Virtual currency in sanctioned jurisdictions: stepping outside of SWIFT

Katherine Kirkpatrick, Christine Savage, Russell Johnston and Matthew Hanson

Abstract

Purpose – *To understand and analyze sanctions evasion and enforcement via virtual currencies.*

Design/methodology/approach – *Discusses various jurisdictions' attempts to further the use of virtual currency to facilitate and maximize access to international funds; analyzes the aspects that make virtual currency uniquely suited to evade sanctions; suggests best practices for industry participants to be sure to account for the differences in crypto asset structure and related risks.*

Findings – *The US Treasury Department's Office of Foreign Assets Control (OFAC) has explicitly stated that despite virtual currency's anonymity, industry participants are still responsible for policing and enforcing client compliance. Although sanctioned jurisdictions are thinking creatively about ways around SWIFT, the use of virtual currency to skirt sanctions presents certain challenges.*

Practical implications – *Virtual currency industry participants should understand OFAC's specific guidance regarding compliance obligations in the cryptocurrency space, and should implement best practices and conservative measures to avoid unknowingly running afoul of sanctions laws.*

Originality/value – *Expert analysis and guidance from experienced investigations and sanctions lawyers.*

Keywords *Iran, Enforcement, Cryptocurrency, Virtual currency, Sanctions, US Treasury Department's Office of Foreign Assets Control (OFAC)*

Paper type *Technical paper*

Katherine Kirkpatrick (kkirkpatrick@kslaw.com) is a partner in the Chicago, Illinois, USA office; Christine Savage (csavage@kslaw.com) is a partner in the Washington, DC, USA office; Russell Johnston (rjohnston@kslaw.com) is a partner in the New York, New York, USA office; and Matthew Hanson (mhanson@kslaw.com) is a senior associate in the Washington, DC, USA office of King & Spalding LLP.

The concept of cryptocurrency[1] has been global since its inception more than a decade ago. Today, as virtual currencies proliferate, jurisdictions like Japan, South Korea, United Arab Emirates, the United Kingdom, Brazil, Switzerland, and China[2] have served as major markets. Switzerland has a "Crypto Valley," Japan recently launched a Self-Regulatory Organization, and the leaders of G20 countries have called for international cryptocurrency taxation – all steps that legitimize this systemically disruptive but economically promising industry.

As Iran, Russia, Venezuela, and other sanctioned jurisdictions join the pack and warm to cryptocurrency, however, this raises a question: Could sanctioned countries use cryptocurrencies to avoid regulatory systems designed to keep them from participating in the global marketplace?

Cryptocurrency in sanctioned jurisdictions

In April 2018, the Central Bank of Iran ("CBI") banned Iranian banks from using cryptocurrencies, including Bitcoin, citing money laundering concerns. The language was clear, and echoed other jurisdictions who were wary of embracing cryptocurrency, given its operation outside of established financial systems: "Banks and credit institutions and currency exchanges should avoid any sale or purchase of these currencies or taking any action to promote them [...] [Cryptocurrencies] have the

option to be used for money laundering, supporting terrorism and exchange of sums between wrongdoers[3]."

Subsequent comments from Iranian parties, however, indicated that the country's position had softened. For example, in October 2018, General Gholam Reza Jalali, head of Iran's Civil Defense Organization, talked about the "great opportunities" presented by cryptocurrencies and specifically noted that they "can help bypass certain sanctions through untraceable banking operations." (Gogo, 2018)

Then, in January 2019, on the eve of the Tehran-based, "blockchain revolution" themed Electronic Banking and Payment Systems conference, the CBI made an about-face by reversing its ban. The CBI released an early draft of regulations and encouraged feedback from the tech community. As of now, "Version 0.0" of Iran's regulatory framework is aimed at organizing and defining the boundaries of ongoing crypto operations in the country. Among other things, it authorizes Initial Coin Offerings, tokens, wallets, exchange bureaus, and mining, and it allows the use of global, central bank, and regional cryptocurrencies. In an attempt to restrain its use, however, the CBI barred the use of global cryptocurrency for payments within the country and restricted the personal holding of digital assets – much like similar limits in place restricting Iranians from holding more than 10,000 euros.

