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

Crypto and Blockchain
January 25, 2019
10:15 a.m. – 11:30 a.m.

Chair:
Jonathan Marcus (Skadden)

Panel:
Katherine Cooper (Murphy & McGonigle)
Dan Davis (CFTC)
Steve Mickelson (3Degrees Inc.)
Charley Mills (Steptoe & Johnson)
Michael Spafford (Paul Hastings)
Petal Walker (WilmerHale)
CFTC’s Policy Goals of its Regulation of Cryptocurrencies, Its Jurisdiction to so Regulate, and the Relationship of this Work to its Traditional Oversight of Commodity Derivatives

December 7, 2018

By: Katherine Cooper*

This paper will explore what the answers may be to three interrelated questions:

- Why is the CFTC regulating cryptocurrencies (what are the policy concerns here)?
- What is the scope of the CFTC's jurisdiction over cryptocurrencies: (a) derivatives; and (b) cash markets?
- How is the Commission's traditional exercise of jurisdiction over futures contracts affected by the novelty of cryptocurrency products and relatively unregulated nature of cash markets for cryptocurrencies?

I. CFTC’s Policy Goal in “Regulating” Cryptocurrency

To be clear, the CFTC to date has not attempted to “regulate” cryptocurrencies in the manner that it regulates the futures, options and swaps markets with a comprehensive scheme requiring, among other things, registration, competency requirements, adequate capital thresholds for intermediaries and examinations of trading platforms. Congress has not given the CFTC the authority to regulate the cash cryptocurrency markets with such a comprehensive scheme. Rather it has exercised its authority over the cash markets for cryptocurrencies with the two limited tools Congress has given it to police commodity cash markets in general: limiting retail customers access to margin trading of commodities¹ and rooting out alleged fraud and manipulation in the sale of commodities in interstate commerce.²

---

* Katherine Cooper is a shareholder at Murphy & McGonigle P.C. where she advises and represents clients in matters involving commodity derivatives and futures, securities and cryptocurrencies. She previously served as the Chief Regulatory Officer of NYSE LIFFE US and as a Senior Trial Attorney at the Commodity Futures Trading Commission.

¹ CEA Section 2(c)(2)(D); 7 U.S.C. § 2(c)(2)(D).
² CEA Section 6(c)(1); 7 U.S.C. § 9(1).
The current CFTC Director of Enforcement recently stated the following at a conference introducing the Division’s Fiscal Year 2018 Year in Review:

The story of virtual currency is also about new technology. And it is a story about the need for robust enforcement to ensure technological development isn’t undermined by the few who might seek to capitalize on this development for unlawful gain. New and potentially market-enhancing technologies like virtual currencies and distributed ledger technology need breathing space to survive. Through work across the Agency, the CFTC has shown its continued commitment to facilitating market-enhancing innovation in the financial technology space. But part of that commitment includes acting aggressively to root out fraud and manipulation from these markets. The Virtual Currency Task Force is dedicated to identifying misconduct in these areas and holding bad actors accountable.3

A similar emphasis on combatting fraud and manipulation was articulated by Chairman Giancarlo in a financial press interview:

When it comes to the oversight of cryptocurrencies, regulators need to avoid inhibiting innovation, yet be vigilant against manipulation, said U.S. Commodity Futures Trading Commission Chairman J. Christopher Giancarlo.

Speaking to CNBC at the annual Singapore Summit on Friday, he said that the internet flourished because the government did not step in too heavily, and applied a "do no harm" approach.

"And I'm advocating the same approach to cryptocurrencies and all things having to do with this new digital revolution of markets, and of currencies, and of asset classes," Giancarlo said.

But, at the same time, caution is required because some kinds of fraud and manipulation often seen in foreign exchange and precious metals are now taking place in cryptocurrency markets, he said.4

These statements indicate that the CFTC sees a need to combat fraud and manipulation in the cryptocurrency cash markets. This answers the question of what the policy goal is that the CFTC is trying to achieve. It does not answer the question of why the CFTC sees itself as the

3 Speech of Enforcement Director James M. McDonald Regarding Enforcement trends at the CFTC, NYU School of Law: Program on Corporate Compliance & Enforcement (Nov. 14, 2018). Available at: https://www.cftc.gov/PressRoom/SpeechesTestimony/opamcdonald1
4 Global financial system is now 'stronger' than it was 10 years ago: CFTC chairman, CNBC Interview with J. Christopher Giancarlo (Sept. 14, 2018). Available at: https://www.cnbc.com/2018/09/14/do-no-harm-in-regulating-cryptocurrencies-but-be-vigilant-cftc.html
government regulator that should be trying to achieve this policy goal. Thus, there appears to be only a partial answer to the question of “Why is the CFTC regulating cryptocurrencies?”

II. The CFTC’s Jurisdiction Over Cryptocurrencies

Much of what delineates the scope of the CFTC’s authority under the Commodity Exchange Act (“CEA”) is based on the statute’s definition of the term “commodity.” Although loosely referred to as the CFTC’s jurisdiction, to be technically accurate, the CEA’s definition of the term “commodity” restricts the causes of action that it can bring because an element of most of these statutorily granted powers require a “commodity” to be involved in one way or another. For instance, CEA Section 6(c)(1) and CFTC Regulation § 180.1, promulgated thereunder, prohibit the use of a fraudulent or manipulative device in connection with “a contract of sale of any commodity in interstate commerce, or for future delivery.” Thus, the definition of the term “commodity” is key to understanding the scope of authority that Congress has granted the CFTC under these provisions.

A. The Background to the Definition of the Term “Commodity”

The definition of the term “commodity” in the CEA stems from the Commodity Futures Trading Commission Act of 1974 (the “1974 Act”) which worked “a sweeping overhaul” of the CEA. It created the CFTC and granted it extensive authority over commodity futures markets not then regulated by the CFTC’s predecessor, the Commodity Exchange Authority, a division of the Department of Agriculture.

---

Prior to 1974, the CEA and its predecessor statutes, the Futures Trading Act of 1921\textsuperscript{7} and Grain Futures Act of 1922,\textsuperscript{8} specifically enumerated commodities subject regulation. As the number of commodities with futures contracts trading on them increased, Congress repeatedly amended the statute to have the new markets regulated. When Congress amended the Grain Futures Act in 1936, renaming it the Commodity Exchange Act, it extended the law’s regulatory authority to cover cotton and other specified commodities. Amendments to the CEA in 1968 added more specifically enumerated commodities under the regulatory purview of the law such as livestock, livestock products, and frozen concentrated orange juice.

By 1974, it had become clear that the strategy of naming specific commodities in the CEA’s definition could not keep up with the growth of the futures markets, which were expanding to cover additional goods and services:

While the futures markets in a number of agricultural commodities had been regulated to varying degrees since 1922, many large and important futures markets were completely unregulated by the federal government prior to 1974. These included such agricultural and forestry commodities as coffee, sugar, cocoa, lumber and plywood plus various metals including the highly sensitive silver market and markets in a number of foreign currencies.

A person trading in one of the then unregulated futures markets needed the same protection afforded to those trading in the regulated markets. . . .\textsuperscript{9}

Discussions were underway concerning futures markets in such things as home mortgages and ocean freight. Accordingly, Congress determined to use two broad classes of products to define the commodities subject to the jurisdiction of the CEA. These included the phrases “all other goods and articles” to cover tangible commodities in addition to the specifically enumerated

\textsuperscript{7} Pub. Law No. 67-66, 42 Stat. 187 (1921). The ill-fated Futures Trading Act of 1921 was Congress’s first attempt to regulate futures trading. It was meant to address speculative excesses on the grain exchanges following World War I. It based its regulatory authority on the taxing power under the Federal Constitution and was declared unconstitutional for that reason in \textit{Hill v. Wallace}, 259 U.S. 44 (1922).

\textsuperscript{8} Pub. Law No. 67-331, 42 Stat. 998 (1922).

agricultural commodities, and “all services, rights, and interests” to cover the intangible commodities such as home mortgages, futures on which seemed just over the horizon to Congress in 1974.10

But Congress did not give the CFTC jurisdiction over all “goods or articles” and “services, rights or interests.” Rather, it limited the definition of the term “commodity” to only include such products “in which contracts for future delivery are presently or in the future dealt in.”11 That the “dealt in” language creating the futures trading requirement was jurisdictional in nature stretches back to the very beginning of Congressional deliberations to amend the CEA in September 1973. On September 25, 1973, Frederick Uhlmann, Chairman of the Board of the Chicago Board of Trade, testifying before a sub-committee of the House Small Business Committee, presented proposed legislation to define “commodity” to be everything deliverable on a futures contract.12 He emphasized the importance of giving the as-yet unnamed commodity regulatory agency exclusive jurisdiction over futures trading. This would prevent any possible conflicts over jurisdiction over futures trading. This would prevent any possible conflicts over jurisdiction.13

After follow-on hearings before the House Agriculture Committee in October 1973,14 W.R. “Bob” Poage, Chairman of the House Agriculture Committee, introduced H.R. 11955 on December 13, 1973. That bill included the “dealt in” phrase. Poage explained that, under his proposed legislation, “[a]ll commodities trading in futures will be brought within federal

11 1974 Act § 201, now codified at 7 U.S.C. § 1a(9).
12 Hearings before the Subcommittee on Special Small Business Problems of the House Permanent Select Committee on Small Business on Problems Involved in the Marketing of Grain and Other Commodities 93rd Cong. 1st Sess. July 25, 26: Sept 18, 25, 26; Oct 2, 3 and 4, 1973 at 144.
13 Id. at 163.
regulation under the aegis of the new Commission.” But that provision also included a proviso that preserved the SEC’s jurisdiction “over those areas traditionally regulated by it.”15

At the hearings held by the Agriculture Committee on this bill in January 1974, many witnesses were critical of the SEC proviso. Among the critics was Leo Melamed, the father of financial futures. He thought the proviso was redundant and likely to be confusing. In his view, the jurisdictional import of the expanded definition of the term commodity together with the “dealt in” phrase was clear, and no mention of the SEC’s jurisdiction was necessary.16 These hearings make plain that the “dealt in” clause was very much meant as a jurisdictional provision.

B. The CFTC’s Claims of Jurisdiction Over Cryptocurrencies

The first jurisdiction exercised by the CFTC over a cryptocurrency came with the certification of Bitcoin swaps by TeraExchange, a registered swap execution facility (“SEF”) on September 11, 2014.17 Not long after that in November 2014, CFTC Commissioner Mark Wetjen asserted at a Bloomberg-sponsored conference that the CFTC had jurisdiction over Bitcoin:

It has not been tested, but I do believe we have the authority because bitcoin, by I think a very rational reading of our statute, classifies as a commodity and the definition of a commodity under the Commodity Exchange Act.18

In December 2014 testimony before a Senate Agricultural Committee, then Chairman Timothy Massad stated:

While the CFTC does not have policies and procedures specific to virtual currencies like bitcoin, the agency’s authority extends to futures and swaps contracts in any commodity

---

16 Hearings before the House Committee on Agriculture on H.R. 11955, 93rd Cong. 2d Sess., January 23, 24, 29, 30 & 31, 1974 at 105; see also id. at 51 & 97 (other witnesses question the necessity of the SEC proviso).
17 CFTC Backgrounder on Oversight of and Approach to Virtual Currency Futures Markets at 2 n.9 (CFTC Jan. 4, 2018) (“CFTC Backgrounder”). Available at: https://www.cftc.gov/sites/default/files/idc/groups/public/%40customerprotection/documents/file/backgrounder_virtualcurrency01.pdf
18 Commissioner Claims CFTC Can Intervene in Bitcoin Markets (Coindesk Nov. 18, 2018). Available at: https://www.coindesk.com/commissioner-claims-cftc-can-intervene-bitcoin-markets
… derivative contracts based on a virtual currency represent one area within our responsibility.\textsuperscript{19}

Massad’s statement seems carefully crafted to be faithful to the “dealt in” limitation on the definition of a commodity, whereas Wetjen’s comments do not. It seems Wetjen’s comments were a harbinger of the CFTC’s thinking in the years to come.

In less than a year, the CFTC issued a speaking order, \textit{In re Coinflip Inc.},\textsuperscript{20} asserting that Bitcoin and other virtual currencies are “commodities” under the CEA:

Section 1a(9) of the Act defines “commodity” to include, among other things, “all services, rights, and interests in which contracts for future delivery are presently or in the future dealt in.” 7 U.S.C. §1a(9). The definition of a “commodity” is broad. See, e.g., Board of Trade of City of Chicago v. SEC, 677 F.2d 1137, 1142 (7th Cir. 1982). Bitcoin and other virtual currencies are encompassed in the definition and properly defined as commodities.\textsuperscript{21}

The CFTC’s reliance on the \textit{Board of Trade v. SEC}\textsuperscript{22} decision as precedent that virtual currencies other than Bitcoin are “commodities” is odd because the Seventh Circuit in that case was very mindful of the “dealt in” requirement. It wrote that with the 1974 Act’s amendment to the definition of the term “commodity:” “literally anything other than onions could become a ‘commodity’ and thereby subject to CFTC regulation simply by its futures being traded on some exchange.”\textsuperscript{23}

The \textit{Coinflip} order offered no rationale for why other virtual currencies other than Bitcoin were “commodities.” Indeed, the only cryptocurrency involved in the matter was Bitcoin. Moreover, the \textit{Coinflip} order does not provide the CFTC’s reasoning for why Bitcoin

\textsuperscript{19} \textit{CFTC Chairman: We Have Oversight of Bitcoin Derivatives} (Coindesk Dec. 11, 2014). Available at: https://www.coindesk.com/cftc-chairman-oversight-bitcoin-derivatives


\textsuperscript{21} Id. at 3.

\textsuperscript{22} 677 F.2d 1137 (7th Cir. 1982).

\textsuperscript{23} Id. at 1142.
was a “commodity.” It is not clear whether the CFTC reasoned that the listing of Bitcoin swaps on TeraExchange satisfied the “dealt in” requirement or the illegal Bitcoin options offered by Coinflip itself satisfied the “dealt in” language. If either or both of those theories explain how the CFTC saw the “dealt in” requirement met, it leaves open the question of why the CFTC sees a swap or an option satisfying the “dealt in” clause, which demands that there be “contracts for future delivery” in the product.

