ABA BUSINESS LAW SECTION
DERIVATIVES & FUTURES LAW COMMITTEE
WINTER MEETING
JANUARY 24-26, 2019
LA PLAYA BEACH & GOLF RESORT
NAPLES, FL

Data, Reporting and the Enforcement Division:
How financial institutions and regulators can,
do and should use data
January 25, 2019
9:00 a.m. – 10:00 a.m.

Chair:
Doug Harris (Promontory)

Panel:
Salman Banaei (Markit)
Debra Cook (DTCC)
Neel Chopra (CFTC)
Kim Johns (Goldman)
Anne Termine (Covington)
The virtual currency regulatory framework in global context
Sharon Brown-Hruska and Trevor Wagener*

Key Points
- As of July 2018, regulatory, enforcement and private litigation developments have followed a different path in the USA than in other major jurisdictions around the world. Whereas the USA has attempted to regulate virtual currencies by applying longstanding commodity, securities and anti-money laundering frameworks, other major jurisdictions have taken very different approaches.
- Starting in late 2017, US regulators began focusing substantial regulatory attention on virtual currency oversight, resulting in a veritable explosion of regulatory guidance, enforcement actions and class action filings.
- This trend only accelerated further in early 2018. The first three months of 2018 featured more US virtual currency regulatory guidance, enforcement actions and private action filings than all of 2017.
- In total, 71 US enforcement actions and 38 private civil actions related to virtual currency, including 29 putative class actions, have been filed. Year 2018 accounts for an outright majority of all virtual currency enforcement actions, private civil actions and putative class actions.
- An outright majority of US private actions filed in matters connected to virtual currencies have been securities class actions, and as a result the issues raised have frequently included familiar artificial price and Rule 10b-5 stock-drop elements.
- The unique features of virtual currency and related digital assets like smart contracts raise distinct questions that need to be answered in many matters.
- As of 2 July 2018, virtual currencies are collectively valued at nearly $300 billion, following a decline from over $600 billion in December 2017.

1. Introduction
The development of a collaged regulatory framework and an upsurge of enforcement actions and private litigation in virtual currency coincided with a dramatic increase in virtual currency market capitalizations and a wave of initial coin offerings. Eight years after the creation of Bitcoin first brought the concept of virtual currency to broad public awareness, 2017 saw an avalanche of regulatory guidance, enforcement actions and class action filings related to virtual currency. As of 26 March 2018, virtual currencies were collectively valued at over $300 billion.

* Dr Sharon Brown-Hruska is Managing Director in the Washington, DC office of National Economic Research Associates, Inc. Dr Brown-Hruska was previously Commissioner and Acting Chairman of the United States Commodity Futures Trading Commission, a federal regulator that has asserted jurisdiction over virtual currency markets. Dr Brown-Hruska has a PhD in economics from Virginia Polytechnic Institute and State University. Trevor Wagener is a Consultant in the Washington, DC office of National Economic Research Associates, Inc. Mr Wagener was previously a commodities analyst and derivatives trader. Mr Wagener graduated with an MSc in applied economics from Johns Hopkins University in 2017 and a BA with distinction in ethics, politics, and economics from Yale University in 2011.
Although virtual currency market capitalizations have fallen by nearly 50 per cent from their peak in December 2017, regulatory guidance and legal actions have only accelerated since then: the first three months of 2018 featured more virtual currency regulatory guidance, enforcement actions and private action filings than all of 2017. In total, at least 46 enforcement actions and 25 private actions related to virtual currency have been filed, with 2018 currently on pace to account for an outright majority of all virtual currency enforcement actions and putative securities class actions.

An outright majority of private actions filed in matters connected to virtual currencies have been securities class actions, and as a result the issues raised have frequently included familiar artificial price and Rule 10b-5 stock-drop elements. However, the unique features of virtual currency and related digital assets like smart contracts create additional distinct questions that need to be answered in many matters.

This article is designed as a primer that introduces readers to the concept and practice of virtual currency and the blockchain. It updates and expands upon a previous study of trends in virtual currency regulation and litigation, incorporating the global regulatory frameworks, recent enforcement actions defining the direction in the US markets, and emerging trends in US private virtual currency litigation, particularly securities class actions.

2. Background

Virtual currencies and cryptocurrencies

A virtual currency is a digital token ‘representation of value that functions as a medium of exchange, a unit of account, and/or a store of value’, but ‘does not have legal tender status’. If the virtual currency can be readily expressed in or substituted for recognized currencies, it is called a convertible virtual currency. Convertible virtual currencies have had volatile total market capitalizations, rising to over $600 billion on 18 December 2017 and falling to $268 billion as of 2 July 2018. These market capitalizations suggest markets have recently considered convertible virtual currencies collectively at least as valuable as Wells Fargo. Figure 1 shows the market capitalization of convertible virtual currencies as of 8 February 2018.

The most prominent subset of convertible virtual currencies, as of February 2018, called cryptocurrencies, utilizes ‘cryptographic proof’ rather than trusted third parties such as financial intermediaries, as a basis for electronic payments in the virtual
currency.\textsuperscript{7} Bitcoin, the largest convertible virtual currency by market capitalization as of February 2018,\textsuperscript{8} is an example of a cryptocurrency that utilizes cryptography and unique digital signatures to allow for decentralized, peer-to-peer electronic payments.\textsuperscript{9}

Although virtual currencies existed prior to Bitcoin,\textsuperscript{10} Bitcoin’s introduction in 2009 changed the paradigm for convertible virtual currencies by establishing a robust decentralized architecture for cryptocurrency peer-to-peer payments. This architecture includes public and private keys, the blockchain ledger, and open-source software facilitating the use of decentralized networks of computers, called ‘miners’, to solve complex mathematical algorithms in order to validate and log peer-to-peer transactions on the blockchain ledger.\textsuperscript{11}

### Blockchain

Distributed ledger technology, better known as blockchain, generally consists of an open, decentralized ledger that allows each party on the blockchain access to the entire database and provides no party with complete control of the data. Generally, this decentralization

---


\textsuperscript{8} Bitcoin’s market capitalization on 20 February 2018 was approximately $200 billion, more than double the market capitalization of the second largest cryptocurrency, Ethereum. See Cryptocurrency Market Capitalizations, <https://coinmarketcap.com/all/views/all/> accessed 20 February 2018.

\textsuperscript{9} Nakamoto (n 7). See also Commodity Futures Trading Commission (n 7) 5.


\textsuperscript{11} Miners are compensated via transaction fees and newly created bitcoins that are supplied to the market at a predefined rate. Commodity Futures Trading Commission (n 7) 5–6. See also Nakamoto (n 7) 1–8.
means a ‘node’ system is used whereby multiple nodes can be used to engage in transactions, and records of those transactions are then forwarded to all other nodes. In order to prevent ‘double spending’, a major concern with virtual currencies, each transaction recorded in the ledger is made unalterable via complex algorithms that ensure each transaction is mathematically linked to every previous transaction. Consequently, an adjustment made to one transaction would require the recalculation of all subsequent transactions, a computationally prohibitive requirement that should, in principle, ensure that all recorded transactions are permanent and inviolable.

**Virtual currency exchanges**

In order to purchase units of convertible virtual currencies using legal tender, or to convert units of a convertible virtual currency into legal tender (or units of other convertible virtual currencies that could in turn be converted into legal tender), users transact with a financial institution known as a virtual currency exchange (or cryptocurrency exchange). Virtual currency exchanges have come under increasing regulatory scrutiny as the entry/exit points from cryptocurrencies whose transaction histories are usually largely anonymous. Consequently, financial regulators, such as the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC), Bank Secrecy Act/Anti-Money Laundering (BSA/AML) authorities like the US Financial Crimes Enforcement Network (FinCEN), tax authorities like the Internal Revenue Service (IRS) and economic and trade sanctions authorities like the Office of Foreign Assets Control (OFAC) have all increasingly focused on virtual currency exchanges as the points on cryptocurrency networks that are most amenable to regulation and scrutiny, investigations and enforcement actions or collections efforts. The IRS issued guidance in 2014 stating that convertible virtual currency is ‘for federal tax purposes, … treated as property’, but has yet to issue further substantive guidance.

12 Double spending occurs when the owner of a virtual currency attempts to use the same individual unit of the virtual currency twice.
14 ‘A virtual currency exchange is a person or entity that exchanges virtual currency for fiat currency, funds, or other forms of virtual currency. Virtual currency exchanges typically charge fees for these services.’ Securities and Exchange Commission, ibid. ‘In a typical transaction, the buyer of virtual currency provides sovereign currency to a business that either holds value in the form of a desired virtual currency or who upon receipt of sovereign currency executes a purchase of the virtual currency from another source. … These transactions are money transmission …’ Washington State Department of Financial Institutions, ‘Interim Regulatory Guidance on Virtual Currency Activities’ 8 December 2014, p 3 <https://dfi.wa.gov/documents/money-transmitters/virtual-currency-interim-guidance.pdf> accessed 13 February 2018.
16 Internal Revenue Service, ibid p 2.
Initial coin offerings

In recent years, a substantial number of new virtual currencies have been sold via initial coin offerings (ICOs), also called token sales. ICOs typically involve the sale of digital tokens to the public in order to raise capital for projects. The projects intended to be capitalized via ICOs are commonly connected to the new virtual currency, such as the development of a blockchain or open source software to support a network on which the digital tokens can be used, or the creation of a service that is intended to use the virtual currency as an access tool.\(^\text{17}\)

According to a December 2017 NERA Economic Consulting report on ICOs (the ‘NERA ICO Report’), ICOs raised more than $2 billion from January through August of 2017 and commonly involved the sale of digital tokens prior to the creation of the underlying services.\(^\text{18}\) The NERA ICO Report concluded that ICOs might attract the attention of regulators and private litigants due to the conjunction of large quantities of capital raised via ICOs, negative returns on the median ICO token, and claims that some ICOs have been promoted using white papers that downplay the risks involved.\(^\text{19}\)

Smart contracts and decentralized autonomous organizations

Smart contracts have been defined as programmes or systems that automatically move, assign or transact in digital assets according to pre-specified rules that are enforced by a peer network.\(^\text{20}\) Many recent smart contract projects are connected to a peer network through distributed ledger technology, and some have attempted to create long-term projects called decentralized autonomous organizations (sometimes called ‘virtual organizations’) that have some analogous features to funds or companies. For example, one white paper for a smart contract project on the Ethereum blockchain described a decentralized autonomous organization as:

[A] virtual entity that has a certain set of members or shareholders which, perhaps with a 67% majority, have the right to spend the entity’s funds and modify its code. The members would collectively decide on how the organization should allocate its funds. . . . This essentially replicates the legal trappings of a traditional company or non-profit but using only cryptographic blockchain technology for enforcement.\(^\text{21}\)

One prominent example of a decentralized autonomous organization was the DAO, which was created with the stated intent to create a lasting smart contract on the Ethereum blockchain that would formalize, automate and enforce contract terms through

---

\(^\text{17}\) See Securities and Exchange Commission (n 13).


\(^\text{19}\) ibid 1 and 6.


software. The DAO raised funds from investors in 2016 in exchange for DAO Tokens, but an attacker exploited a vulnerability in the DAO’s code to take control of approximately one-third of the Ethereum tokens invested in the DAO. In order to make investors whole, the group behind the DAO endorsed a ‘hard fork’ on the Ethereum blockchain, allowing those investors who switched to the new version of the blockchain to exchange their DAO Tokens for Ethereum tokens.

3. Contrasting global regulatory approaches

Overview

As convertible virtual currencies have only recently become widespread, most regulators and supervisory authorities around the globe are still developing regulatory frameworks for virtual currencies. Many of these international virtual currency regulatory frameworks are inconsistent and even mutually incompatible, raising the spectre of potential market fragmentation. Because there are nuanced differences between the regulatory frameworks of almost all countries, this section will cover regulatory developments in a curated sample of major jurisdictions outside of the USA: The UK, Japan, South Korea and China. The regulatory developments in each of these jurisdictions are summarized in Table 1.

The UK

On 3 March 2014, The UKs HM Revenue and Customs released a policy paper that broadly labelled profits and losses on virtual currencies as subject to corporation tax, income tax and capital gains tax, but generally not subject to value-added tax (VAT). In March 2015, the UKs Treasury announced that ‘the government intends to apply anti-money laundering regulation to digital currency exchanges, to support innovation and prevent criminal use’. On 15 December 2017, the European Commission published a fact sheet on its updated Anti-Money Laundering directive that extended anti-money laundering and counter terrorism financing rules to virtual currency exchanges, platforms and wallet services.

On 6 April 2018, the Financial Conduct Authority announced that while cryptocurrencies are not independently regulated and are not considered ‘currencies or commodities for regulatory purposes’, cryptocurrency derivatives like futures, options

23 ibid p 9.
24 ibid pp 9–10.
Table 1. Virtual currency regulatory frameworks in select countries

<table>
<thead>
<tr>
<th>Jurisdiction</th>
<th>Tax framework</th>
<th>Anti-money laundering framework</th>
<th>Securities &amp; commodities framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>United Kingdom</td>
<td>Virtual currencies are covered by corporation, income and capital gains taxes, but not VAT.</td>
<td>Government moving to require AML reporting by virtual currency exchanges. Under EU-wide reforms, AML rules will apply to virtual currency exchanges, platforms and wallet services.</td>
<td>Virtual currencies are not considered securities or commodities, but virtual currency derivatives are considered financial instruments under MiFID II.</td>
</tr>
<tr>
<td>Japan</td>
<td>Consumption taxes on transfers of cryptocurrency were abolished as of 1 July 2017, but capital gains in virtual currency are taxable.</td>
<td>Virtual currency exchanges must register and follow AML requirements like Know Your Customer and suspicious transaction reporting.</td>
<td>Virtual currencies are considered means of payment and not financial products, so exchange-listed virtual currency derivatives are prohibited. Platforms must register, meet capital requirements and follow Japan’s means of payment regulations. ICOs, margin trading in virtual currency and virtual currency futures were banned in 2017. In 2018, South Korea moved toward removing the ban on domestic ICOs.</td>
</tr>
<tr>
<td>South Korea</td>
<td>Capital gains on virtual currency are taxed at 24.2%.</td>
<td>Know Your Customer rules require that virtual currency trading be tied to bank accounts with investors’ real names. Banks are required to follow AML policies with respect to those accounts.</td>
<td>China has effectively banned financial institutions from intermediating virtual currency transactions.</td>
</tr>
<tr>
<td>China</td>
<td>N/A</td>
<td>China has effectively banned financial institutions from intermediating virtual currency transactions.</td>
<td>China has banned fundraising through ICOs, warned banks not to conduct virtual currency transactions and effectively banned private provision of virtual currency services.</td>
</tr>
</tbody>
</table>

and contracts for differences are ‘capable of being financial instruments under the Markets in Financial Instruments Directive II’.  

Japan

On 25 May 2016, Japan passed the Crypto Currency Act, which classified virtual currency as a means of payment and required virtual currency exchange businesses to register, meet capital requirements, follow Know Your Customer rules, report suspicious transactions, submit to periodic audits, separate customer funds from firm funds and follow Japan’s rules for means of payment and settlement. The law went into effect on 1 April 2017.29 Because Japan has classified virtual currencies as a means of payment and not financial products such as securities, Japan does not allow domestic, exchange-listed virtual currency derivatives.30 However, according to an analysis by Greenberg Traurig LLP, contracts for differences may be permitted in some circumstances.31

At least sixteen virtual currency exchanges were registered with Japan’s Financial Services Agency as of 7 March 2018, and Japanese authorities have issued public warnings to exchanges which had yet to register and comply with the Crypto Currency Act.32 In addition, Japanese regulators issued multiple punishment notices to exchanges for inadequate controls following a $530 million theft of virtual currency from the Coincheck virtual currency exchange.33 Japanese regulators have also discouraged virtual currency exchanges from listing so-called ‘privacy coins’ like Monero and Zcash due to the difficulty involved in attempting to identify recipients of transactions.34

Consumption taxes on transfers of virtual currency were abolished in 2017.35 However, capital gains on virtual currencies are taxable in Japan.36 As of 5 July 2018,

approximately 59 per cent of Bitcoin transaction volume was attributed to Japanese Yen.  

