The New York Times https://www.nytimes.com/2022/02/23/business/russia-sanctions-cryptocurrency.html

Russia Could Use Cryptocurrency to Blunt the Force of U.S. Sanctions

Russian companies have many cryptocurrency tools at their disposal to evade sanctions, including a so-called digital ruble and ransomware.


By Emily Flitter and David Yaffe-Bellany

Published Feb. 23, 2022 Updated Feb. 24, 2022

When the United States barred Americans from doing business with Russian banks, oil and gas developers and other companies in 2014, after the country's invasion of Crimea, the hit to Russia's economy was swift and immense. Economists estimated that sanctions imposed by Western nations cost Russia $50 billion a year.

Since then, the global market for cryptocurrencies and other digital assets has ballooned. That's bad news for enforcers of sanctions, and good news for Russia.

On Tuesday, the Biden administration enacted fresh sanctions on Russia over the conflict in Ukraine, aiming to thwart its access to foreign capital. But Russian entities are preparing to blunt some of the worst effects by making deals with anyone around the world willing to work with them, experts said. And, they say, those entities can then use digital currencies to bypass the control points that governments rely on — mainly transfers of money by banks — to block deal execution.

"Russia has had a lot of time to think about this specific consequence," said Michael Parker, a former federal prosecutor who now heads the anti-money-laundering and sanctions practice at the Washington law firm Ferrari & Associates. "It would be naïve to think that they haven't gamed out exactly this scenario."

Sanctions are some of the most powerful tools the United States and European countries have to influence the behavior of nations they don't consider allies. The United States in particular is able to use sanctions as a diplomatic tool because the dollar is the world's reserve currency and used in payments worldwide. But American government officials are increasingly aware of the potential for cryptocurrencies to lessen the impact of sanctions and are stepping up their scrutiny of digital assets.

To apply sanctions, a government makes a list of people and businesses its citizens must avoid. Anyone caught engaging with a member of the list faces heavy fines. But the real key to any effective sanctions program is the global financial system. Banks around the world play a major role in enforcement: They see where money comes from and where it's bound, and anti-money-laundering laws require them to block transactions with entities that are under sanctions and report what they see to authorities. But if banks are the eyes and ears of governments in this space, the explosion of digital currencies is blinding them.

President Biden said his administration would impose sanctions on Russia “far beyond” those the country faced in 2014 after its invasion of Crimea. Al Drago for The New York Times

Banks have to abide by “know your customer” rules, which include verifying their clients’ identities. But exchanges and other platforms that facilitate the buying and selling of cryptocurrencies and digital assets are rarely as good at tracking their customers as banks are, even though they are supposed to follow the same rules. In October, the U.S. Treasury Department warned that cryptocurrencies posed an increasingly serious threat to the American sanctions program and that U.S. authorities needed to educate themselves about the technology.

Should it choose to evade sanctions, Russia has multiple cryptocurrency-related tools at its disposal, experts said. All it needs is to find ways to trade without touching the dollar.

The Russian government is developing its own central bank digital currency, a so-called digital ruble that it hopes to use to trade directly with other countries willing to accept it without first converting it into dollars. Hacking techniques like ransomware could help Russians steal digital currencies and make up revenue lost to sanctions.

And while cryptocurrency transactions are recorded on the underlying blockchain, making them transparent, new tools developed in Russia can help mask the origin of such transactions. That would allow businesses to trade with Russian entities without detection.

There is a precedent for these kinds of workarounds. Iran and North Korea are among countries that have used digital currencies to mitigate the effects of Western sanctions, a trend that U.S. and United Nations officials have recently observed. North Korea, for instance, has used ransomware to steal cryptocurrency to fund its nuclear program, according to a U.N. report.

The offices of the Central Bank of Russia in Moscow. In 2020, representatives for the bank said a new "digital ruble" would help the country mitigate sanctions. Alexander Shcherbak\TASS via Getty Image

In October 2020, representatives of Russia's central bank told a Moscow newspaper that the new "digital ruble" would make the country less dependent on the United States and better able to resist sanctions. It would let Russian entities conduct transactions outside the international banking system with any country willing to trade in digital currency.