A year later, in 2016, the CFTC issued another speaking order, In re Bitfinex,24 which again asserted that Bitcoin and other virtual currencies fell within the definition of the term “commodity” under the CEA. In that case, the CFTC fined Bitfinex for a margin lending program it provided to retail investors which enabled them to trade Bitcoin on margin in violation of CEA Section 2(c)(2)(D). The only virtual currency involved in Bitfinex’s margin lending program was Bitcoin. Nonetheless, in setting forth its view of how a “commodity” was involved in the case, the CFTC repeated the same exact language it had used in Coinflip to assert that “Bitcoin and other virtual currencies are encompassed in the definition and properly defined as commodities.”25 Again, like in Coinflip, the CFTC does not explain how the Bitcoin involved in Bitfinex’s margin lending program constituted “a service, right or interest . . . in which contracts for future delivery are presently or the future dealt in.” The CFTC may have seen the “dealt in” clause satisfied by the Bitcoin swaps listed on TeraExchange, or the CFTC may have seen the Bitcoin traded on margin through the Bitfinex margin lending program as being part of the offer of illegal, off-exchange futures which in themselves satisfied the “dealt in” clause.

---


25 Id. at 5-6.
The CFTC’s discussion of “other virtual currencies,” however, in both *Coinflip* and *Bitfinex* is nothing short of dictum in speaking orders where the respondents had no incentive to challenge or negotiate with the CFTC over that conclusion. That said both *Coinflip* and *Bitfinex* represent the CFTC’s exercise of jurisdiction within its traditional sphere of its regulation of derivatives, and thus, are in keeping with Chairman Massad’s more limited assertion of jurisdiction that the agency has regulatory authority over virtual currency derivatives.

C. The Federal Courts’ Views of the CFTC’s Jurisdiction over Cryptocurrencies

In 2017, the CFTC began to road rest its theories about its jurisdiction over virtual currencies in federal court. Beginning with its *CFTC v. Gelfman Blueprint* case brought in September 2017, the CFTC has brought a number of cases in federal courts to exercise its claimed jurisdiction over virtual currencies. So far, only two cases have generated written decisions of one sort or another.

In *CFTC v. McDonnell*, the CFTC alleged that Patrick McDonnell and related entities fraudulently induced individuals to send them Bitcoin and Litecoin for McDonnell to trade on their behalf. In granting a preliminary injunction against McDonnell, Judge Jack Weinstein concluded that virtual currencies were “commodities,” but rested that conclusion on the “dealt in” clause: “Where a futures market exists for a good, service, right, or interest, it may be regulated by CFTC as a commodity, without regard to whether the dispute involves futures contracts.” At the time the *McDonnell* complaint was filed, there were futures contracts trading on Bitcoin on the CBOE Futures Exchange and the Chicago Mercantile Exchange, and Bitcoin binary options listed on the Cantor Fitzgerald Futures Exchange. Moreover, Bitcoin swaps and

---

27 *CFTC v. Kantor*, Docket No. 18-cv- 2247 (E.D.N.Y.); *CFTC v. Dean*, Docket No. 18-cv- 00345 (E.D.N.Y.)
Bitcoin binary options had been available for trading on TeraExchange and NADEX, respectively, since 2014.\(^{30}\) It is not clear what Judge Weinstein’s thinking was over the CFTC’s jurisdiction over the Litecoin involved in McDonnell’s alleged fraud. It may also be worth noting that McDonnell, a non-lawyer, proceeded in the action pro se.

The second case to have generated a written decision so far is *CFTC v. My Big Coin Pay, Inc.\(^{31}\) There the only virtual currency involved in the case was My Big Coin. The defendants moved to dismiss the amended complaint on the ground that because no futures contracts are traded on My Big Coin, that virtual currency was not a “commodity” – the “dealt in” requirement was plainly not satisfied.

In denying the motion to dismiss, Judge Rya Zobel rested her decision on three grounds. First, she concluded that because the CEA:

> classifies “livestock” as a commodity without enumerating which particular species . . . . signals an intent [by Congress] that courts [should] focus on categories – not specific items – when determining whether the “dealt in” requirement is met.\(^{32}\)

Second, quoting the Supreme Court’s decision in *SEC v. Zandford,\(^{33}\) Judge Zobel reasoned given the antifraud context in which the court was being to construe the meaning of the term “commodity” it was appropriate to “‘construe[] [the CEA] ‘not technically and restrictively, but flexibly to effectuate [the CEA’s] remedial purposes’”\(^{34}\)

Third, although conceding that the caselaw on the question was “scant,” Judge Zobel stated that a series of cases involving natural gas\(^{35}\) “repeatedly rejected arguments that a

---

\(^{30}\) CFTC Backgrounder at 2 nn. 9 & 10.

\(^{31}\) *CFTC v. My Big Coin Pay, Inc.,* Docket No. 18-cv-10077RWZ (D. Mass.).


\(^{34}\) 2018 WL 4261727 at *4 quoting 535 U.S. at 819.

particular *type* of natural gas was not a commodity because that specific type was not the subject of a futures contract."³⁶ Based on these three grounds, Judge Zobel ruled that because My Big Coin was a virtual currency and futures contracts trade on virtual currency, “[t]hat is sufficient, especially at the pleading stage, for plaintiff to allege that My Big Coin is a ‘commodity’.”³⁷ In a footnote, the court elaborated that “[c]ontrary to defendants’ arguments, the amended complaint alleges that My Big Coin and Bitcoin are sufficiently related so as to justify this categorical treatment.”³⁸

At least two of the three grounds that Judge Zobel determined supported the conclusion that My Big Coin is a “commodity” are questionable. First, the fact that the CEA states that “livestock” is a commodity without stating which species of livestock are commodities is irrelevant. Congress added “livestock” to the definition in 1968 when it was still trying to set the CEA’s reach by specifically naming types of things that were commodities. By 1974, however, Congress realized that it had to come up with a new approach to ensure that all futures contracts trading in the United States were regulated under the CEA. Thus, Congress came up with the phraseology of “all goods or articles . . . or services, rights or interests in which contracts for future delivery are . . . dealt in” to make certain that all futures contracts trading in the United States were subject to the CEA. It is unclear how the use of categories for “goods or articles” and “services, rights or interests” advances Congress’s purpose in 1974 that all futures contracts in the United States be subject to the CEA.

Second, the court’s assertion that the natural gas cases it cited stand for the principle that different “types” of natural gas were commodities even though they were not the “type” of

---

³⁶2018 WL 4261727 at *4 (emphasis added).
³⁷Id. at *5.
³⁸Id. at n.8.
natural gas on which the NYMEX Henry Hub futures trade is a misreading of those cases.\textsuperscript{39} None of those cases involved different “types” of natural gas. In those cases, defendants argued that the natural gas involved was not a “commodity” because the gas there was to be delivered at a delivery point in the interstate pipeline system other than the delivery point – the Henry Hub in Louisiana – where the NYMEX futures contract calls for natural gas to be delivered. For instance, the court in \textit{United States v. Brooks} reasoned

it would be peculiar that natural gas at another hub is not a commodity, but suddenly becomes a commodity solely on the basis that it passes through Henry Hub, and ceases to be a commodity once it moves onto some other locale.\textsuperscript{40}

In \textit{United States v. Futch}, another case cited by the court, a Fifth Circuit panel rejected the defendant’s argument that the natural gas involved there was not a “commodity” because it was to be delivered at “Transco Zone 6” instead of the Henry Hub.\textsuperscript{41} Finally, the third decision Judge Zobel relied upon, \textit{United States v. Valencia}, specifically noted that “natural gas is fungible” and found that “natural gas for delivery on the West Coast or otherwise, is a commodity” even if that is a different delivery point than the one used for the NYMEX contract.\textsuperscript{42}

All three of these cases stand for the principle that a product that has a futures contract trading on it does not stop being a commodity simply because the transaction at issue involves a delivery point other than the delivery point specified in the futures contract. They do not support a conclusion that different types of products within a broad category are all commodities if a futures contract is traded on one of them. As the \textit{Valencia} court noted, natural gas on the West

\textsuperscript{40} 681 F.3d 678, 694-95 (5th Cir. 2012).
\textsuperscript{41} 278 F. App’x at 395.
\textsuperscript{42} \textit{Valencia}, 2003 WL 23174749 at *8.
Coast was fungible with natural gas at Henry Hub in Louisiana. In My Big Coin, the CFTC did not allege that My Big Coin was fungible with Bitcoin – only that it had some similar characteristics.

III. The Impact of Cryptocurrency Products and their Unregulated Cash Markets on CFTC’s Traditional Jurisdiction over Futures Contracts

As noted above, the CFTC’s first exercise of jurisdiction over cryptocurrency came with TeraExchange’s self-certification of bitcoin swaps. This self-certification, NADEX’s listing of bitcoin binary options later in 2014 and the CFTC’s approval of LedgerX’s swap execution facility and derivatives clearing organization applications in 2017 all passed with little fanfare. The industry’s placid acceptance of these developments proved to be “the calm before the storm.”

On December 1, 2017, the CME and CFE self-certified bitcoin futures contracts and the Cantor Exchange self-certified bitcoin binary option contracts. The prospect of the launch of bitcoin futures products on U.S. futures exchanges was met with concern from many market participants. In an open letter on November 14, 2017 to CFTC Chairman Giancarlo, Thomas Peterffy, the Chairman of Interactive Brokers, requested the CFTC “require that any clearing organization that wishes to clear any cryptocurrency or derivative of a cryptocurrency do so in a separate clearing system isolated from other products.”

43 Of course, there are not different “types” of natural gas in the interstate pipeline system. Under the Federal Power Commission, “pipeline quality gas” standards were set to ensure the fungibility of the natural gas in the interstate pipeline network. M.M. Foss, Interstate Natural Gas—Quality Specifications & Interchangeability at 11 (Univ of Texas 2004) (under the Federal Power Commission, “‘Pipeline quality’ gas came to be defined as natural gas (1) within + / - 5 percent of the heating value of pure methane, or 1,010 Btu per cubic foot under standard atmospheric conditions, and (2) free of water and toxic or corrosive contaminants”). Available at: http://www.beg.utexas.edu/files/energyecon/global-gas-and-lng/CEE_Interstate_Natural_Gas_Quality_Specifications_and_Interchangeability.pdf; see also POLICY STATEMENT ON PROVISIONS GOVERNING NATURAL GAS QUALITY AND INTERCHANGEABILITY IN INTERSTATE NATURAL GAS PIPELINE COMPANY TARIFFS at 12 (FERC June 15, 2006) (only FERC authorized pipeline tariff standards may be enforced). Available at: https://www.ferc.gov/whats-new/comm-meet/061506/G-1.pdf

44 Letter dated Nov. 14, 2017 from Thomas Peterffy to J. Christopher Giancarlo available at:
There is no fundamental basis for valuation of Bitcoin and other cryptocurrencies, and they may assume any price from one day to the next. This has been illustrated quite clearly in 2017 as the price of Bitcoin has increased by nearly 1000% [and that margining] such a product in a reasonable manner is impossible. While the buyer (the long side) of a cryptocurrency futures contract or call option could be required to put up 100% of the value to ensure safety, determining the margin requirement for the seller (the short side) is impossible.\textsuperscript{45}

Peterffy expressed fear that if “the Chicago Mercantile Exchange or any other clearing organization clears a cryptocurrency together with other products, then a large cryptocurrency price move that destabilizes members that clear cryptocurrencies will destabilize the clearing organization itself.” He noted that even clearing firms that chose not to clear cryptocurrency futures and options were still exposed to their unquantifiable risk due to their clearing fund contributions and default waterfall assessment obligations.\textsuperscript{46}

Following the CFE, CME and Cantor self-certifications, on December 6, 2017, Futures Industry Association President Walt Lukken also wrote to Chairman Giancarlo. Lukken shared the FIA’s concerns regarding the launch of bitcoin futures and options. In light of the potential risk to the futures industry clearing infrastructure these products may pose that Peterffy had highlighted, Lukken questioned the use of the self-certification process for such novel products:

While suited for standardized products, this process does not distinguish for a product’s risk profile or unique nature. We believe that this expedited self-certification process for these novel products does not align with the potential risks that underlie their trading and should be reviewed. Given the lack of historical data on these products, it is further concerning to clearing members that they will bear the brunt of the risk associated with them through their guarantee fund contributions and assessment obligations, even if not participating in these markets directly, rather than the exchanges and clearinghouses who have listed them. A public discussion should have been had on whether a separate guarantee fund for this product was appropriate or whether exchanges put additional capital in front of the clearing member guarantee fund.\textsuperscript{47}
In response to the certifications the CFTC took no action to stay the listing of the bitcoin futures and options contracts. It did issue a “CFTC Backgrounder on Self-Certified Contracts for Bitcoin Products.” The Backgrounder notes that when an exchange self-certifies a new contract that it must determine that the contract complies with the CEA and Commission regulations, including that the new contract is not readily susceptible to manipulation.

The backgrounder goes on to assert that:

Unless the Commission finds that a new product would violate the CEA or Commission regulations, the DCM may list the new product no sooner than one full business day following the self-certification.

It states that the CFTC “has limited ability to require the DCMs to make changes to their contracts or to require the DCOs to change their approaches to clearing the contracts.” In response to calls from many quarters for the clearinghouses clearing bitcoin contracts to establish a separate clearing fund for them to insulate the risks posed by the products from the rest of the clearing ecosystem, the Backgrounder stated: “the Commission does not have the authority to require the DCOs to establish separate clearing systems or guaranty funds to clear these contracts.”

Thus, the backgrounder stresses that the CFTC was not “approving” the contracts and says it had limited ability to require the exchanges “to make changes to their contracts.”