**South Korea**

In September 2017, South Korea’s Financial Services Commission banned ICOs as a fundraising tool and banned margin trading in virtual currencies. On 6 December 2017, South Korea’s Financial Services Commission followed up on the ICO ban with a new ban on the trading of virtual currency futures arising from South Korea’s lack of recognition of virtual currency as a security, commodity or financial interest that could serve as a futures contract’s underlying asset. However, on 8 March 2018, reports emerged that South Korean regulators were preparing to allow ICOs subject to upcoming regulations, and in May 2018 South Korea’s National Assembly officially proposed to allow domestic ICOs.

In January 2018, South Korean regulators announced Know Your Customer requirements for virtual currency trading and associated bank accounts, effectively subjecting virtual currency trading to anti-money laundering compliance requirements. South Korea’s government announced it would collect taxes on virtual currency capital gains at a 24.2 per cent tax rate at approximately the same time it imposed the Know Your Customer requirements.

**China**

In 2013, China barred financial institutions from using Bitcoin. In March and April 2014, the People’s Bank of China warned banks that continued to provide financial services to virtual currency entities to cease and desist, effectively cutting virtual

---


currencies off from domestic Chinese financial institutions. In September 2017, China banned fundraising through ICOs. In effect, China has banned domestic private sector virtual currency firms, pushing Chinese virtual currency investors to use offshore financial services and virtual currency platforms. However, virtual currency mining remains substantial in China—as much as 70 per cent of Bitcoin mining occurs in China—despite China’s efforts to suppress domestic virtual currency financial services.

**International contrasts**

Many of these regulatory frameworks appear to contrast with each other, and some appear internally inconsistent. China and South Korea offer noteworthy examples of apparent internal contradictions:

- China remains a dominant player in virtual currency mining while suppressing domestic virtual currency financial services.
- South Korea’s prohibition on virtual currency futures results from its failure to recognize virtual currency as a security, commodity or other financial interest, but South Korea’s move toward legalizing ICOs would appear to mark a recognition that virtual currencies can represent financial interests or instruments.

With respect to differences between different jurisdictions’ regulatory frameworks, noteworthy examples include:

- Japan’s and South Korea’s prohibitions on domestic trading of virtual currency futures appear to fragment those markets from others that allow virtual currency derivatives in regulated markets, such as the UK.
- While the UK, Japan and South Korea have all moved to integrate virtual currency services with their financial sectors and apply Know Your Customer and/or anti-money laundering requirements, China has effectively banned its domestic financial institutions from providing financial services to virtual currency platforms. In effect, China has prevented the application of Know Your Customer and anti-money laundering rules to virtual currency markets through the traditional financial institution channels used in most other markets.

As will be explored throughout this article, these and other international jurisdictions offer substantial contrasts and even contradictions with the developing US regulatory framework for virtual currencies.

---


4. The developing US regulatory framework

US regulatory overview

As of July 2018, the US regulatory framework for virtual currencies has taken shape. Several prominent federal regulators have articulated particular regulatory frameworks or issued substantial relevant guidance, and several states have promulgated rules, guidance or consistent patterns of enforcement actions that are illustrative of the short- to medium-term shape of regulatory trends for virtual currencies.

Federal and state laws do not currently provide for consolidated, comprehensive oversight of virtual currency markets by a single regulator. However, multiple regulators are increasingly coordinating to provide a ‘multifaceted, multi-regulatory’ approach to virtual currency markets:

- The SEC has asserted authority over virtual currencies that have features consistent with securities, and has asserted its enforcement authority over ICOs and similar capital-raising activities.
- The CFTC has declared virtual currencies to be commodities and thus asserted its full jurisdiction over virtual currency derivatives and derivatives markets, as well as virtual currency spot and cash markets for fraud and manipulation enforcement purposes.
- FinCEN oversees BSA/AML compliance for money transmitters and exchangers of virtual currencies for fiat currency or other virtual currencies. FinCEN generally treats virtual currencies as equivalent to transfers of cash or cash equivalents for reporting purposes.
- The IRS treats virtual currencies as property for capital gains tax purposes.
- OFAC treats transactions in virtual currencies issued by sanctioned regimes as potential extensions of credit to sanctioned regimes.
- State banking and financial regulators oversee some virtual currency spot exchanges through state laws governing money transfers.

There are some similarities to the international approaches examined in the previous section. The US BSA/AML framework’s application to virtual currencies and the application of Know Your Customer and other AML requirements to virtual currency financial services in the UK, Japan and South Korea share many common features, for example. However, there are substantial contrasts as well: US regulators consider virtual currencies commodities and in many cases also securities, whereas the UK, Japan and South Korea have not classified virtual currencies as financial products subject to traditional regulatory frameworks. The UKs decision to classify virtual currency derivatives as financial instruments, but not the underlying virtual currencies themselves, represents a nuanced distinction from the US regulatory approach.

As shown in Figure 2, several US regulators have promulgated virtual currency guidance, customer or investor alerts, interpretations with respect to existing regulations, or new rulemakings since 2013. Until 2017, most regulatory publications with respect to virtual currencies came from FinCEN, the IRS, or state regulators such

---

as the New York Department of Financial Services (NYDFS).\textsuperscript{49} This dynamic changed in the second half of 2017, as the CFTC and SEC began publishing a substantial number of documents on virtual currencies, followed soon after by their respective self-regulatory organizations (SROs), the National Futures Association (NFA) and the Financial Industry Regulatory Authority (FINRA). Approximately two-thirds of all substantive regulatory publications on virtual currency have been published since the second half of 2017.

**Securities and exchange commission**

The SEC and its leadership have stated that most or all virtual currencies offered in ICOs as of early 2018 have been securities in practice,\textsuperscript{50} although they have recognized that it is


\textsuperscript{50}See, eg 'When investors are offered and sold securities—which to date ICOs have largely been—they are entitled to the benefits of state and federal securities laws[].' SEC Chairman Jay Clayton, 'Chairman’s Testimony on Virtual Currencies: the Roles of the Public and Private Sector' 26 July 2017.
in principle possible for a virtual currency to not be considered a security based on a facts and circumstances test. While the SEC did initiate several enforcement actions in matters related to virtual currencies before it published official guidance and interpretations in 2017, those pre-2017 virtual currency-related enforcement actions did not explicitly rely on the conclusions that virtual currencies were securities, that entities issuing virtual currencies were securities issuers, or that platforms facilitating transactions in virtual currencies were exchanges. The pre-2017 SEC enforcement actions are described in more detail in Section 3.

The SEC first defined its perspective on virtual currencies as likely securities in its 25 July 2017 Report of Investigation Pursuant to section 21(a) of the Securities Exchange Act of 1934: The DAO (‘DAO Report’). In this report, the SEC opined that US securities laws were applicable to ‘virtual organizations or capital raising entities that use distributed ledger or blockchain technology to facilitate capital raising and/or investment and the related offer and sale of securities’, and that ‘the automation of certain functions through this technology, “smart contracts”, or computer code, does not remove conduct from the purview of U.S. federal securities laws’.51

The DAO Report described the SEC’s investigation of The DAO, a ‘decentralized autonomous organization . . . embodied in computer code and executed on a distributed ledger or blockchain’ that the SEC concluded was created ‘with the objective of operating as a for-profit entity that would create and hold a corpus of assets through the sale of DAO Tokens to investors’.52 According to the DAO Report, investors in DAO Tokens could re-sell DAO Tokens on secondary trading platforms or hold on to DAO Tokens in expectation of sharing in anticipated earnings of the assets and projects of The DAO.53

The DAO Report explained the SEC’s reasoning as follows: DAO Tokens are securities because the Howey test suggests as much, given that investors in DAO Tokens invested money54 with a reasonable expectation of profit derived from the managerial efforts of the team behind The DAO.55 The SEC concluded more broadly that the DAO was an issuer of securities and should have registered its offers and sales of securities unless an exemption applied; online platforms that traded DAO Tokens met the definition of an exchange and thus either had to register or operate pursuant to an exemption from registration; and entities and issuers with similar facts and circumstances to the DAO and DAO Token platforms would likewise have to register or operate pursuant to an exemption.56

51 Securities and Exchange Commission (n 22) p 2.
52 ibid p 1.
53 ibid p 1.
54 The SEC indicated that it considered the investors’ exchange of another convertible virtual currency for DAO Tokens to be equivalent to an investment of money: ‘the investment of “money” need not take the form of cash’. Securities and Exchange Commission, ibid p 11.
56 ibid pp 15–18.
The SEC followed the DAO Report with an 28 August 2017 Investor Alert entitled ‘Public Companies Making ICO-Related Claims’, which notified investors that the SEC had recently suspended trading in the common stock of several companies that ‘made claims regarding their investments in ICOs or touted coin/token related news’ in response to concerns such as ‘a lack of current, accurate, or adequate information about the company’, ‘questions about the accuracy of publicly available information’, or ‘questions about trading in the stock’. Although these suspensions of trading in common stock did not explicitly rely on the conclusion that virtual currencies were securities, they signalled the SEC’s increasing scrutiny of virtual currency issuers. These suspensions are described in more detail in Section 3.

The SEC thereafter issued a 1 November 2017 statement that warned investors to be cautious of celebrity-backed ICOs. Notably, the SEC directed investors and virtual currency market participants to review the SEC’s DAO Report and stated that ‘virtual tokens or coins sold in ICOs may be securities, and those who offer and sell securities in the United States must comply with the federal securities laws’.58

The following week, SEC Chairman Jay Clayton made remarks at the PLI 49th Annual Institute on Securities Regulation in New York that called out virtual currencies and ICOs as a source of concern. After noting that there was ‘a lack of information about many online platforms that list and trade virtual coins or tokens offered and sold in Initial Coin Offerings’, Chairman Clayton restated the SEC’s position that ‘instruments, such as “tokens,” offered and sold in ICOs may be securities, and those who offer and sell securities in the United States must comply with the federal securities laws’ including registration requirements.59

On 11 December 2017, Chairman Clayton issued a Statement on Cryptocurrencies and Initial Coin Offerings that he ‘directed principally to two groups: “Main Street” investors and market professionals [such as] broker-dealers, investment advisers, exchanges, lawyers and accountants … whose actions impact Main street investors’.60 Chairman Clayton opined that ‘any [ICO] activity that involves an offering of securities must be accompanied by the important disclosures, processes and other investor protections that our securities laws require’.61 In addition, he stated that ‘tokens and offerings that incorporate features and marketing efforts that emphasize the potential for profits based on the entrepreneurial or managerial efforts of others continue to contain the hallmarks of a security under U.S. law’, and advised financial market professionals, ‘including securities lawyers, accountant and consultants’ to keep that in mind.62

---

61 ibid.
62 ibid.
also warned ‘brokers, dealers and other market participants that allow for payments in cryptocurrencies, allow customers to purchase cryptocurrencies on margin, or otherwise use cryptocurrencies’ to treat payments in cryptocurrencies as though they were payments in cash and ensure that ‘their cryptocurrency activities are not undermining their anti-money laundering and know-your-customer obligations’.63

Chairman Clayton’s statement was followed a month later by a brief joint statement from the SEC and CFTC enforcement directors regarding virtual currency enforcement actions. The 19 January 2018 joint statement emphasized that both agencies would focus on the ‘substance’ of virtual currency activities rather than the ‘form’ of such activities:

When market participants engage in fraud under the guise of offering digital instruments—whether characterized as virtual currencies, coins, tokens, or the like—the SEC and the CFTC will look beyond form, examine the substance of the activity and prosecute violations of the federal securities and commodities laws. The Divisions of Enforcement for the SEC and CFTC will continue to address violations and to bring actions to stop and prevent fraud in the offer and sale of digital instruments.64

Three days later, SEC Chairman Clayton presented opening remarks at the Securities Regulation Institute that were directed toward ‘securities lawyers, accountants, underwriters, and dealers’.65 He stated that he had ‘instructed the SEC staff to be on high alert for approaches to ICOs that may be contrary to the spirit of our securities laws and the professional obligations of the U.S. securities bar’, such as not counselling clients involved in ICOs that ‘the product they are promoting likely is a security’.66 He also warned that the SEC ‘is looking closely at the disclosures of public companies that shift their business models to capitalize on the perceived promise of distributed ledger technology and whether the disclosures comply with the securities laws, particularly in the case of an offering’.67

Two days later, SEC Chairman Clayton and CFTC Chairman Christopher Giancarlo published a joint op-ed in the Wall Street Journal titled ‘Regulators Are Looking at Cryptocurrency’. The op-ed stated that ‘federal authority to police cryptocurrencies is clear’ in some areas, such as with respect to the ‘Bank Secrecy Act and its implementing regulations [that] establish federal anti-money-laundering obligations that apply to most people engaged in the business of accepting and transmitting, selling or storing cryptocurrencies’.68 The op-ed also acknowledged some possible limits on the jurisdiction of the SEC over virtual currencies, but noted that ‘some products that are labeled as

63 ibid.
66 ibid.
67 ibid.
cryptocurrencies have characteristics that make them securities’ and the SEC ‘is devoting a significant portion of its resources to the ICO market’. The op-ed warned ‘market participants, including lawyers, trading venues and financial services firms’ that ‘we are disturbed by many examples of form being elevated over substance, with form-based arguments depriving investors of mandatory protections’. 69

The testimony of Chairman Clayton before the Senate Committee on Banking, Housing, and Urban Affairs on 6 February 2018 summarized the documents described above and emphasized Chairman Clayton’s concern regarding public companies that change their business models or names to reflect a focus on distributed ledger technology without adequate disclosures to investors about business model changes and the risks involved. It also emphasized that ‘the SEC and CFTC are collaborating on our approaches to policing these markets for fraud and abuse. We will also continue to work closely with our federal and state counterparts, including the Department of the Treasury, Department of Justice and state attorneys general and securities regulators’. 70

On 7 March 2018, the SEC issued a public statement regarding ‘Unlawful Online Platforms for Trading Digital Assets’ that warned investors ‘that many online trading platforms appear to investors as SEC-registered and regulated marketplaces when they are not’ by, for example, ‘refer[ring] to themselves as “exchanges”’. 71 The SEC statement recommended that ‘market participants operating online trading platforms’ should ‘consult with legal counsel to aid in their analysis of federal securities law issues and to contact SEC staff, as needed, for assistance in analyzing the application of the federal securities laws’, such as when a platform ‘must register as a national securities exchange or operate under an exemption from registration, such as the exemption for [alternative trading systems] under SEC Regulation ATS’. 72

On 14 June 2018, William Hinman, the Director of the SEC’s Division of Corporation Finance, made remarks before the Yahoo Finance All Markets Summit in which he addressed the SEC’s evolving perspective on the application of the Howey test to digital assets like convertible virtual currencies. Hinman stated that neither Bitcoin nor Ether appeared to be securities at present given the decentralized structure of both virtual currencies, and that ‘applying the disclosure regime of the federal securities laws to the offer and resale’ of Bitcoin and Ether ‘would seem to add little value’ today. 73 Hinman also suggested that ‘the fundraising that accompanied the creation of Ether’ did appear to have the characteristics of a securities offering, raising the possibility that some

69 ibid.
72 ibid.
convertible virtual currencies could evolve organically from securities to non-securities under the *Howey* test if they become sufficiently decentralized.\footnote{ibid.}


### Commodity futures trading commission


On 17 October 2017, the CFTC published ‘A CFTC Primer on Virtual Currencies’ (the ‘Primer’). The Primer stated that ‘Bitcoin and other virtual currencies are properly defined as commodities’, and the CFTC’s jurisdiction ‘is implicated when a virtual
currency is used in a derivatives contract, or if there is fraud or manipulation involving a virtual currency traded in interstate commerce’. 80

On 15 December 2017, the CFTC issued a proposed interpretation 81 on virtual currency in retail transactions that would interpret the ‘actual delivery’ exception to CEA section 2(c)(2)(D) to require ‘physical settlement’. One example of ‘actual delivery’ in this context is ‘a record on the relevant public distributed ledger network or blockchain’ indicating that the entire quantity of purchased virtual currency is transferred to the purchaser’s blockchain wallet (or ‘other relevant storage system’) that is consistent with the purchaser having full control of and title to the virtual currency and the offeror having no control of, title to, or interests in the virtual currency within 28 days of entering into a transaction. 82 If full control and title are not transferred within 28 days, the CFTC may consider the transaction a futures transaction subject to the full panoply of CFTC regulation and enforcement authority.

