Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

February 8, 2018

Digital Currencies: Sanctions Evasion Risks

Introduction

As the market for digital currencies evolves, one area on which Congress has focused is the potential use of digital currencies for sanctions evasion. Digital currencies face an uneven international regulatory environment, and countries are considering different approaches to regulating and/or issuing digital currencies. Some governments are exploring the possibility of issuing digital currency as a means of sanctions evasion (as in the case of Venezuela and Russia), while others are exploiting weaknesses in existing virtual currency markets to evade restrictions on access to the international banking system (as in the case of North Korea).

Digital Currency Market

Money is the set of assets used to buy goods and services from others. It functions in the economy as a: (1) medium of exchange; (2) unit of account; and (3) store of value. Although money may be made of materials that have intrinsic value, such as gold, most countries today use **fiat currency**, which has no intrinsic value, but serves as money by government decree.

Virtual currencies are digital representations of value that can be digitally traded and function like money. Unlike fiat currencies, virtual currencies do not have legal tender status. Virtual currencies may be **convertible** or **non-convertible**. Convertible virtual currencies can be exchanged for fiat currencies. Non-convertible virtual currencies are restricted to online domains (such as multiplayer online gaming).

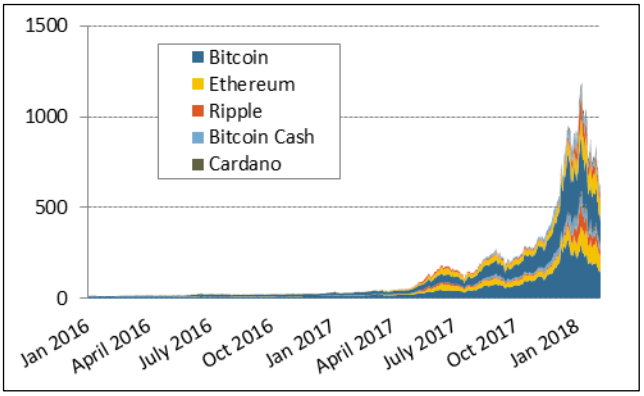
Some virtual currencies are run by a **centralized** administrator that issues currency and maintains a central payment ledger. Other virtual currencies are **decentralized**, for which transactions are recorded on a blockchain ledger and rely on encryption techniques to control the creation of monetary units and to verify the transfer of funds. Convertible, decentralized currencies are also called **cryptocurrencies**.

Many central banks worldwide, including the U.S. Federal Reserve and the People's Bank of China, are evaluating the creation of digital representations of fiat currencies, or **digital fiat currencies**. In September 2017, the Bank for International Settlements, an organization of 60 central banks including the U.S. Federal Reserve, recommended that central banks pay attention to the development of virtual currencies and consider the issuance of their own digital currencies.

Growth in the Cryptocurrency Market

Bitcoin, launched in 2009, was the first and continues to be the most widely used "cryptocurrency." Today, there are nearly 1,500 cryptocurrencies in circulation with a total market capitalization of $340 billion, although valuations have fluctuated widely (**Figure 1**). The five largest cryptocurrencies account for 70% of total virtual currency market capitalization, and include Bitcoin ($121 billion); Ethereum ($70 billion); Ripple ($28 billion); Bitcoin Cash ($15 billion); and Cardano ($9 billion).

Figure 1. Market Capitalization of Major Cryptocurrencies ($ in billions)



Source: https://coinmarketcap.com/.

Benefits and Risks of Virtual Currencies

Virtual currencies have the potential to revolutionize the financial and banking industries. They could increase payment efficiency, reduce transaction costs of payments and fund transfers, increase participation in the financial system, and facilitate transactions. Digital currencies, however, also present risks. Virtual currency platforms remain largely unregulated, and could be vulnerable to fraud and theft. There are also risks related to security, payment beneficiary identification, and currency volatility.

Virtual currencies may also pose a variety of illicit finance concerns. They provide total or partial anonymity to users and transactions and can be used as an alternative to the formal banking sector, which is more highly regulated. The uneven international regulatory environment surrounding the rapidly evolving virtual currency market is also attractive to illicit actors, who may seek to exploit virtual currencies operating in unregulated jurisdictions to launder ill-gotten funds, finance terrorism, or evade sanctions.

Sanctions Evasion Risks

Recent events have highlighted the interest of some governments subject to economic sanctions in exploiting virtual and digital currencies to evade U.S. sanctions. According to Treasury officials, however, sanctions evasion risks posed by virtual currencies have been limited in

practice. Individuals, entities, and transactions subject to U.S. jurisdiction are required to comply with all U.S. sanctions, regardless of the currency, including virtual currencies. Treasury officials also assess that the current domestic anti-money laundering (AML) regulatory approach to virtual currencies is sufficient (see text box on U.S. AML guidance).