It is unclear whether differing processes led the CFTC to reach a different result than the SEC’s approach to Bitcoin ETFs. The Exchange Act requires the SEC to affirmatively approve the amendment of a national securities exchange rule launching a new ETF – in other words,

---

49 Id. at 1.
50 Id.
requiring the SEC to affirmatively find that the new ETF complies with the Exchange Act\textsuperscript{52} – whereas the CEA authorizes designated contract markets to self-certify that a new futures contract complies with the CEA.\textsuperscript{53}

Certainly, one point of difference is how the two agencies took different views of the bitcoin cash market offered by Gemini, a limited purpose trust company regulated by the New York Department of Financial Services. In rejecting Bats proposed rule change to launch a bitcoin ETF that was to track the cash price of bitcoin on the Gemini exchange, the SEC noted that the NYSDFS’s regulations do not require virtual currency businesses registered with it to have the kinds of safeguards national securities exchanges are mandated to have to which are:

- designed to prevent fraudulent and manipulative acts and practices, to promote just and equitable principles of trade, to foster cooperation and coordination with persons engaged in regulating, clearing, settling, processing information with respect to, and facilitating transactions in securities, to remove impediments to and perfect the mechanism of a free and open market and a national market system, and, in general, to protect investors and the public interest.\textsuperscript{54}

In contrast, the CFE’s certification of its bitcoin futures contract\textsuperscript{55} is based on the integrity of the trading on the Gemini exchange. The CFE’s bitcoin future is cash-settled to an auction conducted on the Gemini exchange, as long as that price is within five percent of the Winklevoss Blended Bitcoin Index. That index is “a ten-minute volume weighted average price (“VWAP”) of bitcoin transactions in U.S. dollars on the Gemini Exchange and other bitcoin trading venues. These other bitcoin trading venues currently include the Bitstamp, itBit, and

\textsuperscript{52} Exchange Act Section 19(b)(2)(C) (the SEC “shall approve a proposed rule change of a self-regulatory organization if it finds that such proposed rule change is consistent with the requirements of this chapter and the rules and regulations issued under this chapter”).
\textsuperscript{53} CEA Section 5c(c); 7 U.S.C. § 7a-2(c).
GDAX trading venues.” The extent of regulation (or lack thereof) applicable to Gemini to guard against the use of fraudulent and manipulative acts and practices in its cash trading of bitcoin seemed to be less challenging to the CFTC than the SEC.

All of that said, it is not the case that the CFTC is entirely sanguine about the challenges posed by the unregulated nature of the cryptocurrency cash markets. Commissioner Brian Quintenz has advocated for the creation of a self-regulatory organization to regulate the cash cryptocurrency markets. The CFTC’s Division of Enforcement is reported to have subpoenaed Bitstamp, Coinbase, itBit and Kraken, trading on which generates the index to which the CME bitcoin futures are cash-settled. The CFTC’s investigation is reported to be in coordination with the Department of Justice and the two agencies are said to be looking into whether traders may have attempted to influence the bitcoin “through old-school tactics such as sending large numbers of fake orders.”

In conclusion, the CFTC’s acquiescence in the certification of bitcoin futures contracts has not caused the sky to fall as some worried. That said, the contracts have limited open interest. Moreover, the cryptocurrency cash market has a fairly small capitalization and that capitalization has fallen of late. As Chairman Giancarlo observed at the 2018 ABA Derivatives and Futures Law Committee Meeting:

> Whatever one’s opinion, an objective perspective helps. As of the morning of January 16, the total value of all outstanding Bitcoin was about $200 billion based on a Bitcoin price of $12,000. The total value of all outstanding virtual currencies was about $577 billion. The Bitcoin “market capitalization” is comparable to the stock market capitalization of a single “large cap” business, such as Intel or Citigroup (both around $200 billion). Because virtual currencies like Bitcoin are sometimes considered to be comparable to

---

56 Id. at 3.
57 Keynote Address by Commissioner Brian Quintenz before the DC Blockchain Summit (Mar. 7, 2018) available at: https://www.cftc.gov/PressRoom/SpeechesTestimony/opaquintenz8
59 Id.
gold as an investment vehicle, it is important to recognize that the total value of all the
gold in the world is estimated by the World Gold Council to be about $8 trillion which
continues to dwarf the virtual currency market size. Clearly, the column inches of press
attention to virtual currency far surpasses its importance in today’s global economy.\textsuperscript{60}

With bitcoin trading at a third of its price when Chairman Giancarlo spoke last year, the threat to
the clearinghouses clearing the bitcoin futures contracts as a systemic matter has only decreased.
Of course, the price of bitcoin has been volatile, but the clearinghouses and clearing firms have
weathered the volatility with very healthy initial margin requirements. The CFTC appears to be
investigating along with the DOJ suspicious activity that may represent attempted or actual
manipulation of the cash market underlying the bitcoin futures the CFTC regulates. And with
the CFTC’s encouragement, progress is being made on establishing SROs for the cryptocurrency
cash markets.\textsuperscript{61} In these ways, it seems that the CFTC is working to find ways to apply its
traditional jurisdiction over futures to the cryptocurrency space.

\textsuperscript{60} Remarks of Chairman J. Christopher Giancarlo to the ABA Derivatives and Futures Section Conference, Naples, Florida (Jan. 19, 2018) available at: https://cftc.gov/PressRoom/SpeechesTestimony/opagiancarlo34
Aiding and Abetting Liability for Smart Contract Coders under the Commodity Exchange Act

American Bar Association, Derivatives & Futures Law Committee Meeting
January 24-26, 2019, Naples, FL

Jonathan L. Marcus
Of Counsel, Derivatives, Skadden, Arps, Slate, Meagher & Flom LLP

On October 16, 2018, Commodity Futures Trading Commission (CFTC) Commissioner Brian Quintenz spoke at the 38th Annual GITEX Technology Week Conference in Dubai about how the existing Commodity Exchange Act (CEA) regulatory framework may apply to emerging smart contract applications on the blockchain. In particular, Quintenz addressed how the CFTC may approach enforcement if it determines that smart contracts programmed on the blockchain fit the definition of or facilitate trading in futures, swaps, options or event contracts. While Quintenz framed different potential approaches in hypothetical terms, the rapid advent of trading applications on the blockchain will require the CFTC to expand its focus to smart contracts and determine how the CEA and its rules apply. In fact, the Securities and Exchange Commission (SEC) recently settled an enforcement action against Zachary Coburn, the founder of EtherDelta, an unregistered platform that used a smart contract to facilitate the trading of digitized securities. The SEC found that Coburn caused EtherDelta to violate Section 5 of the Securities Exchange Act of 1934 by failing to register as a national securities exchange.¹

Commissioner Quintenz—focusing on smart contracts that resemble products that the CFTC regulates or that provide functionality that would permit or facilitate trading of those products—observed that many smart contracts may not be in compliance with the CEA and CFTC rules and, assuming that were the case, addressed who would bear legal responsibility. He suggested that while developers of the underlying blockchain, miners and others play a role in the use of smart contracts, it is the smart contract code developers who could be held accountable, at least where they “could reasonably foresee, at the time they created the code, that it would likely be used by U.S. persons in a manner violative of CFTC regulations.”² The Commissioner's remarks contemplate a novel use of a longstanding form of liability: that the CFTC could prosecute smart contract code developers for aiding and abetting violations of the CEA and CFTC rules by others, such as smart contract users who engage in unlawful off-exchange retail transactions on the blockchain, based on protocols created by the smart contract code developers. In practice, it may prove difficult for the CFTC to prevail on that theory.


because the CFTC may face challenges—i.e., proving a primary violation and the aider and abettor’s intent—that are far easier to address in typical aiding and abetting cases.

CEA Section 13(a) provides that “[a]ny person who . . . willfully aids, abets, counsels, commands, induces, or procures the commission of, a violation of [the CEA or CFTC rules] . . . may be held responsible for such violation as a principal.” It is settled that the CFTC must establish three elements in order to prove aiding and abetting liability: “(1) the CEA was violated, (2) the aider and abettor had knowledge of the wrongdoing underlying the violation, and (3) the aider and abettor intentionally assisted the primary wrongdoer.”3 The aider and abettor must have “actual knowledge of the primary wrongdoer’s conduct,” but does not necessarily need to know that the primary wrongdoer’s conduct is unlawful.4 Moreover, “[k]nowing assistance can be inferred from the surrounding facts and circumstances.”5 The CFTC has said that “[i]ntentional assistance is demonstrated if the aider and abettor ‘knowledgeably participate[s] in the [unlawful] venture and seek[s] by his actions to make it succeed.’”6

In a typical aiding and abetting case, the CFTC identifies one or more primary wrongdoers. The CFTC often will identify primary wrongdoers by name and charge them for the primary conduct underlying an aiding and abetting violation. Based on the CFTC’s prior actions, it appears that the primary violator also typically has a direct or special relationship with the aider and abettor. This direct relationship facilitates the CFTC’s ability to prove both knowledge of wrongdoing and intent to assist. For example, in Brenner v. CFTC,7 the Seventh Circuit affirmed the Commission’s findings of liability against a woman for aiding and abetting her husband’s CEA violations by knowingly assisting him in opening accounts and trading in her name.8 In affirming the Commission’s findings, the court cited testimony from an employee of a trading firm who stated that, based on his contacts with the husband and wife, he believed the wife was aware that her husband was trading on her account.9 In CFTC v. MF Global Holdings

---


8 See Brenner, 338 F.3d at 717-19, 723. The husband had been barred from trading on CFTC-regulated markets as a consequence of failing to satisfy a judgment for churning customer accounts. See id. at 715-16.

9 See id. at 720. The trading firm employee based his testimony on discussions he had with both the husband and wife regarding the account. See In re Brenner & Brenner, Comm. Fut. L. Rep. (CCH), ¶ 28,499, at *5 (Mar. 30, 2001).
the U.S. District Court for the Southern District of New York found that the assistant treasurer of MF Global’s Treasury Department aided and abetted the firm’s customer fund segregation violations by directing, approving or causing transfers of funds from customer segregated accounts to firm proprietary accounts, “knowing” that the customer segregated funds would be transferred to proprietary accounts. Other cases have involved:

- A firm aiding and abetting a customer’s concealment of material facts from an exchange by failing to report a trade until after the close of trading.\(^{12}\)

- An associated person of a futures commission merchant aiding and abetting a colleague’s fraudulent solicitations by creating a false audit of trading results, helping to pay for the distribution of a fraudulent email and making misrepresentations in meetings with prospective investors.\(^{13}\)

- A firm’s controller aiding and abetting the firm’s regulatory violations by failing to notify the CFTC promptly upon detecting a shortfall in certain customer accounts, and ordering a subordinate to transfer money from the firm’s own account to its customer segregated account.\(^{14}\)

- A broker aiding and abetting unlawful disclosures of customer information by soliciting exchange employees for the information, and providing them with information needed to identify the data that he sought.\(^{15}\)

- An unregistered commodity trading advisor aiding and abetting a scheme by the firm that compensated him to conceal payments from the National Futures Association by creating false invoices.\(^{16}\)

- An attorney aiding and abetting his clients in operating unlawful precious metals schemes by “crafting the illusion that their schemes were legitimate and complied with the law.”\(^{17}\)

\(^{10}\) No. 11-cv-7866 (S.D.N.Y. Jan. 5, 2017) (consent order against Edith O’Brien).

\(^{11}\) See id. at *7.

\(^{12}\) See In re UBS Secs. LLC, CFTC No. 10-11 (Apr. 29, 2010).

\(^{13}\) See In re Hinman, CFTC No. 16-13 (Apr. 12, 2016).

\(^{14}\) See In re Cunningham Commodities, LLC, No. 16-15 (May 9, 2016).


Even in the absence of a direct or special relationship, the CFTC has often cited specific facts—such as direct communication between the primary violator and aider and abettor—to demonstrate that the primary violator and aider and abettor acted in a coordinated manner. For instance, the CFTC has found aiding and abetting violations where traders at banks allegedly coordinated with traders at other banks to manipulate benchmark rates and other financial instruments, frequently pointing to specific communications between traders—such as messages in private chat rooms—to support the agency's findings.  

Against this backdrop, the CFTC would face unique challenges in attempting to prosecute smart contract code developers for aiding and abetting a smart contract user’s violation of the CEA or CFTC rules. First, the anonymized nature of blockchain transactions will undoubtedly make it more difficult for the CFTC to identify a primary violator. Second, that same anonymity will likely prove an evidentiary obstacle in establishing that the smart contract code developer had knowledge of the primary violation, and intentionally assisted the primary violator—in other words, that the developer “knowingly participate[d] in the venture.”

For example, smart contract code developers charged with aiding and abetting a CEA violation may try to argue that they did not know the identity of the contract user, did not know how the contract would be used, did not intend for the contract to be used as a “live” product for engaging in actual transactions on the blockchain, or were only a partial contributor to the development of the contract and lacked full visibility into its function or purpose.

Perhaps the closest analog for such a case is the CFTC’s complaint against software developer Jitesh Thakkar and his firm, Edge Financial Technologies, Inc. The CFTC charged Thakkar and Edge with aiding and abetting a trader’s spoofing scheme by developing customized trading software for the trader that contained a “Back-of-Book” function. The Back-of-Book function allegedly helped the trader place orders that he intended to cancel before execution by “minimizing the chance that [the spoof orders] would result in executed trades” before the trader could cancel them. Although the CFTC did not identify the trader by name in its complaint — only referring to him as “Trader A” — his identity was clearly known to the CFTC, and the complaint makes clear that the CFTC alleged that Trader A was the primary violator. In announcing the filing of the complaint, the CFTC noted that Trader A “cooperated

---

18 See, e.g., *In re Barclays PLC*, CFTC No. 12-25, at *2-3, 15-18, 27-28. See also *In re Lansing Trade Grp., LLC*, CFTC No. 18-16 (July 12, 2018) (aiding and abetting counterparty’s attempt to manipulate corn cash prices); *In re ICAP Capital Markets LLC*, CFTC No. 18-33 (Sept. 18, 2018) (aiding and abetting clients’ attempts to manipulate USD ISDAFIX); *In re Citibank, N.A.*, CFTC No. 15-03 (Nov. 11, 2014) (aiding and abetting attempts by traders at other banks to manipulate foreign exchange benchmark rates); *In re ICAP Europe Ltd.*, CFTC No. 13-38 (Sept. 25, 2013) (aiding and abetting client’s attempts to manipulate Yen LIBOR).


