

**WRITTEN TESTIMONY OF
J. CHRISTOPHER GIANCARLO
CHAIRMAN, COMMODITY FUTURES TRADING COMMISSION
BEFORE THE
SENATE BANKING COMMITTEE
WASHINGTON, D.C.
FEBRUARY 6, 2018**

Introduction: Virtual Currency

Thank you, Chairman Crapo, for the invitation to testify before the Committee. Thank you, Ranking Member Brown, and all the members of the Committee for this opportunity to discuss virtual currencies.

At the outset, I would like to note that this hearing is timely, even fortuitous. Emerging financial technologies broadly are taking us into a new chapter of economic history. They are impacting trading, markets and the entire financial landscape with far ranging implications for capital formation and risk transfer. They include machine learning and artificial intelligence, algorithm-based trading, data analytics, “smart” contracts valuing themselves and calculating payments in real-time, and distributed ledger technologies, which over time may come to challenge traditional market infrastructure. They are transforming the world around us, and it is no surprise that these technologies are having an equally transformative impact on US capital and derivatives markets.

The more specific topic for today’s hearing, however, is virtual currency. Broadly speaking, virtual currencies are a digital representation of value that may function as a medium of exchange, a unit of account, and/or a store of value. Virtual currencies generally run on a decentralized peer-to-peer network of computers, which rely on certain network participants to validate and log transactions on a permanent, public distributed ledger, commonly known as the blockchain.

Supporters of virtual currencies see a technological solution to the age-old “double spend” problem – that has always driven the need for a trusted, central authority to ensure that an entity is capable of, and does, engage in a valid transaction. Traditionally, there has been a need for a trusted intermediary – for example a bank or other financial institution – to serve as a gatekeeper for transactions and many economic activities. Virtual currencies seek to replace the need for a central authority or intermediary with a decentralized, rules-based and open consensus mechanism.¹ An array of thoughtful business, technology, academic, and policy leaders have

¹ See generally, CFTC Talks, Episode 24, Dec. 29, 2017, Interview with Coincenter.org Director of Research, Peter Van Valkenburgh, at <http://www.cftc.gov/Media/Podcast/index.htm>.

extrapolated some of the possible impacts that derive from such an innovation, including how market participants conduct transactions, transfer ownership, and power peer-to-peer applications and economic systems.²

Others, however, argue that this is all hype or technological alchemy and that the current interest in virtual currencies is overblown and resembles wishful thinking, a fever, even a mania. They have declared the 2017 heightened valuation of Bitcoin to be a bubble similar to the famous “Tulip Bubble” of the seventeenth century. They say that virtual currencies perform no socially useful function and, worse, can be used to evade laws or support illicit activity.³ Indeed, history has demonstrated to us time-and-again that bad actors will try to invoke the concept of innovation in order to perpetrate age-old fraudulent schemes on the public. Accordingly, some assert that virtual currencies should be banned, as some nations have done.⁴

There is clearly no shortage of opinions on virtual currencies such as Bitcoin. In fact, virtual currencies may be all things to all people: for some, potential riches, the next big thing, a technological revolution, and an exorable value proposition; for others, a fraud, a new form of temptation and allure, and a way to separate the unsuspecting from their money.

Perspective is critically important. As of the morning of February 5, the total value of all outstanding Bitcoin was about \$130 billion based on a Bitcoin price of \$7,700. The Bitcoin “market capitalization” is less than the stock market capitalization of a single “large cap” business, such as McDonalds (around \$130 billion). The total value of all outstanding virtual currencies was about \$365 billion. Because virtual currencies like Bitcoin are sometimes considered to be comparable to 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 surpass its size and magnitude in today’s global economy.

