Crypto Never Sleeps:

Vigilance Required in OFAC Sanctions Compliance Involving Virtual Currencies and Digital Assets

Dechert LLP

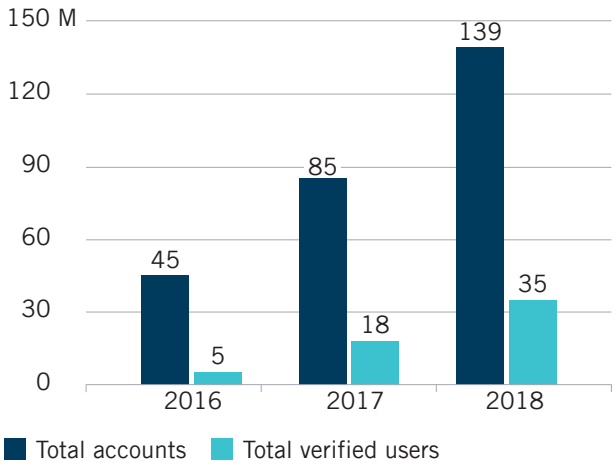
Introduction

For years, regulators around the world have struggled with whether and how to police the offering and exchange of digital assets (including virtual currencies such as Bitcoin). In the United States, such efforts were stymied in part by laws and regulations that did not contemplate the rise of distributed and decentralized payment networks. Efforts at regulation were also hampered, however, by a more fundamental problem – digital assets are not "one" single thing but several, and not all digital assets share the same attributes.

U.S. regulators have lately taken a much more active interest in the issue, however, since Bitcoin's market surge in early 2018 and amidst the broader popular acceptance of virtual currencies. That has compelled regulators to actually define what digital assets are – securities, commodities, debt instruments, currencies, or something else entirely. The answer will, in part, determine which regulators claim jurisdiction over distributed and decentralized payment networks.

Less conspicuously but no less consequentially, the answer may also determine how the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) administers and enforces U.S. economic sanctions as they apply to transactions involving digital assets. Given the attention OFAC has already paid to distributed and decentralized payment networks, businesses operating in this space should closely watch how other regulators (as well as courts) characterize digital assets and use that as a guide for what obligations might attach under U.S. sanctions law.

Users of Cryptocurrency Continue to Increase



Source: Cambridge Centre for Alternative Finance

The Emerging Regulatory Regime

Digital assets - and the underlying blockchain technologies that power them - were initially conceived as a distributed and decentralized alternative to the traditional financial system, and have operated in a legal and regulatory grey area for several years. Although criminal laws were used to prosecute illicit actors who were popularly linked to certain virtual currencies – such as the money laundering and conspiracy charges brought against Silk Road marketplace administrators in 2013 – the use of digital assets themselves was incidental to the underlying charges. Indeed, in the first congressional hearing on digital currencies, held shortly after the Silk Road marketplace was shut down in 2013, the overwhelming consensus among government witnesses was that virtual currencies are legitimate financial instruments whose risks are unique but not qualitatively different from those posed by other payment systems.

Even while they declined to craft additional rules and regulations that were specifically applicable to digital assets and blockchain technologies, many federal and state regulators maintained a watchful eye over the sector. For example, the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) published guidance about digital currencies in 2013, emphasizing that administrators and exchangers of virtual currencies qualified as money services businesses subject to certain registration, reporting, and recordkeeping regulations under the Bank Secrecy Act.

However, many businesses operating in the digital assets space were not directly regulated. For instance, coin developers, miners, and wallet providers generally viewed themselves as operating outside the jurisdiction and purview of regulators. As a result, many such businesses developed rudimentary legal and compliance policies, and it was not always clear whether or how such policies were implemented to protect against illicit finance and money laundering concerns.