21 Id. ¶ 1.
with the CFTC in the course of [its] investigation.” The complaint contains detailed and numerous allegations of specific instances in which Trader A used Thakkar’s Back-of-Book function to spoof E-mini S&P 500 futures near month contracts on CME. The complaint also alleges many instances of direct contact between Thakkar and Trader A, through a variety of methods and over a period of years. For example, according to the CFTC, “Thakkar and Trader A communicated by phone, emails, and web meetings to discuss Trader A’s specific requirements.” The complaint identifies specific examples of such communications, including discussions related to further development and troubleshooting of the Back-of-Book function after Thakkar released the product to Trader A. The CFTC spared no effort in making clear in its allegations that Thakkar knew precisely what sort of conduct he was assisting, alleging that “Thakkar understood that Trader A intended to use the Back-of-Book function to place Spoof Orders,” that Thakkar was knowledgeable about spoofing, and that Thakkar participated in web meetings with Trader A in which he could observe Trader A’s trading activity and hear Trader A explain what he wanted Thakkar’s software to do.

At a high level, Thakkar contains some superficial similarities to a hypothetical aiding and abetting case against a smart contract code developer who codes a smart contract to allow users to execute unlawful trades. But the Thakkar complaint alleges facts that may well prove extremely difficult to establish in the type of case Commissioner Quintenz contemplated in his October remarks. Thakkar involved an identifiable primary violator, trading on an exchange, who cooperated with the CFTC, rather than anonymous smart contract users trading on the blockchain. Thakkar was allegedly sophisticated and well-versed in the intricacies of the markets in which Trader A operated. Not all smart contract code developers will necessarily fit the same profile or be able to foresee all of the functions their code may achieve. Moreover, the CFTC alleged a years-long relationship between Thakkar and Trader A that left a trail strewn with correspondence showing Trader A’s intentions, as well as Thakkar’s knowledge of those intentions and his willingness to help Trader A achieve them. Even assuming the CFTC could ultimately identify the individuals who used a smart contract to conduct activity that violates the CEA or CFTC rules, the Commission may be hard pressed to develop an evidentiary record reflecting a smart contract code developer’s knowledge and intent sufficient to prevail in litigation. Indeed, given the decentralized nature of the blockchain, the developer may not have any preexisting relationship with the primary violator who chose to utilize the smart contract.

---


23 See, e.g., Thakkar Compl. ¶¶ 36-39.

24 See id. ¶ 17.

25 See, e.g., id. ¶¶ 17-27, 29-32, 40-44.

26 Id. ¶ 27.

27 Id. ¶ 33.

28 Id. ¶ 25.
Additionally, aiding and abetting cases against smart contract code developers may implicate temporal issues that do not arise in typical aiding and abetting cases. In many aiding and abetting cases, the aider and abettor’s conduct occurs contemporaneously with the primary violator’s conduct. In the Thakkar complaint, the CFTC emphasized that Thakkar’s relationship with Trader A continued as Trader A engaged in spoofing. Smart contract code developers may create code and make it available for use by others, without necessarily knowing who is using the smart contract or why they are using it. Smart contract code developers’ substantive involvement with a smart contract may conclude long before others begin trading on their protocol. Smart contract code developers may anticipate that activity, and may profit from it, but may not be “aware” of the activity in the traditional sense. At a minimum, it will not be easy for the CFTC to build its case, and the Commission may need to rely on an expansive concept of knowledge to prevail.

Nonetheless, in light of Commissioner Quintenz’s remarks and the availability of aiding and abetting liability under the CEA, smart contract code developers need to be comfortable that the code they are building will not likely facilitate activity that violates the CEA, such as the trading of off-exchange swaps between retail customers. Given that these are unchartered waters, it also could be prudent for smart contract code developers to reach out to the CFTC’s LabCFTC, a group that Chairman J. Christopher Giancarlo established to promote dialogue between the agency and the fintech community for their mutual benefit, before rolling out their product. Quintenz encouraged precisely such engagement, observing that he “would much rather pursue engagement than enforcement—but in the absence of engagement, enforcement is our only option.” Given the CFTC’s support for innovation, Quintenz noted that such engagement could spur “the Commission to rethink its existing regulations or provide regulatory relief—both courses of action that I think would be appropriate depending upon the technology in question.”

Commissioner Quintenz’s speech highlighted the challenge of adapting a preexisting regulatory scheme to new technologies—in this case, a technology whose decentralized structure is fundamentally different from the structure of intermediation on which the CEA is based. To date, the CFTC has mainly exercised its enforcement authority in the blockchain and cryptocurrency space by policing fraud in the sale of cryptocurrency to retail purchasers and ensuring that leveraged spot transactions with retail investors are not unlawful futures.

---

29 See, e.g., id. ¶ 40-44.

30 See CEA Section 2(e).

31 Quintenz Remarks, supra note 2.

32 Id.

contracts. However, as blockchain innovators develop applications that facilitate the execution of contracts falling under CFTC jurisdiction or create platforms on which CEA-covered products will be traded, both the developers and the CFTC will need to consider whether and to what extent CEA provisions and CFTC rules apply.

Blockchain and Cryptocurrencies: A Cross-Border Conundrum

By Michael L. Spafford, Daren F. Stanaway, and Sabin Chung

Michael L. Spafford is a partner in the White Collar Defense and Investigations practice of Paul Hastings LLP. Mr. Spafford represents companies, committees of the board of directors, officers and directors, and other individuals in connection with government investigations, enforcement proceedings brought by the Department of Justice, the Securities and Exchange Commission, the Commodity Futures Trading Commission, the Federal Energy Regulatory Commission, and other federal, state, and local government enforcement entities, and related parallel litigation. Mr. Spafford currently represents clients involved in multiple government investigations of alleged manipulation of Libor, FX, ISDA Fix, and other benchmarks referenced in connection with the trading of various derivatives. Mr. Spafford has been featured in Chambers USA, White Collar Crime & Government Investigations (District of Columbia), The Best Lawyers in America®, Derivatives and Futures, and Super Lawyers, Washington, D.C., Criminal Defense.

Daren F. Stanaway is a senior associate in the White Collar Defense and Investigations practice of Paul Hastings LLP. Her practice focuses on white collar litigation and defense and government investigations and enforcement initiatives. Ms. Stanaway represents prominent individuals, corporations, and financial institutions in federal and state court litigation and administrative actions, and in connection with investigations by the Department of Justice, the Securities and Exchange Commission, the Federal Energy Regulatory Commission, the Commodity Futures Trading Commission, and congressional committees. Ms. Stanaway earned her J.D. from Harvard Law School, where she received the Dean’s Scholar Prize. She graduated with a B.A., magna cum laude, Phi Beta Kappa, from Harvard College.

Sabin Chung is an associate in the Litigation practice and is based in the Washington, D.C. office of Paul Hastings LLP. Her practice focuses on antitrust, competition law, and investigations. Ms. Chung represents clients in antitrust and competition-related matters including merger and acquisition approval under the Hart-Scott-Rodino Act, as well as state and federal antitrust litigation matters. She has handled multi-jurisdictional merger control filings and international investigations into anticompetitive practices, and also has experience with white-collar criminal defense and enforcement matters.

I. INTRODUCTION.

In an October 17, 2018 speech, Commodity Futures Trading Commission (“CFTC”) Chairman J. Christopher Giancarlo suggested that the CFTC transform its current “ad-hoc cross-border regime” of swaps regulation into a “holistic risk-based framework that furthers the cause of swaps market reform.” This would require the CFTC to exercise “regulatory deference” to foreign regulators, and Chairman Giancarlo thus committed to “establishing a CFTC cross-border framework that is risk-based and offers deference to comparable non-U.S. regulations.”

---

1 With special thanks to Paul Hastings Foreign Exchange Professional Lara Kaplan for her assistance.
3 Id.
Like swaps, cryptocurrencies and blockchain technologies are inherently global in nature and subject to potentially divergent regulation by authorities in multiple jurisdictions. These innovations traverse a number of different sectors—from consumer protection and cybersecurity to financial services, investment services, and insurance—thereby further complicating efforts to maintain consistent, coordinated cross-border policies. Notwithstanding the new frontiers and opportunities that these technologies afford, they also bring a host of new challenges for government regulators, including in the anti-money laundering ("AML"), anti-terrorism financing, payment systems, and cross-border verification spaces. Chairman Giancarlo’s call to dramatically overhaul the CFTC’s approach to cross-border swaps regulation and exercise cooperation with, and deference to, foreign regulators (at least insofar as they have enacted comparable regulatory regimes) thus resonates with respect to cryptocurrencies and blockchain as well. The CFTC may wish to exercise deference to and cooperate with foreign counterparts who have enacted regimes to govern these new technologies, thereby avoiding overlapping and potentially conflicting regulation while fostering an innovative growth environment for emerging technologies.

A. Chairman Giancarlo’s White Paper.

Chairman Giancarlo’s October 2018 speech followed his recently published White Paper on cross-border swaps regulation, which acknowledged the CFTC’s previously over-expansive assertion of jurisdiction in applying Title VII of the Dodd-Frank Act outside the United States. As the White Paper concedes, the Commodity Exchange Act (“CEA”) provides that the CFTC’s swap authority “shall not apply” to activities outside the United States unless those activities “have a direct and significant connection with activities in, or effect on, commerce of the United States.” In light of that restriction, the White Paper advocates rolling back overreaching CFTC enforcement efforts and circumscribing the CFTC’s attempts to pursue extraterritorial conduct that lacks a “direct and significant” impact on the United States—particularly given that many jurisdictions now have robust swaps regulations in place. In 2013, the CFTC promulgated Cross-Border Guidance, which Chairman Giancarlo now deems “out of step with the world’s major swaps trading regimes,” given its assumption that virtually every swap entered by a U.S. person, regardless of location or manner of transaction, has the requisite direct and significant connection with U.S. activities and thus remains subject to CFTC rules. Chairman Giancarlo suggests that the CFTC “should operate on the basis of comity, not uniformity, with non-U.S. regulators that oversee comparable regulatory regimes,” to avoid a “completely untenable state of overlapping and conflicting rules.” His White Paper advocates a new alternative cross-border framework premised upon the following principles:

- The CFTC should distinguish between swaps reforms intended to mitigate systemic risks and reforms intended to address market integrity, such as specific trading practices, and

---

6 7 U.S.C. § 1, et seq.
7 White Paper at 20 (quoting 7 U.S.C. § 2(i)).
8 Id. at 82.
9 Id. at 24.
limit its cross-border oversight of the latter, because those requirements may be adapted to local market conditions.

- The CFTC should pursue multilateralism, as opposed to unilateralism, for swaps reforms designed to mitigate systemic risks.
- The CFTC should not divide the global swaps markets into separate U.S. person and non-U.S. person marketplaces. Markets in regulatory jurisdictions that have adopted comparable G20 swaps reforms each should function as a unified marketplace, under one set of comparable trading rules and a single regulator.
- The CFTC must be a “rule maker,” not a “rule taker,” in overseeing U.S. markets.
- The CFTC should defer to non-U.S. regulators in jurisdictions that have adopted comparable G20 swaps reforms and seek stricter comparability for requirements intended to address systemic risk and more flexible comparability for requirements intended to address market and trading practices.
- The CFTC should encourage adoption of similar swaps reforms in other markets that have not yet adopted the G20 reforms.

In short, Chairman Giancarlo’s White Paper recommends changes to a range of cross-border issues in swaps regulation, including those related to non-U.S. swaps central counterparties (“CCPs”), non-U.S. trading venues, and non-U.S. swap dealers, advocating CFTC deference to its foreign counterparts that have adopted robust swaps regulations—a “sea-change in approach,” with “deference to overseas regulation” at its core.

**B. Blockchain Technology and Cryptocurrencies.**

Chairman Giancarlo’s White Paper focuses primarily upon cross-border issues related to swaps, but the underlying considerations, concerns, and principles set forth therein may apply with equal force in another emerging market area: cryptocurrencies and blockchain technologies. Blockchain is a type of distributed ledger technology; it is a shared, immutable chronological record of transactions, often referenced as a digital ledger. Blockchain technology utilizes a decentralized digital ledger to eliminate the need for a trusted third-party intermediary or central authority, such as a bank or government, to verify the transaction. Cryptocurrencies are a species of blockchain technology, and cryptocurrency markets have grown exponentially in recent years. Although the mechanics and applications of different blockchain technologies and cryptocurrencies vary, cryptocurrencies like Bitcoin may be purchased on exchanges or directly from other market participants using fiat currency (cash, credit or debit cards, or wire transfers)

---

10 The G20 swaps reforms stem from commitments made by G20 leaders in 2009. Id. at i.
11 Id. at ii–iii.
or other cryptocurrencies. Today, hundreds of cryptocurrency exchanges are in operation and purchase and sell cryptocurrency on behalf of users (with varying degrees of liquidity and security). Cryptocurrencies also may be transacted off-exchange. As of December 2018, the global cryptocurrency market had formed a nearly $130 billion digital payment ecosystem, and nearly $15 billion in cryptocurrency transactions are executed daily around the world, with the number increasing each day. Initial coin offerings (“ICOs”), which raise funds by promoting sales of cryptocurrency to investors, have contributed significantly to the explosion of the cryptocurrency market as well.

Given their virtual nature, cryptocurrencies are widely transacted and cross borders easily. ICOs often are global in nature as well; they frequently involve non-domestic issuers and domestic investors or vice versa. The global nature of blockchain technologies and cryptocurrencies presents unique international regulatory challenges, including how to and who should regulate them. For this reason, a number of international bodies like the European Securities Markets Authority (“ESMA”) and the International Organization of Securities Commissions (“IOSCO”) have endeavored to issue guidance in these areas. Individual countries also have begun to formulate their own rules and regulations, which often take into account local considerations and market conditions and thus vary by country. That said, many countries look to guidance from larger international organizations (and from one another) and engage in collaborative discussions, thereby leading to a more cooperative, unified approach to this area—particularly among G20 members. Although regulation of these areas remains in its infancy—and much uncertainty remains—in many jurisdictions, cryptocurrencies and blockchain technologies present challenging cross-border issues analogous to those present in swaps markets, and it would behoove the CFTC to adopt the principles set forth in Chairman Giancarlo’s White Paper in its approach to cryptocurrency and blockchain regulation as well.

