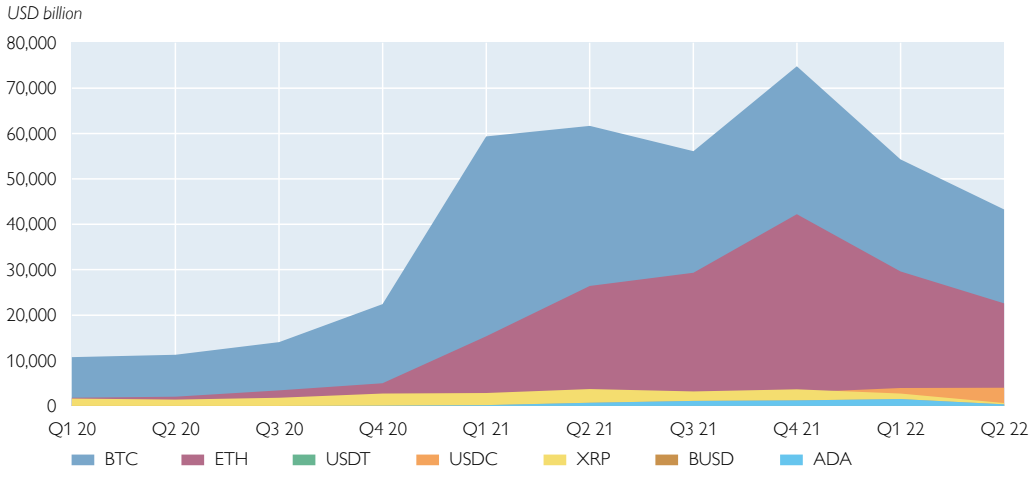
Widening the portfolio with other reasonably reliable crypto assets does not change the picture significantly either (see chart 3).

Ether is the second-most dominant crypto asset besides bitcoin and has gained significant market capitalization in the last two years, whereas the next-biggest cryptos show nowhere near the same level of capitalization. Taken together, the top seven crypto assets would raise the free-floating crypto capital to somewhere between 130% and 170% relative to ruble forex volumes[26], which also indicates a rise in volatility brought in by less dominant crypto assets. Because of the currently high uncertainty in crypto markets and uncertain Russian trade perspectives, we refrain from making any predictions with such loosely aggregated figures, though.

According to the Bloomberg Billionaires Index, the richest 15 sanctioned oligarchs have a net worth of USD 190 billion, with USD 83 billion in cash. Even

Chart 3

Free-float market capitalization of top 7 crypto assets



Source: Coin Metrics.

[25] *For the purposes of this study, we deliberately emphasize market liquidity of the pre-Ukraine war time period. Our reasoning is that we try to examine circumvention methods under ideal crypto market conditions. The current crypto market crisis only stresses the point that under worse market conditions the liquidity situation naturally becomes more critical.*

[26] *Evaluated within the period from Q1/20 to Q2/22.*

though the net worth of these individuals may theoretically fit into global quarterly crypto transaction volumes, if they all shifted their assets to the crypto economy, this would have significant effects on prices. Therefore, we conclude that even the liquidity of dominant crypto assets like bitcoin does not seem vast enough for subtly and systematically preserving wealth for major individuals. However, liquidity would probably be sufficient for minor oligarchs (Bloomberg, 2022).

We conclude that if crypto liquidity is not nearly sufficient to provide enough crypto assets for Russian foreign exchange, it most certainly is insufficient for sanction evasion on any larger scale. If used in "smaller doses" and only for selected parts of sectors or selected portfolios, there is also the problem that relevant transactions are generally sent over a transparent, public blockchain. Whether for payment purposes or wealth storage, such transactions would still be widely recognizable because of the significant sizes of value involved. Authorities could almost conveniently observe and analyze such transactions in real time (Jiang et al., 2021). Such transactions could even help countries that are trying to implement sanctions to identify intermediary model-style networks and business partners for further action.

In the months following the invasion in Ukraine, crypto prices and crypto market capitalization have dropped significantly, which further strengthens our point that, even with the most liquid crypto assets, wide-ranging sanction evasion is not viable via the crypto economy.

4 Conclusions

We started out by looking at crypto policy in Russia, showing that, while there was a lot of speculation and activity surrounding the regulation of the crypto economy in the country, Russia seems open to using it on a transnational basis. Additionally, we show that in the month following the invasion in Ukraine, crypto activity in Russia surged.

We then described the three categories of sanctions imposed by the EU (personal, sectoral and regional), showing that circumventing EU sanctions through the crypto economy is a demanding and potentially complex undertaking with bleak results for circumventors. In light of the official EU sanctions regime and leaving aside regional sanctions, different motives for sanction evasion can be directly derived from personally sanctioned individuals and from sanctions with a sectoral focus.

