US Blockchain Enforcement and Litigation Update

January 2019

Dechert LLP

Overview

In the second half of 2018, cryptocurrency investors and businesses faced sustained attention from financial regulators and persistent declines in cryptocurrency prices. Federal and state regulators have continued their efforts to regulate cryptocurrency transactions and punish fraud. Regulatory enforcement actions and court decisions issued in 2018 provide insight regarding the application of federal securities and commodities laws to cryptocurrency. Through enforcement actions and informal policy statements, key regulators have also provided helpful guidance concerning steps cryptocurrency industry participants can take to remedy past violations.

Background on cryptocurrencies and initial coin offerings

Virtual currency is an umbrella category for digitally represented value without legal tender status. It can be either convertible (with equivalent value in real currency) or non-convertible (with value only in a specific virtual world). It can also be either centralized (with a single administrator or a small group of administrators) or decentralized (with distribution across peer-to-peer networks with no central administrator).

The term "cryptocurrency" typically refers to convertible, decentralized virtual currency exchanged over a cryptographically secure distributed ledger called a "blockchain." The blockchain permits the transfer of value among a network of individual actors conducting encrypted but publicly recorded transactions. Bitcoin is just one example of a cryptocurrency that has gained widespread usage and acceptance. Cryptocurrency developers can create new types of coins either on existing cryptocurrency protocols (like Litecoin, which was built on the Bitcoin protocol) or on new protocols (like Ether, which uses its own protocol). A valuable feature of some, though not all, cryptocurrencies is the possibility of constructing self-executing ("smart") contracts embodied in actual computer code to implement certain transactions.

Various functions of digital assets cross regulators' jurisdictional boundaries, creating challenges for government agencies seeking a proper regulatory approach.

During 2017, an increasing number of entrepreneurs and start-ups began conducting initial coin offerings ("ICOs") for so-called "tokens," which enable buyers to use platforms or other blockchain-based resources that they plan to construct. The industry quickly began to describe these tokens as either "utility tokens," which function as credits for a new product or service, or "security tokens," which confer rights to own real assets or company shares. The term "digital assets" refers to both virtual currencies and utility or security tokens.

These various functions of digital assets cross regulators' jurisdictional boundaries, creating challenges for government agencies seeking a proper regulatory approach. The Commodity Futures Trading Commission ("CFTC") has treated virtual currencies as "commodities" under the broad definition of the term in the Commodity Exchange Act ("CEA"), enabling the agency to regulate virtual currency derivatives contracts and target cases of fraud involving underlying virtual currencies. The Securities and Exchange Commission ("SEC") has also exercised jurisdiction in this area, though its focus has turned mostly to tokens (often marketed as investment opportunities) rather than to virtual currencies (such as Bitcoin and Ether) that function solely as a store of value. Importantly, the categories of commodities and securities are not necessarily mutually exclusive under existing law, meaning that the SEC and CFTC may wield overlapping jurisdiction in this field — at least in the absence of contrary federal legislation. To add further layers of complication for participants in the cryptocurrency industry, the U.S. Department of Justice ("DOJ") can always pursue investigations and criminal prosecutions against those who violate the federal wire and securities-fraud laws, and state regulators and prosecutors can pursue civil and criminal remedies under analogous state laws.

SEC cryptocurrency enforcement

Legal authority to regulate cryptocurrencies

The SEC's claim of authority to regulate digital assets derives from the broad definition of the term "security" in the federal securities laws, which includes "investment contracts" in addition to other instruments such as stocks, bonds, and options. As interpreted by the Supreme Court in *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946), a transaction constitutes an "investment contract" where it involves (1) an investment of money (2) into a common enterprise (3) with an expectation of profit (4) based solely on the efforts of another. Because the DOJ has parallel authority to prosecute criminal violations of the federal securities laws, the DOJ and the SEC have a common institutional interest in whether digital assets are "securities," and both have advanced the view that certain digital assets are "investment contracts" under *Howey*.

Importantly, neither the SEC nor the DOJ has asserted that all digital assets are securities, but both have generally been successful in their efforts to apply the federal securities laws in the context of token ICOs. In September, the U.S. District Court for the Eastern District of New York applied the *Howey* factors to determine whether a cryptocurrency sold by a criminal was a security, and held that it was.[1] The U.S. District Court for the Southern District of California limited the SEC's broad claim of authority somewhat in its November decision in *SEC v. Blockvest*, which held that the token at issue was not a security because the defendant was able to show that it had only distributed tokens for testing purposes.[2] However, the long-term impact of the decision is unclear because it was not a final decision on the merits, and the SEC has asked the court to reconsider its decision. Moreover, the court reached its holding by applying the *Howey* factors, implicitly confirming the SEC's general view that it has authority to regulate cryptocurrencies satisfying the *Howey* test.

The SEC has also prevailed in a challenge to the extraterritorial reach of the federal securities laws to cryptocurrency sales. In *SEC v. PlexCorps*,[3] the U.S. District Court for the Eastern District of New York denied a motion to dismiss by Canada-based promoters of an ICO who argued that they were not subject to suit in the U.S. Based on the SEC's

[1] *United States v. Zaslavskiy*, No. 17 CR 647 (RJD), 2018 WL 4346339 (E.D.N.Y. Sept. 11, 2018).

[2] *SEC v. Blockvest*, LLC, No. 18CV2287-GPB(BLM), 2018 WL 6181408 (S.D. Cal. Nov. 27, 2018).

[3] No. 17-CV-7007 (CBA) (RML), 2018 WL 4299983 (E.D.N.Y. Aug. 9, 2018).

allegations that defendants solicited digital asset purchases in the U.S., travelled to the U.S. in connection with the ICO, used U.S.-based payment processors to receive funds, and hosted a website promoting the ICO in the U.S., the court in *PlexCorps* found no reason to depart from long-standing case law concerning the territorial reach of the securities laws and federal court jurisdiction.

