Crypto-assets as a blind spot in sanctions against Russia?

Robby Houben

01.03.2022 doi: 10.17176/20220301-121102-0

On 24 February 2022, Russia invaded the territory of Ukraine. The international community was quick to condemn this military aggression. Immediately, the EU, US, UK, Japan and Canada issued economic and individual sanctions against Russia and Russian individuals, under which president Putin, minister Lavrov and members of the Russian State Duma. These sanctions include import and export bans, restrictions on money flows, a restricted access to bank accounts, to international capital, money and payment markets. Essentially, these sanctions are designed to dry up Russian funding for the war in Ukraine. Of course, anticipating further sanctions, Russia will have built up a reserve of assets in the immediate past, allowing the nation to bridge a period of months if not years. But, undoubtedly, the sanctions imposed the last few days will have their effect on Russian funding of the war in the foreseeable future.

Missing in today's sanctions strategy, however, is the approach to crypto-assets. This is worrying, as it is highly likely that crypto-assets are used to fund the Russian war machine without anyone really seeing it.

Why is this likely?

First of all, a significant number of crypto-assets, such as Bitcoin, are characterised by (pseudo)anonomity. This makes it difficult – and in some cases impossible – to find out who is using them. It is easily conceivable, therefore, that a state or individuals targeted by sanctions would turn to crypto-assets to continue their activities unseen and, doing so, could evade the sanctions imposed.

Secondly, crypto-assets can carry significant value. This is evidenced, for example, by Bitcoin. Nowadays more or less 19 million Bitcoins are in circulation and 1 Bitcoin is valued at approximately 35.000 Euros. Hence, the value in circulation in the form of Bitcoin is quite significant. Even if the Kremlin can use only a fraction of that value for purposes of war, amounts can still be substantial. Morever, Bitcoin is just one example of a crypto-asset. Crypto-assets today come in more than 10.000 varieties, most of which are able to be bought, traded and sold, allowing owners to move around value.

Thirdly, as of today, crypto-assets largely escape regulation and supervision. Virtual currencies are already included in the scope of EU anti-money laundering legislation, and crypto-asset exchanges and custodian wallet providers are already anti-money laundering gatekeepers (see the EU Directive on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing), yet there are still important blind spots, such as token based transactions, transactions via crypto-to-crypto-exchanges, the mining of coins, and so forth (see my analysis with Alexander Snyers e.g. in a 2018 and a 2020 study for the European Parliament, and our chapter on Cryptoassets and financial crime: a European Union perspective, in K.T. Liaw (ed.) The Routledge handbook of FinTech, 2021). Additional regulatory efforts are in the making, especially the enlargement of the scope of the so-called 'travel rule', denoting information sharing duties in the context of transfers (see the Proposal for an EU Regulation on information accompanying transfers of funds and certain crypto-assets), but are not yet a reality.

Fourthly, numbers show that crypto-assets are already quite widely adopted in the region, and the scenario is therefore definitely not utopian.

These are all factors explaining why crypto-assets can be – and probably already are – used as a means to fund Russia's war against Ukraine, going largely unde-

tected, and outside of the scope of the economic and individual sanctions currently in place. Moreover, reportedly, the Russian government is experimenting with the digital Ruble. Once operational, a digital Ruble will allow transactions with whoever is willing to engage outside of traditional banks and traditional payment infrastructure, further adding to the 'alternative funding toolbox'.

Funding of war through crypto-assets is a real threat, but should be put into perspective too. Crypto-assets will not in themselves allow the Kremlin to continue to finance the war in Ukraine. For instance, crypto markets are sizable, but still a lot smaller than other traditional markets, such as FX markets. Furthermore, crypto-assets that are not stablecoins can be highly volatile, making them less suitable to carry value than traditional money. Another element is that possessing crypto-assets is one thing, but acquiring them (via exchanges) is another and, especially in current circumstances, potentially a lot less easy or secure. Lastly, and interestingly, there is also another side to the 'crypto-warcoin': reportedly, private actors have transferred Bitcoins to Ukraine too, so as to allow them to fund their defence against Russia.

Policy considerations

Policy makers should be aware that crypto-assets likely contribute to Russia's funding of the war in Ukraine, and they should adequately address that risk. Crypto-assets should immediately be included in the scope of the sanctions against Russia. This may seem contradictory to the (pseudo)anonymous nature of the crypto-assets used to fund the war, yet it is not. It is a necessary first step, because as long as crypto-assets are not in scope of the sanctions, funding the war via crypto-assets does not constitute an infraction of the sanctions. Subsequently, the fundamental issue is to be able to trace the crypto-assets used for the funding of war and link them to the Kremlin. This is a task for law enforcement agencies. Therefore, at the same time as including crypto-assets in the scope of the sanctions, law enforcement agencies who are able to trace the use of crypto-assets to fund war should be reinforced. This is a viable strategy: although not easy, law enforcement agencies are increasingly effective in detecting criminal use of crypto-assets and thereby piercing the shield of anonimity, at least for those crypto-assets that are pseudo-anonymous, as is evidenced for example by the EU Titanium-project, the recent establishment of an FBI Cryptocurrency Unit adding to the growing US enforcement measures taken to stop crypto crimes and recent succesful Bitcoin seizures. The approach becomes even more effective when private crypto-actors reach out to government agencies and offer a helping hand. Increasing levels of cybersecurity to prevent theft of crypto-assets or ransomware attacks is equally relevant.

Furthermore, at EU regulatory level, the expansion of the scope of the 'travel rule' to crypto-asset transactions can be sped up, so that crypto-asset transactions via crypto-asset service providers will have to be accompanied by payment information, including identities of payer and payee, making it easier to identify and sanction criminal use cases. Additionally, the scope of the anti-money laundering rules relating to crypto-assets should once again be reconsidered against the background of the Russian aggression today. For example, it could be considered to what extent digital state currencies, such as the digital Ruble, are in need of further anti-money laundering scrutiny.

Crypto-assets and especially their underlying technology provide for valuable societal use cases. The lawful crypto-asset market and crypto-asset service providers should therefore receive full regulatory support to further develop their activities in a legally certain, and thus regulated, environment. This is what the envisaged Markets in Crypto-Assets Regulation (see the Proposal for a Regulation on Markets in Crypto-assets) is attempting to achieve, and rightly so. Furthermore, it is not crypto-assets that are flawed. It is the use of crypto-assets for criminal purposes that is reprehensible and it is that use that should be targeted.

In this respect, it is not appropriate to be naive. The features of certain crypto-assets, especially (pseudo)anonimity, make them attractive for nations gone rogue and in need of funding. The latter has

remained largely theoretical so far, but is now more than ever topical.

ABOUT THE AUTHOR

Robby Houben

Robby Houben is a professor corporate and capital markets law at the University of Antwerp.Robby Houben is Professor of Sports Law & Business at the University of Antwerp. He is the founder of the Football College powered by UAntwerp.

SUGGESTED CITATION

Houben, Robby: Crypto-assets as a blind spot in sanctions against Russia?, Verfassungsblog, 01.03.2022, doi: 10.17176/20220301-121102-0.

Licensed under CC BY-SA 4.0.

Langzeitarchiviert bei IntRechtDok unter: doi.org/10.17176/20220301-121102-0.