² See Marc Andreessen, *Why Bitcoin Matters*, New York Times DealBook (Jan. 21, 2014), <https://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/>; Jerry Brito and Andrea O’Sullivan, *Bitcoin: A Primer for Policymakers*, George Mason University Mercatus Center (May 3, 2016), <https://www.mercatus.org/publication/bitcoin-primer-policymakers>; Christian Catalini and Joshua S. Gans, *Some Simple Economics of the Blockchain*, Rotman School of Management Working Paper No. 2874598, MIT Sloan Research Paper No. 5191-16 (last updated Sept. 21, 2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2874598; Arjun Kharpal, *People are ‘underestimating’ the ‘great potential’ of bitcoin, billionaire Peter Thiel says*, CNBC (Oct. 26, 2017), <https://www.cnbc.com/2017/10/26/bitcoin-underestimated-peter-thiel-says.html>; Hugh Son, *Bitcoin ‘More Than Just a Fad,’ Morgan Stanley CEO Says*, Bloomberg (Sept. 27, 2017), <https://www.bloomberg.com/news/articles/2017-09-27/bitcoin-more-than-just-a-fad-morgan-stanley-ceo-gorman-says>; Chris Brummer and Daniel Gorfine, *FinTech: Building a 21st-Century Regulator’s Toolkit*, Milken Institute (Oct. 21, 2014), available at <http://www.milkeninstitute.org/publications/view/665>.

³ Virtual currencies are not unique in their utility in illicit activity. National currencies, like the US Dollar, and commodities, like gold and diamonds, have long been used to support criminal enterprises.

⁴ Countries that have banned Bitcoin include Bangladesh, Bolivia, Ecuador, Kyrgyzstan, Morocco, Nepal, and Vietnam. China has banned Bitcoin for banking institutions.

Yet, despite being a relatively small asset class, virtual currency presents novel challenges for regulators. SEC Chairman Clayton and I recently wrote:

*The CFTC and SEC, along with other federal and state regulators and criminal authorities, will continue to work together to bring transparency and integrity to these markets and, importantly, to deter and prosecute fraud and abuse. These markets are new, evolving and international. As such they require us to be nimble and forward-looking; coordinated with our state, federal and international colleagues; and engaged with important stakeholders, including Congress*⁵.

It is this perspective that has guided our work at the CFTC on virtual currencies.

Introduction: The Mission of the CFTC:

The mission of the CFTC is to foster open, transparent, competitive, and financially sound derivatives markets.⁶ By working to avoid systemic risk, the Commission aims to protect market users and their funds, consumers, and the public from fraud, manipulation, and abusive practices related to derivatives and other products that are subject to the **Commodity Exchange Act (CEA)**.

The CFTC was established as an independent agency in 1974, assuming responsibilities that had previously belonged to the Department of Agriculture since the 1920s. The Commission historically has been charged by the CEA with regulatory authority over the commodity futures markets. These markets have existed since the 1860s, beginning with agricultural commodities such as wheat, corn, and cotton.

Over time, these organized commodity futures markets, known as **designated contract markets (DCMs)** regulated by the CFTC, have grown to include those for energy and metals commodities, collectively including crude oil, heating oil, gasoline, copper, gold, and silver. The agency now also oversees these commodity futures markets for financial products such as interest rates, stock indexes, and foreign currency. The definition of “commodity” in the CEA is broad. It can mean a physical commodity, such as an agricultural product (e.g., wheat, cotton) or natural resource (e.g., gold, oil). It can mean a currency or interest rate. The CEA definition of “commodity” also includes “all services, rights, and interests . . . in which contracts for future delivery are presently or in the future dealt in.”

In the aftermath of the 2008 financial crisis, President Obama and Congress enhanced the CFTC’s regulatory authority. With passage of the **Dodd-Frank Wall Street Reform and**

⁵ Jay Clayton and J. Christopher Giancarlo, *Regulators Are Looking at Cryptocurrency: At the SEC and CFTC We Take Our Responsibility Seriously*, Wall Street Journal, Jan. 24, 2018, <https://www.wsj.com/articles/regulators-are-looking-at-cryptocurrency-1516836363>.

⁶ See CFTC, *Mission and Responsibilities*, <http://www.cftc.gov/About/MissionResponsibilities/index.htm>.