Russia could find willing partners in other nations targeted by U.S. sanctions, including Iran, that are also developing government-backed digital currencies. China, Russia's largest trading partner in both imports and exports, according to the World Bank, has already launched its own central bank digital currency. The country's leader, Xi Jinping, recently described China's relationship with Russia as having "no limits."

The developing system in which central banks directly exchange digital currencies creates new risks, said Yaya Fanusie, a fellow at the Center for a New American Security who has studied the effects of cryptocurrency on sanctions. "The lessening of U.S. sanctions power comes from a system where these nation-states are able to do transactions without going through the global banking system."

In early February, independent sanctions monitors told the U.N. Security Council that North Korea was using cryptocurrencies to fund its nuclear and ballistic missile program, according to Reuters. (A spokesman for Norway's permanent mission to the U.N. confirmed the existence of the report, which has not yet been made public.) In May, the consulting firm Elliptic described how Iran was using revenue from Bitcoin mining to make up for the limitations on its ability to sell oil because of sanctions.

Russian entities that are under sanctions could deploy their own evasion strategy, using ransomware attacks. The playbook is straightforward: A hacker breaks into computer networks and locks up digital information until the victim pays for its release, usually in cryptocurrency.

Russia's Attack on Ukraine and the Global Economy

A rising concern. Russia's attack on Ukraine could cause dizzying spikes in prices for energy and food and could spook investors. The economic damage from supply disruptions and economic sanctions would be severe in some countries and industries and unnoticed in others.

Russia is at the center of the growing ransomware industry. Last year, about 74 percent of global ransomware revenue, or more than $400 million worth of cryptocurrency, went to entities that are probably affiliated with Russia in some way, according to a Feb. 14 report by the blockchain-tracking firm Chainalysis.

The Moscow International Business Center. Newly developed tools have made it possible for Russian entities to trade with other businesses without being detected. Sergey Ponomarev for The New York Times

Illegal funds have also flowed into Russia through a dark web marketplace called Hydra, which is powered by cryptocurrency and handled more than $1 billion in sales in 2020, according to Chainalysis. The platform's strict rules — sellers are allowed to liquidate cryptocurrency only through certain regional exchanges — have made it difficult for researchers to follow the money.

“We know that there’s no questions asked, and we know that Hydra operates not just throughout Eastern Europe but throughout Western Europe,” said Kim Grauer, director of research at Chainalysis. “There’s definitely cross-border business happening.”

Digital currencies all use blockchain technology, a form of computer code that is publicly viewable by anyone, anywhere. This public ledger keeps track of the movements of individual digital coins from one “wallet” — as online repositories for digital assets are called — to another. In theory, this should let authorities track all crypto transactions and keep restricted entities from completing them.

But the technology behind Hydra masks the source of transactions, offering a potential tool for Russian users to move money outside the country’s borders. On its own, Hydra is not yet big enough to handle the volume of transactions that Russia would need to successfully evade sanctions. But other money-laundering techniques — including “nesting,” in which an illicit marketplace buries itself within a larger, legitimate structure to hide its activities — could also help.

There are signs that the United States is stepping up its monitoring of cryptocurrency activity. On Feb. 17, the Justice Department announced that it had created a new national cryptocurrency enforcement team, a move that seemed to emphasize that federal prosecutors were paying extra attention to bad behavior among cryptocurrency users.

Mr. Parker, the former prosecutor, said the Feb. 8 arrests of a Manhattan couple for stealing $3.6 billion in Bitcoin from the Hong Kong cryptocurrency exchange Bitfinex were “a tangible example of the government getting very good and up to speed on what they need to do to be able to trace this.”

Administration officials are also urging the cryptocurrency industry to put into place internal controls that prevent bad actors from using their services. In October, the Treasury Department published a 30-page sanctions-compliance manual recommending that cryptocurrency companies use geolocation tools to weed out customers in restricted jurisdictions. In many cases, the report said, crypto companies have taken months or years to carry out such compliance procedures.

That may change as the industry starts to mature. Chainalysis offers a “know your transaction” tool that alerts companies when blacklisted entities use their services. Last year, the company doubled its number of private-sector customers, many of whom use the compliance tool.

But savvy cryptocurrency users can find ways around a blacklist.

“A Treasury designation of a crypto wallet address is not foolproof,” said Mr. Fanusie of the Center for a New American Security. “That designated actor can still open up a new wallet elsewhere. You can do that quite easily.”