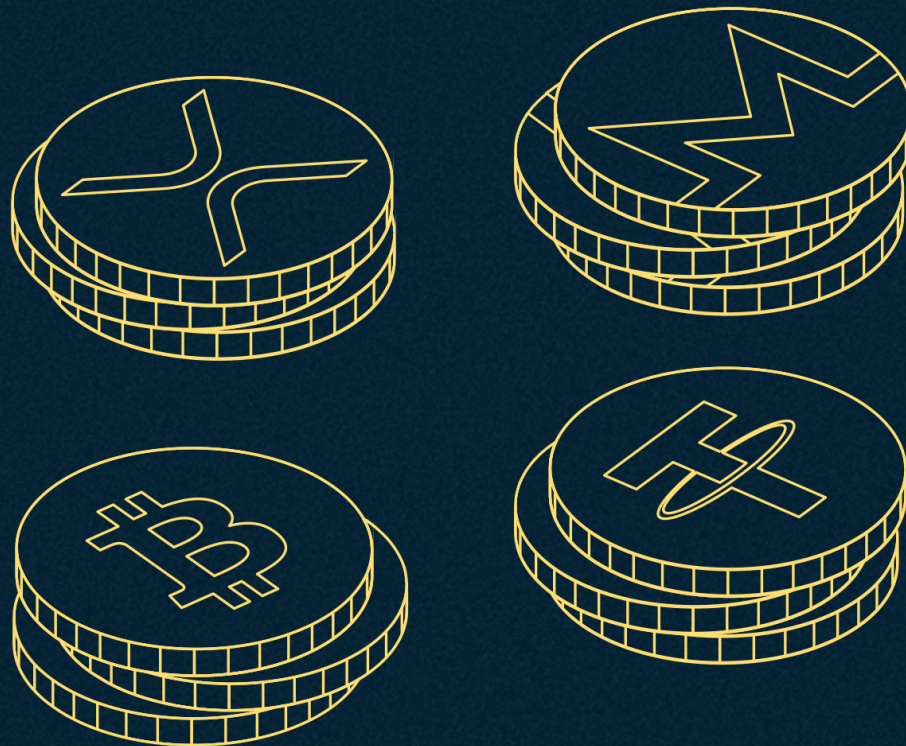




Fintech Sovereignty

Addressing the Growing Threat of Crypto-Asset Circumvention to EU Sanctions

By **Antoine Cerqueira Da Costa**

ESP Series 2, Policy Brief No. 1

Editors: **Sofia Cigolini**, **Antonia Bauk**,
and **Nuno Dias Pereira**

*European
Strategic
Policy*

EP

Sanction circumvention is an adaptation game, and crypto has dealt Russia a new hand. To prevent the erosion of sanctions effectiveness, the EU must adapt to new evasion practices and tools to better target entry points into the formal economy.

Executive Summary

Since the start of Russia's war of aggression on Ukraine, the 21 sanctions packages set out by the EU have been the union's main tool to isolate the Russian economy. However, Decentralised Finance (DeFi) has enabled the emergence of new sanctions-circumvention practices and tools, undermining the effectiveness of sanctions. In particular, the crypto-ecosystem's open-source, permissionless and non-custodial nature enables bypassing banking chokepoints that sanctions enforcement relies on.

Russia's use of these technological innovations has enabled it to adapt beyond traditional financial freezes. Sanctioned entities use on-chain and off-chain practices to bypass blockchain transparency, seamlessly funnelling

crypto into traditional finance. In response, the EU has expanded from individual listings to broad sectoral bans and restrictions on third-country platforms. Nonetheless, significant gaps persist, as the unique nature of decentralised code impedes state action.

For the EU to deal with crypto-enabled sanctions circumvention, it must update its sanctions framework to actively scrutinise the next frontier of practices and tools used by sanctioned entities, and raise its requirements for the regulated crypto-economy, while simultaneously helping those actors comply through proper information and tools. These steps are vital to avoid superficial political signalling and successfully freeze assets on blockchain ledgers.

Antoine Cerqueira Da Costa is Euro Prospects' Fintech Sovereignty Analyst within the European Strategic Policy Unit (ESP). Read the author's full description [here](#).

Euro Prospects is an independent publication focused on the analysis of European politics and policy. *ESP* is Euro Prospects' dedicated think tank unit on EU strategic policy.