Enforcement actions and priorities

In 2017 and the first half of 2018, the SEC primarily initiated cryptocurrency-related enforcement actions to remedy fraud in the context of ICOs. This focus on fraud continued in the second half of 2018, during which the SEC announced several new enforcement actions, and one settlement of a previously filed action, involving fraud or other misleading conduct:

– In August, the SEC announced a settled enforcement action against Tomahawk Exploration LLC and its founder, David Laurance.[4] The SEC found that, after unsuccessfully attempting to raise capital for oil drilling activity, Tomahawk attempted to sell tokens it called "Tomahawkcoins" through an ICO. Tomahawk also offered Tomahawkcoins to investors through a "Bounty Program" in exchange for online promotional and marketing services. In connection with both the ICO and the Bounty Program, Tomahawk made false statements concerning the company's exposure to risk, the drilling rights it had acquired, the background of Tomahawk's principals, and the marketability of Tomahawkcoins. The SEC found that "Tomahawkcoins" constituted both "investment contracts" and "options," and that the offer and sale of these tokens violated the registration and antifraud provisions of the federal securities laws. Based on Tomahawk's failure to raise money through its ICO and Laurance's inability to pay a fine, the SEC imposed a fine of just US$30,000 on Laurance. However, Laurance was barred from serving as an officer or director of any public issuer or from participating in any offering of a penny stock.

– In September, the SEC announced settled charges against Crytpo Asset Management, LP ("CAM") and its founder for offering securities to individuals with whom it had no pre-existing relationship and failing to register the fund as an investment company. CAM raised more than US$3.6 million from investors and held US$37 million in assets as of the end of 2017. The SEC also alleged that CAM falsely claimed to have filed a registration statement and to have been operating the "first regulated crypto asset fund in the United States." In consideration of "remedial acts promptly undertaken" by the respondents and of their cooperation with the SEC staff, the SEC "censured" the respondents and imposed a US$200,000 penalty.[5]

– The SEC commenced the *Blockvest* litigation described above in October.[6] In *Blockvest*, the SEC brought suit against Blockvest LLC and its founder in the U.S. District Court for the Southern District of California, and sought a preliminary injunction to block the defendants from proceeding with an ICO for its tokens. The SEC alleged that the defendants had lied to investors about the registration of these tokens, including by suggesting the tokens were regulated by a fictitious regulatory agency called the "Blockchain Exchange Commission." As noted above, the court denied the injunction because the SEC did not make a sufficient showing that the tokens were "investments contracts" under the Howey test, but that is only a preliminary finding and the SEC may ultimately prevail on the merits.

---

[4] *In re Tomahawk Exploration LLC, et al.*, Securities Act Release No. 10530 (Aug. 14, 2018).

[5] *In re Crypto Asset Management, LP, et al.*, Securities Act Release No. 10544 (Sept. 11, 2018).

[6] *See Blockvest*, 2018 WL 6181408 at *[1].

[7] *In re Mayweather*, Securities Act Release No. 10578 (Nov. 29, 2018); *In re Khaled*, Securities Act Release Nos. 10579 (Nov. 29, 2018).

– At the end of November, the SEC announced settled charges against professional boxer Floyd Mayweather Jr. and music producer Khaled Khaled, known as DJ Khaled, for failing to disclose payments they received for promoting investments in ICOs. The SEC found that these undisclosed promotional payments violated Section 17(b) of the Securities Act. Mayweather agreed to pay US$600,000 in disgorgement and penalties, and Khaled agreed to pay US$150,000 in disgorgement and penalties.[7]

– In December, the SEC announced a settlement with the two individual defendants in *SEC v. AriseBank*, a case filed in January 2018 in the U.S. District Court for the Northern District of Texas. The complaint alleged that the bank and its co-founders engaged in the unregistered sale of securities and defrauded investors by claiming that AriseBank would offer branded debit cards that could be used to spend various cryptocurrencies, and by misrepresenting its executives' credentials. Before a settlement was reached, the SEC secured court orders halting an ICO conducted by AriseBank and appointing a receiver to preserve its assets before a settlement was readed, the settling defendants[8] agreed to pay a total of US$2.3 million in restitution and civil penalties of US$184,767 for each defendant. They also consented to an order barring them from serving as officers or directors of public companies or participating in future offerings of digital assets constituting securities.[9]

The SEC's enforcement actions have not been limited solely to fraudulent and misleading conduct in the sale of crytpocurrencies. Since June, the SEC has announced five enforcement actions based on violations of SEC registration requirements with no allegation of fraud or other misleading conduct:

– On September 11, the SEC announced settled charges against TokenLot, LLC and its principals based on the company's operation as an unregistered broker-dealer.[10] The SEC found that TokenLot processed orders relating to more than 200 different digital tokens in connection with ICOs and secondary market sales through its website, which it described as an "ICO Superstore." The SEC also found that TokenLot received US$112,000 in commissions for the ICOs they promoted, US$232,000 from secondary sales, and approximately US$127,000 in marketing fees. Importantly, the SEC found that TokenLot took "prompt remedial measures" in response to its investigation, including voluntarily halting new purchase orders for tokens and sales of new ICO tokens, beginning to wind up the business, alerting the SEC to a pending unregistered ICO, and agreeing to refund investors' payments for unfilled secondary market sales. In view of these remedial efforts, the SEC agreed to resolve the charges in exchange for US$471,000 in disgorgement and civil penalties of US$45,000 for each of the two individual respondents. In settling the charges, the respondents also agreed to the appointment of an independent intermediary to take possession of and destroy TokenLot's digital tokens.