15 Id.
17 Id.
II. THE PRINCIPLES SET FORTH IN CHAIRMAN GIANCARLO’S WHITE PAPER APPLY EQUALLY TO BLOCKCHAIN TECHNOLOGIES AND CRYPTOCURRENCIES, AND THE CFTC GENERALLY SHOULD REFRAIN FROM EXTRATERRITORIAL REGULATION IN THOSE AREAS.

Regulators in the United States and abroad have amplified their efforts to regulate cryptocurrencies in recent months. In January 2018, for example, the chairmen of the U.S. Securities and Exchange Commission (“SEC”) and the CFTC published a joint article warning that regulators planned to take enforcement action against misconduct in the cryptocurrency space. The SEC subsequently issued multiple subpoenas and information requests to companies and advisers involved in ICOs and launched an investigation into cryptocurrency-focused hedge funds, and in May 2018 obtained a court order halting an alleged ongoing ICO fraud that raised as much as $21 million from investors. The CFTC, too, pursued several cases in 2018 relating to fraud and manipulation involving cryptocurrencies.

Given the inherent cross-border nature of cryptocurrencies and the heightened regulatory focus on them, the principles and concerns set forth in Chairman Giancarlo’s White Paper—though tailored to swaps regulation—apply in the cryptocurrency context and militate against extraterritorial regulation in that area as well. First, in light of the cross-border nature of cryptocurrencies and blockchain technologies, the CFTC (or another U.S. regulator) could find itself in perpetual conflict (or in an ongoing jurisdictional fight) with foreign regulators, with multiple regulators endeavoring to exercise jurisdiction over the same conduct. Second, over-expansive extraterritorial regulation could be operationally impractical, increase transaction costs, and reduce economic growth and opportunity. Third, market fragmentation would be detrimental to cooperation among regulators and diminish market resilience in the event of global market shocks. Fourth, the CFTC may wish to afford more deference to foreign regulators that have adopted appropriate rules and regulations concerning blockchain and cryptocurrencies in light of international comity. Finally, individual and corporate actors may not reasonably expect to be hauled into U.S. court for their foreign activities, which further weighs against extraterritorial regulation in these areas.

A. Extraterritorial Regulation May Lead to Conflicts with Other Foreign Regulators.

Blockchain and cryptocurrency platforms operate without borders, and the intangible

26 See generally White Paper, §§ III, V.
nature of cryptocurrencies permits them to exist in and move fluidly between countries. Regulators in multiple jurisdictions therefore may find themselves simultaneously seeking to assert jurisdiction over the same conduct or alleged misconduct. Absent deference, U.S. regulations potentially could clash with different but effective non-U.S. regulatory frameworks, resulting in an untenable state of overlapping and conflicting rules. This, in turn, could create adverse consequences, including (i) unpredictability to investors and other market participants regarding which rules and guidance apply; (ii) potentially duplicative sanctions in multiple jurisdictions for the same conduct; (iii) fragmentation of the global cryptocurrency marketplace; (iv) protectionism; and (v) regulatory arbitrage. For these reasons, the very real potential of conflicting regulations weighs against extraterritorial application of U.S. regulations to cryptocurrencies and other blockchain technologies.

B. Cross-border Regulation Is Impractical and May Lead to Increased Transaction Costs and Reduced Economic Growth and Opportunity.

As Chairman Giancarlo’s White Paper highlights, the CFTC’s over-expansive cross-border approach to swaps regulation has driven market participants away from transacting with entities subject to the CFTC’s regulations and fragmented global markets. In the swaps context, an approach to jurisdiction that focuses only upon whether a transaction involves a U.S. person, without taking into account where and how the transaction is entered, effectively disregards whether the transaction has a direct and significant connection with activities in, or effect on, U.S. commerce—the only circumstance under which the CEA’s swaps provisions may apply to activities outside the United States. By analogy, the CFTC should have little interest in pursuing cryptocurrency-related conduct that has little or no connection to the United States and should instead leave such conduct to its foreign counterparts to pursue, lest the CFTC risk driving away foreign market participants, fragmenting cryptocurrency markets, and denying domestic businesses and commercial enterprises opportunities to raise funds, hedge risks, and engage in technological innovation that could lead to business expansion, job creation, and economic development.

C. Market Fragmentation May Lead to Diminished Resilience to Global Cryptocurrency Market Shocks.

Over-expansive cross-border regulation may lead to market fragmentation, which in turn may not only reduce economic growth and opportunity for domestic enterprises, but also impede resilience following sudden market tumult, resulting in greater price and transaction volatility. Given their nascent, unpredictable, uncertain nature, cryptocurrency markets are especially vulnerable to market shocks and price swings. Bitcoin, for example, has experienced wild volatility and repeated crashes over the last few years, including a 71% overnight price drop in

---

27 See id. at 24.
28 Id. at ii.
29 7 U.S.C. § 2(i).
30 Moreover, as discussed infra, the CEA does not authorize the CFTC to act extraterritorially (other than pursuant to the exception applicable to swaps and certain other narrow exceptions), so deference to foreign regulators may be advisable not only from a policy standpoint, but also a practical necessity, given that the CFTC may lack jurisdiction to pursue most extraterritorial conduct tied to cryptocurrencies or other blockchain technologies.
31 See White Paper at 27.
32 Id.
2013. More recently, in October 2018, the International Monetary Fund (“IMF”) warned that the Bitcoin and blockchain boom facilitating the rapid growth of cryptocurrency assets could create “new vulnerabilities in the international financial system.” Shortly after the IMF’s warning, the values of Bitcoin and other leading cryptocurrencies, including Ripple and Ethereum, plunged, wiping out billions of dollars within minutes. Such unpredictability and vulnerability associated with cryptocurrencies weigh in favor of regulatory cooperation and against market fragmentation.

D. International Comity Warrants Deference to Foreign Regulators.

In cases involving cross-border conduct, international comity and increased deference to foreign regulators may achieve more harmonious and cooperative operation of unified cryptocurrency markets. As discussed above, international organizations and G20 countries have begun to adopt rules and regulations concerning blockchain and cryptocurrencies to achieve compatible and comparable regulatory outcomes and minimize the need for individual regulators to expand or transgress their jurisdictional limits.

At a March 2018 summit, for example, G20 members committed to apply Financial Action Task Force (“FATF”) standards to crypto-assets and called on international bodies, including the Financial Stability Board (“FSB”), the Committee on Payments and Market Infrastructures (“CPMI”), the FATF, and IOSCO to report back to the G20 in July 2018, continue monitoring cryptocurrencies and associated risks, and assess multilateral responses. IOSCO subsequently reported at the July 2018 summit and emphasized the importance of coordination among financial regulators in different jurisdictions in the cryptocurrency space. In October 2018, the FSB published an additional report for G20 highlighting potential risks associated with cryptocurrencies, including fragmented markets, insignificant liquidity,

---

37 The FATF is an inter-governmental body established to set standards and “promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system.” Who We Are, FATF, http://www.fatf-gafi.org/about/.
38 The FSB is an “international body that monitors and makes recommendations about the global financial system” to “promote[] financial stability” by “coordinating national financial authorities and international standard-setting bodies as they work toward developing strong regulatory, supervisory and other financial sector policies.” About the FSB, FSB, http://www.fsb.org/about/.
39 CPMI, a committee of the Bank for International Settlements (“BIS”), “promotes the safety and efficiency of payment, clearing, settlement and related arrangements,” “monitors and analyses developments in these arrangements, both within and across jurisdictions,” and “serves as a forum for central bank cooperation in related oversight, policy and operational matters.” Committee on Payments and Market Infrastructures (CPMI) – overview BIS, (last updated May 13, 2015), https://www.bis.org/cpmi/.
40 Communiqué and Communiqué Annex, supra note 21.
41 See CRYPTO-ASSETS: REPORT TO THE G20 ON WORK BY THE FSB AND STANDARD-SETTING BODIES, supra note 21, at 6.
volatility, leverage, technology risks related to mining-based systems, and institutionalization, which necessitate “vigilant monitoring” in light of the “speed of market developments.” Such vigilance may be best achieved via cooperation and collaboration among regulators, including via exercising deference to one another with respect to conduct occurring within each of their respective jurisdictions.

Notably, a number of foreign authorities already have begun to implement regulations and guidance in the blockchain and cryptocurrency space. The United Kingdom’s Financial Conduct Authority (“FCA”), for example, has determined that firms conducting business in cryptocurrency derivatives in the UK must comply with both applicable FCA rules and relevant provisions in European Union (“EU”) regulations and directives. The FCA also has deemed it likely that “dealing in, arranging transactions in, advising on or providing other services that amount to regulated activities in relation to derivatives that reference either cryptocurrencies or tokens issued through an initial coin offering (ICO),” such as cryptocurrency futures, cryptocurrency contracts for differences (“CFDs”), and cryptocurrency options, “will require authorisation by the FCA.” Violating these authorization requirements constitutes a criminal offense in the UK and may subject a violating firm to enforcement action.

In addition to these UK-specific mandates, other EU requirements also may apply, both in the UK and throughout the EU more broadly. The Markets in Financial Instruments Directive (“MiFID”) II, for example, is a European Directive governing firms that provide investment services in relation to “financial instruments,” defined in MiFID II as transferable securities, money-market instruments, units in collective investment undertakings, and certain options, futures, forward rate agreements, and swaps, among other items. Whether a coin or token involved in an ICO qualifies as a financial instrument depends on its characteristics and nature, but firms providing services in the EU in relation to ICOs or other activities involving a coin or token that so qualifies may be subject to MiFID II requirements, and several other EU Directives also may apply. The UK’s apparent continuing focus on and interest in monitoring and regulating cryptocurrencies (and the focus of the EU more broadly in this regard) suggests that U.S. regulators may wish to cooperate with and defer to UK and other EU member state authorities in this space, to avoid overlapping and potentially conflicting regulation.

E. Unfairness and Unpredictability Concerns Weigh Against Extraterritorial Application of U.S. Regulatory Regimes.

Extraterritorial application of U.S. regulations to cryptocurrencies and blockchain
technologies could render non-U.S. actors subject to charges in the United States and prompt questions of fairness and unpredictability (as occurs in other circumstances). Absent a mutual commitment to cross-border regulatory deference, actors in cryptocurrency markets would have little visibility regarding which sets of rules and regulations apply to their activities and in some instances may have to confront and determine how best to comply with conflicting or contradictory mandates.50

III. THE CFTC HAS LIMITED AUTHORITY TO REGULATE BLOCKCHAIN TECHNOLOGIES AND CRYPTOCURRENCIES EXTRATERRITORIALLY.

Under the Supreme Court’s holding in Morrison v. National Australia Bank Ltd., an “affirmative indication . . . that a statute applies extraterritorially” is required as “clear evidence of congressional intent” to overcome the presumption against extraterritoriality.51 The CEA is largely silent as to its extraterritorial reach; its provisions related to the purchase or sale of any commodity for future delivery, for example, “contain [] nothing on [their] face that suggests extraterritorial application.”52 Given the general absence of an explicit grant of extraterritorial application in the CEA (subject to a few narrow exceptions), Morrison’s presumption against extraterritoriality applies, and courts thus must determine what conduct is—and is not—“domestic,” and therefore subject to the CEA’s prohibitions. Stated simply, “a claim is within the CEA’s domestic application if it involves (1) commodities in interstate commerce or (2) futures contracts traded on domestic exchanges.”53

The CEA does carve out a few exceptions to the presumption against extraterritoriality, however—most notably, the provisions governing swaps. Indeed, Dodd-Frank granted the CFTC the authority to regulate swap-related activities outside the United States that (1) “have a direct and significant connection with activities in, or effect on, commerce of the United States;” or (2) contravene certain CFTC rules or regulations.54 Accordingly, whether the CFTC has jurisdiction to regulate a particular cryptocurrency or cryptocurrency exchange may well turn upon the specific nature of the cryptocurrency in question (such as whether it involves a U.S. or foreign swap, or a futures contract traded on a domestic exchange) and, in instances involving exchanges, whether the exchange is foreign or domestic.55 For cryptocurrencies that have

50 See White Paper at 31.
54 7 U.S.C. §§ 2(i)(1)-(2).
55 Several courts have acknowledged that the CFTC has authority to regulate virtual currencies as commodities, however. For example, the CFTC recently pursued an antifraud enforcement action relating to alleged fraud and misappropriation involving Bitcoin and Litecoin. See Press Release, CFTC, Federal Court in New York Enters Preliminary Injunction Order against Patrick K. McDonnell and His Company CabbageTech, Corp. d/b/a Coin Drop Markets in Connection with Fraudulent Virtual Currency Scheme (Mar. 6, 2018), https://www.cftc.gov/PressRoom/PressReleases/pr7702-18. The defendants contended that the CFTC lacked authority to regulate virtual currencies in the first place, but the federal district court disagreed, holding that “[v]irtual currencies can be regulated by [the] CFTC as a commodity,” and that the CFTC’s authority covers fraud and manipulation in virtual currency spot markets. CFTC v. McDonnell, 287 F. Supp. 3d 213, 228 (E.D.N.Y. 2018); see also Press Release, CFTC, Court Denies Defendants’ Motion to Dismiss in Commodity Fraud Case Involving
minimal, if any, U.S. ties, however—such as those premised upon exchanges located abroad—the CFTC (and perhaps other U.S. regulators) may need to enlist the assistance of foreign regulators (and defer to foreign regulatory regimes) out of necessity, because its jurisdictional reach simply does not extend that far.