Key Recommendations

| Wallet/address-level designation

To improve the ease and effectiveness of CASPs' blockchain screening procedure and give them an identifiable target to screen against, under Regulations [269/2014](#) and [833/2014](#), extend the existing designation requirements to custodial wallets and OTC addresses.

| Correspondent-banking-style duty for CASPs

To handle the one-to-two-hop laundering gap that name-matching alone can not help mitigate: amend Regulations [269/2014](#) and [833/2014](#) to turn CASPs compliance obligations into active one or two-hop tracing, using existing MiCA authorisation relationships and Travel Rule data ([Regulation 2023/1113](#)).

| Product/practice bans on privacy-enhancing protocols

To cut off suspicious transactions using privacy-enhancing protocols: adopt a delegated act under AMLR ([2024/1624 - Article 79](#)) to prohibit CASPs from interacting with addresses flagged as touching mixers, suspicious and non-compliant DEXs and SE-MEV.

| EU-level derogation mechanism for crypto-asset freezes

To avoid excessive CASPs' legal exposure in distinguishing between legitimate and suspicious transactions: amend Regulation [269/2014](#) to add crypto-asset freezes to its derogation procedures, creating a single EU-level authorisation (licence) point for CASPs processing a flagged but legitimate transaction, hosted by AMLA.

| Scaled public-private forensic tooling and sanctions-address database

To harmonise, scale and improve blockchain forensics at the EU level:

- In collaboration with the crypto industry, scale [Horizon Europe's CRYPTOACTION](#) project to build public-private forensic tooling against on-chain and off-chain circumvention techniques.
- Replace periodic sanctions list updates with a live database pairing entities, persons and wallets to map circumvention networks, hosted by the EBA through an extension of its Travel Rule mandate and shared directly with CASPs.

Analysis

DeFi and Sanctions Erosion

Since the EU adopted its very first [sanctions package](#) against Russia's war of aggression on Ukraine, Russia has continuously tried to link itself back to the financial system through circumvention.

Circumvention strategies are practices by which individuals or legal entities seek to evade the effects of restrictive measures. Sanctions rely on enforcement and checks by the country of governing jurisdiction, so circumvention tries to obscure the provenance, transparency and identification processes on which these checks rely. While the tangible part of this story is the Russian shadow fleet, which circumvents [crude oil price cap sanctions](#) (e.g. through [flags-of-convenience](#) practices), the bulk of the circumvention takes a more digital form.

Decentralised Finance (DeFi) offers Russia a range of new evasion pathways and tools. DeFi is the open financial system in which smart contracts [replace traditional financial intermediaries](#). It is most often open-source, permissionless and decentralised: a libertarian innovation to money. Yet DeFi also poses challenges to the traditional playbook of global sanctions enforcement. It is becoming an entry

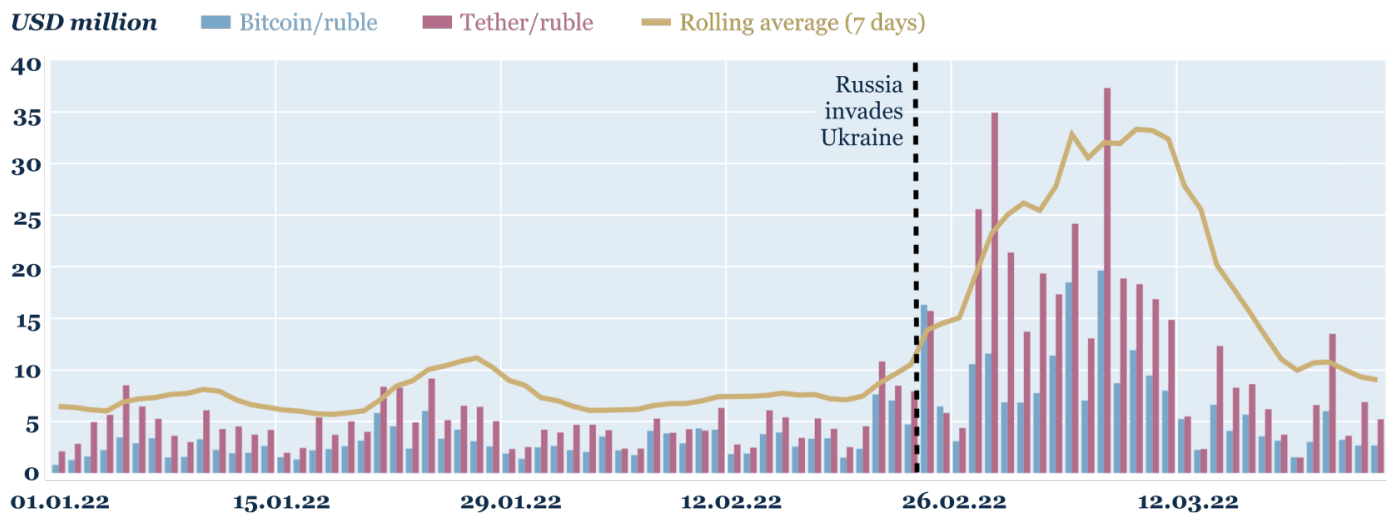
point into the traditional financial ecosystem by removing chokepoints and benefiting from less stringent oversight. DeFi fuels regulatory challenges, as it lacks legal grounding and can easily be instrumentalised for circumvention.