On 4 January 2018, the CFTC published a backgrounder on ‘Oversight of and Approach to Virtual Currency Futures Markets’ that stated the CFTC’s intent to ‘assert ... legal authority over virtual currency derivatives in support of the CFTC’s anti-fraud and manipulation efforts, including in underlying spot markets’ and pursue ‘robust enforcement’ including both ‘general regulatory and enforcement jurisdiction over virtual currency derivatives markets’ and policing ‘fraud and manipulation in cash or spot markets’. 83

On 19 January 2018, the CFTC and SEC enforcement directors issued a brief joint statement on both agencies’ intent to look beyond ‘form’ to the ‘substance’ of virtual currency activities for enforcement purposes. 84

On 24 January 2018, CFTC Chairman Giancarlo published a joint op-ed with SEC Chairman Clayton on virtual currency regulation. The op-ed noted that with the emergence of bitcoin futures products on CFTC-regulated exchanges, ‘the CFTC gained oversight over the U.S. bitcoin futures market and access to data that can facilitate the detection and pursuit of bad actors in underlying spot markets’. 85

On 6 February 2018, CFTC Chairman Giancarlo testified before the Senate Banking Committee on virtual currency. In his written testimony, he stated that the ‘CFTC has sufficient authority under the CEA to protect investors in virtual currency derivatives’ but ‘the CFTC does NOT have regulatory jurisdiction over markets or platforms conducting cash or “spot” transactions in virtual currencies or over participants on those platforms’.

80 Commodity Futures Trading Commission (n 7) p 11.
83 Commodity Futures Trading Commission, (n 48) pp 1–2.
84 Commodity Futures Trading Commission, (n 64).
85 SEC Chairman Jay Clayton and CFTC Chairman J Christopher Giancarlo, (n 68).
except for ‘enforcement jurisdiction to investigate and, as appropriate, conduct civil enforcement action against fraud and manipulation’. 86

The CFTC also issued customer advisories in late 2017 and early 2018 that warned virtual currency customers and investors about ‘the risks of virtual currency trading’ 87 and complaints the CFTC had received regarding ‘pump-and-dump schemes’ 88 in virtual currency. In the latter advisory, the CFTC advised virtual currency customers and investors that ‘the CFTC maintains general anti-fraud and manipulation enforcement authority over virtual currency cash markets as a commodity in interstate commerce’. 89

On 6 March 2018, a federal district court ruled in favour of the CFTC’s jurisdiction over virtual currencies as commodities. According to the memorandum and order, ‘virtual currencies can be regulated by the CFTC as a commodity’ because ‘virtual currencies are “goods” exchanged in a market for uniform quality and value’. 90 The order concludes that ‘the CFTC has standing pursuant to Title 7 U.S.C. § 13a-1(a) to seek injunctive and other relief related to misleading advice, and the fraudulent scheme and misappropriation of virtual currencies’ and ‘the CFTC[s] . . . expansion into spot trade commodity fraud is justified by statutory and regulatory guidelines’. 91 The order also notes that ‘the jurisdictional authority of CFTC to regulate virtual currencies as commodities does not preclude other agencies from exercising their regulatory power when virtual currencies function differently than derivative commodities’, 92 consistent with the CFTC and SEC’s published perspectives on their non-exclusive authority over virtual currency under facts and circumstances tests.

The 6 March 2018 and 26 September 2018 rulings bolster the CFTC’s position that virtual currencies are commodities under the Commodity Exchange Act. However, as the only two rulings affirming the CFTC’s position, they may not permanently settle the jurisdictional questions about virtual currency until and unless other courts rule similarly. An open question going forward is whether other courts will agree with the 6 March 2018 ruling’s conclusion that ‘the jurisdictional authority of CFTC to regulate virtual currencies as commodities does not preclude other agencies from exercising their regulatory power when virtual currencies function differently than derivative commodities’, 93 which may be relevant in cases where both the CFTC and SEC pursue enforcement actions against the same targets, or where private litigants dispute whether virtual currencies are commodities, securities, both or neither.

89 ibid.
91 ibid pp 24–25.
92 ibid p 24.
93 ibid p 24.
Financial crimes enforcement network

Federal BSA/AML regulator FinCEN has issued interpretive guidance and administrative rulings asserting its jurisdiction over virtual currency money services businesses (MSBs). Currently, as it stated in guidance issued 18 March 2013, FinCEN considers ‘administrators’ (i.e. issuers or redeemers) of virtual currency and ‘exchangers’ of virtual currency for real currency or other virtual currencies to be MSB ‘money transmitters’ subject to the full range of FinCEN BSA/AML requirements, such as suspicious activity reporting. The guidance further stated that ‘the definition of a money transmitter does not differentiate between real currencies and convertible virtual currencies.’ FinCEN clarified that it considered ‘an administrator or exchanger that (1) accepts and transmits a convertible virtual currency or (2) buys or sells convertible virtual currency’ to be a money transmitter subject to FinCEN regulations, but that FinCEN did not consider ‘a user who obtains convertible virtual currency and uses it to purchase real or virtual goods or services’ to be a money transmitter or other MSB absent administration and/or exchange behaviour in the virtual currency.

In 2015, FinCEN issued an administrative ruling declaring a company to be a money transmitter (as well as a dealer in precious metals, precious stones or jewels) for engaging in a business including accepting bitcoins in exchange of issuing physical or digital negotiable certificates of ownership of precious metals. This business involved holding precious metals in custody for buyers by opening a digital wallet for a customer and issuing a digital proof-of-custody certificate that can be linked to a customer’s wallet on the Bitcoin blockchain ledger. The digital proof-of-custody certificates were designed such that the customer could trade or exchange their precious metals holdings at the company by any means through which the customer could trade or exchange bitcoins.

Internal revenue service

The IRS in March 2014 issued a notice and news release providing that ‘virtual currency is treated as property for U.S. federal tax purposes’. The notice noted among other details that ‘mining’ virtual currency could count as a form of self-employment, and that ‘taxpayers may be subject to penalties’ for ‘underpayments attributable to virtual currency transactions’ under section 6662 or ‘failure to timely or correctly report virtual currency transactions’ under section 6721s and 6722.
Office of foreign assets control

On 19 January 2018, the Office of Foreign Assets Control (OFAC) of the US Department of the Treasury, a federal regulator overseeing sanctions, issued guidance regarding Venezuela’s December 2017 announcement of intent to create a digital or virtual currency. According to the guidance, a virtual currency issued by Venezuela connected to the right to receive commodities at a later date would appear to be an extension of credit to the Venezuelan government, and thus prohibited under Executive Order 13808.100 This suggests that for sanctions purposes in general, cryptocurrencies issued by foreign governments may be considered extensions of credit to those governments by OFAC.

On 19 March 2018, President Donald Trump issued Executive Order 13827, ‘Taking Additional Steps to Address the Situation in Venezuela’, expressly prohibiting ‘All transactions related to, provision of financing for, and other dealings in, by a United States person or within the United States, any digital currency, digital coin, or digital token, that was issued by, for, or on behalf of the Government of Venezuela on or after January 9, 2018’.101 While this is one case study, it is reasonable to expect OFAC may apply similar reasoning if other countries subject to sanctions attempt to obtain financing through ICOs or other virtual currency transactions with US persons.

State regulatory frameworks

Some state financial regulators have considered creating regulatory frameworks for virtual currency. New York’s NYDFS moved early, publishing a notice of inquiry on new regulatory guidelines specific to virtual currencies in August 2013.102 NYDFS followed the notice with a 17 July 2014 proposed regulatory framework for virtual currency firms called ‘BitLicense’ that required virtual currency firms to comply with a wide range of requirements, including anti-money laundering rules such as ‘Know your Customer’ (ie verifying the identity of account holders).103 The final BitLicense Regulatory Framework rules were published in the New York State Register at 23 NYCRR Part 200 in June 2015.104

The final BitLicense rules required that BitLicense licensees report transactions worth more than $10,000 in virtual currencies in aggregate in one day that are not subject to federal currency transaction reports to the NYDFS within 24 hours, monitor transactions for suspicious activity and file suspicious activity reports, and collect and maintain information on the identity and physical address of account holders of the licensee.105

On 22 September 2015, the NYDFS reported that it had approved its first BitLicense application for Circle Internet Financial in a press release that described BitLicense as the ‘First Comprehensive Regulatory Framework for Firms Dealing in Virtual Currency’. As of 7 March 2018, 4 firms were listed on the NYDFS website as state-regulated virtual currency institutions.

Other states’ regulatory approaches have garnered less attention than New York’s. Some states have chosen to interpret virtual currency as ‘money’ for the purposes of state money transmitter laws and regulations or have otherwise required virtual currency issuers and/or exchanges to register, while others have chosen not to, or have yet to take action.

5. Increasing US enforcement actions

General enforcement trends

The US regulators have pursued enforcement actions related to virtual currencies since at least the first half of 2013, but there has been a substantial increase in enforcement activity from the second half of 2017 onwards: 50 of the 71 total virtual currency enforcement actions through 30 June 2018 were brought since 1 July 2017, and 41 were brought in the first half of 2018 alone. Although total enforcement actions have increased substantially, the largest increase has been in the form of enforcement actions seeking no monetary penalties or criminal charges, such as cease-and-desist orders and temporary trading suspensions. A breakdown of virtual currency enforcement actions by penalty-type sought through 30 June 2018 is shown in Figure 3.

State regulators collectively brought 29 enforcement actions, but no individual state agency brought more than 10 (Texas). The SEC brought the most virtual currency enforcement actions, with 19 as of 30 June 2018; the Department of Justice (DOJ) brought 10; the CFTC brought 8; FinCEN and the FTC each brought 2; and the IRS brought 1 virtual currency enforcement action. Figure 4 displays a breakdown of enforcement actions by regulatory agency.

NERA’s analysis of the financial penalties imposed in resolved enforcement actions that have sought such penalties shows no strong trend over time. Among the 13 enforcement actions with published penalty amounts, only three have imposed penalties larger than $1 million, but those were for amounts in the tens or hundreds of millions of dollars, with one large enforcement action each from the DOJ, FinCEN and the SEC. The large penalties were imposed on the alleged perpetrator of a bitcoin-denominated Ponzi Scheme, Trendon T. Shavers, and his online entity, Bitcoin Savings and Trust; the alleged operator of the ‘Silk Road’ online criminal marketplace, Ross Ulbricht, also known as ‘Dread Pirate Roberts’; and an unlicensed exchanger of convertible virtual currencies, BTC-e, and its administrator.

Alexander Vinnik, who allegedly violated BSA/AML requirements. Financial penalties broken down by enforcement agency and date are displayed in Figure 5.

In the following sections, trends in enforcement activities are analysed by general category of alleged unlawful behaviour: violation of registration requirements; fraud-related allegations; trading violations; and BSA/AML violations.

**Alleged violations of registration requirements**

Enforcement authorities have pursued at least 26 enforcement actions that have alleged that targets violated registration requirements. Enforcement actions alleging violations of registration requirements tend to fall into a few categories depending on the enforcement agency involved:

- **FinCEN and the DOJ**: Registration requirement enforcement actions by FinCEN\(^{109}\) and the DOJ\(^{110}\) have typically alleged that firms or individuals acting as exchangers of convertible virtual currencies have operated unlicensed MSBs;

---


Figure 4. Number of virtual currency enforcement actions by agency. H1 2013 through H1 2018, Semi-annually.

Notes and Sources: Data from NERA research into enforcement actions on enforcement agency websites. H1 2018 data through 30 June 2018.

- **SEC and State Securities Regulators:** Those by the SEC and state securities regulators have typically alleged either (1) that firms or individuals associated with ICOs or digital token sales have offered unregistered securities,\(^{111}\) or (2) that firms or individuals operating online platforms to trade convertible virtual currencies have operated an unregistered exchange or broker-dealer;\(^{112}\)

- **CFTC:** Those by the CFTC have alleged (1) that firms or individuals offering financed retail transactions in convertible virtual currencies have failed to register as designated contract markets or swap execution facilities,\(^{113}\) or (2) that firms or individuals that have accepted funds and orders in convertible virtual currencies have failed to register as futures commission merchants,\(^{114}\) or (3) that firms or individuals accepting convertible virtual currencies in exchange for commodity interests have failed to register as commodity pool operators or associated persons of commodity pool operators.\(^{115}\)

**Fraud-related allegations**

Enforcement authorities have pursued at least 33 enforcement actions that have alleged that targets engaged in or conspired to engage in fraud-related activities ranging from

---


\(^{114}\) See ibid.

providing insufficient or inaccurate information to prospective investors, to operating a Ponzi scheme. Fraud-related allegations have been broadly similar across enforcement agencies, and thus are analysed by the sub-type of activity alleged rather than the enforcement agency involved:

- **Insufficient or Inaccurate Information Provided to Investors**: Enforcement agencies such as the SEC and state securities regulators have issued cease and desist orders to, 116 or temporarily suspended, 117 firms or individuals on at least 12 occasions in matters alleging insufficient or inaccurate information provided to investors. The cease and desist orders have been targeted at a range of entities and individuals connected to virtual currencies, whereas the temporary suspensions have generally targeted publicly traded companies with recent announcements of projects involving issuing, mining, exchanging or administering convertible virtual currencies or blockchains. These enforcement actions have generally involved no assessment of monetary penalties.

- **Commercial and financial fraud schemes**: Enforcement agencies have sought injunctions and equitable relief in at least 14 matters alleging behaviour amounting to operating fraud schemes, with allegations

---


ranging from failing to deliver advertised and paid-for Bitcoin mining computers to operating a Ponzi scheme. Enforcement agencies have sought criminal charges, financial penalties and/or injunctions in cases alleging such fraud schemes.

**Bank secrecy act/anti-money laundering allegations**

Enforcement authorities have pursued at least six enforcement actions related to virtual currencies that have alleged violations of BSA/AML statutes or regulations. These enforcement actions either alleged that individuals or entities were operating unlicensed or BSA/AML non-compliant money transmitters/MSBs or that they were aiding or engaged in money laundering:

- **Operating Unlicensed or BSA/AML Non-Compliant MSBs**: FinCEN has pursued two enforcement actions against alleged unlicensed money transmitters/MSBs, the DOJ has pursued two such enforcement actions and the State of Florida has pursued one. Penalties imposed included prison terms in two cases, financial penalties of $122 million and $950 thousand, and, notably, in one case a dismissal of all charges in Florida state court in 2016—the only such total loss in a virtual currency enforcement action—in a ruling that cited the alleged vagueness of the relevant Florida statutes on MSBs.

- **Money Laundering**: The DOJ brought two money laundering enforcement actions alleging money laundering activity in connection with the ‘Silk Road’ online criminal marketplace. The better-publicized of the two, against the alleged owner and operator of ‘Silk Road’, Ross Ulbricht, alleged that he engaged in money laundering connected with the sale of drugs and criminal services on ‘Silk Road’. Ulbricht was sentenced to life in prison and ordered to forfeit nearly $184 million. The less-publicized enforcement action targeted two men who allegedly ran a Bitcoin exchange on ‘Silk Road’ to facilitate drug purchases, and resulted in criminal convictions, prison sentences and nearly $1 million in financial penalties.