Consumer Protection Act (Dodd-Frank Act), the agency now also oversees most of the U.S. swaps market in addition to exchange traded futures markets.

Futures, swaps and other derivatives markets are essential means for commercial and financial risk mitigation and transfer. These markets allow the risks of variable production costs, such as the price of raw materials, energy, foreign currency and interest rates, to be transferred from those who cannot afford them to those who can. They are the reason why American consumers enjoy stable prices in the grocery store, whatever the conditions out on the farm.

But derivatives markets are not just useful for agricultural producers. They impact the price and availability of heating in American homes, the energy used in factories, the interest rates borrowers pay on home mortgages and the returns workers earn on their retirement savings. More than 90 percent of *Fortune 500* companies use derivatives to manage commercial or market risk in their worldwide business operations. In short, derivatives serve the needs of society to help moderate price, supply and other commercial risks to free up capital for economic growth, job creation and prosperity.

To ensure the integrity of US derivatives markets, the CFTC regulates derivatives market participants and activities. The agency oversees a variety of individuals and organizations. These include swap execution facilities, derivatives clearing organizations, designated contract markets, swap data repositories, swap dealers, futures commission merchants, commodity pool operators, and other entities. The CFTC also prosecutes derivative market fraud and manipulation, including misconduct in underlying spot markets for commodities.

I. CFTC Authority and Oversight over Virtual Currencies

In 2015, the CFTC determined that virtual currencies, such as Bitcoin, met the definition of “commodity” under the CEA. Nevertheless, the CFTC does NOT have regulatory jurisdiction under the CEA over markets or platforms conducting cash or “spot” transactions in virtual currencies or other commodities or over participants on such platforms. More specifically, the CFTC does not have authority to conduct regulatory oversight over spot virtual currency platforms or other cash commodities, including imposing registration requirements, surveillance and monitoring, transaction reporting, compliance with personnel conduct standards, customer education, capital adequacy, trading system safeguards, cyber security examinations or other requirements. In fact, current law does not provide any U.S. Federal regulator with such regulatory oversight authority over spot virtual currency platforms operating in the United States or abroad. However, the CFTC DOES have enforcement jurisdiction to investigate through subpoena and other investigative powers and, as appropriate, conduct civil enforcement action against fraud and manipulation in virtual currency derivatives markets and in underlying virtual currency spot markets.

In contrast to the spot markets, the CFTC does have both regulatory and enforcement jurisdiction under the CEA over derivatives on virtual currencies traded in the United States. This means that for derivatives on virtual currencies traded in U.S. markets, the CFTC conducts

comprehensive regulatory oversight, including imposing registration requirements and compliance with a full range of requirements for trade practice and market surveillance, reporting and monitoring and standards for conduct, capital requirements and platform and system safeguards.

II. Assertion of CFTC Authority

The CFTC has been straightforward in asserting its area of statutory jurisdiction concerning virtual currencies derivatives. As early as 2014, former CFTC Chairman Timothy Massad discussed virtual currencies and potential CFTC oversight under the Commodity Exchange Act (CEA).⁷ And as noted above, in 2015, the CFTC found virtual currencies to be a commodity.⁸ In that year, the agency took enforcement action to prohibit wash trading and prearranged trades on a virtual currency derivatives platform.⁹ In 2016, the CFTC took action against a Bitcoin futures exchange operating in the U.S. that failed to register with the agency.¹⁰ Last year, the CFTC issued proposed guidance on what is a derivative market and what is a spot market in the virtual currency context.¹¹ The agency also issued warnings about valuations and volatility in spot virtual currency markets¹² and launched an unprecedented consumer education effort (detailed in Section IV herein).

a. Enforcement

The CFTC Division of Enforcement is a premier Federal civil enforcement agency dedicated to deterring and preventing price manipulation and other disruptions of market integrity, ensuring the financial integrity of all transactions subject to the CEA, and protecting market participants from fraudulent or other abusive sales practices and misuse of customer assets. **Appendix A hereto** summarizes recent CFTC enforcement activities.