– In November, the SEC announced settled charges against Zachary Coburn for operating the EtherDelta digital token trading platform as an unregistered national securities exchange.[11] The SEC alleged that EtherDelta was as an online platform for secondary market trading of ERC20 tokens, and used a smart contract to execute and clear the trades on the Ethereum blockchain. The SEC specifically noted that Ether Delta users executed more than 3.6 million orders through the platform, and that "[a]lmost all of the orders . . . were traded after the Commission issued its 2017 DAO Report, which concluded that certain digital assets . . . were securities and that platforms that offered trading of these digital assets securities would be subject to the SEC's requirement that exchanges register or operate pursuant to an exemption." Coburn consented to the order and agreed to pay US$300,000 in disgorgement and US$75,000 in

---

[8] The SEC named AriseBank as a defendant, but as AriseBank is alleged to be an unincorporated association and has not appeared, this settlement appears to have substantially resolved the case.

[9] *SEC v. AriseBank, et al.*, No. 3:18-cv-00186-M (N.D. Tex. Dec. 11, 2018).

[10] *In re TokenLot, LLC, et al.*, Securities Act Release No. 10543 (Sept. 11, 2018).

[11] *In re Zachary Coburn,* Exchange Act Release No. 84553 (Nov. 8, 2018).

penalties. The SEC specifically noted that the penalty took into account Coburn's "cooperation" in its investigation.

– The following week, the SEC announced two settled enforcement actions against Carrier Eq, Inc. d/b/a Airfox and Paragon Coin, Inc., both issuers of ICOs, for failure to register their tokens under Section 5 of the Securities Act.[12] The SEC found that AirFox's and Paragon's ICOs raised approximately US$15 million and US$12 million, respectively. Based on remedial measures and cooperation on the part of both companies, the SEC agreed to settle the charges against them by imposing a US$250,000 civil penalty on each. Additionally, AirFox and Paragon undertook to register their tokens with the SEC as securities and pay damages to investors under § 12(a) of the Securities Act.

– In December, the SEC announced settled charges against CoinAlpha Advisors in connection with its management of an investment fund organized to invest in digital assets.[13] The SEC alleged that CoinAlpha sold limited partnership interests in the Fund to investors with which it had no pre-existing substantive relationships and that it engaged in a general solicitation of public interest in the limited partnership interests, without registering the limited partnership interests with the SEC. Upon being contacted by the SEC concerning its management of the fund, CoinAlpha agreed to unwind the fund, make all investors whole and take other remedial measures. In consideration of these remedial measures, the SEC agreed to accept a civil penalty of US$50,000 from CoinAlpha.

The cases above highlight that, whether or not fraud is at issue, the SEC is willing to reward prompt remedial action to correct any registration deficiency and compensate any harmed investors with substantially reduced civil penalties. However, the window of lenience could be closing in the near future. As the SEC continues to secure its legal authority to regulate digital asset sales, it may be less willing to grant similar leniency even where remedial efforts are taken.

FinHub

In October 2018, the SEC launched its new Strategic Hub for Innovation and Financial Technology ("FinHub"). According to a statement by SEC Chairman Jay Clayton issued in connection with the launch of FinHub, the site is intended to provide "a central point of focus for our efforts to monitor and engage on innovations in the securities markets that hold promise, but which also require a flexible, prompt regulatory response to execute our mission."[14] While not exclusively devoted to cryptocurrency issues, FinHub is a helpful resource regarding the SEC's regulatory and enforcement activities and includes information of interest to the cryptocurrency industry. FinHub is in many ways similar to the CFTC's LabCFTC website, which was launched in May 2017, and was intended to serve as the CFTC's "focal point to promote FinTech innovation and fair competition by making the CFTC more accessible to FinTech innovators and serving as a platform to inform the CFTC's understanding of new technologies."[15]

CFTC cryptocurrency enforcement

Like the SEC, the CFTC continued to play an active role in the regulation of cryptocurrency products in the second half of 2018. The CFTC's enforcement actions to date have generally focused on cases involving fraud or other misleading conduct.

In *CFTC v. My Big Coin Pay, Inc.,*[16] the CFTC obtained a favorable ruling in an action it filed in the District of Massachusetts against the promoters of the My Big Coin ("MBC") virtual currency. The CFTC alleged that the defendants raised

---

[12] *In re Carrier Eq, Inc. d/b/a AirFox,* Securities Act Release No. 10575 (Nov. 16, 2018); *In re In re Paragon Coin, Inc.,* Securities Act Release No. 10574 (Nov. 16, 2018).

[13] *In re CoinAlpha Advisors, LLC*, Securities Act Release No. 10582 (Dec. 7, 2018).

[14] U.S. Securities and Exchange Commission, *SEC Launches New Strategic Hub for Innovation and Financial Technology* (Oct. 18, 2018).

[15] U.S. Commodity Futures Trading Commission, *CFTC Launches LabCFTC as Major FinTech Initiative*, Release 7558-17 (May 17, 2017).

[16] 334 F. Supp. 3d 492 (D. Mass 2018).

approximately US$6 million by falsely characterizing MBC trading markets and prices, along with the coin's functionality, in violation of the CEA and CFTC regulations. The CEA defines the term "commodity" to include, In addition to various agricultural products, any "good or article in which contracts for future delivery are . . . dealt in." Defendants moved to dismiss, arguing that MBC is not a "commodity" within the meaning of the CEA because there is no market for futures contracts in MBC. Substantially following the U.S. District Court for the Eastern District of New York's March 2018 holding in *CFTC v. McDonnell,*[17] the court held that, as a digital currency, MBC fell within the CEA's definition of "commodity" because the statute requires courts to focus on "categories—not specific items—when determining whether the 'dealt in" requirement is met," and it was undisputed that there is a futures market in digital currencies generally.[18]

Following its earlier win at the motion to dismiss stage in *CFTC v. McDonnell*, the CFTC prevailed on the merits following a four-day bench trial held in July.[19] The U.S. District Court for the Eastern District of New York found that Patrick McDonnell and CabbageTech, Corp. d/b/a Coin Drop Markets ("CDM") had engaged in a deceptive and fraudulent virtual currency scheme to induce customers to send money and virtual currencies to CDM. The court found that McDonnell had misappropriated customer funds and entered judgment against the defendants imposing restitution and penalties of nearly US$1.2 million.