**Trading allegations**

Enforcement authorities have pursued at least three enforcement actions relating to virtual currencies that have alleged trading violations:

- In 2015, the CFTC issued an order against TeraExchange LLC, a provisionally registered Swap Execution Facility, for purportedly allowing wash trades and prearranged trades on its platform. According to the CFTC, TeraExchange allowed two market participants to trade two ‘completely offsetting’ contracts consisting of non-deliverable forward contracts based on the relative value of Bitcoin and the US dollar,

---

120 The State of Florida vs Michell Abner Espinoza, ‘Order Granting Defendant’s Motion to Dismiss the Information’ Judge Teresa Pooler, 22 July 2016.
122 Department of Justice, ‘Former CEO of Bitcoin Exchange Company Sentenced in Manhattan Federal Court to Two Years in Prison for Helping to Sell Nearly $1 Million in Bitcoins for Drug Buys on Silk Road’ 19 December 2014.
and issued a press release advertising Bitcoin swap trading without disclosing that the sales were pre-
arranged wash sales. The settlement involved no financial penalty.  

- In 2016, the SEC settled an enforcement action against Bitcoin Investment Trust, a Delaware trust 
invested in bitcoins, and SecondMarket, a broker-dealer, alleging violations of Rules 101 and 102 of 
Regulation M. The SEC alleged that Secondmarket, the sole authorized participant in Bitcoin 
Investment Trust, purchased shares in Bitcoin Investment Trust from shareholders and earned 
redemption fees during a continuous distribution, and hence, during the applicable restricted period. 
The SEC settled with the respondents for $53,756 in disgorgement and prejudgment interest and 
agreement to a cease and desist order.  

- In 2018, the CFTC filed a complaint against Blake Kantor, Nathan Mullins and entities associated with 
the two, alleging the operation of an unregistered futures commission merchant, the offering of illegal off-
exchange retail swaps (binary options), the use of manipulative and deceptive devices in connection with 
swaps (including the manipulation or fabrication of purported trades in customer accounts to the 
disadvantage of customers), and the exchange of customer balances for virtual currencies that could not be 
monetized for the US dollar value reported to customers in an effort to cover up the previous fraud.  

6. Developing private litigation trends

Noteworthy private litigation related to virtual currencies is a very recent trend, with 36 out of 38 noteworthy private actions identified by NERA brought since July 2017. Figure 6 shows the temporal distribution of noteworthy private litigation related to 
virtual currencies.

Private litigation has featured recurring categories of allegations:

- Allegations of fraud or misappropriation (17 out of 38 cases);
- Allegations of negligence or breach/rescission of contract (14 out of 38 cases); and
- Allegations of violations of securities laws or regulations (22 out of 38 cases).

As is explained below, many virtual currency-related lawsuits have featured more than one 
category of allegations. About 29 of the 38 identified lawsuits have been putative class actions.

Allegations of fraud or misappropriation

Allegations of fraud or misappropriation have been common in private virtual currency 
litigation. Such allegations range from claims of misleading promotional or marketing 
campaigns to allegations of outright theft of customer or investor assets.

The first noteworthy virtual currency litigation was a putative class action alleging 
fraud and misappropriation of customer assets filed in 2014 against the Bitcoin exchange 
Mt Gox, its owner, Mark Karpeles, its bank, Mizuho Bank, and others following the 
collapse of Mt Gox in February 2018. Plaintiffs alleged that Mt Gox’s owner either stole
customers’ bitcoins and fiat currency or negligently failed to safeguard customer assets, and alleged that Mizuho Bank continued to allow customers to deposit funds into Mt Gox after suspending withdrawals while concealing from customers that it had ceased providing withdrawal services.\footnote{See First Amended Class Action Complaint in Greene et al v Mtgox Inc et al, 14 March 2014.}

Numerous lawsuits since then have alleged fraud or misappropriation. In early 2018, three distinct putative class actions alleging fraud were brought against Bitconnect, a Bitcoin lending platform with its own convertible virtual currency, and individuals and/or entities accused of being affiliates or promoters of Bitconnect. Bitconnect allegedly guaranteed a high rate of return on bitcoins invested in order to attract victims to a Ponzi scheme, achieving a market capitalization above $2 billion in December 2017.\footnote{See <https://coinmarketcap.com/currencies/bitconnect/historical-data/> accessed 10 July 2018.} On 13 January 2018, after several state authorities had issued cease and desist orders against Bitconnect, Bitconnect’s platform allegedly ceased operating for several days. When the website came back online, the lending platform was allegedly shut down, and investors were allegedly repaid their Bitcoin loans at an exchange rate that was no longer closer to the market exchange rate, as the price of Bitconnect’s ‘coin’ fell by more than 90 per cent between 13 January and 16 January 2018.\footnote{See Class Action Complaints in Charles Wildes et al v Bitconnect International PLC et al (Filed 24 January 2018); Brian Page et al v Bitconnect International PLC et al (Filed 29 January 2018); and Andrew Kline et al v Bitconnect et al (Filed 7 February 2018).}
As with most virtual currency litigation alleging fraud or misappropriation, the ongoing Bitconnect litigation is likely to involve disputes over expert opinions, such as determining whether Bitconnect was covered by state and federal securities laws and estimating reasonable damages. With respect to damages, the ongoing Bitconnect litigation may have to determine whether damages, if any, should be calculated based on Bitconnect investors’ losses as denominated in US dollars or in Bitcoin, given that Bitconnect was a Bitcoin lending platform. Figure 7 shows the relative change in the price of Bitconnect in US dollars and in Bitcoin immediately following the price crash.

Allegations of negligence or breach/rescission of contract

Allegations of negligence or breach/rescission of contract have also featured prominently in virtual currency litigation. Allegations of negligence and breach/rescission of contract have often targeted virtual currency service providers. For example, a putative class action filed on 1 March 2018 against virtual currency exchange Coinbase and two of its executives alleged that Coinbase’s handling of the ‘hard fork’ in the Bitcoin blockchain that produced the new virtual currency Bitcoin Cash had been negligent. The lawsuit alleged that Coinbase negligently allowed employees to engage in insider trading and failed to use reasonable due care in ensuring that Coinbase could handle the large number of Bitcoin Cash transactions that occurred upon the virtual currency’s launch on Coinbase, and claimed that the price of Bitcoin Cash was ‘artificially manipulated’ as a result, resulting in delayed or incomplete fills of customer orders at higher prices.129 Important outstanding questions related to the Coinbase litigation include whether Bitcoin Cash price movements can be attributed to Coinbase, whether putative class action members with distinct orders were similarly situated, and how customers’ alleged losses should be quantified. Similar questions are outstanding in many virtual currency lawsuits alleging negligence or breach/rescission of contract, which also often contain allegations of artificial prices.

Allegations of violations of securities laws and regulations

The most common category of allegations in virtual currency litigation has been violations of securities laws. Most virtual currency litigation followed the SEC’s publication of the DAO Report, which suggested the applicability of traditional securities laws to ICOs. About 16 out of 25 total lawsuits, and 16 out of 21 total putative class actions, have featured allegations referencing federal or state securities laws or regulations. Some such lawsuits have alleged that unregistered ICOs constituted unregistered securities offerings and/or sales and that the proceeds from such sales should be used to repay ICO investors, whether or not fraud or deception were involved. For example, the 2018 putative class action Davy v Paragon Coin, Inc et al argued that proceeds from the $70 million ParagonCoin ICO should be repaid to investors based on the unregistered nature of the ICO and without reference to any alleged deception because ‘proof of deceptive activity or calculated deprivation of investors’ rights and

129 Class Action Complaint in Jeffrey Berk v Coinbase Inc, Brian Armstrong, and David Farmer (Filed 1 March 2018).
protections under the federal securities laws is not required or determinative as to Plaintiff’s claim’.130

Other virtual currency lawsuits have made allegations of violations of section 10(b) of the Exchange Act and Rule 10b-5 related to transactions in stocks and bonds of firms purportedly engaged in virtual currency or blockchain activities. For example, a putative class action against Xunlei Limited, an online storage and cryptocurrency ‘mining machine’ firm, alleged ‘material misstatements and omissions’ in press releases and filings with the SEC related to the firm’s blockchain projects and issuance of a virtual currency, followed by negative press and substantial declines in the firm’s stock price. The putative class action complaint made loss causation arguments reminiscent of event studies commonly conducted by expert witnesses in stock-drop cases.131

7. Conclusions

While the global regulatory framework for virtual currency continues to develop, its general outlines have taken shape in many jurisdictions, including the USA. In the USA:

- The CFTC has defined convertible virtual currencies as commodities;
- the SEC has indicated that most convertible virtual currencies are securities and most ICOs are securities offerings;

131 Class Action Complaint in Dookeran v Xunlei Limited et al (Filed 18 January 2018).
FinCEN has applied MSB BSA/AML requirements to convertible virtual currency exchanges and administrators; the IRS has decided to treat convertible virtual currencies as property for tax purposes; OFAC has suggested that convertible virtual currencies offered by sanctioned regimes may be considered extensions of credit to such regimes; and state regulators have varied in their treatment of virtual currencies, ranging from a virtual currency-specific licensing framework in New York to broad exemptions from state regulations in other states.

The US regulatory framework contrasts with developments in other major markets around the globe:

- Virtual currencies are not considered either securities or commodities in the UK, Japan, South Korea or China.
- The UK does consider virtual currency derivatives to be financial instruments under MiFID II, and generally allows virtual currency derivatives.
- Japan classifies virtual currencies as means of payment, and because it does not consider virtual currencies to be financial products, it prohibits virtual currency futures.
- South Korea has yet to fully classify virtual currencies, but prohibits future transactions while allowing virtual currency spot markets.
- One area of general consensus across most markets is in preventing money laundering: The UK, Japan and South Korea have moved in the same direction as the USA and pushed to integrate virtual currency platforms with the financial sector. They have all also applied Know Your Customer and anti-money laundering compliance requirements to either the financial institutions serving virtual currency platforms or the virtual currency platforms themselves.
- China, by contrast, has largely banned domestic financial institutions from providing financial services to virtual currency platforms, effectively pushing domestic virtual currency investors to foreign platforms, but tolerates substantial cryptocurrency mining.

Enforcement actions by US regulatory authorities have also established discernable trends. For example, out of 71 total virtual currency enforcement actions identified, far more than half were brought since July 2017, though a majority of enforcement actions since that time have sought no criminal charges and imposed no financial penalties. In terms of categories of alleged violations, 49 enforcement actions have alleged registration violations, 33 have alleged fraud-related violations, 6 have alleged BSA/AML violations, and 3 have alleged trading violations.

Finally, private litigation related to virtual currency has been a very recent phenomenon—36 out of 38 total private lawsuits identified have been brought since July 2017. Moreover, the lawsuits have featured several recurring allegations: 22 of those lawsuits alleged securities violations, 17 alleged fraud or misappropriation, and 4 alleged negligence or breach/rescission of contract. Although some of the lawsuits have featured virtual currency-specific allegations such as misappropriation of digital assets, many have included traditional securities litigation issues, such as Rule 10b-5 stock-drop allegations and artificial price allegations applied to firms with virtual currency or blockchain projects.
Crypto Market Surveillance Has Arrived

By Sharon Brown-Hruska, Jordan Milev and Trevor Wagener (May 25, 2018, 12:42 PM EDT)

The U.S. Department of Justice and the U.S. Commodity Futures Trading Commission have launched a criminal investigation into potential cryptocurrency market manipulation, according to May 24, 2018, news reports. Reports indicate the investigations are looking into possible spoofing — the submission of orders that aren’t intended to execute to affect other participants’ orders — and wash trading — trading between two accounts controlled by the same person or entity to affect market perceptions of demand or liquidity — in cryptocurrency spot markets.[1] These reports come a few months after the DOJ and CFTC announced a series of coordinated criminal and civil enforcement actions targeting “commodities fraud and spoofing schemes”[2] that the DOJ called “the largest futures market criminal enforcement action” ever.[3] The DOJ announcement highlighted market surveillance, emphasizing that the DOJ and CFTC “have developed the ability to identify spoofing patterns through sophisticated analysis of market-level data” and the DOJ and CFTC “expect to use data analysis to an even greater degree in order to identify fraudulent and manipulative conduct in our financial markets.”[4]

This spoofing and manipulation enforcement wave was announced just one month after bitcoin futures markets launched on the Cboe Global Markets[5] and the Chicago Mercantile Exchange.[6] Shortly after Cboe and CME certified their contracts were in compliance with CFTC requirements, the CFTC published documents outlining its approach to bitcoin futures, noting in a backgrounder on virtual currencies that “in 2014, the CFTC declared virtual currencies [like bitcoin] to be a ‘commodity’ subject to oversight under its authority under the Commodity Exchange Act.”[7] The document further asserted that “the CFTC not only has clear legal authority, but now also will have the means to police certain underlying spot markets for fraud and manipulation” through “heightened market surveillance, emphasizing that the DOJ and CFTC ‘have developed the ability to identify spoofing patterns through sophisticated analysis of market-level data’ and the DOJ and CFTC ‘expect to use data analysis to an even greater degree in order to identify fraudulent and manipulative conduct in our financial markets.’”[8]

Gemini, the digital currency exchange whose bitcoin auction is used to determine the settlement price of the bitcoin XBT futures contracts that trade on Cboe’s CFE Exchange, announced on April 25, 2018, that it would use Nasdaq’s SMARTS Market Surveillance system to “monitor [its] marketplace” and “become a market leader in custom surveillance rule creation and alerting for the crypto-asset market” in order to build “a rules-based marketplace.”[9] According to Nasdaq’s parallel announcement, “Nasdaq’s SMARTS surveillance technology automates the detection, investigation and analysis of potentially abusive or disorderly trading” and will be used to “surveil activity across the Gemini auction process.”[10]

Market surveillance is generally the way regulators identify potential spoofing and/or market manipulation. Use of such tools can also serve to discourage market manipulation. Thus, the emergence of institutionalized market surveillance on both futures and spot markets in crypto products can be seen as a strong sign for the long-term future of crypto markets. In the short run, however, media coverage of the tools may create negative sentiment among market participants to the extent it is believed that market surveillance can lead to a flurry of future enforcement actions and civil litigation that can hamper the resources of crypto exchanges.

Researchers Analyzing 2013 Exchange Transaction Data Conclude Manipulation Drove a Previous Bitcoin Price Spike

According to researchers, evidence has emerged that such trading practices likely occurred on a large scale nearly five years ago in crypto markets.

Cryptocurrency manipulation theories have notoriously abounded online, including more than 186,000 Google search results for “bitcoin manipulation” and 1.41 million results for “bitcoin spoofing.” However, concrete evidence to support such allegations has generally been lacking. That may have changed in January 2019 with the publication of an article titled “Price Manipulation in the Bitcoin Ecosystem” in the Journal of Monetary Economics.[12]

The JME article described allegedly suspicious trading activity on the Mt. Gox Bitcoin exchange in late 2013 that its authors say coincided with both the theft of $188 million in bitcoins and a spike in the U.S. dollar value of bitcoin from $150 to more than $1,000. The JME article authors state that they used leaked Mt. Gox transaction history data and publicly available daily aggregate values to conduct their analysis, using regression analysis to control for events other than allegedly suspicious trades that might have affected bitcoin prices. The JME article concludes that the suspicious trading activity on the Mt. Gox exchange was highly correlated with the rise in the price of Bitcoin during the period studied” and that “manipulations can have important real effects” on bitcoin prices.[13]

Takeaway: While the conclusions of the JME article apply narrowly to market conditions nearly five years ago, the findings leave open the possibility that manipulation on a substantial scale may be plausible in the present. In order to determine whether manipulative trading is occurring today, crypto spot and futures market trade and futures contract settlement data would need to be analyzed in detail — the sort of market surveillance the CFTC suggested it is working on with exchanges, or, alternatively, the sort of economic analysis that litigants would use to analyze the plausibility of causation claims in a manipulation case. Notably, such techniques are not new in principle, although the particular application to crypto markets does necessitate a judicious approach to how they are applied.