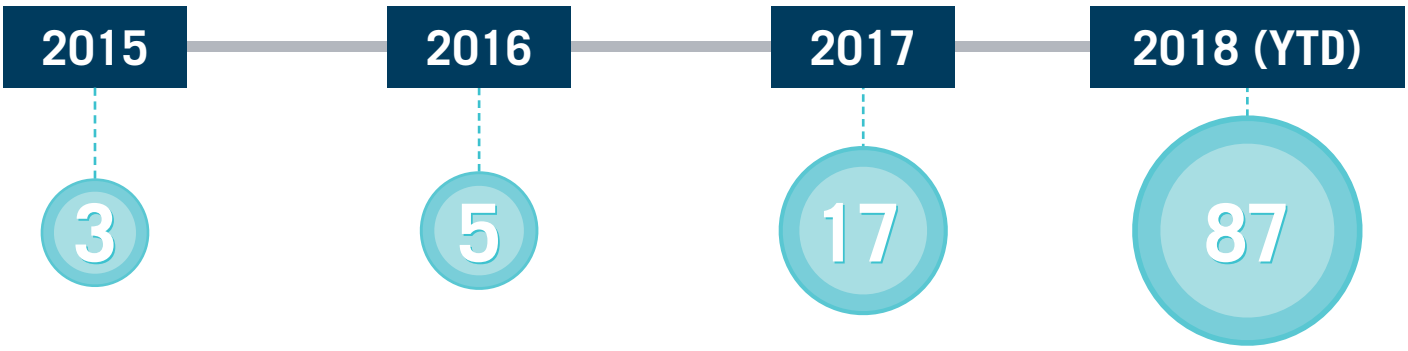
This compliance landscape began to change in late 2017, however. First, the Securities and Exchange Commission (SEC) took a series of actions to regulate certain initial coin offerings (ICOs) involving securities, targeting both the initial issuers as well as platforms and investment vehicles that bought and sold such digital assets. The SEC's assertion of jurisdiction was based upon the premise that the coins or tokens in such cases were within the definition of securities because they constituted investment contracts under the so-called "Howey" test.[1] Notably, the SEC has also made clear that not *all* digital assets are categorizable as securities, and therefore the offering or dealing in such coins would not be subject to its jurisdiction.

Second, the Commodity Futures Trading Commission (CFTC) has also stepped into the breach, arguing that virtual currencies such as Bitcoin and Ether are categorizable as commodities subject to its jurisdiction because, in part, they are an asset class in which contracts for future delivery are dealt in. The CFTC's determination was recently upheld by a United States District Court in Massachusetts, which held that the CFTC did not need to determine whether any particular virtual currency underlies a futures contract – it was sufficient that futures trading occurs within the broader virtual currency asset class.

Thus, according to the SEC, the CFTC, and a handful of courts, some digital assets are securities, while other digital assets that operate as virtual currencies are commodities. Other characterizations might also apply, however, depending on the specific characteristics of any particular coin – for instance, some might operate as debt instruments or as asset-backed currencies.

Securities Litigation Referencing Blockchain, Cryptocurrency, or Bitcoin

Number of Cases



Source: Lex Machina

[1] *See* SEC v. W.J. Howey Co., 328 U.S. 293 (1946), and our *Dechert OnPoint* which discusses the Howey test and its key elements, SEC Focuses on Initial Coin Offerings: Tokens May Be Securities Under Federal Securities Laws.