On October 18, the CFTC announced that it reached a settlement of more than US$2.5 million in penalties in restitution in *CFTC v. Gelfman Blueprint, Inc.*,[20] a case it commenced in 2017, and obtained a default judgment for more than US$1.9 million in penalties and restitution in *CFTC v. Dean*,[21] a case filed in early 2018. *Gelfman* was filed in the U.S. District Court for the Southern District of New York and *Dean* was filed in the U.S. District Court for the Eastern District of New York. Like *McDonnell* and *My Big Coin Pay*, both *Gelfman Blueprint* and *Dean* involved allegations of fraud.

The CFTC also announced a new settled enforcement action on November 9. In *In re Kim*, [22] the CFTC alleged that Joseph Kim had misappropriated approximately 980 Litecoins and 339 Bitcoins from his employer between September and November 2017 to cover personal trading losses and, when questioned about the missing funds by his employer, provided false explanations. After his fraud was discovered by the employer, Kim was terminated. He then fraudulently obtained more than US$500,000 from other individuals by misrepresenting the circumstances of his departure from his prior employer, and continued trading virtual currencies in what the CFTC described as "an ill-fated attempt to cover his previous losses." When Kim began to experience losses as a result of his trading activity, he concealed those losses by sending false account statements to his customers. To settle the CFTC's charges, Kim agreed to pay more than US$1.1 million in restitution. Separately, the DOJ also filed criminal charges against Kim in the U.S. District Court for the Northern District of Illinois for the same underlying conduct. After pleading guilty, Kim was sentenced to a 15-month prison term. [23]

The CFTC will likely continue its focus on aggressively pursuing fraud charges in connection with virtual currency sales. In its 2018 annual report, the CFTC's Division of Enforcement highlighted "the need for robust enforcement to ensure technological development isn't undermined by the few who might seek to capitalize on this development for an unlawful gain."[24] In the Division of Enforcement's words, these enforcement efforts are intended "to facilitat[e] market-enhancing innovation in the financial technology space." However, if the CFTC follows the same course charted by the SEC in the second half of 2018, it may begin to more aggressively enforce the registration requirements of the CEA in the near future.

---

[17] 287 F. Supp. 3d 213 (E.D.N.Y. 2018).

[18] 334 F. Supp. 3d at 498.

[19] U.S. Commodity Futures Trading Commission, *CFTC Wins Trial Against Virtual Currency Fraudster* (Aug. 24, 2018).

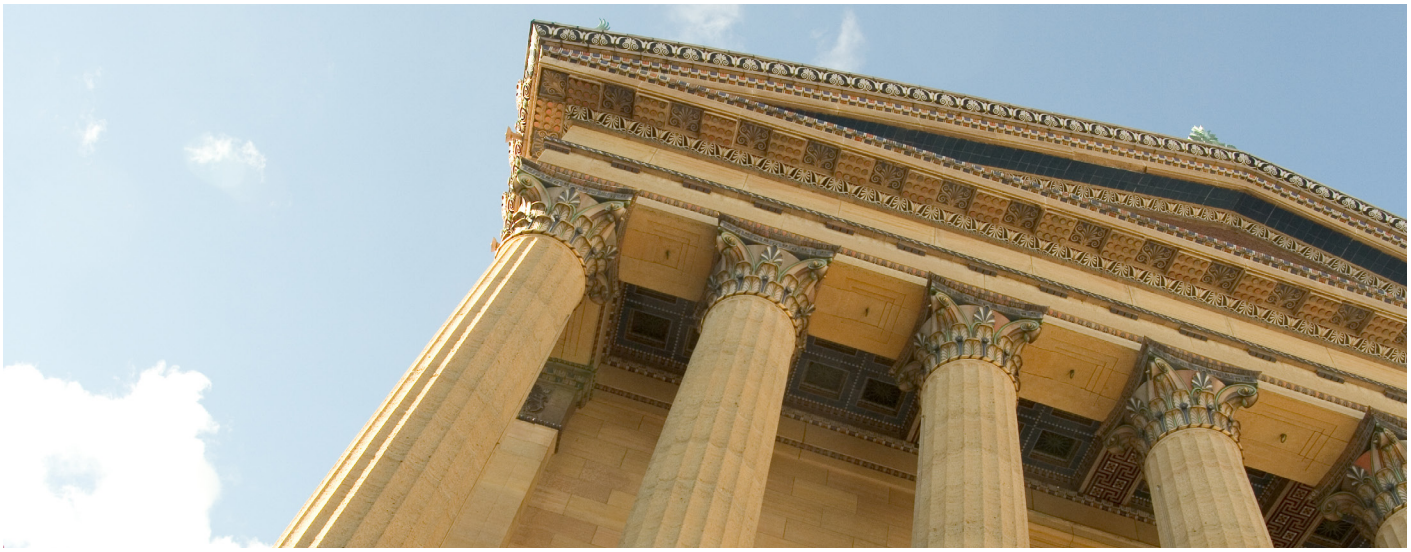
[20] No. 1:17-cv-07181 (S.D.N.Y. Oct. 2, 2018).

[21] No. 2:18-cv-00345 (C.D.N.Y. July 9, 2018).

[22] U.S. Department of Justuce, *Order Instituting Proceedings Dechert LLP. 19-02* (Oct. 29, 2018).

[23] U.S. Department of Justice, *Trading Sentenced to 15 Months in Federal Prison for Misappropriating $1.1 Million in Cryptocurrencies* (Nov. 13, 2018).