The Russian Adaptation Game

DeFi, especially cryptocurrencies, provides Russia with shiny new toys to innovate from. In December 2023, when US President Joe Biden issued [Executive Order 14114](#), which froze conventional Russia-China payment corridors, Russia adapted by establishing a state-backed architecture that used cryptocurrencies as a settlement tool: the [A7 network](#). Through innovative tech workarounds (VPN gateways, automated "invoicer" software for edit trade documents, etc.), particularly through the elaboration of a ruble-backed stablecoin ([A7A5](#)), Russia was able to continue settling dual-use military trades with counterparties in over [80 jurisdictions](#), including EU member states Hungary and Germany.

Post-invasion, Russia's stance on cryptocurrency has rapidly shifted. Prior to 2022, the Central Bank of Russia (CBR) considered banning crypto mining, investing and trading. A position that was quickly reversed to show support towards [crypto retail and wholesale adoption](#) and its promotion for international settlements, including the most volatile assets. In June 2023, the Governor of the CBR himself advised Russian businesses to [raise their crypto](#)

"DeFi poses challenges to the traditional playbook of global sanctions enforcement... by removing chokepoints and benefiting from less stringent oversight."

Figure 1: USDT and BTC exchange for RUB (USD Million)

Source: Ahari et al., "Is It Easy to Hide Money in the Crypto Economy? The Case of Russia."

adoption. The signs that crypto-enabled circumvention has reached a state-backed, institutional-scale, don't lie. Recent studies that expand beyond the focus on Bitcoin and Ethereum to incorporate a broader range of blockchains (USDT, XMR and XRP) support this narrative. By simply adding USDT into the equation, "an unusually high increase" in flows from RUB to blockchains becomes visible (Figure 1). In addition, cryptocurrencies have become net recipients of return spillovers from the RUB/USD exchange rate, confirming "capital flight-to-crypto" in Russia.

However, to understand the depth of Russian circumvention, volume alone is an insufficient measure. As blockchain transparency is becoming a myth, a growing number of privacy-enhancing and obfuscating practices and tools (e.g., Mixers, Privacy coins, On-Chain movements) are reducing the traceability and identification that are inherently possible on a ledger. Crypto markets do lack the liquidity to replace Russia's national foreign exchange (FX), but stopping here would be a misunderstanding of illicit finance. Circumvention oper-

ates on the margins. Through isolated transactions, targeted actors (e.g, oligarchs) use crypto to absorb only a part of their capital. In the adaptation game of circumvention, the EU is unravelling with latency the techniques and pathways that Russia has put in place since 2022.

The Tools of Crypto-Enabled Sanctions Circumvention

Because circumvention occurs below the radar, the solution is to examine every layer of the crypto system and ecosystem.