Nevertheless, the characteristics of virtual currencies that make them attractive to criminals may also make them attractive to sanctions evaders. The risks could increase if virtual currencies were more widely adopted, such that daily financial life could be conducted for the most part in an entirely virtual currency universe.

Selected Country Case Studies

Venezuela. In December 2017, Venezuelan President Nicolás Maduro announced plans to launch a new digital currency, the "petro" backed by oil reserves and other commodities. Maduro stressed the petro would help Venezuela overcome U.S. sanctions and provide a fresh infusion of funds to the government. The Venezuelan government refers to the petro as a cryptocurrency, but it would operate very differently from other cryptocurrencies. The petro would have a central administrator (the government) and be backed by commodity assets. On January 19, 2018, the U.S. Treasury's Office of Foreign Assets Control (OFAC) stated that any purchases of the proposed petro currency would appear to be an extension of credit to the Venezuelan government, and thus U.S. investors who deal in petros could found to be in violation of U.S. sanctions.

Russia. The Russian government is exploring ways to create a new, state-run cryptocurrency, or "cryptorouble." According to Russian officials, a primary motivation is to "settle accounts with our counterparties all over the world with no regard for sanctions." Reportedly, the cryptocurrency would be a digital version of the rouble. As with the Venezuelan petro, the proposed cryptorouble appears to resemble a digital fiat currency: it would be administered by the Russian government rather than a decentralized network, although the Russian government may provide some anonymity to users. There are a number of questions about how a cryptorouble would operate. The Russian central bank is reportedly pushing back against the proposal.

Iran. Despite the lifting of some sanctions against Iran in 2015, other U.S. sanctions remain in effect. Meanwhile, European and other major global banks have been slow to reenter the Iranian market since implementation of the 2015 Joint Comprehensive Plan of Action. In light of Iran's ongoing banking challenges and popular interest in expanding its virtual currency market, the Central Bank of Iran (CBI) has been reportedly studying the issue of virtual currencies and intends to announce the results of their studies sometime in 2018. CBI is designated by Treasury as a jurisdiction of primary money laundering concern, and remains subject to restrictions that prohibit CBI's transactions with U.S. accounts in foreign banks.

North Korea. Beginning in 2017, observers indicate that purported North Korean cyber operations targeted virtual currency exchanges and investors—through the theft of digital wallets, deployment of ransomware and phishing campaigns, as well as mining operations—for financial gain and to ease the economic burden of ongoing sanctions pressure. This observed trend includes the WannaCry attack, during which attackers locked users worldwide out of their computers until they paid a ransom in Bitcoins; several Bitcoin wallets associated with WannaCry have reportedly been emptied. Several suspected North Korean cyberattacks also targeted South Korean exchanges.

U.S. Anti-Money Laundering (AML) Guidance

Treasury's Financial Crimes Enforcement Network (FinCEN) monitors the exchange of virtual currency for legal tender (and vice versa) for compliance with AML requirements.

- Since the mid-2000s, U.S. authorities have targeted virtual currency businesses and exchanges, as well as websites that brokered transactions involving virtual currency through a variety of enforcement actions.
- In 2011, FinCEN amended its rule dealing with Money Services Businesses (MSBs) to regulate those engaged in accepting convertible virtual currency from one person and transmitting it to another person or location.
- In 2013, FinCEN issued guidance to clarify that administrators and exchangers of virtual currency are considered MSB money transmitters and must register as such with FinCEN as well as implement relevant AML recordkeeping, reporting, and compliance measures.
- Since 2014 (FY2015), FinCEN has worked with the Internal Revenue Service (IRS), to identify licensed and unlicensed MSBs operating in the virtual currency marketplace subject to U.S. jurisdiction for AML compliance examination.
- In 2016, Treasury conducted risk assessments on money laundering and terrorist financing, which described criminal exploitation of virtual currencies as a vulnerability deserving of further scrutiny.
- As of January 2018, approximately 100 virtual currency providers and exchangers have registered in the United States as money transmitters; IRS and FinCEN have examined approximately 40 registered and unregistered MSBs involved in the virtual currency market.

Outlook

Digital currencies face an uneven international regulatory environment, and countries are considering different approaches to regulating and/or adopting digital currencies. A growing area of concern is potential exploitation of digital currencies to evade sanctions. Policymakers may continue to monitor their impact on the efficacy of sanctions.

For more, see CRS In Focus IF10824, *Introduction to Financial Services: "Cryptocurrencies"*, by David W. Perkins.

Rebecca M. Nelson, Specialist in International Trade and Finance
Liana W. Rosen, Specialist in International Crime and Narcotics

IF10825

Disclaimer