IV. CONCLUSION

Notwithstanding the uncertainties and vulnerabilities of the cryptocurrency markets and blockchain applications, the principles articulated in Chairman Giancarlo’s White Paper provide valuable guidance regarding how best to structure future cross-border regulation of these new technologies. The CFTC already has taken positive steps in this direction. In October 2018, for example, the CFTC and the Australian Securities and Investments Commission (“ASIC”) signed an agreement to cooperate and support innovation in the financial technology (“FinTech”) space, and other domestic and foreign regulators have taken parallel approaches. In this way, the CFTC can work more cooperatively with its foreign counterparts to ensure consistency, predictability, and a unified global market approach.

---

the Virtual Currency My Big Coin (Oct. 3, 2018), https://www.cftc.gov/PressRoom/PressReleases/7820-18 (acknowledging court holding that the virtual currency at issue was a commodity under the CEA).

The Commodity Exchange Act (CEA) and the federal securities laws establish a jigsaw puzzle of exclusive and overlapping jurisdictions between the Commodity Futures Trading Commission (CFTC) and Securities and Exchange Commission (SEC).\(^1\) Clear guidance of how this jurisdictional scheme applies to cryptocurrency and other digital asset transactions is a work in progress. Over the past eighteen months, each agency has gradually announced through formal reports, informal agency staff guidance, and selective enforcement actions how their statutes apply to those transactions. Some of the foundational issues are whether a digital asset transaction involves a security, a commodity or both, and whether entities that operate online platforms for transacting in digital assets or their derivatives must register in a statutory capacity under the CEA or the federal securities laws.

Although they only partially concern digital assets, the agencies’ parallel enforcement actions filed in September 2018 against an overseas online derivatives trading platform known as 1pool Ltd. (1pool) and its chief executive officer embrace these jurisdictional questions. Both actions seek permanent injunctions, disgorgement of ill-gotten gains, and financial penalties. \textit{SEC v. 1pool Ltd., et al., No. 1:18-cv-02244} (D.D.C., Sept. 27, 2018) (SEC Compl.), and \textit{CFTC v. 1pool Ltd., et al., No. 1:18-cv-02243} (D.D.C., Sept. 27, 2018) (CFTC Compl.).

\section*{A. The Factual Allegations}

The complaints alleged that 1pool is registered as a limited liability company in the Republic of the Marshall Islands and its CEO is a resident of Austria, but 1pool is not registered with the SEC or CFTC in any capacity. The complaints alleged that 1pool provided an electronic platform by which persons around the world could enter into leveraged or margined transactions in “contracts for differences” (CFDs) with 1pool as their counterparty. Both complaints alleged that 1pool accepted transactions with retail persons, i.e., persons who did not qualify as “eligible contract participants” (ECPs) as defined in CEA Section 1a(18).

The CFDs were a financial vehicle for accountholders to speculate, going either long or short, on the price changes of “Indices, Stocks, Commodities, Forex, and Crypto.” SEC Compl. ¶15. As the SEC explained, the CFDs allowed 1pool’s accountholders to “participate in the price movements of securities and other assets without

\footnote{This paper does not contain legal advice; should not be relied upon as legal advice; and does not create an attorney-client relationship. Readers desiring legal advice should consult with legal counsel with respect to their particular circumstances.}
actually owning the underlying assets.” *Id.* at ¶2. Accordingly, as the CFTC alleged, “[t]here is no actual delivery of the underlying asset or commodity,” and “customers close out their trading position by placing an equal and opposite order.” CFTC Compl. ¶31. The CFTC alleged that 1pool accepted bitcoin “to margin, guarantee, or secure” the trades, *id.* at ¶3, and transactions could be settled only in bitcoin.

**B. The SEC’s Charges**

The SEC alleged that each CFD based on a single security was within the definition of security-based swap as an “agreement, contract, or transaction that is based on a single security or the occurrence, non-occurrence, or extent of an occurrence of an event relating to a single issuer of a security, provided that such event directly affects the financial statements, financial condition, or financial obligations of the issuer.” SEC Compl. ¶18. It charged that, because security-based swaps are within the definition of “security” in the Securities Act and the Securities Exchange Act (SEA) and the CFDs were not registered with the SEC, 1pool violated both Securities Act Section 5(e) and SEA Section 6(l) by selling unregistered security-based swaps to non-ECPs. The SEC asserted that only registered security-based swaps may be offered and sold to non-ECPs and that those sales must be executed only through a national securities exchange, which 1pool is not. The SEC also charged violation of Exchange Act Section 15(a)(1) because 1pool was required to be registered as a dealer to effectuate the sales of securities and it was not so registered.

The SEC claimed jurisdiction because the CFDs were offered and accepted from US investors. The SEC alleged that an undercover Special Agent of the Federal Bureau of Investigation (FBI) accessed 1pool’s website and opened an account while physically located in Houston, Texas, and later, while in Washington, DC, logged onto 1pool’s website and bought and sold CFDs that track the price of the common stock of Ford Motor Company.

**C. The CFTC’s Charges**

In contrast to the SEC’s charges, the CFTC did not allege that the CFDs on commodities were swaps. Rather, it alleged that 1pool illegally offered and entered into off-exchange margined or leveraged “retail commodity transactions” within the meaning of CEA Section 2(c)(2)(D) to non-ECPs located in the United States and in the District of Columbia specifically. Unlike the SEC’s complaint, the CFTC did not allege any specific transactions by an FBI Special Agent or otherwise.

CEA Section 2(c)(2)(D) prohibits the solicitation and acceptance of orders from non-ECPs of leveraged or margined retail commodity transactions unless either (i) “actual delivery” occurs within 28 days of the sale or (ii) the seller complies with the terms of CEA Section 4(a) “as if” the transactions were futures transactions. The CFTC alleged that 1pool did not satisfy the “actual delivery” exclusion from regulation because “there is no actual delivery of the underlying asset or commodity and customers closed their trading position by placing an equal and opposite order.” CFTC Compl. ¶31. The CFTC thus charged 1pool with unlawfully operating as an unregistered futures commission merchant (FCM).

Additional claims included alleged liability for 1pool’s failure to implement an adequate supervisory system required of FCMs under CFTC Rule 166.3 that included “know-your-customer” and “customer identification program” procedures. The CFTC charged 1pool’s CEO with personal liability for 1pool’s violations pursuant to the provision for “control person” liability in CEA Section 13(b).
D. Transaction-Centric Jurisdictional Lines and Asymmetrical Statutory Treatment

A separate enforcement action by each agency was necessary to address all of the CFDs on the 1pool platform because neither agency had authority to regulate or prohibit all of 1pool's CFD transactions. The SEC asserted claims only with respect to the CFDs on single securities because CFDs on commodities other than single stock securities and narrow-based securities indices are not within the statutory definitions of security-based swap or security. The CFTC could not assert claims with respect to the CFDs on single securities because CEA Section 2(c)(2)(D)(ii)(II) expressly excludes retail transactions in securities from the retail commodity transactions restrictions of the CEA.

The asymmetrical statutory treatment between the federal securities laws and the CEA of the same types of transactions is noteworthy. The SEC's complaint asserts a clear and absolute standard: (1) A CFD on a single security is within the definition of security-based swap as a “agreement, contract, or transaction that is based on a single security;” (2) security-based swaps may not be sold to a non-ECP unless the CFD is registered with the SEC; and (3) the sale of a registered security-based swap must occur on a national securities exchange. The CFTC's complaint, in contrast, implies that the CEA permits the off-exchange sale of a CFD to a non-ECP if “actual delivery” is effected or if the seller is a registered FCM. The CEA's requirements have proven to be potentially more problematic in application because the agency has not had an easy time developing a commonly accepted and consistent meaning of what constitutes “actual delivery” across the many different types of commodities and transactions that involve retail transactions. See, e.g., CFTC v. Monex Credit Co., 2018 WL 2306863 (C.D. Cal. 2018).

1pool's CFDs implicate the “actual delivery” issue. To determine whether the statutory exclusion is met for a retail commodity transaction that results in “actual delivery” requires first determining the commodity that is the subject of the transaction. The CFTC complaint posits that the actual delivery exclusion is not met for 1pool's CFDs because the underlying referenced commodity is not delivered. The SEC and CFTC complaints, however, are clear that the CFDs do not involve actually owning the underlying asset – the customer is not trying to purchase, sell or receive title to the underlying asset. This calls into question whether the underlying asset is the correct commodity to consider in assessing actual delivery.

The CEA's definitions of “commodity” in Section 1a(9) and “excluded commodity” in Section 1a(19) are broad and their precise scope can be debated. But together they specifically denominate a “commodity” to include, for example, an “article,” “good,” “interest,” “rate,” “differential,” “index” and “measure of economic . . . value.” Since, as described in the complaints, a 1pool CFD is just a speculation on a commodity price differential over time, the commodity that is the subject of a 1pool CFD potentially might be more properly analyzed to be either the commodity price index on which the CFD is priced or the differential between the index's opening and closing values. If this is accepted, it could be argued that “actual delivery” occurs upon settlement of the CFD and might operate to exclude CFDs settled within 28 days of the initiating transaction from the scope of the CEA.

E. Jurisdiction to Charge Non-US Actors

The CFTC and SEC complaints reflect their positions that each agency has regulatory jurisdiction over transactions offered to or executed by persons located in the United States on an online platform operated outside the United States. Their position is clear – offering to or doing business with persons located in the United States triggers the application of their statutes to that activity regardless of where the transaction is
consummated. However, court decisions on the extraterritorial application of the SEA and the CEA to offshore transactions warrant consideration.

The Supreme Court’s decision in *Morrison v. National Australia Bank Ltd.*, 561 US 247 (2010), held that there is a presumption against the extraterritorial application of US law and that the “location of the transaction” (i.e., whether it is in the United States or not) controls whether the SEA applies. *Id.* at 268. *Morrison* announced that SEA Section 10(b) “applies only to transactions and securities listed on domestic exchanges and domestic transactions in other securities.” The Court therefore held that Section 10(b) claims of Australian purchasers relating to securities in a US company that were traded on an Australian securities exchange were outside the subject matter jurisdiction of US courts. The court opined that “nothing in [the SEA] suggests that [the] national public interest pertains to transactions conducted upon foreign exchanges and markets.” The Court also found that the reference in Section 30(b) of the SEA to the extraterritorial reach of the statute “to prevent . . . evasion” of it was “directed at actions abroad that might conceal a domestic violation, or might cause what would otherwise be a domestic violation to escape on a technicality.” *Id.* at 264.

*Morrison* did not consider the scenario in which direct access to and trading on foreign markets occurs from within the United States. The Second Circuit, however, has opined that a “domestic” securities transaction occurs, and therefore US law applies, when "the purchaser [has] incurred irrevocable liability within the United States to take and pay for a security, or ... the seller [has] incurred irrevocable liability within the United States to deliver a security." *Absolute Activist Value Master Fund Ltd. v. Ficeto*, 677 F.3d 60, 68 (2d Cir. 2012). Facts that demonstrate “irrevocable liability” include the “formation of the contracts, the placement of purchase orders, the passing of title, or the exchange of money” when someone is in the United States. *Absolute Activist*, 677 F.3d at 69, 70. More recently, in *Giunta v. Dingman*, 893 F.3d 73 (2d Cir. 2018), the court opined that the fact that a transaction in a non-US security might be subject to a condition subsequent, such as approval of the purchase by a foreign governmental authority, would not prevent finding irrevocable liability arising in the United States if, the US person had no right to revoke the purchase prior to the condition subsequent.

In *Loginovskaya v. Batrachenko*, 764 F.3d 266 (2d Cir. 2014), the Second Circuit declared that private claims under the CEA are subject to the same extraterritoriality analysis applied in *Morrison*. In *Myun-Uk Choi v. Tower Research Capital LLC*, 890 F.3d 60 (2d Cir. 2018), the Second Circuit held that an allegation that the plaintiffs’ futures orders on the Korean Exchange (KRX) were matched by the Chicago Mercantile Exchange’s matching engine in the United States during the hours when the KRX was closed sufficiently alleged a prima facie claim that “irrevocable liability” arose in the United States to survive a motion to dismiss on jurisdictional grounds. The restriction on extraterritorial application of the SEA has been held to apply to both governmental enforcement actions and private claims. *United States v. Vilar*, 729 F.3d 62 (2d Cir. 2013) (*Morrison* applied to criminal prosecution of SEA Section 10(b)).

The foregoing precedents suggest that the use of the instrumentalities of interstate commerce by itself may not be sufficient to confer jurisdiction over such transactions. Rather, they indicate that the application of the SEA and CEA to a transaction executed on a foreign trading platform by a person located in the United States will turn on whether “irrevocable liability” for the transaction arises in the United States.
F. Conclusion

The SEC and CFTC enforcement actions against 1pool show the limitations in each agency’s jurisdiction relating to over-the-counter derivatives transactions with retail persons but also demonstrate that the agencies will coordinate their enforcement efforts when needed to secure complete relief against a derivatives trading platform if neither agency by itself has jurisdiction to seek relief as to all transactions on the platform. They also demonstrate that each agency asserts jurisdiction with respect to transactions on non-United States trading platforms that are initiated by persons located in the United States. The precedents following *Morrison*, however, might provide a basis to block CFTC and SEC jurisdiction where “irrevocable liability” for a transaction does not arise within the United States.
Katherine Cooper is a shareholder at Murphy & McGonigle P.C. where she advises and represents clients in matters involving commodity derivatives and futures, securities and cryptocurrencies. She previously served as the Chief Regulatory Officer of NYSE Liffe US and as a Senior Trial Attorney at the Commodity Futures Trading Commission.
Jonathan Marcus is Of Counsel in the Derivatives Group in Skadden's Washington, D.C. office. Before joining Skadden last year, he spent six years at the Commodity Futures Trading Commission, where he served as General Counsel from 2013-2017 and as Deputy General Counsel for Litigation from 2011-2013. As General Counsel, Jonathan advised the Commission on rulemakings, interpretations and policy statements, with a focus on the Commission's implementation of the Dodd-Frank swaps market reforms and cross-border regulation. As Deputy General Counsel for Litigation, Jonathan led the CFTC's successful effort to defend the agency's Dodd-Frank rules against industry challenge. Jonathan also previously served at the U.S. Department of Justice as an Assistant to the Solicitor General, where he briefed and argued numerous cases for the United States in the Supreme Court.
Steve Mickelsen is the General Counsel and Corporate Secretary at 3Degrees Group, an environmental commodity trading and consulting firm. Steve advises management regarding governance, compliance and transaction issues. Steve is leading 3Degrees’ efforts exploring blockchain applications for renewable energy tracking and trading. Steve has extensive experience with futures and derivatives regulation having previously worked at the CFTC and in private practice.
Charles Mills is a partner with Steptoe & Johnson LLP in Washington DC. He represents clients in the financial services industry and the energy and commodities sectors in enforcement investigations and litigation and regulatory matters involving the Commodity Futures Trading Commission, the Federal Energy Regulatory Commission, the U.S. Securities and Exchange Commission, the Department of Justice, the regulated futures exchanges, and the derivatives and securities industry self-regulatory organizations. Charley’s compliance practice includes preparation of internal compliance procedures, compliance training, CFTC and SEC registration, preparation of risk disclosures, requests for no-action letters, and advocacy on proposed agency rules. Charley’s advice is informed by his prior work as a litigator and regulatory attorney at the CFTC.

