GLOBAL BANKING & Finance review®
Global Insights & Analysis of the Financial & Business Markets

Cryptocurrencies: Solving New Problems with Old Solutions

11/09/2018

By **David Bitkower**, Michael Ross, Jolene Negre, Partners, and Emily Bruemmer and Jessica Martinez, Associates, at Jenner & Block

Despite continuing volatility in the markets, the buzz surrounding digital assets persists, and evidence continues to mount in support of both the promise and the peril of cryptocurrencies.

Companies dealing in or with cryptocurrency, such as payment processors or exchange operators, need to keep up with-or better yet stay ahead of-the concerns that regulators have expressed, and approach their compliance strategies with the same energy and ingenuity they bring to their financial products. This article discusses some ways in which businesses that come into contact with cryptocurrencies can avoid letting their platforms become conduits for criminality, by being on guard for signs of fraud or market manipulation, and by employing traditional tools such as know your customer (KYC) and anti-money laundering (AML) programs.

Over the past year, regulators have brought cases alleging that a cryptocurrency was used in furtherance of a fraud scheme-or that the cryptocurrency project was itself a fraud scheme. Among the first wave of enforcement actions brought by the Securities and Exchange Commission (SEC)'s new Cyber Unit were several cases involving garden-variety fraud charges. The very first such action involved a Canadian entity called PlexCorps, which as part of its supposed initial coin offering (ICO) purported to issue "PlexCoins" or "PlexCoin Tokens" that would enrich investors in under a month. The SEC's complaint alleged that, rather than being a legitimate ICO, the "outlandish" promises made by PlexCorps were in fact a fraud scheme. Along similar lines, in April the SEC announced charges related to a different alleged fraudulent scheme involving Centra Tech Inc.'s ICO in 2017. Meanwhile, the Commodity Futures Trading Commission (CFTC) rang in 2018 by charging multiple virtual currency operators with fraud. And in April, the CFTC filed another complaint against multiple individuals and corporations, alleging operation of a fraudulent scheme involving the virtual currency ATM Coin.

Most recently, as part of Special Counsel Robert Mueller's investigation, a federal grand jury indicted 13 Russian nationals and three Russian entities for crimes aimed at disrupting the 2016 presidential election. According to the indictment, these activities were in part facilitated by cryptocurrency, as the individuals sought to "capitalize on the perceived anonymity of cryptocurrencies such as bitcoin" when "purchasing servers, registering domains, and otherwise making payments in furtherance of hacking activity." They even mined bitcoin in order to fund computer infrastructure purchases. The hackers attempted to cover their tracks by providing payment processors with obviously fake addresses such as "usa Denver AZ," "gfhgh ghfhgfh fdgfdg WA," and "1 2 dwd District of Columbia." The existence and content of the indictment suggests the attempts at covering their tracks were successful only up to a point.

As a whole, these recent enforcement actions and others indicate that regulators will expect companies dealing with cryptocurrencies to be up to date on the risks that come with the territory. Such companies should therefore be on heightened alert for signs of fraud, which can often be spotted in the cryptocurrency context just as in a more traditional setting. Traditional principles involving KYC, AML, and efforts to prevent market manipulation can be applied in this new setting to protect businesses that interface with cryptocurrencies.

KYC and AML. The threats posed by ICO and cryptocurrency fraud schemes can sometimes be addressed through the application of old-fashioned due diligence and good judgment, such as policies and procedures that ensure a company has knowledge of its clients and their business purposes. For example, in the PlexCorps case, legitimate businesses whose platforms were used by the alleged perpetrators could have identified (and, in fact, did identify) the potential risks of doing business with PlexCorps due to the lack of information provided about the business purposes of the company that opened an account with their platforms, the statements in the publicly posted promotional materials for the ICO, and prior regulatory action in Quebec. Following established principles of due diligence, several of the payment processors at issue flagged PlexCorps-related accounts for suspicious activity and suspended them or reversed the payments at issue.

Conducting due diligence on the users of a platform may sometimes involve new techniques, however, given the unique anonymity characteristics of some cryptocurrencies. Regulators throughout the world have already identified this danger and targeted cryptocurrency exchanges, along with those who seek to use cryptocurrencies to launder money. In June, for example, Japan's Financial Services Agency ordered multiple cryptocurrency exchanges to improve their AML programs. And last December, SEC Chairman Jay Clayton cautioned in a statement on cryptocurrencies and ICOs that companies should ensure that "their cryptocurrency activities are not undermining their anti-money laundering and know-your-customer obligations."