The CFTC has been particularly assertive of its enforcement jurisdiction over virtual currencies. It has formed an internal virtual currency enforcement task force to garner and deploy relevant expertise in this evolving asset class. The task force shares information and works cooperatively with counterparts at the SEC with similar virtual currency expertise.

⁷ Testimony of CFTC Chairman Timothy Massad before the U.S. Senate Committee on Agriculture, Nutrition and Forestry (Dec. 10, 2014), <http://www.cftc.gov/PressRoom/SpeechesTestimony/opamassad-6>.

⁸ *In re* Coinflip, Inc., Dkt. No. 15-29 (CFTC Sept. 17, 2015), <http://www.cftc.gov/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcoinfliporder09172015.pdf>.

⁹ *In re* TeraExchange LLC, Dkt. No. 15-33 (CFTC Sept. 24, 2015), <http://www.cftc.gov/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfteraexchangeorder92415.pdf>.

¹⁰ *In re* BXFNA Inc. d/b/a Bitfinex, Dkt. No. 16-19 (CFTC June 2, 2016), <http://www.cftc.gov/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfbfxnaorder060216.pdf>.

¹¹ CFTC, Retail Commodity Transactions Involving Virtual Currency, 82 Fed. Reg. 60335 (Dec. 20, 2017), www.gpo.gov/fdsys/pkg/FR-2017-12-20/pdf/2017-27421.pdf.

¹² CFTC, A CFTC Primer on Virtual Currencies (Oct. 17, 2017), http://www.cftc.gov/idc/groups/public/documents/file/labcfct_primercurrencies100417.pdf.

In September 2017, the CFTC took enforcement action against a virtual currency Ponzi scheme.¹³ Over the past few weeks, the CFTC filed a series of civil enforcement actions against perpetrators of fraud, market manipulation and disruptive trading involving virtual currency. These include:

- (i) ***My Big Coin Pay Inc.***, which charged the defendants with commodity fraud and misappropriation related to the ongoing solicitation of customers for a virtual currency known as My Big Coin;
- (ii) ***The Entrepreneurs Headquarters Limited***, which charged the defendants with a fraudulent scheme to solicit Bitcoin from members of the public, misrepresenting that customers' funds would be pooled and invested in products including binary options, and instead misappropriated the funds and failed to register as a Commodity Pool Operator; and
- (iii) ***Coin Drop Markets***, which charged the defendants with fraud and misappropriation in connection with purchases and trading of Bitcoin and Litecoin.

These recent enforcement actions confirm that the CFTC, working closely with the SEC and other fellow financial enforcement agencies, will aggressively prosecute bad actors that engage in fraud and manipulation regarding virtual currencies.

b. Bitcoin Futures

It is important to put the new Bitcoin futures market in perspective. It is quite small with open interest at the CME of 6,695 bitcoin¹⁴ and at Cboe Futures Exchange (Cboe) of 6,695 bitcoin (as of Feb. 2, 2018). At a price of approximately \$7,700 per Bitcoin,¹⁵ this represents a notional amount of about \$94 million. In comparison, the notional amount of the open interest in CME's WTI crude oil futures was more than one thousand times greater, about \$170 billion (2,600,000 contracts) as of Feb 2, 2018 and the notional amount represented by the open interest of Comex gold futures was about \$74 billion (549,000 contracts).

Prior to the launch of Bitcoin futures, the CFTC closely observed the evolution of virtual currencies over the past several years. One exchange, CME Group, launched a Bitcoin Reference Rate in November 2016. And, another exchange, CBOE Futures Exchange (Cboe), first approached the CFTC in July 2017. The CFTC anticipated receiving proposals for the launch of Bitcoin futures products in late 2017.

¹³ On September 21, 2017, the CFTC filed a complaint in federal court in the Southern District of New York against Nicholas Gelfman and Gelfman Blueprint, Inc., *see* <http://www.cftc.gov/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfgelfmancomplaint09212017.pdf>.