[24] U.S. Commodity Futures Trading Commission, *FY 2018 Division of Enforcement Annual Report* (November 2018).



DOJ investigation and enforcement

Like the SEC and CFTC, the DOJ is actively pursuing cases in the cryptocurrency industry, with a strong emphasis on preventing the use of cryptocurrency in connection with fraud and to further other criminal activity. In the second half of 2018, the DOJ brought at least nine new criminal cases relating to Bitcoin and other digital assets. The DOJ has also used civil forfeiture to recover criminal proceeds to complement these criminal prosecutions, such as in *United States v. 2013 Lamborghini Aventador LP700-4*, a civil forfeiture action brought by the DOJ following the death of AlphaBay digital marketplace founder Alexandre Cazes while facing criminal charges.[25]

The DOJ appears to be continuing to work with the CFTC to investigate potential Bitcoin price manipulation alleged to have occurred in late 2017. According to November 2018 reports from Bloomberg and CNBC, the DOJ is now focusing its investigation on whether a cryptocurrency backed by U.S. dollars was used to stabilize and manipulate the price of Bitcoin.[26] Neither the DOJ nor the CFTC has commented publicly on the investigation, so it is not possible to ascertain its precise scope at this time.

In *United States v. Zaslavskiy*,[27] a case resulting from an investigation that the DOJ pursued in parallel with the SEC, defendant Maksim Zaslavskiy moved to dismiss criminal securities fraud charges filed in the U.S. District Court for the Eastern District of New York in 2017. The DOJ had alleged that Zaslavskiy committed fraud in connection with two ICOs, REcoin and Diamond. Zaslavskiy argued that these tokens were beyond the reach of the federal securities laws and that the federal securities laws are unconstitutionally vague as applied. In September, the Eastern District of New York rejected both arguments. The court wrote that, "[s]tripped of the 21st-century jargon, including the Defendant's own characterization of the offered investment opportunities, the challenged Indictment charges a straightforward scam, replete with the common characteristics of many financial frauds." Following the court's decision denying his motion to dismiss, Zaslavskiy pleaded guilty on November 15, 2018. Although federal trial court decisions are not binding on other courts, the U.S. District Court for the Eastern District of New York's decision in *Zaslavskiy* is likely to influence similar cases in the future.

---

[25] No. 1:17-cv-00967-ljo-sko, 2018 WL 3752131 (E.D. Cal. Aug. 8, 2018).

[26] Bloomberg News, *Bitcoin-Rigging Criminal Probe Focused on Tie to Tether*, (Nov. 20, 2018); CNBC, *As bitcoin nosedives, regulators said to be investigating whether it was propped up illegally* (Nov. 20, 2018).

[27] No. 17 CR 647 (RJD), 2018 WL 4346339 (E.D.N.Y. Sept. 11, 2018).

Treasury Department regulation and enforcement

The Treasury Department's Financial Crimes Enforcement Network ("FinCEN") and Office of Foreign Assets Control ("OFAC") have also taken important steps to regulate the cryptocurrency industry and protect participants against fraud and other abuse.

In an October advisory, FinCEN provided advice to U.S. financial institutions concerning the detection of illicit transactions by or on behalf of Iran.[28] The advisory noted that "virtual currency is an emerging payment system that may provide potential avenues for individuals and entities to evade sanctions," and that while the Central Bank of Iran has banned domestic financial institutions from handling decentralized virtual currencies, individuals and businesses in Iran can still access virtual currency platforms through the Internet." The advisory further recommended that institutions dealing in digital assets review blockchain ledgers for activity that may originate or terminate in Iran and monitor open blockchains and investigate transactions to or from peer-to-peer exchanges. Financial institutions are also advised to maintain systems to comply with relevant sanctions requirements and Anti-Money Laundering and Countering the Financing of Terrorism ("AML/CFT") obligations, including by screening against OFAC's List of Specially Designated Nationals and Blocked Persons (commonly known as the "SDN list"). FinCEN also provided three "red flags" for potential illicit transactions that relate specifically to digital asset businesses: (1) logins from Iran-based IP addresses or using Iran-based email servers; (2) payments to or from Iran-based exchanges; and (3) "[u]nexplained transfers into a customer account from multiple individual customers combined with transfers to or from virtual currency exchanges."

In November 2018, for the first time, OFAC added digital currency addresses to its SDN List.[29] This move had been anticipated since at least March 2018, when OFAC released a set of Frequently Asked Questions relating to virtual currency indicating that it may add digital currency addresses to the SDN List and encouraging any parties "who identify digital currency identifiers or wallets that they believe are owned by, or otherwise associated with, an SDN and hold such property should take the necessary steps to block the relevant digital currency and file a report with OFAC that includes information about the wallet's or address's ownership, and any other relevant details."[30] Cryptocurrency industry participants should ensure that their compliance systems are capable of identifying and utilizing digital asset addresses added to the SDN List going forward.

During the ABA's Financial Crimes Enforcement Conference held in December 2018, Under Secretary for Terrorism and Financial Intelligence Sigal Mandelker outlined Treasury's enforcement priorities.[31] With respect to digital currencies in particular, Under Secretary Mandelker encouraged the "digital currency industry . . . to harden its networks and undertake the steps necessary to prevent illicit actors from exploiting its services." Under Secretary Mandelker also emphasized that financial industry participants should implement "effective sanctions compliance program[s]" designed to commit senior management to compliance efforts, conduct frequent risk assessments, develop and deploy internal controls and procedures to identify and report prohibited activity, conduct frequent testing and auditing, and ensure training for all

---

[28] Office of Foreign Assets Control, *Advisory on the Iranian Regime's Illicit and Malign Activities and Attempts to Exploit the Financial System*, FIN-2018-A006 (Oct. 11, 2018).