Taking the same approach as regulators, private companies can harness the traceability of the underlying blockchain technology to facilitate review of cryptocurrency transactions and to comply with their KYC and AML obligations. Law enforcement authorities have certainly taken advantage of that feature: in June, the U.S. Department of Justice (DOJ) announced the results of a nationwide undercover operation targeting Darknet vendors, which led to the arrest of over 35 individuals selling illicit goods and laundering money. Government agents involved in the operation seized more than $20 million in cryptocurrencies, in addition to bitcoin mining equipment. This operation was unique because the government effectively operated an undercover currency exchange, posing as willing money launderers for criminals using cryptocurrencies for their crimes. It appears that the agents then used the ledger technology to trace and identify specific vendors. These features of digital assets can similarly be used by private companies to ensure that they are in compliance with applicable regulations, including anti-money laundering regimes.

Market Manipulation. A second area where regulators appear to be focusing energy is the risk posed to otherwise legitimate cryptocurrency markets by another danger familiar to any securities lawyer: market manipulation, including spoofing and wash trading. Both of these practices aim at influencing market prices through artificial means: spoofing involves the submission of bids or offers with the intent to cancel them before execution, in order to give other investors a false impression of the market; wash trading involves a person buying and selling at the same time in order to create an illusion of activity in the market. There is already growing evidence that cryptocurrency markets are particularly susceptible to such manipulation because of their comparatively limited size, the lack of transparency surrounding key market participants, and the gold rush mentality held by even legitimate traders. In January, for example, the authors of an article in the Journal of Monetary Economics concluded based on transaction history from the Mt. Gox bitcoin exchange that suspicious trading activity by one trader caused a spike in bitcoin prices from $150 to $1,000 during 2013. In late May, Bloomberg reported that DOJ had opened a large-scale criminal probe into potential market manipulation of cryptocurrencies, including bitcoin and Ether, sold in spot markets. Although DOJ has not publicly released any information regarding the investigation, it reportedly focuses on spoofing and wash trading. Finally, in June, researchers at the University of Texas at Austin published a paper theorizing that the rise in prices of cryptocurrency such as bitcoin may have been caused by market manipulation related to the cryptocurrency token Tether.

The reported DOJ investigation highlights the potential for market surveillance by regulators to identify suspicious patterns and other indications of manipulative conduct in cryptocurrency markets. Market surveillance, however, can also serve as a powerful deterrent if employed by cryptocurrency exchanges themselves. Recognizing this, some exchanges have begun to use market surveillance systems to monitor for potentially abusive trading of digital assets on their exchanges. In the short run, participants in the markets may fear the specter of increased enforcement action, as the CFTC and other regulators analyze trade data to find potentially manipulative trading behavior. Ultimately, however, the emergence of institutionalized market surveillance may positively impact the future of cryptocurrency markets by protecting against price spikes and market volatility. Indeed, in the absence of such monitoring, the prevalence of fraud and manipulative conduct could result in exchanges being shut out of certain markets, subject to even stricter regulations, or abandoned by the customers they need in order to thrive. Companies seeking to establish a record of trust for customers, and avoid negative repercussions from regulators, should ensure their own policies are ahead of the curve.

Other Risk Areas. Digital assets present additional compliance issues beyond the ones highlighted above. For example, even companies that are not issuers should be aware of whether digital assets with which they interact are deemed to be “securities” and whether their platforms could be abused by third parties issuing or marketing those securities. Indeed, a number of companies, such as social media platforms, have banned or given closer scrutiny to communications relating to ICOs due to the risk of fraud or illegal securities offerings. Companies must also be alert to legal risks stemming from transacting in or holding cryptocurrencies, relating to fiduciary responsibilities or pricing, for example, due to the volatility of the digital assets markets. Finally, any companies that buy or sell cryptocurrencies should be aware of the potential tax consequences of their transactions given the treatment of cryptocurrency as property.

In all, participants in the cryptocurrency market are exposed to risks associated with fraud, money laundering, market manipulation, and other misdeeds that can occur as the space continues to develop. The lesson for such companies is to employ the same principles of due diligence and critical thought as they would in operating in any market, including common-sense due diligence and monitoring efforts based on the information that blockchain technology makes readily accessible. Moreover, companies operating globally must be attentive to local legal developments in the cryptocurrency space just as in any other regulatory area. Employing these practices can help keep market participants on the right side of the line in the event bad actors try to use their platforms to further illegal ends and put those market participants in better standing with regulators should they ultimately come knocking.