¹⁴ Each CME contract represents 5 Bitcoin.

¹⁵ The price changes day to day.

Under CEA and Commission regulations and related guidance, futures exchanges may self-certify new products on twenty-four hour notice prior to trading. In the past decade and a half, over 12,000 new futures products have been self-certified.¹⁶ It is clear that Congress and prior Commissions deliberately designed the product self-certification framework to give futures exchanges, in their role as self-regulatory organizations, the ability to quickly bring new products to the marketplace. The CFTC’s current product self-certification framework has long been considered to function well and be consistent with public policy that encourages market-driven innovation that has made America’s listed futures markets the envy of the world.

Practically, both CME and Cboe had numerous discussions and exchanged numerous draft product terms and conditions with CFTC staff over a course of months prior to their certifying and launching Bitcoin futures in December 2017. This type of lengthy engagement is not unusual during the self-certification process for products that may raise certain issues. The CFTC staff undertook its review of CME’s and Cboe’s Bitcoin futures products with considered attention. Given the emerging nature and heightened attention of these products, staff conducted a “heightened review” of CME’s and Cboe’s responsibilities under the CEA and Commission regulations to ensure that their Bitcoin futures products and their cash-settlement processes were not readily susceptible to manipulation,¹⁷ and the risk management of the associated Derivatives Clearing Organizations (DCOs) to ensure that the products were sufficiently margined.¹⁸

Staff obtained the voluntary cooperation of CME and Cboe with a set of enhanced monitoring and risk management steps.

1. Designated contract markets (DCMs) setting exchange large trader reporting thresholds at five bitcoins or less;
2. DCMs entering direct or indirect information sharing agreements with spot market platforms to allow access to trade and trader data making up the underlying index that the futures contracts settle to;
3. DCMs agreeing to engage in monitoring of underlying index data from cash markets and identifying anomalies and disproportionate moves;
4. DCMs agreeing to conduct inquiries, as appropriate, including at the trade settlement and trader level when anomalies or disproportionate moves are identified;
5. DCMs agreeing to regular communication with CFTC surveillance staff on trade activities, including providing trade settlement and trader data upon request;

¹⁶ Prior to the changes made in the Commodity Futures Modernization Act of 2000 (CFMA) and the Commission’s subsequent addition of Part 40, exchanges submitted products to the CFTC for approval. From 1922 until the CFMA was signed into law, less than 800 products were approved. Since then, exchanges have certified over 12,000 products. For financial instrument products specifically, the numbers are 494 products approved and 1,938 self-certified. See <http://www.cftc.gov/IndustryOversight/ContractsProducts/index.htm>.

¹⁷ See CEA Section 5(d)(3), 7 U.S.C. 7(d)(3); Section 5(d)(4), 7 U.S.C. 7(d)(4); 17 C.F.R. 38.253 and 38.254(a), and Appendices B and C to Part 38 of the CFTC’s regulations.

¹⁸ CEA Section 5b(c)(2)(D)(iv), 7 U.S.C. 7a-1(c)(2)(D)(iv) (“The margin from each member and participant of a derivatives clearing organization shall be sufficient to cover potential exposures in normal market conditions.”).

6. DCMs agreeing to coordinate product launches to enable the CFTC’s market surveillance branch to monitor developments; and
7. DCOs setting substantially high initial¹⁹ and maintenance margin for cash-settled instruments.

The first six of these elements were used to ensure that the new product offerings complied with the DCM’s obligations under the CEA core principles and CFTC regulations and related guidance. The seventh element, setting high initial and maintenance margins, was designed to ensure adequate collateral coverage in reaction to the underlying volatility of Bitcoin.

In crafting its process of “heightened review” for compliance, CFTC staff prioritized visibility, data, and monitoring of markets for Bitcoin derivatives and underlying settlement reference rates. CFTC staff felt that in gaining such visibility, the CFTC could best look out for Bitcoin market participants and consumers, as well as the public interest in Federal surveillance and enforcement. This visibility greatly enhances the agency’s ability to prosecute fraud and manipulation in both the new Bitcoin futures markets and in its related underlying cash markets.