[29] Office of Foreign Assets Control, *Cyber-related Designations; Publication of New Cyber-related FAQs* (Nov. 28, 2018).

[30] Office of Foreign Assets Control, *OFAC FAQs: Sanctions Compliance*, #562 (March 19, 2018).

[31] Department of the Treasury, *Under Secretary Sigal Mandelker Remarks ABA/ABA Financial Crimes Enforcement Conference* (Dec. 3, 2018).

relevant personnel. She described these "types of compliance commitments" as "an essential element in settlement agreements between OFAC and apparent violators." Finally, Under Secretary Mandelker noted that Treasury is "encouraging our international partners to take urgent action to strengthen their AML/CFT frameworks for virtual currency and other related digital asset activities," and to follow the U.S. lead in bringing enforcement actions.

State regulatory efforts

State regulators and law enforcement officials continue to work with their federal and international counterparts to police the cryptocurrency space.

The North American Securities Administrators Association ("NASAA") released an update in August concerning Operation Cryptosweep, its joint effort to crack down on cryptocurrency-related misconduct.[32] The update announced that "more than 200 active investigations of [ICOs] and cryptocurrency-related investment products are currently underway by state and provincial securities regulators in the United States and Canada." This marked an increase in investigation activity of 185% following NASAA's May 2018 release. NASAA also announced that its investigative activity had resulted in 45 enforcement actions involving ICOs and cryptocurrency-related investment products.

In September, the New York Attorney General ("NYAG") released its report on cryptocurrency trading platforms as part of the state's Virtual Markets Integrity Initiative.[33] Key conclusions from the NYAG's report include that the cryptocurrency exchange industry needs to improve systems to prevent conflicts of interest and abusive trading activity, and for the protection of customer funds. The report also highlighted the need for cryptocurrency exchanges to provide additional information to customers concerning the geographical location of the exchange, the jurisdictions from which customers are authorized to trade, the fees associated with maintaining an account and trading, and other information relating to exchange operations. While this report does not have the force of law, it provides a helpful roadmap of the factors that the NYAG and the New York Department of Financial Services are likely to consider when deciding whether to bring enforcement actions or issue licenses to exchanges operating in New York.

Private litigation

In the second half of 2018, at least 19 private lawsuits pertaining to cryptocurrencies were filed in U.S. state and federal courts. Nearly half of these cases were filed in California, but cases have also been filed in New York, Washington, Delaware, Illinois, and Florida. These cases involve a wide range of claims, including patent infringement, breach of contract, and violations of the federal securities laws. The first antitrust suit involving cryptocurrency products was also filed in December. In *United American Corp. v. Bitmain, Inc.*, the plaintiff alleges that, in connection with a hard fork [34] of the Bitcoin Cash blockchain on November 15, 2018, Bitmain Inc. led a "tight knit network of individuals and organizations to manipulate the cryptocurrency market for Bitcoin Cash" and caused US$4 billion in harm to cryptocurrency products holders in the U.S.[35] The case is still in the very early stages of litigation, but could set interesting precedent for future disputes over hard forks in cryptocurrencies.

---

[32] North American Securities Administrators Association, *NASAA Updates Coordinated Crypto Crackdown* (Aug. 28, 2018).

[33] Office of the New York State Attorney General, *Virtual Markets Integrity Initiative Report* (Sept. 18, 2018).

[34] A "hard fork" is a permanent divergence in a blockchain that typically results from disagreements about changes to the blockchains consensus rules. *See* Bitcon Project Glossery, *Definition of "Hard Fork."*

[35] *See* Complaint, *United American Corp. v. Bitmain, Inc.*, No. 1:18-cv-25106-KMW (S.D. Fla. filed Dec. 6, 2018), ECF No. 1.

Courts have also issued several decisions in private lawsuits that will shape the course of future litigation. These decisions touch on important issues in intellectual property, federal securities laws, and civil procedure.

Intellectual property

In *Founder Starcoin, Inc. v. Launch Labs, Inc.*,[36] the U.S. District Court for the Southern District of California denied the plaintiff's motion for a preliminary injunction barring the defendant from selling celebrity-sponsored collectible digital tokens. The plaintiff claimed that the defendant had developed the token after misappropriating purported trade secrets relating to a "licensing scheme for digital collectibles," but the court found that this lacked sufficient particularity for trade secret protection and that, in any case, "[m]arrying the concept of celebrity licensing blockchain technology appears, on its face, to be unremarkable, obvious, and general knowledge."

In *Telegram Messenger Inc. v. Lantah, LLC*,[37] the U.S. District Court for the Northern District of California granted plaintiff's motion for a preliminary injunction barring defendant from issuing its "GRAM" cryptocurrency. The court found that plaintiff had already used the "GRAM" mark in connection with cryptocurrency sales when defendant began to issue its competing cryptocurrency. Importantly, the court rejected the defendant's argument that the purchase agreements plaintiff had entered into with customers did not constitute a "use in commerce."

Federal securities laws

In *Coffey v. Ripple Labs Inc.*,[38] purchasers of Ripple had originally sued Ripple Labs in California state court, claiming that Ripple was an unregistered securities offering and seeking damages under the Securities Act and the California Corporations Code. The defendants removed the case to the U.S. District Court for the Northern District of California, but the plaintiffs challenged by filing a motion to remand to state court. Specifically, the plaintiff contended that the case was within the scope of the anti-removal provision of the Securities Act. In August, the court held that the case was properly removed to federal court under the Class Action Fairness Act ("CAFA") because the plaintiff had included California state-law claims in the complaint along with federal securities claims, rendering the anti-removal provision inapplicable to the case. Fewer than two weeks later, the plaintiff voluntarily dismissed the case.

