Congressional Research Service
Informing the legislative debate since 1914

INSIGHT

Russian Sanctions and Cryptocurrency

May 4, 2022

The United States has imposed sanctions against certain Russian entities and individuals in response to Russia's invasion of Ukraine—including on virtual currency transactions and cryptocurrency mining. Some Members of Congress and other observers have expressed concern that sanctioned parties may evade sanctions using cryptocurrency to transfer funds out of Russia, convert rubles to other fiat currencies, or receive payments and make purchases. Bills have been introduced in the 117th Congress to prevent such evasion. This Insight focuses on various evasion techniques and potential gaps in existing regulatory oversight.

Potential Sanctions Evasion with Cryptocurrency

Cryptocurrency transactions may enable sanctions avoidance, though there is limited public information on the use of these methods.

Cryptocurrencies are created and exchanged through blockchain networks, which store tamper-resistant records of transactions. Most cryptocurrency transactions between parties are recorded directly on public blockchains—meaning anyone can view the records. Users are identified by public key addresses rather than their real-world identities, which led to concerns that Russian actors may use the "pseudonymity" of cryptocurrency to evade sanctions.

Cryptocurrency supporters argue that sanctions evasion is impossible because transactions are publicly viewable on blockchains, which law enforcement may trace using analytics software and users' public key addresses. Additionally, cryptocurrencies are not a widely accepted form of payment, so most users convert to fiat currency (currency established by sovereign governments) through cryptocurrency exchanges to make purchases. In the United States, many exchanges are required to maintain customer identification programs and follow sanctions, which may limit evaders' ability to use exchanges that comply with U.S. regulations.

However, sanctions evaders may attempt to obscure their blockchain transactions and evade measures imposed by exchanges through the following practices:

- **Chain-hopping** is the process of converting one cryptocurrency into another to hide illicit funds. In 2020, North Korean actors attempted to use chain-hopping to launder stolen cryptocurrency and evade sanctions.

Congressional Research Service
https://crsreports.congress.gov
IN11920

- **Mixers and tumbling services** increase the difficulty of determining the source of illicit funds. Users pay a fee to send cryptocurrency to a mixer account, which combines cryptocurrencies from various customers, before sending it to a recipient.
- Criminals may use **unhosted wallets** to move illicit funds. A wallet is digital software or hardware for storing private keys corresponding to cryptocurrency and other blockchain-based assets. Exchanges may provide "hosted" wallets but are not required to monitor transactions with unhosted wallets. If law enforcement agencies are aware of a sanctioned individual's unhosted wallet, they may be unable to access and recover the cryptocurrency without the wallet's private keys. Nevertheless, unhosted wallets still require an exchange as an "off-ramp" for users to convert to fiat currency. Individuals may use unhosted wallets to shift funds to exchanges in jurisdictions with fewer anti-money laundering (AML) or Know Your Customer (KYC) requirements. The Office of Foreign Assets Control (OFAC) has sanctioned certain Russian-linked cryptocurrency exchanges to cut off avenues for potential sanctions evasion. The Financial Crimes Enforcement Network (FinCEN) has a proposed rulemaking extending reporting requirements to unhosted wallets.
- **Anonymity-enhanced cryptocurrencies**, such as Monero, use additional cryptographic techniques to ensure greater anonymity, increasing the difficulty of tracing illicit activity.
- **Peer-to-peer (P2P) exchanges** are cryptocurrency exchanges that operate without any central intermediary or authority to transmit assets or collect customer information, increasing the difficulty of tracing illicit activity or complying with the Bank Secrecy Act (BSA), which requires U.S. financial institutions to assist the government in detecting and preventing money laundering.

Not all of these practices are illegal or used solely (or even widely) for sanctions evasion, and some fall under existing regulatory regimes. FinCEN considers mixers and P2P exchanges to be money service businesses, but many do not register with FinCEN as required. FinCEN has fined mixing services, and the Department of Justice (DOJ) has prosecuted P2P exchangers for money laundering and BSA violations.

Additionally, sanctioned individuals or entities may use proxies (such as relatives) or stolen identification credentials to access cryptocurrency and bypass attempts to block their transactions on centralized exchanges. In 2020, DOJ charged a Russian national for using stolen identities to open fraudulent cryptocurrency accounts, and OFAC found that three Russian nationals used cryptocurrency to fund illicit activities. Sanctioned individuals may also use foreign exchanges in jurisdictions with fewer AML/KYC requirements to cash out of illicit cryptocurrency.

Considerations for Congress

The extent of illicit cryptocurrency activity has been subject to considerable debate. Older research suggested that illicit finance represents nearly half of all bitcoin (the largest cryptocurrency) activity. As the crypto market has grown, the proportion (but not necessarily the number) of crime-linked addresses may have declined. A more recent study, for example, estimates it to be 3%, and another analysis notes that the figure for all of cryptocurrency (not just bitcoin) may be as low as 0.15%.

Russian sanction evasion using cryptocurrency has likely been limited in scale. FinCEN stated that while sanctioned individuals and institutions may try, "large scale sanctions evasion using [cryptocurrency] by a government such as the Russian Federation is not necessarily practicable." Secretary of the Treasury Janet Yellen expressed a similar assessment at a recent congressional hearing. While media outlets reported an increased demand for bitcoin by Russians, this may have been motivated by a desire to convert from the ruble.

Some policymakers are concerned that sanctioned entities and individuals may use cryptocurrency to avoid sanctions. Although sanctions evasion may be possible in small amounts, capacity and liquidity constraints in several of the methods mentioned above and sanctions enforcement by exchanges may make the wholesale avoidance of sanctions less theoretically feasible. However, given the development of new evasion tactics, Congress may consider the ability of domestic regulatory agencies to monitor blockchains; whether enforcement agencies have the funding, technological tools, and staff expertise for blockchain analytics and oversight; and whether BSA compliance programs at exchanges are adequate.

Finally, Congress may consider whether additional oversight is necessary to enhance broader regulatory and enforcement capabilities related to cryptocurrencies in light of concerns about their use in evading economic sanctions.

Author Information

Kristen E. Busch
Analyst in Science and Technology Policy

Paul Tierno
Analyst in Financial Economics

Disclaimer