As for the interests of clearing members, the CFTC recognized that large global banks and brokerages that are DCO clearing members are able to look after their own commercial interests by choosing not to trade Bitcoin futures, as some have done, requiring substantially higher initial margins from their customers, as many have done, and through their active participation in DCO risk committees.

After the launch of Bitcoin futures, some criticism was directed at the self-certification process from a few market participants. Some questioned why the Commission did not hold public hearings prior to launch. However, it is the function of the futures exchanges and futures clearinghouses - and not CFTC staff²⁰ - to solicit and address stakeholder concerns in new product self-certifications. The CFTC staff’s focus was on how the futures contracts and cash settlement indices are designed to bar manipulation and the appropriate level of contract margining to meet CEA and Commission regulations.

Interested parties, especially clearing members, should *indeed* have an opportunity to raise appropriate concerns for consideration by regulated platforms proposing virtual currency derivatives and DCOs considering clearing new virtual currency products. That is why CFTC staff has added an additional element to the Review and Compliance Checklist for virtual

¹⁹ In the case of CME and Cboe Bitcoin futures, the initial and maintenance margins were ultimately set at 47% and 44% by the respective DCOs. By way of comparison that is more than ten times the margin required for CME corn futures products.

²⁰ Unlike provisions in the CEA and Commission regulations that provide for public comment on *rule* self-certifications, there is no provision in statute or regulation for public input into CFTC staff review of *product* self-certifications. It is hard to believe that Congress was not deliberate in making that distinction.

currency product self-certifications. That is, requesting DCMs and SEFs to disclose to CFTC staff what steps they have taken in their capacity as self-regulatory organizations to gather and accommodate appropriate input from concerned parties, including trading firms and FCMs. Further, CFTC staff will take a close look at DCO governance around the clearing of new virtual currency products and formulate recommendations for possible further action.

The CFTC's response to the self-certification of Bitcoin futures has been a balanced one. It has resulted in the world's first federally regulated Bitcoin futures market. Had it even been possible, blocking self-certification would not have stopped the rise of Bitcoin or other virtual currencies. Instead, it would have ensured that virtual currency spot markets continue to operate without effective and data-enabled federal regulatory surveillance for fraud and manipulation. It would have prevented the development of a regulated derivatives market that allowed participants to take "short" positions that challenged the 2017 rise of Bitcoin prices.

III. Adequacy of CFTC Authority

The CFTC has sufficient authority under the CEA to protect investors in virtual currency derivatives over which the CFTC has regulatory jurisdiction under the CEA. As noted above, the CFTC does NOT have regulatory jurisdiction over markets or platforms conducting cash or "spot" transactions in virtual currencies or over participants on those platforms. For such virtual currency spot markets, CFTC only has enforcement jurisdiction to investigate and, as appropriate, conduct civil enforcement action against fraud and manipulation.

Any extension of the CFTC's regulatory authority to virtual currency spot markets would require statutory amendment of the CEA.²¹ The CFTC is an experienced regulator of derivatives markets that mostly serve professional and eligible contract participants. Such extension of regulatory authority would be a dramatic expansion of the CFTC's regulatory mission, which currently does not give the CFTC regulatory authority (distinct from enforcement authority) over cash commodity markets.

IV. Educating Investors and Market Participants

The CFTC believes that the responsible regulatory response to virtual currencies must start with consumer education. Amidst the wild assertions, bold headlines, and shocking hyperbole about virtual currencies, there is a need for much greater understanding and clarity.

²¹ The CFTC has jurisdiction over retail foreign currency markets and retail commodity transactions that use leverage, margin or financing with some exceptions. Congress responded to concerns in the regulation of leveraged retail FX by providing the CFTC oversight responsibilities for Retail Foreign Exchange Dealers (RFEDs). The CFTC Re-authorization Act of 2008 amended the CEA to create a new registration category for RFEDs that include disclosure requirements and leverage limitations to customers.