RUB stablecoins such as A7A5 and USDKG are now serving to disintermediate the USD clearing mechanism, entering SWIFT through the back door. RUB stablecoins played a key role in the \$37.8 billion in trade transactions that Russia passed through the A7 network. Russia is developing its own exchange platforms, which are proving very hard to restrain. Garantex, which had a lifetime transaction

“It is impossible to sanction on-chain code, which is largely open-source and decentralised. Targeting off-chain circumvention, specifically the bridging infrastructure to the formal economy, is a more viable option...”

volume of \$6-8 billion, saw 35% of its activity used for Russian sanctions evasion. After being sanctioned by the EU and others, the platform rebranded as Grinex and resumed operations, proving that operating under sovereign-state protection renders standard sanctions designations insufficient.

Most importantly, Russian evasion instrumentalises open-source software and protocols. The rise of anonymity-enhancing technologies (AETs) on the blockchain has come at the perfect time for circumvention. For the EU, banning significant privacy coin transactions (e.g., Monero) on Crypto-Assets Service Providers (CASPs) is only the first part of the puzzle. Scaling the practices historically used by Russian ransomware groups to blur transaction traceability, circumvention actors are increasingly turning to mixing and tumbling protocols. Tornado Cash has been the most prominent example, due to the mediatisation of its users' legal battle against the US Office of Foreign Assets Control. Ultimately, the US regulator lost the case and had to remove the protocol from its sanctions list due to its autonomous code nature. Since then, multiple other protocols have gained prominence (e.g., Blender.io and Sinbad.io), ensuring that Russia's financial movements remain invisible to blockchain tracking and forensics. Similarly, decentralised exchanges (e.g., BitPapa) or even exchanges that operate without personal identification (e.g., FixedFloat, simpleswap) all report high volume and activity in Russia.

The taxonomy of crypto-enabled circumvention tools is extensive, but can be clustered into on-chain and off-chain practices. On-chain circumvention disrupts the transparency of a public blockchain and its ledger. Off-chain circumvention exploits DeFi interoperability to layer and obscure funds. Both types of practices create ways for Russia to swap sanctioned fiat for crypto, and reverse these flows back into traditional finance. For the EU, this taxonomy should matter because it is impossible to sanction on-chain code, which is largely open-source and decentralised. Targeting off-chain circumvention, specifically the bridging infrastructure to the formal economy, is a more viable option for any regulator.

Assessing the EU's Current Response

The effectiveness of the EU's response to crypto-enabled sanctions circumvention has been growing. While the first 19 packages maintained the status quo approach by using individual listings, the 20th package signalled a promising shift. In April 2026, rather than extending listings, the EU imposed a total sectoral ban on any Russia-established crypto provider or platform, and prohibited EU entities and individuals from "netting" transactions with Russian counterparts. Effectively, this widened EU sanctions on Russia and showed that the EU was now also targeting the tools Russia used. One month later, the 21st package continued that trend, introducing the

possibility of adding crypto providers or platforms in third countries to the individual listings, and a full third-country ban, as Russia quickly responded to EU sanctions by re-domiciling (e.g., in Georgia, Panama, the UAE, Kyrgyzstan). With a delay, this path was the same as the one that led to EU banking sanctions on Russia.

However, for crypto, that path continues and can't stop here. Gaps still exist in the EU's approach, limiting the effectiveness of its sanctions. Firstly, addressing privacy coins and netting was a first step towards addressing the very practices that make the crypto environment a fertile ground for Russia's circumvention. Nevertheless, as has been observed, on-chain and off-chain practices are plentiful and widespread, and the EU needs to scrutinise the next frontier through which Russia operates.

Secondly, the EU needs to remind the world that its sanctions are not just a signalling tool. Sanctions only work when they are executed, and in the crypto ecosystem, private firms (CASPs) are the ones carrying them out. EU operating firms are legally mandated to comply, but the combination of limited practical means due to the complexity of the blockchain and the fragmented monitoring of their activity across 160 national competent authorities means that a gap most certainly exists.

The EU needs to continue affirming its answer to crypto-enabled circumvention by broadening its sanctions and placing greater demand on its crypto ecosystem. However, extending sanctions is only effective if the entities tasked with enforcement are properly equipped and supported in their compliance journey. Failing this trade-off means generating signals rather than effectively freezing assets on a ledger.

| About Euro Prospects

Euro Prospects is an independent platform for in-depth analysis of European political affairs. We publish articles and policy briefs on the issues shaping Europe today, from the EU–Mercosur trade agreement and Europe’s semiconductor supply chains to the EU’s strategic positioning on Syria and Serbia’s global arms trade.