Economic Analysis Will Depend on Contract Specifications and Market Microstructures
In considering possible market manipulation allegations that could arise in either enforcement actions or civil litigation, one factor to keep in mind is that different futures markets settle using different methodologies and reference prices. For example, the CME bitcoin futures settle against the CME CF Bitcoin Reference Rate, or BRR, at 4 p.m. London time on the expiration date.[14] where the BRR is the mean of 12 median trade prices[15] from 12 consecutive five-minute windows across multiple cryptocurrency spot markets.[16] Cboe bitcoin futures, on the other hand, settle against the Gemini Exchange Auction, which settles using a methodology that prioritizes large orders that minimize the absolute value of the imbalance between total buy and sell orders at a given price.[17] Theoretically, the BRR could potentially be manipulated to the extent enough spot market transactions occur in a five-minute window with low activity to affect that period’s median trade price, pushing the mean of the 12 periods’ median trade prices upward or downward on a CME bitcoin futures settlement date. By contrast, the Gemini Exchange Auction potentially could be manipulated by "banging the close" actions in response to indicative prices published immediately prior to the auction on a Cboe bitcoin futures settlement date.

Illustrative potential manipulation approaches are demonstrated below in figures 1, 2, and 3. In figure 1, a hypothetical CME futures contract settlement is affected by outlier trade prices in the first period of the BRR settlement window that push the settlement price up from $10 to $11.

In figure 2, a hypothetical Cboe futures contract settlement is shown without any manipulation. The simplified Gemini order book is shown at the time of the auction, and both the $9 and $10 prices will execute a quantity of 30, but the $9 price will leave a larger imbalance between buy and sell trade prices. Consequently, the Cboe settlement price will be $10.
In figure 3 below, a hypothetical Cboe futures contract settlement is shown with potential manipulation. The simplified Gemini order book is shown at the time of the auction, and the $9 price shows by far the largest execution quantity, interrupting the order distributions observed in the hypothetical “no manipulation” order book shown in figure 2 above. The figure 3 example could be consistent with cross-market manipulation if the trader(s) placing the large orders at the $9 price have a larger derivatives interest that would benefit from a lower settlement price.

The differences in market design and market microstructures between crypto spot market platforms and established CFTC- and U.S. Securities and Exchange Commission-regulated exchanges may also affect the type of economic analysis that is needed to investigate issues of alleged manipulation. For example, spoofing allegations have often involved the asymmetric use of hidden orders on the side of the market intended to execute versus large visible orders on the side of the market not intended to execute. However, hidden orders are not offered by many crypto spot market platforms, and when offered, some are subject to special execution conditions. Economic analysis of trade data will have to take these subtle market differences from prior spoofing matters into account.

**Takeaway:** Economic analysis of trade data is likely to feature front and center in either enforcement actions or civil litigation.
regarding alleged market manipulation. What economists would look for in the data as potential evidence of causation or the lack thereof will depend on contract specifications, particularly the futures contract settlement methodology. The specifics of the contract settlement methodology would need to be properly analyzed in each case to infer whether the evidence points to manipulation and to rule out alternative explanations. The crypto futures contract settlement methodologies make any flagged instances of possible market manipulation in trade and settlement data well-suited to economic analysis approaches previously applied in alleged benchmark manipulation matters or “bang the close” matters.

**Crypto Futures Beyond Bitcoin**

Crypto futures may expand substantially beyond Bitcoin futures. A U.K. crypto trading platform that already offered futures in bitcoin and ripple announced on May 11, 2018, that it would launch ether futures,[18] and there are signs that additional crypto futures may be arriving across the pond as well. The launch of bitcoin futures on U.S. exchanges in December 2017 was preceded by the creation of the Gemini Exchange Auction in bitcoin in September 2016 and the CME’s creation of the BRR in the fourth quarter of 2016. Gemini announced the creation of an ether auction starting July 28, 2017,[19] and CME Group announced on May 14, 2018, that it was planning to create ether reference rates.[20] While neither CME nor Cboe has announced their intent to launch ether futures, the prerequisites for such futures products are appearing.

**Conclusion**

As market surveillance arrives on the scene for bitcoin futures and spot markets, the prospect of the recent wave of spoofing and manipulation enforcement actions washing over crypto markets, aided by increasing market surveillance, may cause concern in some quarters. However, precedents in established futures and spot markets suggest that sunlight is the best disinfectant and that, in the long run, crypto markets and their participants will likely see benefits from increased market surveillance. In the meantime, analyses of trade data by market surveillance teams working for the CFTC, futures exchanges, and spot market operators are likely to reveal whether potentially manipulative trading practices are being employed in major crypto markets. If any enforcement actions follow, private litigants may follow suit, and the application of financial economic tools to the analysis of trade data for evidence of artificiality will be paramount, as is already the case with other markets.

---

**Dr. Sharon Brown-Hruska** is managing director at NERA Economic Consulting. She is a former commissioner and acting chairwoman of the U.S. Commodity Futures Trading Commission.

**Dr. Jordan Milev** is an associate director and Trevor Wagener is a consultant at NERA.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.


[4] Ibid.


[8] Ibid, p. 3.


[15] Volume-weighted median trade prices from each of the 12 five-minute windows.


All Content © 2003-2018, Portfolio Media, Inc.
From Pit Trading to Big Data

In 1982, the CFTC issued its pivotal Indiana Farm Bureau decision, which soon became the standard of proof for market manipulation under Sections 6(c) and 9(a)(2) of the CEA: activity that intended to produce an artificial price and that produced demonstrable artificiality. For nearly three decades, manipulation enforcement actions hinged on regulators proving the mutual confluence of intent and price artificiality, which created a substantial burden of proof. This high burden of proof meant that regulators could not pursue enforcement actions in cases where intent was clear, but the manipulator failed to create demonstrable artificiality. However, the burden of proof also created a salutary effect by providing market participants with a clear, common sense threshold for wrongdoing. If a market participant traded in a manner indicative of intent to create an artificial price at a time when that participant would stand to benefit from such artificiality, and succeeded in creating artificiality, the CFTC could and would pursue an enforcement action against the participant of sufficient size to deter such behavior.

When I was on the Commission, the CFTC was generally able to meet this high burden of proof to bring manipulation cases against egregious offenders in order to deter manipulative behavior. For example, in the Enron Online case, the CFTC looked at the trading behavior of Enron and one of its traders, Hunter S. Shively, and discovered that Shively had purchased an extraordinary large amount of Henry Hub spot natural gas contracts in a period of 15 minutes, causing an artificial price rise. This unusual trading behavior, combined with Shively’s offer to cover the losses of another trader and evidence he communicated his intent to “bid-up” the market, helped us demonstrate the intent to create artificiality, and the resulting price increase demonstrated the creation of actual artificiality. Immediately after buying the natural gas contracts, Enron began to sell its accumulated Henry Hub spot natural gas contracts. Enron profited from the price artificiality it created earlier, demonstrating Enron’s motive and further evidencing its intent. The CFTC ultimately collected a $35 million civil monetary penalty from Enron in the settlement of its enforcement action.

In 2010, the Dodd-Frank act substantially bolstered CFTC authorities and changed the CFTC’s enforcement approach toward potential price manipulation. Dodd-Frank prohibited three disruptive practices: (1) violating bids or offers, which the CFTC interpreted as a per se offense; (2) disregard for the orderly execution of transactions during the closing period, e.g., “banging the close,” which the CFTC interpreted as requiring a recklessness scienter standard; and (3) bidding or offering with the intent to cancel the bid or offer before execution, i.e., “spoofing,” which the CFTC interpreted as having an intent scienter standard. Importantly, the CFTC interpreted none of the new disruptive trading practices as requiring the creation of actual price artificiality.

Having worked closely with CFTC enforcement staff, I don’t doubt that the lower standards are intended to serve a valid purpose, namely allowing the CFTC to pursue attempted manipulators who did not succeed in causing provable price artificiality. However, the first rule you learn as an economist is TANSTAAFL: “There Ain’t No Such Thing As A Free Lunch.” Policy changes always involve tradeoffs, and a lower burden of proof for manipulation cases creates the risk that the CFTC will pursue enforcement actions against market participants engaging in legitimate trading strategies that, due to circumstances, may be difficult to distinguish from manipulative behavior.

The removal of the requirement to demonstrate price artificiality is particularly troublesome because, absent the creation of artificiality, there is usually uncertainty as to whether trading is actually intended to manipulate. For example, a trader with models suggesting that a prompt month futures contract is substantially undervalued might rationally place large numbers of orders, but if such trading behavior occurs during the closing period, it may resemble banging the close. If the trader stops buying in the close, and the price falls substantially after they stop buying, artificiality may be proven, in which case it suggests manipulation may have occurred. However, if the price plateaus after the trader stops buying, this suggests that the trader may have identified and corrected a legitimate underpricing relative to actual supply and demand in the market. With only a recklessness or intent standard to meet, the CFTC might pursue an enforcement action in the latter case even though the economics suggest the trader was potentially influencing the price with his trades, but did not create an artificial price. Market participants’ uncertainty regarding the precise threshold for manipulation and fear of fines may lead participants to behave with excessive caution in executing certain trading strategies, reducing price discovery and market efficiency.

The CFTC’s interpretive guidance on the new Dodd-Frank disruptive practices has been followed by a parallel shift in the CFTC’s approach toward its long-standing manipulation enforcement powers under Sections 6(c) and 9(a)(2) of the CEA. The CFTC in its 2013 enforcement action against DRW Investments LLC alleged that it only needed to show that DRW intended to affect the price of a product, and did not need to show that DRW intended to create an artificial price.

In commodity markets, market participants are expected to use their proprietary market knowledge to make trading decisions. An interpretation of the CFTC’s manipulation authority that does not require the CFTC to demonstrate intent to create an artificial price could penalize traders using proprietary market information and models in legitimate attempts to bring
prices in line with their expectations. In essence, the CFTC has left open the door to pursuing enforcement actions against firms for fulfilling the price discovery function of markets, which can only reduce the quality of price discovery in commodities markets.

I fear the CFTC effort to lower the burden of proof in the manner it is articulating has the potential to harm the very market and market participants that the Commodity Exchange Act is designed to protect. Basic strategies of arbitrage to capitalize on a suspected mispricing across cash and futures markets would be caught in the CFTC’s interpretation of its authority. An ancient maxim warns that “the road to hell is paved with good intentions.” This seems like an apt warning for the CFTC to remember as it attempts to lower the burden of proof it must overcome in manipulation cases.
Recent Trends in Virtual Currency Regulation, Enforcement, and Litigation

Executive Summary

2017 saw an avalanche of regulatory guidance, enforcement actions, and class action filings related to virtual currency. This development of a regulatory framework and establishment of enforcement and civil litigation trends for virtual currency coincided with a dramatic increase in virtual currency market capitalizations and a wave of initial coin offerings that occurred eight years after the creation of Bitcoin first brought the concept of virtual currency to broad public awareness. As of 26 March 2018, virtual currencies are collectively valued at over $300 billion.

Although virtual currency market capitalizations have fallen by nearly 50% from their peak in December 2017, regulatory guidance and legal actions have only accelerated since then: the first three months of 2018 featured more virtual currency regulatory guidance, enforcement actions, and private action filings than all of 2017. In total, NERA has identified 46 enforcement actions and 25 private action filings related to virtual currency, with 2018 currently on pace to account for an outright majority of all virtual currency enforcement actions and putative securities class actions.

An outright majority of private actions filed in matters connected to virtual currencies have been securities class actions, and as a result the issues raised have frequently included familiar artificial price and Rule 10b-5 stock-drop elements. However, the unique features of virtual currency and related digital assets like smart contracts create additional distinct questions that will need to be answered in many matters. In addition, the introduction of Bitcoin futures on regulated exchanges that settle against cash market reference prices creates the potential for litigation alleging manipulation of Bitcoin cash or futures markets. Plaintiffs in such civil actions may utilize the statistical “screen” approaches common in reference rate litigation regarding LIBOR and ISDAFIX.
This primer introduces readers to the concept and practice of virtual currency and the blockchain, the regulation thereof, recent trends in related enforcement actions, and emerging trends in private virtual currency litigation, particularly securities class actions.

**Background**

**Virtual Currencies and Cryptocurrencies**

A virtual currency is a digital token “representation of value that functions as a medium of exchange, a unit of account, and/or a store of value,” but “does not have legal tender status.” If the virtual currency can be readily expressed in or substituted for recognized currencies, it is called a convertible virtual currency. Convertible virtual currencies have had volatile total market capitalizations, rising to over $600 billion on 18 December 2017 and falling to $304 billion as of 26 March 2018. These market capitalizations put the value of convertible virtual currencies collectively on par with companies as large as Wells Fargo. Figure 1 below shows the market capitalization of convertible virtual currencies as of 8 February 2018.

![Figure 1. Market Capitalization of Convertible Virtual Currencies](source: Data from Coinmarketcap.com, as of 26 March 2018.)

The most prominent subset of convertible virtual currencies, as of February 2018, called cryptocurrencies, utilizes “cryptographic proof” rather than trusted third parties such as financial intermediaries, as a basis for electronic payments in the virtual currency. Bitcoin, the largest convertible virtual currency by market capitalization as of February 2018, is an example of a cryptocurrency that utilizes cryptography and unique digital signatures to allow for decentralized, peer-to-peer electronic payments.
Although virtual currencies existed prior to Bitcoin, Bitcoin’s introduction in 2009 changed the paradigm for convertible virtual currencies by establishing a robust decentralized architecture for cryptocurrency peer-to-peer payments. This architecture includes public and private keys, the blockchain ledger, and open-source software facilitating the use of decentralized networks of computers—called “miners”—to solve complex mathematical algorithms in order to validate and log peer-to-peer transactions on the blockchain ledger.

Blockchain
Distributed ledger technology, better known as blockchain, generally consists of an open, decentralized ledger that allows each party on the blockchain access to the entire database and provides no party with complete control of the data. Generally this decentralization means a “node” system is used whereby multiple nodes can be used to engage in transactions, and records of those transactions are then forwarded to all other nodes. In order to prevent “double spending,” a major concern with virtual currencies, each transaction recorded in the ledger is made unalterable via complex algorithms that ensure each transaction is mathematically linked to every previous transaction. Consequently, an adjustment made to one transaction would require the recalculation of all subsequent transactions, a computationally prohibitive requirement that should, in principle, ensure that all recorded transactions are permanent and inviolable.

Virtual Currency Exchanges
In order to purchase units of convertible virtual currencies using legal tender, or to convert units of a convertible virtual currency into legal tender (or units of other convertible virtual currencies that could in turn be converted into legal tender), users transact with a financial institution known as a virtual currency exchange (or cryptocurrency exchange). Virtual currency exchanges have come under increasing regulatory scrutiny as the entry/exit points from cryptocurrencies whose transaction histories are usually largely anonymous. Consequently, financial regulators, such as the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC), Bank Secrecy Act/Anti-Money Laundering (BSA/AML) authorities like the US Financial Crimes Enforcement Network (FinCEN), tax authorities like the Internal Revenue Service (IRS), and economic and trade sanctions authorities like the Office of Foreign Assets Control (OFAC) have all increasingly focused on virtual currency exchanges as the points on cryptocurrency networks that are most amenable to regulation, market surveillance, investigations, and enforcement actions or collections efforts. The IRS issued guidance in 2014 stating that “for federal tax purposes, [convertible virtual currency is] treated as property,” but has yet to issue further substantive guidance.

Initial Coin Offerings
In recent years, a substantial number of new virtual currencies have been sold via initial coin offerings (ICOs), also called token sales. ICOs typically involve the sale of digital tokens to the public in order to raise capital for projects. The projects intended to be capitalized via ICOs are commonly connected to the new virtual currency, such as the development of a blockchain or open source software to support a network on which the digital tokens can be used, or the creation of a service that is intended to use the virtual currency as an access tool.

According to a December 2017 NERA Economic Consulting report on ICOs (the “NERA ICO Report”), ICOs raised more than $2 billion from January through August of 2017 and commonly involved the sale of digital tokens prior to the creation of the underlying services. The NERA ICO Report concluded that ICOs might attract the attention of regulators and private litigants.
due to the conjunction of large quantities of capital raised via ICOs, negative returns on the median ICO token, and claims that some ICOs have been promoted using white papers that downplay the risks involved. As discussed below, the SEC has taken note of the parallels between ICOs and securities Initial Public Offerings (IPOs), and has initially focused its regulatory attention on this area.