Iran is now on track to announce a state-backed cryptocurrency, which could provide the beginning of a path to join a blockchain-based international payment system akin to SWIFT (Motamedi, 2019). Importantly, in November 2018, when SWIFT excluded certain Iranian banks from the SWIFT system (for fear of becoming subject to USA sanctions after the USA withdrew from the Joint Comprehensive Plan of Action), Iran was unable to use one of the primary systems for making international payments. By operating outside of customary international systems, Iran's state-backed cryptocurrency could serve as an alternative way for Iranian banks, companies, and citizens to send and receive international payments. Iran has also been proactive in finding other blockchain-based alternatives to SWIFT; for example, weeks after SWIFT's decision to exclude certain Iranian banks, Iran signed a trilateral blockchain cooperation agreement with Russia and Armenia. After the agreement was finalized, the head of the Russian Association of Cryptoindustry and Blockchain told sources that he understood that "an active development of an Iranian version of SWIFT is currently underway." (Suberg, 2019)

Initially, Russia had a similarly chilly attitude toward virtual currencies. Russian President Vladimir Putin condemned Bitcoin and called for a ban in October 2017, saying that it created the "[opportunity] to launder funds acquired through criminal activities, tax evasion, even terrorism financing, as well as the spread of fraud schemes." (RT.com, 2017) Likewise, the Russian Central Bank called cryptocurrency a pyramid scheme (RT.com, 2017). Since then, however, Putin has changed his tone, and a growing number of international crypto exchanges are increasing their presence in Russia, potentially as a result of the increasing sanctions on Russia's traditional financial services sector by the USA, EU, and their allies, which aim to isolate Russia from participation in international capital markets (Tassev, 2019).

Venezuela, another jurisdiction subject to sanctions aimed at curtailing its participation in international financial markets, also has embraced cryptocurrency. In December 2017, President Nicolas Maduro announced the launch of an oil-backed cryptocurrency, the Petro. Maduro went so far as to make the Petro the "official alternate currency" in the country and reportedly issued 100 million tokens. The Petro was launched in pre-sale in February 2018 (Palmer, 2018). In December, Maduro told state-run media that Venezuela had a schedule for selling oil in Petros during 2019 as part of an effort to bypass channels that involve USA dollars (Khatri, 2018).

Catching up with crypto

USA regulators and policy-makers are well aware of the development of cryptocurrency in sanctioned jurisdictions and have moved to limit loopholes. For example, USA legislators have denounced the Petro (De, 2018), and President Trump signed an executive order specifically targeting it with sanctions in March 2018[4].

Despite the USA government's awareness, however, certain aspects of how cryptocurrencies function still make them well-suited for sanctioned parties to use to evade enforcement. USA sanctions typically prohibit any person subject to USA jurisdiction from providing services, directly or indirectly, to or for the benefit of a sanctioned party. The USA Department of the Treasury's Office of Foreign Assets Control ("OFAC") may find a USA person who provides a service for the benefit of a sanctioned party to be in violation of USA sanctions, regardless of whether that person knew of the transaction's connection to a sanctioned party. Likewise, under the International Emergency Economic Powers Act, the statute upon which many USA sanctions programs are based, a person can be found liable for "caus[ing] a violation of any [...] [sanctions] regulation[5]." Given this strict liability standard, so as not to run afoul of sanctions, many USA parties, including financial institutions, have systems in place to ensure they are screening parties to transactions to detect the involvement of sanctioned parties so that they may take appropriate steps to reject or block a transaction to ensure their compliance with USA sanctions. But many cryptocurrencies allow for parties trading in them to remain anonymous. The transactions use public keys (commonly strings of numbers and letters that serve as public-facing addresses on the relevant blockchain) to identify the sender and receiver of each trade, but it can be difficult to associate these public keys to other identifiable information. Therefore, a sanctioned individual could potentially engage in cryptocurrency transactions without detection.

Detecting patterns across multiple transactions is one attempted method used to identify the underlying parties to cryptocurrency transactions. Since the transactions (i.e. TXID or hash) on some of the most widely used blockchains are publicly available (at least to those with access to those blockchains and software to parse the components of each transaction), they serve as transparent ledgers open for review. Patterns across broad ranges of transactions can therefore assist both regulators and regulated persons with connecting particular public keys to real-world people or entities.