In *Greenwald v. Ripple Labs, Inc.*,[39] a case similar in some respects to *Coffey* but which did not include California state law claims, the same judge of the U.S. District Court for the Northern District of California remanded to state court. In the absence of state-law claims, the court held that the anti-removal provision of the Securities Act clearly barred removal of the case. Together, *Coffey* and *Greenwald* may seem odd, in that a plaintiff's inclusion of state-law claims can result in removal to federal court, but plaintiffs intent on litigating Securities Act claims in state courts can still avoid removal by drafting complaints that are not removable under CAFA.

In *In re Tezos Securities Litigation*,[40] which also addressed personal jurisdiction questions discussed below, the U.S. District Court for the Northern District of California rejected the defendants' arguments that their claims in connection with the Tezos ICO involved the extraterritorial application of the federal securities laws. Noting that a "significant portion" of the investors in the ICO promoted by the Switzerland-based Tezos Foundation had been located in the United States and that a significant amount of the marketing activity occurred in the United States, the court held that Tezos investors' "contribution of Ethereum to the ICO became irrevocable only after it was validated by a network of global nodes clustered more densely in the United

[36] No. 18-cv-972 JLS (MDD), 2018 WL 3343790 (S.D. Cal. July 9, 2018).

[37] No. 18-cv-02811-CRB, 2018 WL 37535748 (N.D. Cal. Aug. 8, 2018).

[38] 333 F. Supp. 3d 952 (N.D. Cal. Aug. 10, 2018).

[39] No. 18-cv-047980-PJH, 2018 WL 4961767 (N.D. Cal. Oct. 15, 2018).

[40] No. 17-cv-06779-RS, 2018 WL 4293341 (N.D. Cal. Aug. 7, 2018).

States than in any other country." Thus, the court signaled that the technological design and implementation of a blockchain can be relevant for determining the territorial reach of federal law.

Finally, following the clear trend of other federal trial courts, in *Solis v. Latium Network, Inc.*,[41] the U.S. District Court for the District of New Jersey applied the *Howey* test in a December decision finding that Latium X ("LATX") tokens issued in an ICO conducted between July 2017 and March 2018 were sufficiently alleged to be "investment contracts" within the meaning of the federal securities laws. The defendants had attempted to distinguish their tokens from others that had been found to be securities because the tokens were used to facilitate transactions on its "blockchain-based tasking platform," but the court noted allegations that the defendants had led investors to expect a profit from the purchase of LATX tokens," and held that the plaintiff "adequately alleged that any potential return on investment in LATX tokens would have primarily resulted from the defendants' efforts.

Civil procedure

In *Pearce v. Mizuho Bank Ltd.*[42] and *Babiak v. Mizuho Bank, Ltd.*,[43] cases arising from the collapse of the Mt. Gox cryptocurrency exchange filed in the U.S. District Court for the Eastern District of Pennsylvania and the Eastern District of Virginia, respectively, the courts granted the Tokyo-based bank's against Mizuho Bank, Ltd. motions to dismiss for lack of personal jurisdiction. The plaintiffs failed to show that Mizuho Bank's refusal to process their withdrawal requests constituted activity directed to the forum states, and as the *Pearce* Court observed, Mizuho Bank's refusal to process the requests did not cause investors' losses, which were more directly caused by the collapse of Mt. Gox.

In contrast, the U.S. District Court for the Northern District of California in *In re Tezos Securities Litigation*[44] found that certain of the defendants involved in the Tezos ICO were subject to personal jurisdiction in the United States. Pointing to the fact that the Tezos Foundation had employed marketing professionals in California, directed the sale of Tezos to the U.S., and based its website in the United States, the court held that the Switzerland-based Tezos Foundation and its principals were subject to the court's jurisdiction. However, the court granted motions to dismiss for lack of jurisdiction by Bitcoin Suisse, which provided services in connection with the ICO, and venture capital investors based on the plaintiffs' failure to show that they engaged in conduct sufficiently directed to the United States.

In *Kleiman v. Wright*,[45] a case in the U.S. District Court for the Southern District of Florida arising out of a business operated by Craig Wright, who has publicly claimed to be Bitcoin founder Satoshi Nakamoto, and Dave Kleiman, Kleiman's estate alleges that Wright stole over 300,000 bitcoins from wallets owned by their joint business and Kleiman personally. Wright moved to dismiss the complaint on various grounds, but apart from Wright's statute of limitations argument, which the court partially accepted, the motion was denied. Of note is the court's ruling with respect to Wright's argument that the Southern District of Florida is an inconvenient forum for the suit. The court determined that Florida has a strong public interest in retaining jurisdiction over the suit because it "concerns a Florida company, regarding Florida assets (bitcoins mined in Florida) and intellectual property developed by that Florida company, where both the injured parties are Florida citizens."

[41] No. 18-10255 (SDW) (SCM), 2018 WL 6445543 (D.N.J. Dec. 10, 2018).

[42] No. 18-306, 2018 WL 4095812 (E.D. Pa. Aug. 27, 2018).

[43] No. 1:18-cv-352, 2018 WL 4473584 (E.D. Va. Sept. 17, 2018)

[44] No. 17-cv-06779-RS, 2018 WL 4293341 (N.D. Cal. Aug. 7, 2018).

[45] No. 18-cv-80176-BLOOM/Reinhart, 2018 WL 6812914 (S.D. Fla. Dec. 27, 2018).

Looking ahead

The SEC's efforts to enforce the registration requirements of the federal securities laws are likely to continue and increase. As noted previously, the SEC has generally prevailed in its attempts to exercise jurisdiction over certain digital assets as "securities." However, legislation has been proposed that would limit the SEC's authority to regulate cryptocurrencies and many tokens. In December, Congressmen Warren Davidson and Darren Soto introduced bipartisan proposed legislation that would amend the Securities Act and the Exchange Act to exempt "digital tokens" from the scope of the definition of the term "security." As proposed, this "Token Taxonomy Act" would also change the tax treatment for gains from the sale or exchange of virtual currencies, and permit individuals to hold virtual currencies in IRAs. Interestingly, the bill would not attempt to change the CFTC's authority to regulate virtual currencies as commodities.