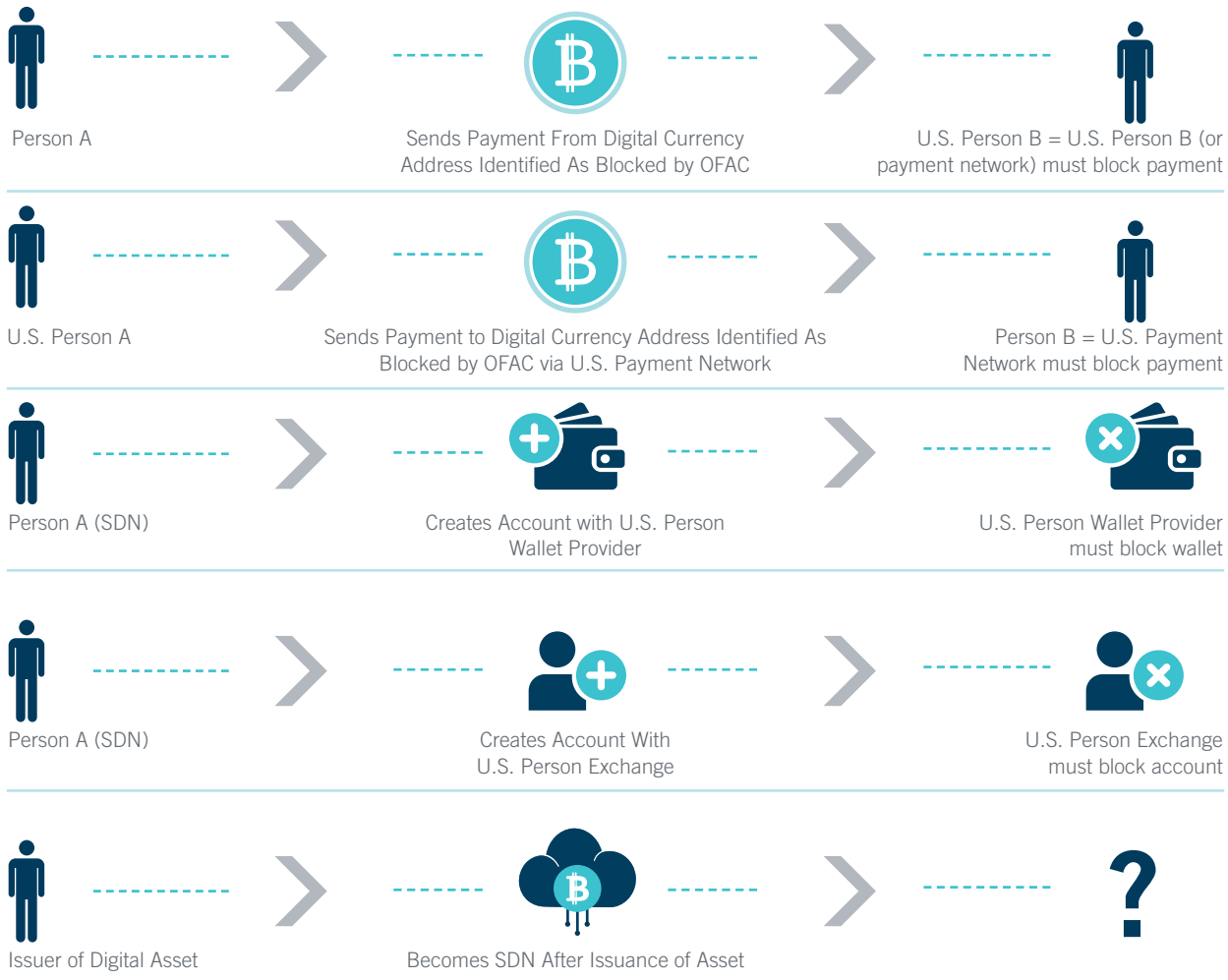
Digital Assets and Sanctions

Businesses transacting or dealing in digital assets have kept a close eye on how regulators will define their legal and compliance obligations. For many, that assessment hinges upon their specific role within the particular ecosystem – for instance, offerors and dealers might be principally concerned with the SEC's enforcement of securities laws, while administrators and exchangers may be primarily implicated by FinCEN's regulation of money services businesses.

One agency, however, has authority over a far broader segment of the market. OFAC, which administers and enforces U.S. sanctions laws, asserts jurisdiction over *U.S. persons* – that is, any entity organized under the laws of the United States (including their foreign branches), as well as any U.S. citizens or permanent residents and any person physically located within the United States.[2] OFAC also asserts jurisdiction over non-U.S. persons who engage in prohibited transactions that involve U.S. persons. This means that a significant proportion of coin developers, coin offerors, administrators, exchangers, cryptominers, and wallet providers will face some OFAC exposure.