In November, for the first time, Treasury imposed sanctions on two Iranians who helped exchange Bitcoin ransom payments into Iranian rial. Pattern recognition played a pivotal role, as OFAC identified two currency addresses used for over 7,000 transactions in Bitcoin that represented millions of dollars based on contemporaneous exchange rates. In the press release announcing the action, Treasury Under Secretary for Terrorism and Financial Intelligence Sigal Mandelker made clear that Treasury would seek out wrongdoers who attempt to avoid sanctions and anti-money laundering ("AML")/Combating the Financing of Terrorism ("CFT") regulations through the use of cryptocurrency: "As Iran becomes increasingly isolated and desperate for access to USA dollars, it is vital that virtual currency exchanges, peer-to-peer exchanges, and other providers of digital currency services harden their networks against these illicit schemes. [...] Treasury will aggressively pursue Iran and other rogue regimes attempting to exploit digital currencies and weaknesses in cyber and AML/CFT safeguards to further their nefarious objectives[6]."

Industry participants are also taking steps to avoid running afoul of Treasury enforcement. For example, several trading sites are blocking Iranian participants to avoid running afoul of Treasury rules[7]. But questions remain – namely, is pattern detection enough? And what can Treasury do about the use of cryptocurrencies as a strategic workaround?

Out of the reach of sanctions

Although it is still developing its own crypto legislation and has not yet fully embraced the industry, Russia may ultimately view cryptocurrency as a strategic means by which to avoid existing and future sanctions (Zuckerman, 2018). Recent press reports indicate that Russia may be planning to replace the dollar with Bitcoin as reserve currency to minimize the impact of sanctions (Kelleher, 2019). These press reports are underscored by comments in January 2018 from Putin's executive advisor, Sergei Glazyev, who said that a government-created "CryptoRuble" would be able to alleviate financial pressure caused by USA sanctions[8].

In theory, Iran, Venezuela, and Russia each could use cryptocurrency to decrease reliance on the dollar, add another layer between themselves and the USA financial system, obfuscate the parties in interest to particular transactions, and thereby potentially increase access to funds. In Iran, for example, where broad USA and international sanctions have made it difficult for an average Iranian businessowner to access banks to facilitate money transfers, this could be a game-changer. Cryptocurrency could effectively cut out those banks, thus opening up a new avenue for commerce.

Best practices for industry participants

Despite crypto's anonymity, USA regulators are intent on enforcement. For example, OFAC has explicitly stated that compliance obligations are the same, regardless of whether a transaction is denominated in cryptocurrency or traditional fiat currency[9]. They have also issued specific guidance on compliance obligations in the crypto space, such as how to block cryptocurrency, whether it is possible to query a cryptocurrency address using OFAC's Sanctions List Search tool (not yet), and how they will identify cryptocurrency-related information on the SDN list[10]. Participants should read and seek to understand and implement this guidance. Notably, any entity that touches cryptocurrency should be sure their existing tailored, risk-based compliance program accounts for the differences in crypto asset structure and related risks.

The obvious initial targets for Treasury enforcement are crypto exchanges. Those that plan to operate in the USA should drop sanctioned jurisdictions from their list of supported countries and impose restrictions on known associated users.

Exchanges, as well as other crypto participants, such as wallet providers, asset managers, and financial institutions, should strengthen AML and CFT frameworks, along with associated know-your-customer ("KYC") procedures, to ensure that cryptocurrency business lines comply. For example, market participants should employ KYC procedures to identify the individual or entity associated with each public key. Perform due diligence to learn more about the nature of certain transactions, for example, by trying to pinpoint the geographic connection on a subset of transactions or using geo-IP blocking to block sanctioned jurisdictions. And carefully track repeated transactions with the same cryptocurrency address to be sure that those align with the initial KYC and Know Your Transaction analysis.

Only time will tell if cryptocurrency is here to stay – and ultimately, whether it is here to replace fiat currency – but as it proliferates beyond borders, regulators will continue to take notice and apply existing rules to this new realm. Market participants would be wise to align compliance procedures now to avoid running afoul of regulators down the line.

Notes

1. Various US regulators use different terms for the concept of cryptocurrency, depending on how cryptocurrency maps on to their existing regulatory jurisdiction. The Financial Crimes Enforcement Network ("FinCEN") uses the term "virtual currency," the Office of Foreign Assets Control ("OFAC") uses the term "digital currency," and the Securities and Exchange Commission ("SEC") uses the

term "cryptocurrency." For purposes of this article, we refer to these variations on the concept collectively as "cryptocurrency."