Finally, the CFTC published a request for industry input regarding technology, mechanics, and markets for the virtual currency Ether and its use on the Ethereum Network on December 17, 2018.[46] The CFTC is already familiar with the leading virtual currency Bitcoin, and futures on Bitcoin are currently traded on the Chicago Mercantile Exchange and CBOE Futures Exchange. The CFTC is seeking to better understand the similarities between Bitcoin and Ether and to understand unique aspects of Ether and the Ethereum Network. Public comments must be received on or before February 15, 2019, and the responses to this request could inform the CFTC's understanding of the market for Ether and any derivatives contracts on Ether that designated contract markets may list in the future.

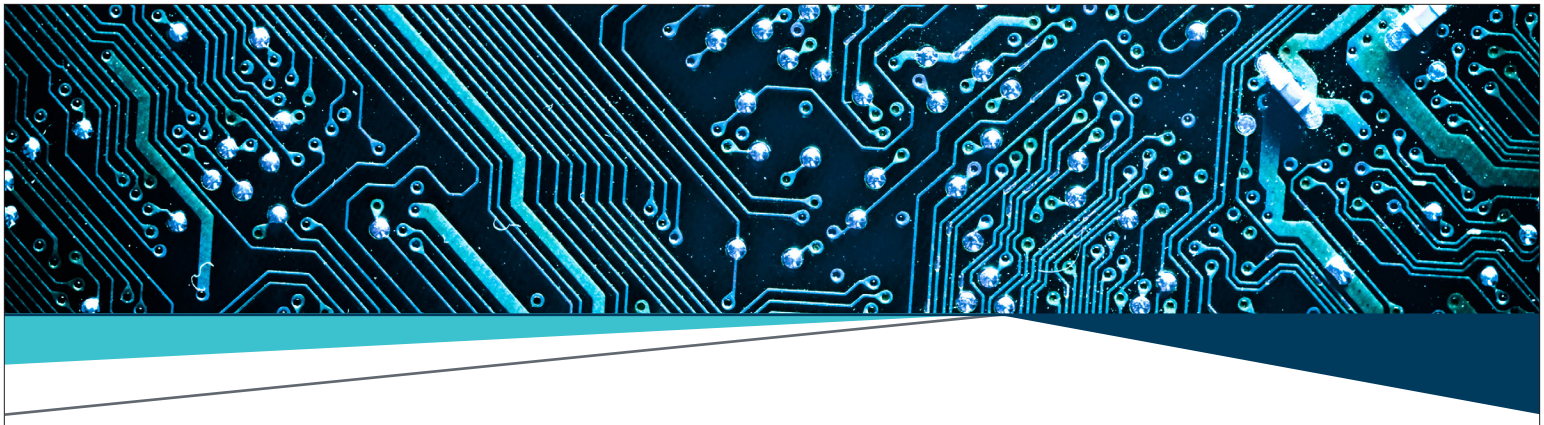
How Dechert can assist

The increasing use of cryptocurrencies and other digital assets has given rise to complex legal issues relating to compliance, securities transactions, litigation and regulatory enforcement. Dechert remains steeped in the industry and will provide updates on critical cases and regulatory actions as they arise.

Dechert offers sophisticated and knowledgeable legal counsel to clients navigating this rapidly evolving space. At the heart of Dechert's cryptocurrency and blockchain practice is a deep understanding of the technologies that drive blockchain and related developments in distributive computing networks. In addition, Dechert is distinctive among leading law firms in this area by bridging the financial service regulation and new financial technology to find solutions for our clients.

Dechert's Investigations and White Collar Defense practice has extensive experience in navigating enforcement actions by the DOJ, SEC, CFTC and other agencies in the United States and throughout the world. In addition, our Financial Services Group is one of the leaders today in advising firms on the regulatory consequences of various cryptocurrency and blockchain-based transactions. As cryptocurrency enforcement policies continue to evolve, we will work with clients to anticipate compliance trends, defend against enforcement actions, and react to any issues that may arise.

[46] CFTC Request for Input on Crypto-Asset Mechanics and Markets, 83 Fed. Reg. 64563 (Dec. 17, 2018).



Dechert's Cryptocurrency and Blockchain Resources Center

Providing the latest news, updates and analysis.

Since the launch of bitcoin in 2009, cryptocurrencies and the encrypted, decentralized blockchain protocol that underpins them have grown from abstract theories to a transformational force that is disrupting the way many industries will operate for decades to come.

Dechert's cryptocurrency and blockchain technology website brings together a selection of resources on this subject, including legal updates and event recordings.

dechert.com/cryptocurrency

Contact us

Joseph A. Fazioli
Partner
Silicon Valley: +1 650 813 4836
San Francisco: +1 415 262 4529
joseph.fazioli@dechert.com

Anthony Kelly
Partner
Washington, D.C.
+1 212 698 3533
anthony.kelly@dechert.com

Christine Isaacs
Associate
New York
+1 2212 641 5675
christine.isaacs@dechert.com

Susie S. Park
Associate
Washington, D.C.
+1 202 261 3455
susie.park@dechert.com

Michael J. Gilbert
Partner
New York
+1 212 698 3886
michael.gilbert@dechert.com

Timothy Spangler
Partner
Orange County: +1 949 442 6044
Silicon Valley: +1 650 813 4803
timothy.spangler@dechert.com

Paul C. Kingsbery
Associate
New York
+1 212 641 5663
paul.kingsbery@dechert.com

Lindsay E. Ray
Associate
New York
+1 212 698 3533
lindsay.ray@dechert.com