Charley has been honored as Derivatives Lawyer of the Year for Washington, DC for 2019, 2017 and 2012 by The Best Lawyers in America; and he is rated in Legal 500, Super Lawyers (Administrative Law), The Best Lawyers in America (Derivatives & Futures and Securities and Capital Markets), and Martindale-Hubbell (AV Preeminent). He is the former Chair of the ABA’s Derivatives and Futures Law Committee and has co-authored Derivatives Regulation - 2019 Cumulative Supplement (Wolters Kluwer), Broker-Dealer Regulation (PLI, 2016), and The Securities Enforcement Manual (ABA, 2007). He taught derivatives and securities law courses as an adjunct professor at Georgetown University Law Center for many years. Education: J.D., Georgetown University Law Center, 1977 (Dean’s List); B.A., Occidental College, 1974 (cum laude). Email: cmills@steptoe.com. Phone: 202-429-6472.
The Legend of the “Secumodity”: Can the Same Coin be a Security or Commodity at Different Points in Its Evolution?
By Petal Walker

I. INTRODUCTION

Can a digital coin be a security one day under the oversight of the Securities and Exchange Commission (SEC), and a commodity the next under the oversight of the Commodity Futures Trading Commission (CFTC), or vice versa? And importantly, can a coin move from one jurisdiction to another without carrying forward lingering baggage from its previous jurisdiction? Though the line between the CFTC’s and the SEC’s jurisdictions over digital coins can be blurry, given the current state of CFTC and SEC oversight, it is possible for a digital coin to move between jurisdictions. In the following, I discuss: (1) the characteristics of digital coins that are defined as securities; (2) the characteristics of digital coins that are defined as commodities; and (3) how a digital coin could move from one definition, and therefore from one jurisdiction, to another.

II. COMMODITY VS. SECURITY

Blurry line between a virtual currency (commodity) and an investment (security)

In reviewing the CFTC’s and SEC’s cases and guidance, the main distinguishing factor between the digital coin that is an investment contract (security) and the digital coin that is a virtual currency (commodity), is its primary, though not necessarily sole, purpose. The primary purpose of the former is to make an investment — though another purpose may be to build a network — what gives life to the contract is the investment opportunity. The opposite is true of the latter — the primary purpose is to establish a unit of exchange to access goods and service — though another purpose may be to acquire a valuable asset — what gives life to the transaction is its utility on a network.¹

What makes a digital coin a virtual currency

Pursuant to its guidance and its enforcement actions, the CFTC has defined a digital coin that is a virtual currency as a commodity. The CFTC has identified a virtual currency as both a “digital representation of value that functions as a medium of exchange, a unit of account, and/or a store of value,”² and a “cryptographic protocol[] to secure transactions . . . recorded on publicly available decentralized ledgers.”³ The CFTC also noted the similarity of virtual currencies to

¹ Both Agencies have asserted that their jurisdictions do not overlap. The CFTC has noted that the SEC’s analysis that some digital coins are securities is not inconsistent with their finding that “virtual currencies are commodities and that virtual tokens may be commodities or derivatives contracts depending on the particular facts and circumstances.” CFTC, Primer on Virtual Currencies, at 14. LabCFTC, 2017; similarly, the SEC has indicated that their jurisdiction is not inconsistent with the CFTC’s noting that, “The CFTC has designated bitcoin as a commodity. Fraud and manipulation involving bitcoin traded in interstate commerce are appropriately within the purview of the CFTC, as is the regulation of commodity futures tied directly to bitcoin.” SEC, “Statement on Cryptocurrencies and Initial Coin Offerings,” note 2. Chairman Jay Clayton. Washington D.C., Dec. 11, 2017.
² CFTC, Primer on Virtual Currencies, at 4. LabCFTC, 2017.
gold, while indicating that they are distinct from “real” currencies since they are not considered legal tender.

Commodities are defined in the Commodity Exchange Act (CEA) as, inter alia, “all ... goods and articles ... and all services, rights, and interests ... in which contracts for future delivery are presently or in the future dealt in.” Consistent with that definition, a number of intangible interests such as currencies and fixed interest rate benchmarks are considered commodities. The CFTC maintained that virtual currencies can be regulated as commodities because they are “‘goods’ exchanged in a market for a uniform quality and value.”

As indicated by its enforcement actions, the CFTC interprets established digital coins on functioning networks such as Bitcoin and Litecoin as virtual currencies that are under its jurisdiction. This interpretation is evident in CabbageTech, where the Commission alleged that the defendants fraudulently misrepresented their trading in Bitcoin and Litecoin, and misappropriated customer funds. And, it is also evident in Gelfman Blueprint where the Commission alleged that the defendants fraudulently misstated their success in trading Bitcoin.

Interestingly, the CFTC has also interpreted un-established, and indeed what the CFTC portrays as fictitious, digital coins that purport to operate as virtual currencies as also being subject to their jurisdiction. A good example of that is My Big Coin Pay. In My Big Coin Pay, the CFTC brought charges against defendants for allegedly fraudulently claiming that My Big Coin (MBC) was a “fully-functioning virtual currency” that could be used to purchase goods and services, was traded on multiple exchanges, was part of a partnership with Mastercard and was backed by gold. The Commission maintained that all of these assertions were untrue and intentionally misleading. The Commission claimed that in reality, MBC was basically a Ponzi

---

4 Id.,
5 Id. at 6.
6 Title 7 U.S.C. § 1(a)(9)
7 See e.g., In re Barclays PLC, CFTC No. 15-25 (May 20, 2015).
8 See supra note 3 at 24. Importantly, digital coins could also be derivatives. If, for instance, what is called a digital coin is not a virtual currency, but actually a smart contract it may fall into the definition of a swap if, inter alia, it (i) is an “option of any kind that is for the purchase or sale, or based on the value, of 1 or more interest or other rates, currencies ... or other financial or economic interests or property of any kind”; or (ii) “provides for any purchase, sale, payment, or delivery ... that is dependent on the occurrence, nonoccurrence, or the extent of the occurrence of an event or contingency associated with a potential financial, economic, or commercial consequence.” 7 U.S. Code § 1a(47)(i)&(ii).

The CFTC has acknowledged this possibility, noting, for example, that “[d]epending on its structure, operation, and relevant facts and circumstances, a smart contract could be a ... futures contract, option on futures contract, [or] swap.” See e.g., CFTC, Primer on Smart Contracts, at 22. LabCFTC, 2018. Indeed, the CFTC’s own definition of a smart contract indicates its susceptibility to being defined as a swap; the CFTC states: a set of coded computer functions ... [which] may incorporate the elements of a binding contract (e.g., offer, acceptance, and consideration), or may simply execute certain terms of a contract ... [and] allows self-executing computer code to take actions at specified times and/or based on reference to the occurrence or non-occurrence of an action or event (e.g., delivery of an asset, weather conditions, or change in a reference rate) (emphasis added) See e.g., CFTC, Primer on Smart Contracts, at 4. LabCFTC, 2018. Though this has not gotten a lot of attention, it is an important aspect of CFTC regulation that could affect the legal standing of applicable digital coins.
9 See supra note 3 at 2.
scheme – that the promoters were falsifying trading results and providing the funds from one set of investors to another set of investors to mimic proceeds from trading, while misappropriating the funds for their own use.\textsuperscript{13} The CFTC also claimed that the promoters of MBC were arbitrarily changing the listed value of the coin to mimic actual activity when, in fact, there was none.\textsuperscript{14}

Despite alleging that MBC was not actually a functioning virtual currency, the Commission still treated it as such for purposes of the commodities fraud rules. The Commission brought charges against the defendants under 7 U.S.C. § 9(l) and Regulation 180.1(a). The former statute makes it unlawful to “use or employ … in connection with … any commodity in interstate commerce … any manipulative or deceptive device or contrivance …” (emphasis added). The latter makes it unlawful

for any person … in connection with … any commodity in interstate commerce … to intentionally or recklessly:
\begin{itemize}
  \item (1) Use or employ … any manipulative device, scheme, or artifice to defraud;
  \item (2) Make … any untrue or misleading statement of a material fact or to omit to state a material fact necessary in order to make the statements made not untrue or misleading;
  \item (3) Engage … in any act, practice, or course of business, which operates or would operate as a fraud or deceit upon any person … (emphasis added).
\end{itemize}

The Commission noted that the promoters violated these rules since, inter alia, in connection with a commodity – the purportedly fictitious coin – they made false and misleading statements.\textsuperscript{15}

The CFTC’s definition is consistent with the description of digital coins that are commodities in SEC Director Hinman’s June 2018 speech.\textsuperscript{16} For instance, in that speech, the list of questions that the Director provides to determine if a digital coin is a commodity all point to whether its primary use is as a medium of exchange for users of a network (as opposed to an investment opportunity). For instance:

\begin{itemize}
  \item (1) Is token creation commensurate with meeting the needs of users or, rather, with feeding speculation?
  \item (2) Is it clear that the primary motivation for purchasing the digital asset is for personal use or consumption, as compared to investment? Have purchasers made representations as to their consumptive, as opposed to their investment, intent …?
  \item (3) Are the tokens distributed in ways to meet users’ needs? For example, can the tokens be held or transferred only in amounts that correspond to a purchaser’s expected use …?\textsuperscript{17} (Emphasis added.)
\end{itemize}

\textsuperscript{13} Id.
\textsuperscript{14} Id. at 10.
\textsuperscript{15} Id. at 17.
\textsuperscript{17} Id.
The picture that emerges is that the digital coin that is a virtual currency is functioning on an operating network, and the primary (but not necessarily the only reason) to purchase it is a means to access goods and services on that network. Thus, for established networks like Bitcoin and Ether, the digital coins are virtual currencies. But even where the promoters make false statements about a network that does not exist – but the portrayed network is a functioning one that allows purchasers to access goods and services in the present – that still would fall into the virtual currency category and be subject to commodities fraud rules.

What makes a digital coin a security

The SEC has asserted, on numerous occasions, that a digital coin that is primarily an investment opportunity is a security – most frequently (though not exclusively) an “investment contract,” and therefore subject to SEC jurisdiction. The SEC outlines the elements in its DAO analysis which is based on the Howey test, namely: “a contract, transaction or scheme whereby a person invests his money in a common enterprise and is led to expect profits solely from the efforts of the promoter or a third party ….”

The elements that cause a digital coin to fall under the security definition are also outlined in Director Hinman’s June 2018 speech. There he also provides a list of questions to determine if a digital coin is a security saying:

1. Is there a person or group that has sponsored or promoted the creation and sale of the digital asset, the efforts of whom play a significant role in the development and maintenance of the asset and its potential increase in value?
2. Has this person or group retained a stake or other interest in the digital asset such that it would be motivated to expend efforts to cause an increase in value in the digital asset? Would purchasers reasonably believe such efforts will be undertaken and may result in a return on their investment in the digital asset?
3. Are purchasers “investing,” that is seeking a return? In that regard, is the instrument marketed and sold to the general public instead of to potential users of the network for a price that reasonably correlates with the market value of the good or service in the network?

These questions highlight the key elements of an investment contract: (1) potential purchasers would reasonably understand, because of the actions of the promoters, that this is primarily an investment opportunity; and (2) profits are generated mainly through the activities of others thereby creating an information differential that needs to be cured through disclosure.

---

20 SEC v. Howey Co., 328 U.S. 293, 298-9 (1946). The SEC has made clear, subsequent to Howey that the Howey test does not require that the third party be solely responsible for the profits, but mainly. See e.g., SEC, “Guidelines as to the Applicability of the Federal Securities Laws to Offers and Sales of Condominiums or Units in a Real Estate Development.” Washington, D.C., Jan. 4, 1973.
The SEC has brought a number of cases under this analysis, but the ones that are the most illustrative are those that are closest to the dividing line between virtual currency and investment. For instance, in AirFox, the SEC order acknowledged that AirFox’s digital coins, AirTokens, had some hallmarks of a virtual currency. For instance, AirFox claimed that AirTokens would be used as means to establish a network to “allow prepaid mobile phone users to earn free or discounted airtime or data by interacting with ads” and AirFox required that potential purchasers acknowledge that they were purchasing the coins to use as a utility not as an investment.\(^22\) Moreover, AirFox apparently intended to build a functioning network by building an ecosystem, adding an AirFox app, and entering into agreements with telecommunication firms.\(^23\)

However, the SEC alleged, that despite these statements and intentions, AirFox’s actual activity demonstrated that it was really selling purchasers a profit-making venture, not a medium to exchange services on mobile phones, including:

1. AirFox noted that it was intentionally reducing its digital coin supply to in order to increase the value of the coin;\(^24\)
2. AirFox touted how its aspects of its functionality would create demand for its digital coins among lenders who would be required to purchase the coins, thereby increasing their value;\(^25\) and
3. AirFox marketed the coins to individuals who would not be able to use them – U.S. persons – on a network that was intended to be used only by non-U.S. persons).\(^26\)

The SEC therefore characterized AirFox’s efforts not mainly as a means to create a functioning network, but to “increase the value of AirTokens.”\(^27\) So, in sum, the SEC characterized a digital coin for which the promoters demonstrated some intentionality to actually create a functioning network as an investment nonetheless because of the SEC’s interpretation of its primary purpose.