The specific prohibitions enforced by OFAC can vary, but in every case U.S. persons must block all property in which an individual or entity on OFAC's List of Specially Designated Nationals and Blocked Persons (SDN List) has an interest, and U.S. persons are generally prohibited from transacting with the same. The same restrictions extend to any entity owned 50% or more by one or more SDNs.

Digital Assets and Sanctions: Potential Scenarios



[2] For transactions involving Iran and Cuba, OFAC also asserts jurisdiction over foreign entities owned or controlled by U.S. persons.

Crucially, although U.S. sanctions are a strict liability enforcement regime, OFAC does not impose specific compliance obligations because it does not view itself as a regulator. Rather, OFAC advises that all businesses subject to its jurisdiction adopt a "risk based" compliance program that depends upon your customer profile and what kind of business you do. For instance, traditional financial institutions engaging in international wire transfers have a higher risk profile than a small regional bank, and their compliance program should be tailored accordingly.

Digital Assets and OFAC

The threat posed by OFAC is not an idle one. In March 2018, OFAC signaled that it was actively monitoring distributed and decentralized payment systems and blockchain technologies by issuing five frequently asked questions (FAQs) relating to digital currencies and sanctions compliance. In so doing, OFAC warned that it would specifically target "the use of digital currencies or other emerging payment systems to conduct proscribed financial transactions and evade U.S. sanctions." OFAC also emphasized that the compliance obligations for U.S. persons do not change when they are transacting or dealing in virtual currencies, stating that firms that "process transactions in digital currency … are responding for ensuring that they do not engage in unauthorized transactions prohibited by OFAC sanctions, such as dealings with blocked persons or property."

Over the ensuing months, OFAC underscored those obligations by reportedly issuing administrative subpoenas to various businesses operating in the digital assets space, requesting reports of any blocked transactions or accounts and further details on internal OFAC compliance policies. However, OFAC conceded the unique challenges facing companies that operate in these ecosystems, stating that it would consider adding "digital currency addresses to the SDN List to alert the public of specific digital currency identifiers associated with blocked persons."

FinCEN further highlighted the emerging risks by issuing an advisory in October 2018 focused on Iran's attempt to evade OFAC sanctions through, in part, the use of digital currencies. FinCEN specifically identified the risk to US and third-country based virtual currency and peer-to-peer exchangers, encouraging businesses to review blockchain ledgers for activity originating or terminating in Iran and to closely scrutinize transactions involving counterparties who may do business in Iran, including any exchangers who offer services there. FinCEN emphasized that financial institutions and digital assets providers must have appropriate systems in place to comply with applicable sanctions and illicit finance laws.

Finally, in November 2018, OFAC took action to formally identify two digital asset addresses that it alleged were the property of two Iranian SDNs. At the same time, OFAC was clear that U.S. persons transacting or dealing in digital assets have an *independent* obligation to identify and block any addresses, wallets, or transactions that they believe are owned by or otherwise associated with SDNs.

Identifying Blockable Property Interests in Digital Assets

The question then arises – how should a business operating in the digital assets space independently identify blockable property interests? It's clear that an SDN counterparty to a digital asset exchange possesses a blockable interest in that transaction, but less clear how such rules would apply in other contexts. Given how broadly OFAC defines "property interest" – it includes an interest of any nature whatsoever, direct or indirect, present, future, or contingent – the potential exposure is vast, especially because OFAC's guidance implies that businesses transacting or dealing in digital assets cannot rely upon the pseudonymous nature of such technologies to avoid OFAC compliance obligations.

Here, how digital assets are broadly defined by courts and other regulatory agencies, as well as the specific characteristics of any given coin, may prove a useful guide. For instance, a purchaser of a digital asset that can be characterized as a security may wind up holding blocked property if the issuer of the ICO becomes an SDN. In that case, the coin itself could be said to act

like an equity share in the SDN, and even secondary market trading in such coins could be prohibited. Similar questions could arise if an SDN purchases 50% or more of the extant coins that can be classified as a security. By contrast, a virtual currency that is decentralized and cannot be characterized as a security – such as Bitcoin and Ether - would likely not be directly impacted by U.S. sanctions laws.