Over the past six months, the CFTC has produced an unprecedented amount of consumer information concerning virtual currencies (listed in **Appendix B hereto**). These consumer materials include an information “primer” on virtual currencies (**Appendix C hereto**), consumer and market advisories on investing in Bitcoin and other virtual currencies (**Appendix D hereto**), a dedicated CFTC “Bitcoin” webpage, several podcasts (available on the Commission’s website and from various streaming services) concerning virtual currencies and underlying technology, weekly publication of Bitcoin futures “Commitment of Traders” data and an analysis of Bitcoin spot market data.

In addition, the CFTC’s **Office of Consumer Education and Outreach (OCEO)** is actively engaging with responsible outside partners to better educate consumers on Bitcoin and other virtual currencies. The OCEO is currently partnering with:

- The **Consumer Finance Protection Bureau (CFPB)** to train US public library staff to identify and report consumer in virtual currencies;
- the **American Association of Retired Persons (AARP)** to distribute a virtual currency “Watchdog Alert” to 120,000 AARP members;
- **North American Securities Administrators Association (NASAA)** Investor Educators, who are responsible for conducting outreach to the public on avoiding investment fraud, including in virtual currencies;
- the **National Attorneys General Training and Research Institute (NAGTRI)**, which is the research and training arm of the National Association of Attorneys General (NAAG), to inform State AGs about the availability of CFTC’s virtual currency resources; and
- The **Federal Reserve Bank of Chicago** to help consumers manage their finances better, OCEO will again coordinate with NFA, FINRA and SEC to hold a webinar on fraud prevention in virtual currencies.

V. Interagency Coordination

As noted, the CFTC’s enforcement jurisdiction over virtual currencies is not exclusive. As a result, the U.S. approach to oversight of virtual currencies has evolved into a multifaceted, multi-regulatory approach that includes:

- The **Securities and Exchange Commission (SEC)** taking increasingly strong action against unregistered securities offerings, whether they are called a virtual currency or initial coin offering in name.
- **State Banking** regulators overseeing certain US and foreign virtual currency spot exchanges largely through state money transfer laws.
- The **Internal Revenue Service (IRS)** treating virtual currencies as property subject to capital gains tax.

- The Treasury’s **Financial Crimes Enforcement Network (FinCEN)** monitoring Bitcoin and other virtual currency transfers for anti-money laundering purposes.

The CFTC actively communicates its approach to virtual currencies with other Federal regulators, including the **Federal Bureau of Investigation (FBI)** and the **Justice Department** and through the **Financial Stability Oversight Council (FSOC)**, chaired by the Treasury Department. The CFTC has been in close communication with the SEC with respect to policy and jurisdictional considerations, especially in connection with recent virtual currency enforcement cases. In addition, we have been in communication with overseas regulatory counterparts through bilateral discussions and in meetings of the **Financial Stability Board (FSB)** and the **International Organization of Securities Commissions (IOSCO)**.

VI. Potential Benefits

I have spoken publicly about the potential benefits of the technology underlying Bitcoin, namely **Blockchain** or **distributed ledger technology (DLT)**.²² Distributed ledgers – in various open system or private network applications – have the potential to enhance economic efficiency, mitigate centralized systemic risk, defend against fraudulent activity and improve data quality and governance.²³

DLT is likely to have a broad and lasting impact on global financial markets in payments, banking, securities settlement, title recording, cyber security and trade reporting and analysis.²⁴ When tied to virtual currencies, this technology aims to serve as a new store of value, facilitate secure payments, enable asset transfers, and power new applications.

Additionally, DLT will likely develop hand-in-hand with new “smart” contracts that can value themselves in real-time, report themselves to data repositories, automatically calculate and perform margin payments and even terminate themselves in the event of counterparty default.²⁵

DLT may enable financial market participants to manage the significant operational,

²² J. Christopher Giancarlo, *Keynote Address of Commissioner J. Christopher Giancarlo before the Markit Group, 2016 Annual Customer Conference New York*, May 10, 2016, <http://www.cftc.gov/PressRoom/SpeechesTestimony/opagiancarlo-15>.