2. China was a major source of cryptocurrency operations – in early 2017, a large majority of blockchain transactions were conducted in yuan – until Chinese government and financial regulatory agencies led by the People's Bank of China effectively banned crypto in late 2017 and 2018.
3. *Iran Central Bank Bans Cryptocurrency Dealings*, Reuters (22 April 2018), available at: www.reuters.com/article/us-crypto-currencies-iran/iran-central-bank-bans-cryptocurrency-dealings-idUSKBN1HT0YN
4. In December 2018, Venezuela filed a suit claiming that the US sanctions against the Petro were "discriminatory coercive trade-restrictive measures."
5. International Emergency Economic Powers Act, 50 U.S.C. §1705(a).
6. US Dep't of Treasury, *Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses*, available at: https://home.treasury.gov/news/press-releases/sm556 (28 November, 2018).
7. For example, major cryptocurrency exchanges Binance and Bittrex are two of the market participants that have informally cut ties with Iran. Although the Treasury action was not the impetus for these changes, it is another reminder that crypto players must abide by the same rules as entities in the traditional fiat currency space.
8. "This instrument suits us very well for sensitive activity on behalf of the state. We can settle accounts with our counterparties all over the world with no regard for sanctions." Seddon and Arnold (2018).
9. See US Dep't of Treasury, *560. Are my OFAC compliance obligations the same, regardless of whether a transaction is denominated in digital currency or traditional fiat currency?*, available at: www.treasury.gov/resource-center/faqs/sanctions/pages/faq_compliance.aspx. "Yes, the obligations are the same. US persons (and persons otherwise subject to OFAC jurisdiction) must ensure that they block the property and interests in property of persons named on OFAC's SDN List or any entity owned in the aggregate, directly or indirectly, 50 per cent or more by one or more blocked persons, and that they do not engage in trade or other transactions with such persons."
10. *Id.* See sections 646, 594, and 562.

References

De, N. (2018), "US senators blast Venezuela's oil-backed cryptocurrency plan", Coindesk, 22 January, available at: www.coindesk.com/u-s-senators-decry-venezuelan-petro

Gogo, J. (2018), "Global cryptocurrency exchanges cut ties with Iran after new US sanctions", Bitcoin.com, 6 November, available at: https://news.bitcoin.com/global-cryptocurrency-exchanges-cut-ties-with-iran-after-new-us-sanctions

Kelleher, K. (2019), "Russia is considering a shift to Bitcoin to limit the impact of US Sanctions, report says", Fortune, 14 January, available at: http://fortune.com/2019/01/14/russia-considering-shift-bitcoin-limit-impact-us-sanctions

Khatri, Y. (2018), "Venezuela to sell oil for petro cryptocurrency in 2019, says maduro", Coindesk, 7 December, available at: www.coindesk.com/venezuela-to-sell-oil-for-petro-cryptocurrency-in-2019-says-maduro

Motamedi, M. (2019), "Iran inches closer to unveiling state-backed cryptocurrency", Aljazeera.com, 27 January, available at: www.aljazeera.com/news/2019/01/iran-inches-closer-unveiling-state-backed-cryptocurrency-190127060320571.html

Palmer, D. (2018), "Venezuela's 'petro' token launches in pre-sale", Coindesk, 20 February, available at: www.coindesk.com/venezuelas-petro-token-launches-pre-sale

RT.com (2017), "Putin: cryptocurrencies bear serious risks, including financing of terrorism", RT.com, 10 October, available at: www.rt.com/news/406269-cryptocurrency-risks-terrorism-putin

Seddon, M. and Arnold, M. (2018), "Putin considers 'cryptorouble' as moscow seeks to evade sanctions", Financial Times, 1 January, available at: www.ft.com/content/54d026d8-e4cc-11e7-97e2-916d4fbac0da

Suberg, W. (2019), "Iran soon to unveil cryptocurrency with aim to skirt US and SWIFT: source", Cointelegraph, 28 January, available at: https://cointelegraph.com/news/iran-soon-to-unveil-cryptocurrency-with-aim-to-skirt-us-and-swift-source

Tassev, L. (2019), "Cryptocurrency exchanges eye russia for expansion despite sanctions", Bitcoin.com, 7 January, available at: https://news.bitcoin.com/cryptocurrency-exchanges-eye-russia-for-expansion-despite-sanctions

Zuckerman, M.J. (2018), "Russia's 'disappointing' cryptocurrency legislation: why experts consider the bill a failure", Cointelegraph, 29 September, available at: https://cointelegraph.com/news/russias-disappointing-cryptocurrency-legislation-why-experts-consider-the-bill-a-failure

Corresponding author

Katherine Kirkpatrick can be contacted at: kkirkpatrick@kslaw.com