**Smart Contracts and Decentralized Autonomous Organizations**

Smart contracts have been defined as programs or systems that automatically move, assign, or transact in digital assets according to pre-specified rules that are enforced by a peer network. Many recent smart contract projects are connected to a peer network through distributed ledger technology, and some have attempted to create long-term projects called decentralized autonomous organizations (sometimes called “virtual organizations”) that have some analogous features to funds or companies. For example, one white paper for a smart contract project on the Ethereum blockchain described a decentralized autonomous organization as:

[A] virtual entity that has a certain set of members or shareholders which, perhaps with a 67% majority, have the right to spend the entity’s funds and modify its code. The members would collectively decide on how the organization should allocate its funds. […] This essentially replicates the legal trappings of a traditional company or non-profit but using only cryptographic blockchain technology for enforcement.

One prominent example of a decentralized autonomous organization was called The DAO and was created with the stated intent to create a lasting smart contract on the Ethereum blockchain that would formalize, automate, and enforce contract terms through software. The DAO raised funds from investors in 2016 in exchange for DAO Tokens, but an attacker exploited a vulnerability in The DAO’s code to take control of approximately one-third of the Ethereum tokens, also known as ether, invested in The DAO. In order to make investors whole, the group behind The DAO endorsed a "hard fork" on the Ethereum blockchain that effectively transferred all funds raised (including those stolen by the attacker) from The DAO to a recovery address, where investors could exchange their DAO Tokens for Ethereum tokens on a new blockchain and avoid any nominal loss of invested Ethereum tokens.

**Evolving Regulatory Frameworks**

**Regulatory Overview**

As convertible virtual currencies have only recently become widespread, most regulators and supervisory authorities around the globe are still developing regulatory frameworks for virtual currencies. However, the US regulatory framework for virtual currencies is starting to take shape. Several prominent federal regulators have articulated particular regulatory frameworks or issued substantial relevant guidance, and several states have promulgated rules and guidance. In addition, consistent patterns of enforcement actions are illustrative of the short- to medium-term shape of regulatory trends for virtual currencies.
Federal and state laws do not currently provide for consolidated, comprehensive oversight of virtual currency markets by a single regulator. However, multiple regulators are increasingly coordinating to provide a “multifaceted, multi-regulatory” approach to virtual currency markets:

- The SEC has asserted authority over virtual currencies that have features consistent with securities, and has asserted its enforcement authority over ICOs and similar capital-raising activities.

- The CFTC has declared virtual currencies to be commodities and thus asserted its full jurisdiction over virtual currency derivatives and derivatives markets, as well as virtual currency spot and cash markets for fraud and manipulation enforcement purposes.

- FinCEN oversees BSA/AML compliance for money transmitters and exchangers of virtual currencies for fiat currency or other virtual currencies. FinCEN generally treats virtual currencies as equivalent to transfers of cash or cash equivalents for reporting purposes.

- The IRS treats virtual currencies as property for capital gains tax purposes.

- OFAC treats transactions in virtual currencies issued by sanctioned regimes as potential extensions of credit to sanctioned regimes.

- State banking and financial regulators oversee some virtual currency spot exchanges through state laws governing money transfers.

As shown in Figure 2 below, several regulators have promulgated virtual currency guidance, customer or investor alerts, interpretations with respect to existing regulations, or new rulemakings since 2013. Until 2017, most regulatory publications with respect to virtual currencies came from FinCEN, the IRS, or state regulators such as the New York Department of Financial Services (NYDFS). This dynamic changed in the second half of 2017, as the CFTC and SEC began publishing a substantial number of documents on virtual currencies, followed soon after by their respective self-regulatory organizations (SROs), the National Futures Association (NFA) and the Financial Industry Regulatory Authority (FINRA). Approximately two-thirds of all substantive regulatory publications on virtual currency have been published since the second half of 2017.
Commodity Futures Trading Commission

The CFTC first took a stance on virtual currencies in December 2014, when then-Chairman Timothy Massad testified before the US Senate Committee on Agriculture, Nutrition & Forestry that virtual currencies like Bitcoin may be commodities. Chairman Massad noted that “the [Commodity Exchange Act] defines the term ‘commodity’ very broadly” and thus “[d]erivative contracts based on a virtual currency represent one area within our [the CFTC’s] responsibility.” In September 2015, the CFTC published its first enforcement action based on the conclusion that virtual currencies were commodities, as explained in more detail in Section III. But it was not until the second half of 2017, shortly after the SEC published the DAO Report, that the CFTC began publishing a large number of regulatory documents related to virtual currencies. Most recently, in March 2018, a federal judge ruled in favor of the CFTC’s interpretation that "virtual currencies can be regulated by CFTC as a commodity." This ruling is explained in more detail below.

On 17 October 2017, the CFTC published “A CFTC Primer on Virtual Currencies” (the “Primer”). The Primer stated that “Bitcoin and other virtual currencies are properly defined as commodities,” and the CFTC’s jurisdiction “is implicated when a virtual currency is used in a derivatives contract, or if there is fraud or manipulation involving a virtual currency traded in interstate commerce.”

---


Figure 2. **Regulatory Guidance by Agency**
H1 2013 through H1 2018, Semi-Annually

---

Figure 2 illustrates the number of regulatory guidance publications per half year by agency from H1 2013 to H1 2018. The chart shows a steady increase in regulatory guidance publications with a peak in H1 2017. The agencies with the highest number of publications include the SEC, FINRA, and the IRS.

---

**Commodity Futures Trading Commission**

The CFTC first took a stance on virtual currencies in December 2014, when then-Chairman Timothy Massad testified before the US Senate Committee on Agriculture, Nutrition & Forestry that virtual currencies like Bitcoin may be commodities. Chairman Massad noted that “the [Commodity Exchange Act] defines the term ‘commodity’ very broadly” and thus “[d]erivative contracts based on a virtual currency represent one area within our [the CFTC’s] responsibility.” In September 2015, the CFTC published its first enforcement action based on the conclusion that virtual currencies were commodities, as explained in more detail in Section III. But it was not until the second half of 2017, shortly after the SEC published the DAO Report, that the CFTC began publishing a large number of regulatory documents related to virtual currencies. Most recently, in March 2018, a federal judge ruled in favor of the CFTC’s interpretation that “virtual currencies can be regulated by CFTC as a commodity.” This ruling is explained in more detail below.

On 17 October 2017, the CFTC published “A CFTC Primer on Virtual Currencies” (the “Primer”). The Primer stated that “Bitcoin and other virtual currencies are properly defined as commodities,” and the CFTC’s jurisdiction “is implicated when a virtual currency is used in a derivatives contract, or if there is fraud or manipulation involving a virtual currency traded in interstate commerce.”
On 15 December 2017, the CFTC issued a proposed interpretation on virtual currency in retail transactions that would interpret the “actual delivery” exception to CEA section 2(c)(2)(D) to require “physical settlement.” One example of “actual delivery” in this context is “a record on the relevant public distributed ledger network or blockchain” indicating that the entire quantity of purchased virtual currency is transferred to the purchaser’s blockchain wallet (or “other relevant storage system”) that is consistent with the purchaser having full control of and title to the virtual currency and the offeror having no control of, title to, or interests in the virtual currency.

In December 2017, Cboe Futures Exchange and CME Group both announced that they were listing cash-settled Bitcoin futures contracts that settle based on reference prices gathered from virtual currency exchanges. CFTC officials told the press that the CFTC and the exchanges would monitor Bitcoin markets, including the underlying cash market, to make sure the futures contract would not be manipulated. On 4 January 2018, the CFTC published a backgrounder on “Oversight of and Approach to Virtual Currency Futures Markets” that stated the CFTC’s intent to “assert[] legal authority over virtual currency derivatives in support of the CFTC’s anti-fraud and manipulation efforts, including in underlying spot markets” and pursue “robust enforcement” including both “general regulatory and enforcement jurisdiction over virtual currency derivatives markets” and policing “fraud and manipulation in cash or spot markets.”

There has been intense media speculation regarding the possibility of manipulation of Bitcoin futures settlements, such as by “banging the close” in underlying cash markets to affect settlement determinations by Bitcoin exchanges. However, as of this writing, no enforcement actions and no civil complaints making such allegations have been identified. Based on the precedent set in reference rate litigation such as LIBOR and ISDAFIX (for which the authors provided expert and economic consulting services), it is quite likely that if any such enforcement actions or civil complaints were filed, they would utilize a “screen” methodology to identify potential pricing and statistical anomalies around the settlement window in the Bitcoin cash or futures markets.

On 19 January 2018, the CFTC and SEC enforcement directors issued a brief joint statement on both agencies’ intent to look beyond “form” to the “substance” of virtual currency activities for enforcement purposes.

On 24 January 2018, CFTC Chairman Giancarlo published a joint op-ed with SEC Chairman Clayton on virtual currency regulation. The op-ed noted that with the emergence of Bitcoin futures products on CFTC-regulated exchanges, “the CFTC gained oversight over the US bitcoin futures market and access to data that can facilitate the detection and pursuit of bad actors in underlying spot markets.”

On 6 February 2018, CFTC Chairman Giancarlo testified before the Senate Banking Committee on virtual currency. In his written testimony, he stated that the “CFTC has sufficient authority under the CEA to protect investors in virtual currency derivatives” but “the CFTC does NOT have regulatory jurisdiction over markets or platforms conducting cash or ‘spot’ transactions in virtual currencies or over participants on those platforms” except for “enforcement jurisdiction to investigate and, as appropriate, conduct civil enforcement action against fraud and manipulation.”
The CFTC also issued customer advisories in late 2017 and early 2018 that warned virtual currency customers and investors about “the risks of virtual currency trading” and complaints the CFTC had received regarding “pump-and-dump schemes” in virtual currency. In the latter advisory, the CFTC advised virtual currency customers and investors that “the CFTC maintains general anti-fraud and manipulation enforcement authority over virtual currency cash markets as a commodity in interstate commerce.”

On 6 March 2018, a federal district court ruled in favor of the CFTC’s jurisdiction over virtual currencies as commodities. According to the memorandum and order, “virtual currencies can be regulated by the CFTC as a commodity” because “virtual currencies are ‘goods’ exchanged in a market for uniform quality and value.” The order concludes that “the CFTC has standing pursuant to Title 7 U.S.C. § 13a-1(a) to seek injunctive and other relief related to misleading advice, and the fraudulent scheme and misappropriation of virtual currencies” and “the CFTC’s […] expansion into spot trade commodity fraud is justified by statutory and regulatory guidelines.” The order also notes that “the jurisdictional authority of CFTC to regulate virtual currencies as commodities does not preclude other agencies from exercising their regulatory power when virtual currencies function differently than derivative commodities,” consistent with the CFTC and SEC’s published perspectives on their non-exclusive authority over virtual currency under facts and circumstances tests.

The 6 March 2018 ruling bolsters the CFTC’s position that virtual currencies are commodities under the Commodity Exchange Act. However, as the only ruling affirming the CFTC’s position, it is unlikely to permanently settle the jurisdictional debate over virtual currency until and unless other courts rule similarly. An open question going forward is whether other courts will agree with the 6 March 2018 ruling’s conclusion that “the jurisdictional authority of CFTC to regulate virtual currencies as commodities does not preclude other agencies from exercising their regulatory power when virtual currencies function differently than derivative commodities,” which may be relevant in cases where both the CFTC and SEC pursue enforcement actions against the same targets, or where private litigants dispute whether virtual currencies are commodities, securities, both, or neither.

**Securities and Exchange Commission**

The SEC and its leadership have stated that most or all virtual currencies offered in ICOs as of early 2018 have been securities in practice, although they have recognized that it is in principle possible for a virtual currency to not be considered a security based on a facts and circumstances test. While the SEC did initiate several enforcement actions in matters related to virtual currencies before it published official guidance and interpretations in 2017, those pre-2017 virtual currency-related enforcement actions did not explicitly rely on the conclusions that virtual currencies were securities, that entities issuing virtual currencies were securities issuers, or that platforms facilitating transactions in virtual currencies were exchanges. The pre-2017 SEC enforcement actions are described in more detail in Section III.

The SEC first defined its perspective on virtual currencies as likely securities in its 25 July 2017 Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO (“DAO Report”). In this report, the SEC opined that US securities laws were applicable to “virtual organizations or capital raising entities that use distributed ledger or blockchain
technology to facilitate capital raising and/or investment and the related offer and sale of securities,” and that “the automation of certain functions through this technology, ‘smart contracts,’ or computer code, does not remove conduct from the purview of US federal securities laws.”

The DAO Report described the SEC’s investigation of The DAO, a “decentralized autonomous organization […] embodied in computer code and executed on a distributed ledger or blockchain” that the SEC concluded was created “with the objective of operating as a for-profit entity that would create and hold a corpus of assets through the sale of DAO Tokens to investors.” According to the DAO Report, investors in DAO Tokens could re-sell DAO Tokens on secondary trading platforms or hold on to DAO Tokens in expectation of sharing in anticipated earnings of the assets and projects of The DAO.

The DAO Report explained the SEC’s reasoning as follows: DAO Tokens are securities because investors in DAO Tokens invested money when they exchanged another virtual currency for DAO Tokens, and the investors did so with a reasonable expectation of profit derived from the managerial efforts of the team behind The DAO. The SEC concluded more broadly that The DAO was an issuer of securities and should have registered its offers and sales of securities unless an exemption applied; online platforms that traded DAO Tokens met the definition of an exchange and thus either had to register or operate pursuant to an exemption from registration; and entities and issuers with similar facts and circumstances to The DAO and DAO Token platforms would likewise have to register or operate pursuant to an exemption.

The SEC followed the DAO Report with a 28 August 2017 Investor Alert entitled “Public Companies Making ICO-Related Claims,” which notified investors that the SEC had recently suspended trading in the common stock of several companies that “made claims regarding their investments in ICOs or touted coin/token related news” in response to concerns such as “a lack of current, accurate, or adequate information about the company,” “questions about the accuracy of publicly available information,” or “questions about trading in the stock.” Although these suspensions of trading in common stock did not explicitly rely on the conclusion that virtual currencies were securities, they signaled the SEC’s increasing scrutiny of virtual currency issuers. These suspensions are described in more detail in Section III.

On 11 December 2017, Chairman Clayton issued a Statement on Cryptocurrencies and Initial Coin Offerings stating that “any [ICO] activity that involves an offering of securities must be accompanied by the important disclosures, processes and other investor protections that our securities laws require.” In addition, he stated that “tokens and offerings that incorporate features and marketing efforts that emphasize the potential for profits based on the entrepreneurial or managerial efforts of others continue to contain the hallmarks of a security under US law,” and advised financial market professionals, “including securities lawyers, accountant and consultants” to keep that in mind.

Chairman Clayton’s statement was followed a month later by a brief joint statement from the SEC and CFTC enforcement directors regarding virtual currency enforcement actions. The 19 January 2018 joint statement emphasized that both agencies would focus on the “substance” of virtual currency activities rather than the “form” of such activities.
Three days later, SEC Chairman Clayton presented opening remarks at the Securities Regulation Institute that were directed toward “securities lawyers, accountants, underwriters, and dealers.” He stated that he had “instructed the SEC staff to be on high alert for approaches to ICOs that may be contrary to the spirit of our securities laws and the professional obligations of the US securities bar,” such as not counseling clients involved in ICOs that “the product they are promoting likely is a security.”

Two days later, SEC Chairman Clayton and CFTC Chairman Christopher Giancarlo published a joint op-ed in the *Wall Street Journal* titled “Regulators Are Looking at Cryptocurrency.” The op-ed acknowledged some possible limits on the jurisdiction of the SEC over virtual currencies, but noted that “some products that are labeled as cryptocurrencies have characteristics that make them securities” and the SEC “is devoting a significant portion of its resources to the ICO market.” The op-ed warned “market participants, including lawyers, trading venues and financial services firms” that “we are disturbed by many examples of form being elevated over substance, with form-based arguments depriving investors of mandatory protections.”