While influential sanctioned individuals and oligarchs would mainly be interested in preserving and securely storing their wealth, enterprises and businesses faced with sectoral sanctions would be strongly motivated to find solutions for acquiring banned components and material as well as ways to preserve their payment and financing capabilities. Any considerations of sanction evasion via the crypto economy are not made easier by the fact that inherently transparent blockchain-based transactions are currently under scrutiny at the gateways of exchange. Keeping one's anonymity by using unhosted wallets may seem attractive for obfuscating ownership but may be daunting when attempting to reconvert at exchanges with strict KYC regimes.

Furthermore, we categorized three potential methods for sanction evasion: the direct peer-to-peer system, the intermediary model and the escrow model. All three are based on cases observed in the global crypto economy and have been

applied to varying degrees. The direct peer-to-peer system is the simplest method, involving simple digital trade between two peers, and to some extent forms the basis for the other two models. As for usage on a big and systemic scale, we argue that this method is rather simple and not sufficiently automatable and scalable.

The intermediary model is a more fine-tuned and complex model for sanction evasion. It relies on the exchange of money via correspondent financial institutions in sympathetic countries and a large number of coordinated peer-to-peer transactions carried out to exchange and broadly invest crypto assets outside of the sanctioned country and then channeling them back there. While the intermediary model offers advantages like versatility for oligarchs trying to circumvent sanctions or for sanctioned states looking to keep up imports and exports in an alternative way, there are also significant downsides. There is the constant possibility that middlemen might be recognized and end up on sanctions lists themselves. Also, the model depends on highly complex business networks and dedicated efforts and costs to keep these networks running. Nevertheless, in theory, the intermediary model may be a feasible option for major oligarchs and the most viable way of systemic sanction evasion on a national level.

The escrow model builds on peer-to-peer interactions but supplements them with automated smart contracts as facilitators and reputable intermediaries providing escrow services. The escrow model is versatile, discreet and builds on an already highly accepted business model as we show in an example. That said, it still mostly qualifies for small-scale trade, and we currently do not see a larger-scale applicability of this model.

Last but not least, we examined available crypto market liquidity. We can see that the crypto economy grew significantly in the years before Russia's invasion in Ukraine, but even so, the adjusted global bitcoin transaction volumes are not sufficient to cover required ruble foreign exchange capacities. Following Russia's invasion of Ukraine, crypto valuations strongly dropped, which further underlines that crypto assets do not seem to be perceived as a viable option for large-scale sanction evasion (otherwise prices would have increased). There may be ways for businesses or parts of the economy to use the crypto economy to circumvent sanctions, but we conclude that, in the current situation, such attempts would mainly be doubtful emergency measures for preserving parts of individual wealth.

5 References

Ahmad, A., S. B. Maynard and A. Gupta. 2019. The Dark Web Phenomenon: A Review and Research Agenda. Paper presented at the 30th Australasian Conference on Information Systems. Perth, Australia.

Aksakov, A. G. 2020. Bill on Federal Law Nr. 419059-7 "On digital financial assets, digital currency and amendments to certain legal acts of the Russian Federation" **(О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации).** July 2020.

Aksakov, A. G. 2022. Drafted Bill on Federal Law Nr. 138674-8 "On Amendments to Certain Legislative Acts of the Russian Federation and on Suspension of Certain Provisions of Article 5.1 of the Federal Law 'On Banks and Banking Activities' " **(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").** July 2022.

Alkousaa, R., L. Barrington, A. Cornwell and Y. Saba. 2022. EXCLUSIVE Russians liquidating crypto in the UAE as they seek save heavens. March 11. Reuters. https://www.reuters.com/business/exclusive-russians-liquidating-crypto-uae-seek-safe-havens-2022-03-11/

Allinger, K., S. Barisitz and A. Timel. 2022. Russia's large fintechs and digital ecosystems – in the face of war and sanctions. In: Focus on European and Economic Integration Q3/22. OeNB. 47–65.

BAE Systems and SWIFT. 2020. Follow the Money: Understanding the money laundering techniques that support large-scale cyber-heists. BAE Systems. Guildford, UK, Surrey. https://www.swift.com/sites/default/files/files/swift_bae_report_Follow-The%20Money.pdf

Bartenstein, B. 2022. Binance Limits Russia Services After EU Sanctions on Crypto. April 21. Bloomberg. https://www.bloomberg.com/news/articles/2022-04-21/binance-set-to-curb-services-to-russia-users-after-eu-sanctions?leadSource=uverify%20wall

Bitpapa. 2022. Safely buy and sell cryptocurrencies with no third parties involved. https://bitpapa.com/

Bloomberg. 2022. Bloomberg Billionaires Index. Bloomberg. https://www.bloomberg.com/billionaires/

Bonneau, J., R. Gennaro, S. Goldfeder, A. Narayanan. 2017. Escrow Protocols for Cryptocurrencies: How to Buy Physical Goods Using Bitcoin. In: Kiayias, A. (ed.) Financial Cryptography and Data Security.

CBR. 2022. Cryptocurrencies: Trends, Risks, and Regulation. Bank of Russia. Moscow.