Similarly, in AriseBank, the SEC brushed off the virtual currency elements of the digital coin at issue there and characterized its offering as a security. The SEC claimed that the promoters of AriseBank offered AriseCoin as a means to raise money to establish a cryptocurrency bank, and in doing so, made false statements including that it had acquired a commercial bank\(^28\) and that it could offer a credit card.\(^29\) The SEC maintained, despite the virtual currency indications, that the venture was mainly a profit-making scheme since: (1) the promoters did not screen the individuals who purchased the coins (to limit it to the persons who

---


\(^24\) *Id.*

\(^25\) *Id.*

\(^26\) *Id.*

\(^27\) *Id.*


\(^29\) *Id.*
could use it); and (2) the purchasers would be partly paid in an expiring coin – eACO – purposely designed to increase the value of AriseCoin.\textsuperscript{30}

In Blockvest, the exception proved the rule. There, the SEC maintained that though the promoters’ stated goal was to create a virtual currency that would withstand volatility, the real purpose was to promote an investment opportunity.\textsuperscript{31} Specifically, the promoters stated goal was to raise money from the sales of the coin in order to fund a series of products including an index fund, a stablecoin, a portfolio management tool, and an exchange.\textsuperscript{32} The SEC alleged that there were multiple indications that the purpose of the coin was to raise capital, including promises in the white paper that the Blockvest holder would make specified profits per share.\textsuperscript{33} The Court however disagreed, finding instead that the SEC failed to prove conclusively that the buyers were influenced by the defendant’s promotional materials\textsuperscript{34} or an expectation of profits.\textsuperscript{35} So, in Blockvest, the Court accepted the Howey paradigm, but found that, under these facts, the SEC did not prove that the purchasers relied on the promoters’ promises in deciding to purchase the coins.

Probably one of the closest SEC cases is Plexcorps, a digital coin designed for use in the cannabis industry. As in the other cases, Plexcorps engaged in activities that suggested that it wanted to create a functioning coin. For instance, the promoters claimed that they would use generated proceeds to build an ecosystem and purchase real estate.\textsuperscript{36} Further, the SEC noted that Plexcorps did take actual steps to execute the plan including establishing a ParagonSpace working space that, at the time, was operational.\textsuperscript{37} The SEC also noted that the promoters of the PlexCoin Tokens made false statements in the sale of the coin including claiming that (1) there was a cadre of experts developing the coin when there was no such team; (2) they could not name the executives overseeing the coin to avoid anti-competitive practices when in fact they were trying to hide their identity because of their record of past misconduct; and (3) the Plexcoin would be used to pay for other products.\textsuperscript{38}

In reviewing Plexcorps, many of the actual activities of the promoters – and the allegedly fictitious ones – seemed to suggest that it was a functioning coin. But despite all of this evidence, the SEC noted the multiple references to potential increase in value of the coin in the advertising materials, including the advertisement of a deflation algorithm “which was designed to decrease supply of PRG tokens and in turn, increase the value of PRG tokens” and “burning” certain fees because that would “decreas[e] the amount of coins in circulation. More adoption = less coins, more value.”\textsuperscript{39}

\begin{itemize}
\item \textsuperscript{30} Id. at 6.
\item \textsuperscript{31} See SEC v. Blockvest et al., Case No. 18CV2287-GPB(BLM) (S.D. Cal. Nov. 27, 2018), at 9 (Order Denying Plaintiff’s Motion for a Preliminary Injunction).
\item \textsuperscript{32} Id.
\item \textsuperscript{33} See SEC v. Blockvest et al., Case No. 18CV2287-GPC (BLM) (S.D. Cal. Oct. 3, 2018), at 13 (Complaint).
\item \textsuperscript{34} See supra note 31 at 13.
\item \textsuperscript{35} Id.
\item \textsuperscript{37} Id. at 3.
\item \textsuperscript{38} SEC v. Plexcorps et al., Case No. CV 17-7007 (EDNY Dec. 1, 2017), at 3 (Complaint).
\item \textsuperscript{39} See supra note 36 at 5.
\end{itemize}
Defining the blurry line: commodity vs. security

The CFTC and SEC cases help to bring into sharp relief the edge between the SEC’s and CFTC’s jurisdictions. At first glance, several of the SEC cases seem as though they could have been brought as CFTC cases since, for all intents and purposes, the coin was either actually intended, or was allegedly falsely portrayed as, a fully functioning currency. Conversely, in the CFTC case, *My Big Coin Pay*, there are elements that are investment-like. For instance, the MBC promoters did advertise that the MBC was increasing in value. The CFTC noted that the promoters “tout[ed] the rising trading value of MBC in U.S. Dollars.”40 And indeed, the allegedly false prices that the CFTC listed did *increase* over time.41

So what makes *My Big Coin Pay* meaningfully different than *Plexcorps* or *AriseBank*? They all have some elements that are indicative of a virtual currency and an investment. The answer seems to be two-fold: (1) their primary purpose; and (2) their developmental stage. First, though their conclusions are subject to debate, the SEC does present the alleged securities as primarily investments, and the CFTC portrays the alleged virtual currencies as primarily mediums of exchange.42 And second, the digital coins that are pre-network or much more likely to be considered securities, and the digital coins that are on a network are much more likely to be considered commodities.

In fact, the SEC cases demonstrate how difficult it is for a coin without a functioning network to avoid the “security” designation, and explains the statements of SEC officials that, from the SEC’s perspective, virtually every initial coin offering is a security.43 Before a network has been established and the coin is operational, the digital coin is little more than a concept – it may be a well-described concept in a thorough white paper, but it is a concept nonetheless. The promoters describe what the digital coin will do, and the network that it will operate on, in order to convince would-be buyers to purchase it. The promoter has to entice the buyer with something; and that “something” can be easily interpreted by the SEC as a promise of future growth. Conversely, when a coin is operating on a network, it could be considered a digital coin even though it may have investment elements. For instance, Director Hinman noted in his speech that Bitcoin and Ether today would both fall into the virtual currency category. This assertion is illustrative because both Bitcoin and Ether are currently trading on exchanges and are being purchased by individuals who are interested not only in using them as mediums of exchange but also in holding them in hopes their value will increase.

III. TRANSFORMING COIN

40 See supra note 12 at 10, 11.
41 Id. at 10.
42 See supra note 12 at 10-12.
Given the distinction between a commodity and a security, it is possible for a digital coin to be defined as a virtual currency and an investment at different points in its evolution. While this option is not available for all securities, it is a possibility for securities that consist of a non-security element coupled with another aspect of the contract that together create an investment opportunity (“coupled” contracts).

A prime example of that is *Howey* where the Court found a security was formed by the coupling of a land sale on units on a citrus grove with a service contract to cultivate the groves.44 According to the Court, the facts demonstrate that the land sales contract and the service contract were inextricably linked – for instance: (1) clients were told that it was not feasible for them to make the investment unless they agreed to the service contracts;45 (2) the service contract gave the Howey Company, the contract company, a lease and possession of the land;46 and (3) the clients were business people who lacked the expertise to otherwise cultivate the orange groves themselves.47

Thus, what constituted the security was not the land sales contract, or for that matter, the land, the groves, or the oranges – what constituted the security was the combination of the land sales contract, the warranty deed and the service contract together.48 Similarly, in *Stevens*, the Court found a security where the defendants sold a “lease” (ownership agreement) in rabbits, coupled with a contract with a third party to breed them.49 And, in *Joiner*, the Court similarly determined that a combination of oil leases coupled with an agreement that the defendant would drill for oil constituted a security.50

Importantly, according to the SEC, to form a security, the two contracts are not merely coupled but the adjoining contract is really at the heart of the entire transaction; it creates the investment opportunity. For instance, in *Joiner*, the Court explained that the drilling agreement gave life to the entire investment scheme, forming the consideration for the whole enterprise.51 The Court noted, “It is clear that an economic interest in this well-drilling undertaking was what brought into being the instruments that defendants were selling and gave to the instruments most of their value and all of their lure.”52 Similarly, in *Howey*, the Court found that the entire enterprise only made sense as an investment for profit, including that the plots of land sold were actually too small to be profitably cultivated on their own.53

Nowhere in any of these “coupled” contracts did the courts indicate that the non-investment component of the package was transformed into a security by being part of a security. There was no indication that a lease in orange groves, sale of rabbits, a purchase of cemetery lots, or any of the other examples were in and of themselves securities because they had been part of a security. In fact, the language suggests the opposite. For instance, in *Joiner*, the Court

---

45 *Id.* at 295.
46 *Id.* at 296.
47 *Id.*
48 *Id.* at 297, 299.
50 SEC v. C.M. Joiner Leasing Corp. et al., 320 U.S. 344 (1943).
51 *Id.* at 348.
52 *Id.* at 349.
53 See *supra* note 44 at 300.
noted that without the drilling agreement, the overall contract would not have been a security saying, “[h]ad the offer mailed by defendants omitted the economic inducements of the proposed and promised exploration well, it would have been a quite different proposition.”54 Also, in a 1973 guidance, the SEC noted that if real estate that was part of a coupled contract was offered without the additional contract, it would not be considered a security.55

If the non-investment component of the investment contract is not transformed by its coupling then it is possible for it to be de-coupled. Therefore, a digital coin could be decoupled from the profit-making aspect of its package, and continue as a commodity on an established network. This idea is supported by a speech by Director Hinman, where he stated:

Can a digital asset that was originally offered in a securities offering ever be later sold in a manner that does not constitute an offering of a security?” In cases where the digital asset represents a set of rights that gives the holder a financial interest in an enterprise, the answer is likely ‘no’ …. But what about cases where there is no longer any central enterprise being invested in or where the digital asset is sold only to be used to purchase a good or service available through the network on which it was created? I believe in these cases the answer is a qualified “yes.”56 (Emphasis added.)

As the Director notes, in instances where there is a digital coin that is a virtual currency that is being sold as an investment, but it itself is virtual currency, the coin could be sold separately in the future outside the securities laws – i.e., as a commodity. In order to be considered a separate virtual currency on a network, Director Hinman noted that “purchasers would no longer reasonably expect a person or group to carry out essential managerial or entrepreneurial effort – the assets may not represent an investment contract.”57 The Director indicates that both Bitcoin and Ether meet these criteria and are virtual currencies.58

Consistent with the Director’s statements, the CFTC subsequently issued a Request for Input (RFI) about Ethereum.”59 The CFTC notes that one of motives for the RFI is to understand Ethereum because of its possible effect on Bitcoin, which, like Ether, the CFTC has defined as a virtual currency under its jurisdiction.60 Consistent with its jurisdictional claim, the CFTC asks questions in its RFI about, inter alia, the Ethereum network’s anticipated change from a “proof of work” consensus mechanism to a “proof of stake” mechanism.61 The questions demonstrate the CFTC’s concern that this change may inhibit the efficient validation of blocks, and potentially cause a fragmentation in the network.62 The RFI is a clear indication that the CFTC’s view is

54 See supra note 50 at 348.
57 Id.
58 Id.
60 Id. at 7.
61 Id. at 6.
62 E.g., id. at 8-9 (“Relative to a proof of work consensus mechanism does proof of stake have particular vulnerabilities, challenges, or features that make it prone to manipulation? In responding consider, for example, that under a proof of stake consensus mechanism, the chance of validating a block may be proportional to staked wealth.”)
consistent with Director Hinman’s assertion that even if an offering of a digital coin may be a security, once the coin is operating as a true virtual currency on an operating network, it can shed its security definition.

This conclusion is logical. If, for sake of argument, the Howey Company later tried to sell its orange groves outright, it would be illogical to assume that that sale would be a security. In the same way, if a bona fide virtual currency is wrapped in an investment contract at the pre-network stage, but used as a stand-alone currency on that network, it would be illogical and inconsistent with SEC case law and Director Hinman’s remarks, to call it a security. What is essential in this analysis is the understanding that the investment contract and the coin are regulatorily two different things. If the entire investment contract were sold on a platform, given the SEC’s assertions, that platform would have to register as a securities exchange. But extricating a true virtual currency from the investment contract creates an entirely different transaction.

IV. CONCLUSION

Therefore, it is possible for a digital coin to be treated as a security or commodity at different points in its evolution. Importantly though, it is not the same asset that is changing from a security to a commodity. In the offering stage, the digital coin could be part of a package that presents an investment opportunity which is therefore a security. Once the network is established, the virtual currency within the initial package can be extracted and survive on the network as a virtual currency. Thus, the coin is not changing from one definition to another. The coin that is a security remains a security, and the coin that is a virtual currency remains one as well. However, depending on how a digital coin that is a virtual currency is packaged, it could be treated as both a commodity and security at different stages of its evolution.
Michael Spafford is a partner in the White Collar Defense practice of Paul Hastings LLP. Mr. Spafford represents companies, committees of boards of directors, officers and directors, and other individuals in connection with government investigations and enforcement proceedings brought by the Department of Justice, Securities and Exchange Commission, Commodity Futures Trading Commission, Federal Energy Regulatory Commission, and other federal, state, and local government enforcement entities, and related parallel litigation. In particular, Mr. Spafford has represented clients in connection with numerous government investigations of trading of natural gas, power, crude oil, natural gas liquids, gasoline, ethanol, and other commodities. Mr. Spafford also currently represents clients involved in multiple government investigations of alleged manipulation of Libor, FX and other benchmarks referenced in connection with various derivatives. Mr. Spafford has been featured in Chambers USA, White Collar Crime & Government Investigations (District of Columbia) (2014-2015), The Best Lawyers in America®, Derivatives and Futures (2007-2018), and Super Lawyers, Washington, D.C., Criminal Defense (2013-2018).