On 7 March 2018, the SEC issued a public statement regarding “Unlawful Online Platforms for Trading Digital Assets” that warned investors “that many online trading platforms appear to investors as SEC-registered and regulated marketplaces when they are not” by, for example, “refer[ring] to themselves as ‘exchanges.’” The SEC statement recommended that “market participants operating online trading platforms” should “consult with legal counsel to aid in their analysis of federal securities law issues and to contact SEC staff, as needed, for assistance in analyzing the application of the federal securities laws,” such as when a platform “must register as a national securities exchange or operate under an exemption from registration, such as the exemption provided for [alternative trading systems] under SEC Regulation ATS.”

The SEC has yet to approve any of several proposed Bitcoin exchange-traded funds (ETFs). However, on 23 March 2018, the SEC issued an order instituting proceedings and requesting public comment on a proposed rule change to list and trade the shares of the ProShares Bitcoin ETF and the ProShares Short Bitcoin ETF at NYSE Arca, an exchange owned by Intercontinental Exchange. On 5 April 2018, the SEC issued a similar order requesting public comment on a proposal to list and trade the shares of the GraniteShares Bitcoin ETF and GraniteShares Short Bitcoin ETF on Cboe BZX Exchange. Both orders reference proposed ETFs with objectives to seek results corresponding to the direct or inverse performance of lead month Bitcoin futures contracts regulated by the CFTC.

**Financial Crimes Enforcement Network**

Federal BSA/AML regulator FinCEN has issued interpretive guidance and administrative rulings asserting its jurisdiction over virtual currency money services businesses (MSBs). Currently, as it stated in guidance issued 18 March 2013, FinCEN considers “administrators” (i.e., issuers or redeemers) of virtual currency and “exchangers” of virtual currency for real currency or other virtual currencies to be MSB “money transmitters” subject to the full range of FinCEN BSA/AML requirements, such as suspicious activity reporting. The guidance further stated that “the definition of a money transmitter does not differentiate between real currencies and convertible virtual currencies.” FinCEN clarified that it considered “an administrator or exchanger that
(1) accepts and transmits a convertible virtual currency or (2) buys or sells convertible virtual currency” to be a money transmitter subject to FinCEN regulations, but that FinCEN did not consider “a user who obtains convertible virtual currency and uses it to purchase real or virtual goods or services” to be a money transmitter or other MSB absent administration and/or exchange behavior in the virtual currency.  

In 2015, FinCEN issued an administrative ruling declaring a company to be a money transmitter (as well as a dealer in precious metals, precious stones, or jewels) for engaging in a business including accepting bitcoins in exchange of issuing physical or digital negotiable certificates of ownership of precious metals. This business involved holding precious metals in custody for buyers by opening a digital wallet for a customer and issuing a digital proof-of-custody certificate that can be linked to a customer’s wallet on the Bitcoin blockchain ledger. The digital proof-of-custody certificates were designed such that the customer could trade or exchange their precious metals holdings at the company by any means through which the customer could trade or exchange bitcoins. FinCEN’s ruling suggests the general principle that FinCEN considers a business involved in exchanges of fiat or virtual currency for transferable digital tokens representing commodity interests to be a money transmitter, because “it is allowing the unrestricted transfer of value from a customer’s commodity position to the position of another customer or third-party, […] going beyond the activities of a broker or dealer in commodities and is acting as a convertible virtual currency administrator (with the freely transferable digital certificates being the commodity-backed virtual currency).”  

**Internal Revenue Service**

The IRS in March 2014 issued a notice and news release providing that “virtual currency is treated as property for US federal tax purposes.” The notice noted among other details that “mining” virtual currency could count as a form of self-employment, and that “taxpayers may be subject to penalties” for “underpayments attributable to virtual currency transactions” under section 6662 or “failure to timely or correctly report virtual currency transactions” under section 6721 and 6722.  

**Office of Foreign Assets Control**

On 19 January 2018, the Office of Foreign Assets Control (OFAC) of the US Department of the Treasury, a federal regulator overseeing sanctions, issued guidance regarding Venezuela’s December 2017 announcement of intent to create a digital or virtual currency backed by Venezuela’s oil reserves. According to the guidance, a virtual currency issued by Venezuela connected to the right to receive commodities at a later date “would appear to be an extension of credit to the Venezuelan government,” and thus US persons dealing in such a virtual currency may be exposed to US sanctions risk under Executive Order 13808. This suggests that for sanctions purposes in general going forward, virtual currencies issued by foreign governments may be considered extensions of credit to those governments by OFAC. On 19 March 2018, the publication of Executive Order 13827 announced the prohibition of all transactions related to Venezuela’s virtual currency by US persons.
State Regulatory Frameworks

Some state financial regulators have considered creating regulatory frameworks for virtual currency. New York’s NYDFS moved particularly early, publishing a notice of inquiry on new regulatory guidelines specific to virtual currencies in August 2013. NYDFS followed the notice with a 17 July 2014 proposed regulatory framework for virtual currency firms called “BitLicense” that required virtual currency firms to comply with a wide range of requirements, including anti-money laundering rules such as “Know your Customer” (i.e., verifying the identity of accountholders). As of 24 June 2015, the final BitLicense Regulatory Framework rules were published in the New York State Register at 23 NYCRR Part 200.

The final BitLicense rules required that BitLicense licensees report transactions worth more than $10,000 in virtual currencies in aggregate in one day that are not subject to federal currency transaction reports to the NYDFS within 24 hours, monitor transactions for suspicious activity and file suspicious activity reports, and collect and maintain information on the identity and physical address of accountholders of the licensee. On 22 September 2015, the NYDFS reported that it had approved its first BitLicense application for Circle Internet Financial in a press release that described BitLicense as the “First Comprehensive Regulatory Framework for Firms Dealing in Virtual Currency.” As of 7 March 2018, four firms were listed on the NYDFS website as state-regulated virtual currency institutions.

Other states’ regulatory approaches have garnered less attention than New York’s. Some states have chosen to interpret virtual currency as “money” for the purposes of state money transmitter laws and regulations or have otherwise required virtual currency issuers and/or exchanges to register, while others have not provided any specific guidance.

Increasing Enforcement Actions

General Enforcement Trends

Regulators have pursued enforcement actions related to virtual currencies since at least the first half of 2013, but there has been a substantial increase in enforcement activity from the second half of 2017 onwards: more than half of the 46 total virtual currency enforcement actions have been brought since 1 July 2017. Although total enforcement actions have increased substantially, the largest increase has been in the form of enforcement actions seeking no monetary penalties or criminal charges, such as cease-and-desist orders and temporary trading suspensions. A breakdown of virtual currency enforcement actions by penalty-type sought is shown below in Figure 3.
The SEC has brought the most virtual currency enforcement actions, with at least 17 as of 9 March 2018; state agencies have brought 11; the CFTC and the Department of Justice (DOJ) have brought seven each; FinCEN has brought two; and the IRS and the FTC have each brought one virtual currency enforcement action. Figure 4 below displays a breakdown of enforcement actions by regulatory agency.
NERA’s analysis of the financial penalties imposed in resolved enforcement actions that have sought such penalties shows no strong trend over time. Among the 13 enforcement actions with published penalty amounts, only three have imposed penalties larger than $1 million, but those were for amounts in the tens or hundreds of millions of dollars, with one large enforcement action each from the DOJ, FinCEN, and the SEC. The large penalties were imposed on the alleged perpetrator of a bitcoin-denominated Ponzi Scheme, Trendon T. Shavers, and his online entity, Bitcoin Savings and Trust; the alleged operator of the “Silk Road” online criminal marketplace, Ross Ulbricht, also known as “Dread Pirate Roberts;” and an unlicensed exchanger of convertible virtual currencies, BTC-e, and its administrator, Alexander Vinnik, who allegedly violated BSA/AML requirements. Financial penalties broken down by enforcement agency and date are displayed in Figure 5 below.
In the following sections, trends in enforcement activities are analyzed by general category of alleged unlawful behavior: violation of registration requirements, fraud-related allegations, trading violations, and BSA/AML violations.

**Alleged Violations of Registration Requirements**

Enforcement authorities have pursued at least 26 enforcement actions that have alleged that targets violated registration requirements. Enforcement actions alleging violations of registration requirements tend to fall into a few categories depending on the enforcement agency involved:

- **FinCEN and the DOJ:** Registration requirement enforcement actions by FinCEN and the DOJ have typically alleged that firms or individuals acting as exchangers of convertible virtual currencies have operated unlicensed MSBs;

- **SEC and State Securities Regulators:** Those by the SEC and state securities regulators have typically alleged either (1) that firms or individuals associated with ICOs or digital token sales have offered unregistered securities, or (2) that firms or individuals operating online platforms to trade convertible virtual currencies have operated an unregistered exchange or broker-dealer;
• **CFTC:** Those by the CFTC have alleged (1) that firms or individuals offering financed retail transactions in convertible virtual currencies have failed to register as designated contract markets or swap execution facilities,86 (2) that firms or individuals that have accepted funds and orders in convertible virtual currencies have failed to register as futures commission merchants,87 or (3) that firms or individuals accepting convertible virtual currencies in exchange for pooled commodity interests have failed to register as commodity pool operators or associated persons of commodity pool operators. Platforms to trade convertible virtual currencies have operated an unregistered exchange or broker-dealer.88

**Fraud-Related Allegations**

Enforcement authorities have pursued at least 26 enforcement actions that have alleged that targets engaged in or conspired to engage in fraud-related activities ranging from providing insufficient or inaccurate information to prospective investors, to operating a Ponzi-scheme. Fraud-related allegations have been broadly similar across enforcement agencies, and thus are analyzed by the sub-type of activity alleged rather than the enforcement agency involved:

• **Insufficient or Inaccurate Information Provided to Investors:** Enforcement agencies such as the SEC and state securities regulators have issued cease and desist orders to,89 or temporarily suspended,90 firms or individuals on at least 12 occasions in matters alleging insufficient or inaccurate information provided to investors. The cease and desist orders have been targeted at a range of entities and individuals connected to virtual currencies, whereas the temporary suspensions have generally targeted publicly traded companies with recent announcements of projects involving issuing, mining, exchanging, or administering convertible virtual currencies or blockchains. These enforcement actions have generally involved no assessment of monetary penalties.

• **Commercial and Financial Fraud Schemes:** Enforcement agencies have sought injunctions and equitable relief in at least 14 matters alleging behavior amounting to operating fraud schemes, with allegations ranging from failing to deliver advertised and paid-for Bitcoin mining computers91 to operating a Ponzi scheme.92 Enforcement agencies have sought criminal charges, financial penalties, and/or injunctions in cases alleging such fraud schemes.

**Bank Secrecy Act/Anti-Money Laundering Allegations**

Enforcement authorities have pursued at least six enforcement actions related to virtual currencies that have alleged violations of BSA/AML statutes or regulations. These enforcement actions either alleged that individuals or entities were operating unlicensed or BSA/AML non-compliant money transmitters/MSBs or that they were aiding or engaged in money laundering:

• **Operating Unlicensed or BSA/AML Non-Compliant MSBs:** FinCEN has pursued two enforcement actions against alleged unlicensed money transmitters/MSBs, the DOJ has pursued two such enforcement actions, and the State of Florida has pursued one. Penalties imposed included prison terms in two cases, financial penalties of $122 million and $950,000, and, notably, in one case a dismissal of all charges in Florida state court in 2016—the only such total loss in a virtual currency enforcement action—in a ruling that cited the alleged vagueness of the relevant Florida statutes on MSBs.93
• **Money Laundering**: The DOJ brought two enforcement actions alleging money laundering activity in connection with the “Silk Road” online marketplace. The better-publicized of the two, against the purported owner and operator of “Silk Road,” Ross Ulbricht, alleged in part that he engaged in money laundering connected with the sale of drugs and criminal services on “Silk Road.” Ulbricht was sentenced to life in prison and ordered to forfeit nearly $184 million.94 The less-publicized enforcement action targeted two men who allegedly ran a Bitcoin exchange on “Silk Road” to facilitate drug purchases, and resulted in criminal convictions, prison sentences, and nearly $1 million in financial penalties.95

**Trading Allegations**

Enforcement authorities have pursued two enforcement actions relating to virtual currencies that have alleged trading violations:

• In 2015, the CFTC issued an order against TeraExchange LLC, a provisionally registered Swap Execution Facility, for purportedly allowing wash trades and prearranged trades on its platform. According to the CFTC, TeraExchange allowed two market participants to trade two “completely offsetting” contracts consisting of non-deliverable forward contracts based on the relative value of Bitcoin and the US dollar, and issued a press release advertising Bitcoin swap trading without disclosing that the sales were pre-arranged wash sales. The settlement involved no financial penalty.96

• In 2016, the SEC settled an enforcement action against Bitcoin Investment Trust, a Delaware trust invested in bitcoins, and SecondMarket, a broker-dealer, alleging violations of Rules 101 and 102 of Regulation M. The SEC alleged that SecondMarket, the sole authorized participant in Bitcoin Investment Trust, purchased shares in Bitcoin Investment Trust from shareholders and earned redemption fees during a continuous distribution, and hence, during the applicable restricted period. The SEC settled with the respondents for $53,756 in disgorgement and prejudgment interest and agreement to a cease and desist order.97

**Developing Civil Litigation Trends**

Noteworthy civil litigation related to virtual currencies is a very recent trend, with 23 out of 25 noteworthy civil actions identified by NERA brought since July 2017. Figure 6 below shows the temporal distribution of noteworthy civil litigation related to virtual currencies.
Civil litigation has featured recurring categories of allegations:

- Allegations of fraud or misappropriation (11 out of 25 cases);
- Allegations of negligence or breach/rescission of contract (eight out of 25 cases); and
- Allegations of violations of securities laws or regulations (16 out of 25 cases).

As explained below, many virtual currency-related lawsuits have featured more than one category of allegations. Of the 25 identified lawsuits, 21 have been putative class actions.

### Allegations of Fraud or Misappropriation in Civil Litigation

Allegations of fraud or misappropriation have been common in private virtual currency litigation. Such allegations range from claims of misleading promotional or marketing campaigns to allegations of outright theft of customer or investor assets.

The first noteworthy virtual currency litigation was a putative class action alleging fraud and misappropriation of customer assets filed in 2014 against the Bitcoin exchange Mt. Gox; its owner, Mark Karpeles; its bank, Mizuho Bank; and others following the collapse of Mt. Gox in February 2018. Plaintiffs alleged that Mt. Gox’s owner either stole customers’ bitcoins and fiat currency or negligently failed to safeguard customer assets, and alleged that Mizuho Bank continued to allow customers to deposit funds into Mt. Gox after suspending withdrawals while concealing from customers that it had ceased providing withdrawal services. The case against Mizuho Bank and Mark Karpeles is ongoing.
Numerous lawsuits since then have alleged fraud or misappropriation. In early 2018, three distinct putative class actions alleging fraud were brought against Bitconnect, a Bitcoin lending platform with its own convertible virtual currency, and individuals and/or entities accused of being affiliates or promoters of Bitconnect. The putative class action complaints against Bitconnect alleged that Bitconnect guaranteed a high rate of return on bitcoins invested in order to attract victims to a Ponzi scheme, achieving a market capitalization above $2 billion in December 2017.\textsuperscript{99} The complaints further alleged that on 13 January 2018, after several state authorities had issued cease and desist orders against Bitconnect, Bitconnect’s platform ceased operating for several days; when the website came back online, the lending platform was shut down; and investors were repaid their Bitcoin loans at an exchange rate that was far from the market exchange rate, as the price of Bitconnect’s “coin” fell by more than 90% between 13 January and 16 January 2018.\textsuperscript{100}

As with most virtual currency litigation alleging fraud or misappropriation, the ongoing Bitconnect litigation is likely to involve disputes over questions requiring expert opinions, such as determining the application of relevant commodities and/or securities laws and regulations to particular products and entities, estimating reasonable damages, examining market structures, and analyzing transaction histories. For example, with respect to possible damages, the ongoing Bitconnect litigation may have to determine whether damages, if any, should be calculated based on Bitconnect investors’ losses as denominated in US dollars or in Bitcoin, given that Bitconnect was a Bitcoin lending platform. Figure 7 below shows the relative change in the price of Bitconnect in US dollars and in Bitcoin immediately following the price crash.
Allegations of Negligence or Breach/Rescission of Contract

Allegations of negligence or breach/rescission of contract have also featured prominently in virtual currency litigation. Allegations of negligence and breach/rescission of contract have often targeted virtual currency service providers. For example, a putative class action filed on 1 March 2018 against virtual currency exchange Coinbase and two of its executives alleged that Coinbase’s handling of the “hard fork” in the Bitcoin blockchain that produced the new virtual currency Bitcoin Cash had been negligent. The lawsuit alleged that Coinbase negligently allowed employees to engage in insider trading and failed to use reasonable due care in ensuring that Coinbase could handle the large number of Bitcoin Cash transactions that occurred upon the virtual currency’s launch on Coinbase, and claimed that the price of Bitcoin Cash was “artificially manipulated” as a result, resulting in delayed or incomplete fills of customer orders at higher prices. Important outstanding questions related to the Coinbase litigation include whether Bitcoin Cash price movements can be attributed to Coinbase, whether putative class action members with distinct orders were similarly situated, and how customers’ alleged losses should be quantified. Similar questions are outstanding in many virtual currency lawsuits alleging negligence or breach/rescission of contract, which often contain allegations of artificial prices.