Chainalysis. 2020. The 2020 Geography of Cryptocurrency Report – Analysis of Geographic Trends in Cryptocurrency Adoption, Usage, and Regulation. September 2020.

Chainalysis. 2022. The 2022 Crypto Crime Report – Original data and research into cryptocurrency-based crime. February 2022.

Chator, A., S. Goldfeder, H. Kalodner, M. Möser and A. Narayanan. 2017. BlockSci: Design and applications of a blockchain analysis platform.

Confidus Solutions. 2022. Sberbank of Russia escrow account opening. https://www.confiduss.com/en/banks/list/the-russian-federation/sberbank-of-russia/escrow-account-open/

Hu, X., Z. Lin, A. B. Whinston and H. Zhang. 2004. Hope or Hype: On the Viability of Escrow Services as Trusted Third Parties in Online Auction Environments. Information Systems Research 15(3). 236–249.

Iain, M. 2022. Russian Billionaires Lost More Than $126 Billion In Wealth Amid Ukraine Invasion. 24 February. Forbes. https://www.forbes.com/sites/iainmartin/2022/02/24/russian-billionaires-have-lost-nearly-90-billion-in-wealth-amid-ukraine-invasion/?sh=4da8acea3a60

Jiang, X., S. Liu, X. Liu and C. Tse. 2021. Knowledge Discovery in Cryptocurrency Transactions: A Survey. In: IEEE Access.

Kharif, O. 2022. Ukraine Buys Military Gear With Donated Cryptocurrencies. March 5. In: TIME. https://time.com/6155209/ukraine-crypto/

Kolganowa, V. 2022. Набиуллина допустила использование криптовалют в международных расчетах. June 16. Kommersant. https://www.kommersant.ru/doc/5413012

Kulikova, X. 2022. Криптовалютам расписали оборот. April 15. Kommersant. https://www.kommersant.ru/doc/5306943

Liang, A. 2022. Russia considers accepting Bitcoin for oil and gas. March 25. BBC. https://www.bbc.com/news/business-60870100

Medentseva, E. and M. Tokmanov. 2017. Escrow International Experience and Perspectives of Application in Russia. In: Journal of Advances Research in Law and Economics. ASERS Publishing. Vol 8(3). 906–909.

OeNB. 2022. Leitfaden der OeNB zu Russland/Belarus-Sanktionen 2022. Version June 7, 2022. Retrieved from: https://www.oenb.at/Ueber-Uns/Rechtliche-Grundlagen/Finanzsanktionen/russland-belarus-ukraine.html

Reuters. 2021. Iran uses crypto mining to lessen impact of sanctions. 21 May. In: Reuters. https://www.reuters.com/technology/iran-uses-crypto-mining-lessen-impact-sanctions-study-finds-2021-05-21/

Reuters. 2022. U.S. ties North Korean hacker group Lazarus to huge cryptocurrency theft. April 15. Reuters. https://www.reuters.com/technology/us-ties-north-korean-hacker-group-lazarus-huge-cryptocurrency-theft-2022-04-14/

Robinson, M. 2022. Roman Abramovich and Oleg Deripaska's FROZEN fortunes: From £3BN Chelsea FC, luxury superyachts, country estates and Mayfair 'crash pads'... Russian oligarchs' multi-billion pound assets now sanctioned by UK. March 10. MailOnline. https://www.dailymail.co.uk/news/article-10597729/Roman-Abramovichs-FROZEN-fortune-including-3BN-Chelsea-FC.html

Singh, A. 2022. Ukraine Is Buying Bulletproof Vests and Night-Vision Goggles Using Crypto – Some of the military suppliers to Ukraine have crypto accounts, said the Ukraine government. March 7. CoinDesk. https://www.coindesk.com/policy/2022/03/07/ukraine-is-buying-bulletproof-vests-and-night-vision-goggles-using-crypto/

Smith, J. 2022. Crypto crash threatens North Korea's stolen funds as it ramps up weapons tests. June 29. Reuters. https://www.reuters.com/technology/crypto-crash-threatens-north-koreas-stolen-funds-it-ramps-up-weapons-tests-2022-06-28/

Tassev, L. 2022a. Crypto Payments Possible if They Don't Penetrate Russia's Financial System, Central Bank Says. news.bitcoin.com. https://news.bitcoin.com/crypto-payments-possible-if-they-dont-penetrate-russias-financial-system-central-bank-says/

Tassev, L. 2022b. Tough Crypto Law Expected in Russia Despite Central Bank's Softer Stance on Crypto Payments. https://news.bitcoin.com/tough-crypto-law-expected-in-russia-despite-central-banks-softer-stance-on-crypto-payments/

Tkachev, A. O., V. V. Plyakin, G. V. Shilkin and S. V. Avksentieva. 2022. Drafted Bill on Federal Law Nr. 127303-8 "On Mining in the Russian Federation" **(О майнинге в Российской Федерации).** July 2022.

U.S. Department of the Treasury. 2020. Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group. March 2. https://home.treasury.gov/news/press-releases/sm924