A similar analysis could apply to an asset-backed coin or token if the underlying asset becomes encumbered by U.S. sanctions. For instance, issues could arise if a coin was backed by real estate assets and that real estate later became blocked because it was the property of an SDN. At the very least, such coins could not be exchanged for the underlying real estate assets, and thus could lose most of their value.

Complicating matters still further, OFAC itself issued guidance in January 2018 to state that the Government of Venezuela's new digital currency, the "petro," could constitute an extension of *debt* to the Venezuelan government because it carried with it rights to receive commodities (e.g., oil, gas, and gold) at a later date. Although the Government of Venezuela is not an SDN, it is subject to OFAC restrictions on the dealing in and extension of new debt with certain maturities. Although OFAC emphasized that its guidance was limited to a digital asset with the petro's specific characteristics, the example underscores the circumstantial nature of such analyses.

Sanctions Risk Assessment for Digital Assets Businesses Depending on Currency Classification

	Security	Commodity	Debt	Asset Backed Currency	Fiat Currency
Administrators/Issuers	High	Low	Medium	Low	Low
Exchangers	High	Medium	High	Medium	Medium
Wallet Providers	Medium	Medium	Medium	Medium	Medium
Investors	High	Low	High	High	Low
Users	Medium	Medium	Medium	Medium	Medium

What Should You Do?

Because of the evolving nature of the regulatory regime around digital assets and virtual currencies, and the fluid nature of OFAC sanctions programs, it is difficult to predict all of the potential issues that could arise in the near future. What is abundantly clear is that OFAC, among other US regulatory agencies, is actively monitoring digital asset transactions, and is intent to impede their use by illicit actors. As part of this effort, OFAC can be expected to step up enforcement of U.S. sanctions laws against businesses operating or dealing with digital assets. Companies will need to be armed with well-tailored (and implementable) sanctions compliance policies to ensure they are screening transactions and counterparties for potential risks.

The potential liability for violations of U.S. sanctions laws is significant, but having systems in place to assess and mitigate exposure to U.S. sanctions is prudent for another reason – no one wants to be stuck holding an asset of diminishing (or zero) value. Investors in companies that end up being sanctioned by OFAC are often compelled to divest such assets at a significant loss, if they are authorized to sell them at all.

In addition, traditional financial institutions are often reluctant to deal with customers who don't have adequate sanctions and anti-money laundering policies in place. Having been put on notice by both OFAC and FinCEN, counterparties and financial institutions are likely to place greater scrutiny on businesses operating in or dealing with digital currency. For instance, they may ask:

- Whether you have a sanctions compliance policy, and whether it prohibits transactions with, or access and use by, persons subject to U.S. sanctions;
- What know your customer (KYC) protocols and customer identification program (CIP) policies are in place;
- Whether and how you conduct screening for persons subject to U.S. sanctions, including location screening for persons located in sanctioned jurisdictions like Iran;
- Whether you have IP blockers in place that allow you to prohibit network access for persons located in sanctioned jurisdictions;
- Whether you have identified any "hits" to sanctioned persons or jurisdictions, and how your business handled them; and
- Whether you regularly audit and assess your compliance policies and procedures to ensure they are fit for purpose, and whether and how employees are trained to implement them.

While no business can predict the future with perfect clarity, a well-tailored and implemented compliance program that properly accounts for the risks attaching to digital assets and specific transactions serves a business, reputational, and legal imperative.

Contact us

Jeremy B. Zucker
Partner
+1 202 261 3322
jeremy.zucker@dechert.com

Timothy Spangler
Partner
+1 949 442 6044
+1 650 813 4803
timothy.spangler@dechert.com

Sean Kane
Counsel
+1 202 261 3407
sean.kane@dechert.com