Sources: Data from Coinmarketcap.com, as of 26 March 2018. Both prices are indexed from 100 as of the 12 January 2018 closing price for illustrative purposes.
Allegations of Civil Violations of Securities Laws and Regulations

The most common category of allegations in virtual currency litigation has been violations of securities laws. Most virtual currency litigation followed the SEC’s publication of the DAO Report, which suggested the applicability of traditional securities laws to ICOs. Sixteen out of 25 total lawsuits, and 16 out of 21 total putative class actions, have featured allegations referencing federal or state securities laws or regulations. Some such lawsuits have alleged that unregistered ICOs constituted unregistered securities offerings and/or sales and that the proceeds from such sales should be used to repay ICO investors, whether or not fraud or deception were involved. For example, the 2018 putative class action Davy v. Paragon Coin, Inc. et al. argued that proceeds from the $70 million ParagonCoin ICO should be repaid to investors based on the unregistered nature of the ICO and without reference to alleged deception because “proof of deceptive activity or calculated deprivation of investors’ rights and protections under the federal securities laws is not required or determinative as to Plaintiff’s claim.”\(^{102}\)

Other virtual currency lawsuits have made allegations of violations of Section 10(b) of the Exchange Act and Rule 10b-5 related to transactions in stocks and bonds of firms purportedly engaged in virtual currency or blockchain activities. For example, a putative class action against Xunlei Limited, an online storage and cryptocurrency “mining machine” firm, alleged “material misstatements and omissions” in press releases and filings with the SEC related to the firm’s blockchain projects and issuance of a virtual currency, followed by negative press and substantial declines in the firm’s stock price. The putative class action complaint made loss causation arguments reminiscent of event studies commonly conducted by expert witnesses in stock-drop cases.\(^{103}\)
Summary and Conclusions

While the regulatory framework for virtual currency in the US continues to develop, its general outlines have taken shape: the CFTC has defined convertible virtual currencies as commodities; the SEC has indicated that most convertible virtual currencies are securities and most ICOs are securities offerings; FinCEN has applied MSB BSA/AML requirements to convertible virtual currency exchanges and administrators; the IRS has decided to treat convertible virtual currencies as property for tax purposes; OFAC has suggested that dealing in convertible virtual currencies offered by sanctioned regimes may be prohibited; and state regulators have varied in their treatment of virtual currencies, ranging from a virtual currency-specific licensing framework in New York to broad exemptions from state regulations in some other states.

Enforcement actions by regulatory authorities have also established discernable trends. For example, out of 46 total virtual currency enforcement actions identified by NERA, more than half have occurred since July 2017, though a majority of enforcement actions since that time have sought no criminal charges and imposed no financial penalties. In terms of categories of alleged violations, 26 enforcement actions have alleged registration violations, 26 have alleged fraud-related violations, six have alleged BSA/AML violations, and two have alleged trading violations.

Finally, civil litigation related to virtual currency has been a very recent phenomenon—23 of out 25 total private lawsuits identified by NERA have been brought since July 2017. Moreover, the lawsuits have featured several recurring allegations: 16 of those lawsuits alleged securities violations, 11 alleged fraud or misappropriation, and eight alleged negligence or breach/rescission of contract. Although some of the lawsuits have featured virtual currency-specific allegations such as misappropriation of digital assets, many have included traditional securities litigation issues, such as Rule 10b-5 stock-drop allegations and artificial price allegations applied to firms with virtual currency or blockchain projects.
Notes

1 Dr. Sharon Brown-Hruska is a Managing Director in NERA’s Securities and Finance and White Collar, Investigations, and Enforcement Practices. Dr. Brown-Hruska previously served as Commissioner and Acting Chairman of the US Commodity Futures Trading Commission, and has recently served as a Professor in Tulane University’s Energy Institute and a Visiting Professor of Finance in Tulane University’s A.B. Freeman School of Business. She has a PhD in Economics from Virginia Polytechnic Institute and State University.

2 Mr. Trevor Wagener is a Consultant in NERA’s Securities and Finance Practice. He previously worked as a trader and investment analyst in commodities and derivatives markets. He has an MS in Applied Economics from Johns Hopkins University and a BA with distinction in Ethics, Politics, and Economics from Yale University.


4 For example, US dollars.


7 Wells Fargo had a $257 billion market cap as of 26 March 2018, according to Bloomberg, LP.


9 Bitcoin’s market capitalization on 20 February 2018 was approximately $200 billion, more than double the market capitalization of the second largest cryptocurrency, Ethereum. See “Cryptocurrency Market Capitalizations,” available at https://coinmarketcap.com/all/views/all/.


13 Double spending occurs when the owner of a virtual currency attempts to use the same individual unit of the virtual currency twice.


20 Ibid, pp. 1, 6.


25 A hard fork is a change in protocol software that creates a divergence from the previous iteration of a blockchain such that transactions on the new blockchain would be regarded as invalid on the old blockchain, and additional transactions on the old blockchain would be regarded as invalid on the new blockchain.


43 Ibid.


48 See, for example, “When investors are offered and sold securities—which to date ICOs have largely been—they are entitled to the benefits of state and federal securities laws[.]” SEC Chairman Jay Clayton, “Chairman’s Testimony on Virtual Currencies: the Roles of the SEC and CFTC,” 6 February 2018, available at https://www.sec.gov/news/testimony/virtual-currencies-oversight-role-us-securities-and-exchange-commission.


53 Ibid, pp. 15–18.


56 Ibid.


59 Ibid.

61 Ibid.
63 Ibid.
86 Ibid.


100 See Class Action Complaints in Charles Wildes et al. v. Bitconnect International PLC et al. (Filed 24 January 2018); Brian Page et al. v. Bitconnect International PLC et al. (Filed 29 January 2018); and Andrew Kline et al. v. Bitconnect et al. (Filed 7 February 2018).

101 Class Action Complaint in Jeffrey Berk vs. Coinbase Inc., Brian Armstrong, and David Farmer (Filed 1 March 2018).

102 Class Action Complaint in Davy v. Paragon Coin, Inc. et al. (Filed 30 January 2018), p. 4.

103 Class Action Complaint in Dookeran v. Xunlei Limited et al. (Filed 18 January 2018).
About NERA

NERA Economic Consulting (www.nera.com) is a global firm of experts dedicated to applying economic, finance, and quantitative principles to complex business and legal challenges. For over half a century, NERA’s economists have been creating strategies, studies, reports, expert testimony, and policy recommendations for government authorities and the world’s leading law firms and corporations. We bring academic rigor, objectivity, and real world industry experience to bear on issues arising from competition, regulation, public policy, strategy, finance, and litigation.

NERA’s clients value our ability to apply and communicate state-of-the-art approaches clearly and convincingly, our commitment to deliver unbiased findings, and our reputation for quality and independence. Our clients rely on the integrity and skills of our unparalleled team of economists and other experts backed by the resources and reliability of one of the world’s largest economic consultancies. With its main office in New York City, NERA serves clients from more than 25 offices across North America, Europe, and Asia Pacific.

Contacts
For further information and questions, please contact the authors:

Dr. Sharon Brown-Hruska
Managing Director
Washington, DC: +1 202 466 9222
sharon.brown.hruska@nera.com

Trevor Wagener
Consultant
Washington, DC: +1 202 466 9221
trevor.wagener@nera.com

To receive publications, news, and insights from NERA, please visit www.nera.com/subscribe.

The opinions expressed herein do not necessarily represent the views of NERA Economic Consulting or any other NERA consultant. Please do not cite without explicit permission from the author.
Debra W. Cook  
Managing Director and Deputy General Counsel  
The Depository Trust & Clearing Corporation (DTCC)

Debra W. Cook is Managing Director and Deputy General Counsel of The Depository Trust & Clearing Corporation (DTCC). She is lead counsel for DTCC’s Tampa office with a focus on supporting DTCC’s derivatives businesses globally.

Debra joined DTCC in 2005 upon the establishment of its Tampa office. She has been instrumental in establishing DTCC’s trade repositories and advising on its Trade Information Warehouse business from inception to its current move to a distributed ledger.

Prior to DTCC, Debra was an attorney for the Federal Reserve Bank of New York where she was engaged on the committee to revise UCC Article 8 which introduced the concept of entitlements; worked on policy matters related to revisions of the bankruptcy code to protect swaps; and provided analytical research on interbank netting for the Lamfalussy Report. Following her career at the FRBNY, Debra served as Counsel at Citigroup, advising the over-the-counter derivatives and foreign exchange trading businesses.

Debra received a B.A. from the College of William and Mary and her J.D. from the Washington College of Law at American University.
Dr. Sharon Brown-Hruska

Partner, National Economic Research Associates and Professor, Tulane University Energy Institute

- Board of Directors, PRIME Finance Dispute Resolution and Education Foundation, 2017–Present
- Visiting and Adjunct Professor, Energy Institute, A.B. Freeman School of Business, Tulane University, 2012–Present
- Chairman of the Regulatory Oversight Committee of the Board of Directors, Electronic Liquidity Exchange (ELX,) 2009–16
- Public Director and Corporate Governance Committee, MarketAxess Holdings, 2010–13
- Board of Trustees, International Securities Exchange (ISE), 2009–16
- President Elect Transition Landing Team Leader, 2016–17

Dr. Brown-Hruska provides advice and economic analysis to global corporations, industry associations, and governments on risk, regulation, and compliance. She is an expert on corporate governance, and has served as an advisor to and director of corporate boards of commercial and financial firms, exchanges, associations, and government agencies. She has offered expert witness testimony in cases alleging fraud or manipulation in securities and derivatives markets, as well as numerous regulatory enforcement, litigation, and compliance matters. She has analyzed big data and testified before regulatory authorities, served as a damages and liability expert, analyzed bankruptcy losses, and testified in arbitrations before FINRA on industry practices on securities markets, asset management, and structured finance. She is a NFA arbitrator and a P.R.I.M.E. Finance expert in dispute resolution.

Twice appointed as Commissioner of the CFTC, and twice confirmed by the Senate, she was chosen by the President as Acting Chairman of the CFTC, and in that role she served on key working groups and task forces, including the President’s Working Group on Financial Markets. She also served on the President’s Corporate Fraud Task Force, and played a leadership role in cooperative enforcement with national and international authorities. Designated to take the lead on energy enforcement matters as Commissioner, she worked closely with staff attorneys and the CFTC Office of Cooperative Enforcement to facilitate interagency actions in enforcement and litigation, including the successful prosecution of prominent Ponzi schemes involving fraud, manipulation, and money laundering in foreign currency and other commodities. She led the agency’s efforts in developing anti-money laundering (AML) and “Know Your Customer” procedures for financial entities governed by the commodities and securities laws, and has written reports and testified in matters involving regulatory requirements for banks, broker-dealers, and other financial institutions.

She has testified before the U.S. Senate Agriculture, Nutrition and Forestry Committee and the House of Representatives General Farm Commodities and Risk Management Subcommittee of the Committee on Agriculture. In 2004, she was awarded the Key Women in Energy’s Global Leadership Award.

Dr. Brown-Hruska has published her work in Forbes, Barron’s, the Capital Markets Law Review, the Wall Street Journal, International Commodities Review (2005), and various practitioner and scholarly publications.

PhD and MA in Economics
BA in Economics and International Studies
Virginia Polytechnic Institute and State University

Cell: +1 202-230-1764
Sharon.hruska@nera.com
Web Page
Managing Director

Doug advises clients on regulatory matters involving risk management, compliance, investment products, derivatives, and capital markets. He also counsels financial services companies on general corporate governance, internal controls, and strategic advisory matters. He has considerable experience with the regulatory and compliance issues associated with trading, clearing, and capital markets activities, having served as Senior Deputy Comptroller for Capital Markets at the Office of the Comptroller of the Currency, and as General Counsel of a futures commission merchant and a designated-contract-market and derivatives clearing organization.

Immediately prior to joining Promontory, Doug was the General Counsel and Chief Operating Officer of BrokerTec Futures Exchange and BrokerTec Clearing Co. He has also served as Senior Deputy Comptroller for Capital Markets at the Office of the Comptroller of the Currency, where he was responsible for the regulation and supervision of national bank capital markets activities, including trading, dealing, and investing in derivatives and emerging markets instruments, as well as the development of risk management policies and guidelines. Doug was the principal draftsman of OCC Banking Circular 277, “Risk Management of Financial Derivatives,” the first bank regulatory guidance on managing the risks associated with derivatives, capital markets, and trading activities. He also served on the Inter-Agency Task Force on Bank-Related Derivatives Activities and as senior staff member of the President’s Working Group on Financial Markets. Prior to his time at the OCC, Doug served as Assistant General Counsel of JPMorgan and General Counsel of JPMorgan Futures Inc.

Doug earned a J.D. from Harvard Law School and an A.B. (with honors) from Harvard College.
Kimberly Johns is a Managing Director and Associate General Counsel in the Legal Department of Goldman Sachs & Co. LLC where she advises the Derivatives Clearing Services, Prime Clearing, and Digital Assets businesses and is a member of the firm’s Clearing House Risk Committee. Previously, she was a litigation associate at Sidley Austin LLP and served as Chief Administrative Law Clerk to The Honorable Peter Paul Olszewski, Superior Court of Pennsylvania. Kim earned her J.D. (summa cum laude) from St. John's University School of Law and a B.A. in International Studies from Johns Hopkins University.
Neel Chopra joined the CFTC from the law firm Lankler Siffert & Wohl LLP. Earlier in his career, Mr. Chopra served as a law clerk to the Honorable John M. Walker, Jr., on the United States Court of Appeals for the Second Circuit, and, before that, as a law clerk to the Honorable Leonard B. Sand, on the United States District Court for the Southern District of New York. Mr. Chopra is a graduate of the University of Wisconsin and New York University School of Law.
B. SALMAN BANAEI is an Executive Director and Global Head of Clearance & Settlement and the Americas Head of Regulatory Affairs for North America at IHS Markit. Mr. Banaei is responsible for the regulated businesses arising out of IHS Markit’s new Stax distributed ledger technology, currently focused on developing a clearance and settlement business for the $5 trillion US syndicated loans markets.

Before joining IHS Markit, Mr. Banaei served at the U.S. Commodity Futures Trading Commission (CFTC) where he was most recently an advisor to a CFTC commissioner. Mr. Banaei began his professional career in Paris and has worked for law firms in Denver and Abu Dhabi. Mr. Banaei is also a regular lecturer and subject matter expert for Commodities and Derivatives Law at the J.P. Morgan Center for Commodities, and holds degrees from the University of Virginia, University of Denver – Sturm College of Law, Colorado School of Mines, and the Institut Francais du Petrole. Mr. Banaei is a member of the District of Columbia and Texas bar associations.