But informing readers is only part of our Mission. Euro Prospects was founded to help cultivate a European public sphere, a transnational space of political curiosity and civic engagement among Europe’s citizens. A healthy European democracy depends on citizens who transcend pro- or anti-EU debates and instead engage in the substantive policies before them.

To this end, Euro Prospects offers a platform for reflection and debate on Europe’s politics, policies, and prospects, bringing together a diverse team from across the continent.

Visit Euro Prospects

| Partnerships

Are you an organisation interested in partnering with Euro Prospects? We are actively building relationships with researchers, institutions, and publications working on European policy. If you'd like to discuss this issue or explore ways to work together, email us.

Contact Us

| About ESP

The ESP is Euro Prospects’ dedicated think tank unit dedicated to advising on EU strategic policy across security, technology, trade, energy, industry, and digital infrastructure.

Francesco Bernabeu Fornara
Head of Unit; Editor-in-Chief, EP

Giulia Convertini
Digital Systems Sovereignty

Finn Sands Robinson
Trade & Industrial Strategy

Rimsha Arif
Energy Market Resilience

Matilde Minetti
EU-China Strategic Competition

Orla Harris
Digital Infrastructure Sovereignty

Jerfi Wigley
Supply Chain Resilience

Annika Gerbig
Defence Industrial Autonomy

Trinabh Banerjee
Strategic Digital Security

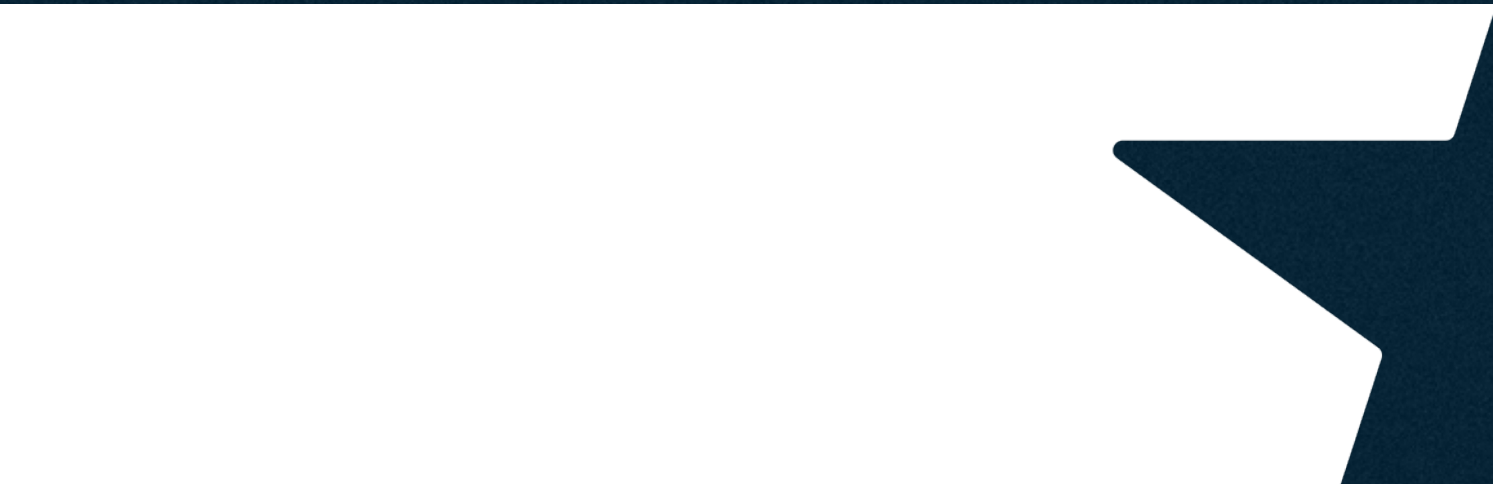
Luka Okropirashvili
Eastern Neighbourhood

Juan Carlos Leunissen
Transport & Energy Connectivity

Antoine Cerqueira Da Costa
Fintech Sovereignty Analyst

Sofia Cigolini
EU Fiscal & Monetary Sovereignty Analyst

Erik Giuliano Würthner
*ESP Outreach & Partnerships
Coordinator*



EP | *European
Strategic
Policy* 