²³ *Id.*

²⁴ See, e.g., Larry Greenemeier, *Can't Touch This: New Encryption Scheme Targets Transaction Tampering*, *Scientific American*, May 22, 2015, <http://www.scientificamerican.com/article/can-t-touch-this-new-encryption-scheme-targets-transaction-tampering/>.

²⁵ See Massimo Morini & Robert Sams, *Smart Derivatives Can Cure XVA Headaches*, *Risk Magazine*, Aug. 27, 2015, <http://www.risk.net/risk-magazine/opinion/2422606/-smart-derivatives-can-cure-xva-headaches>; see also Jeffrey Maxim, *UBS Bank Is Experimenting with “Smart-Bonds” Using the Bitcoin Blockchain*, *Bitcoin Magazine*, June 12, 2015, <https://bitcoinmagazine.com/articles/ubs-bank-experimenting-smart-bonds-using-bitcoin-blockchain-1434140571>; see also Pete Harris, *UBS Exploring Smart Bonds on Block Chain*, *Block Chain Inside Out*, June 15, 2015, http://harris-on.typepad.com/block_chain_io/2015/06/ubs-exploring-smart-bonds-on-block-chain.html; See generally Galen Stos, *Blockchain: Getting Beyond the Buzz*, *Profit & Loss*, Aug.–Sept. 2015, at 20, <http://www.profit-loss.com/articles/analysis/technology-analysis/blockchain-getting-beyond-the-buzz>.

transactional and capital complexities brought about by the many mandates, regulations and capital requirements promulgated by regulators here and abroad in the wake of the financial crisis.²⁶ In fact, one study estimates that DLT could eventually allow financial institutions to save as much as \$20 billion in infrastructure and operational costs each year.²⁷ Another study reportedly estimates that blockchain could cut trading settlement costs by a third, or \$16 billion a year, and cut capital requirements by \$120 billion.²⁸ Moving from systems-of-record at the level of a firm to an authoritative system-of-record at the level of a market is an enormous opportunity to improve existing market infrastructure.²⁹

Outside of the financial services industry, many use cases for DLT are being posited from international trade to charitable endeavors and social services. International agricultural commodities merchant, Louis Dreyfus, and a group of financing banks have just completed the first agricultural deal using distributed ledger technology for the sale of 60,000 tons of US soybeans to China.³⁰ Other DLT use cases include: legal records management, inventory control and logistics, charitable donation tracking and confirmation; voting security and human refugee identification and relocation.³¹

Yet, while DLT promises enormous benefits to commercial firms and charities, it also promises assistance to financial market regulators in meeting their mission to oversee healthy markets and mitigate financial risk. What a difference it would have made on the eve of the financial crisis in 2008 if regulators had access to the real-time trading ledgers of large Wall Street banks, rather than trying to assemble piecemeal data to recreate complex, individual trading portfolios. I have previously speculated³² that, if regulators in 2008 could have viewed a real-time distributed ledger (or a series of aggregated ledgers across asset classes) and, perhaps, been able to utilize modern cognitive computing capabilities, they may have been able to recognize anomalies in market-wide trading activity and diverging counterparty exposures indicating heightened risk of bank failure. Such transparency may not, by itself, have saved Lehman Brothers from bankruptcy, but it certainly would have allowed for far prompter, better-informed, and more calibrated regulatory intervention instead of the disorganized response that unfortunately ensued.

²⁶ See, e.g., *Oversight of Dodd-Frank Act Implementation*, U.S. House Financial Services Committee, <http://financialservices.house.gov/dodd-frank/> (last visited Mar. 2, 2016).

²⁷ Santander InnoVentures, Oliver Wyman & Anthemis Group, *The Fintech Paper 2.0: Rebooting Financial Services 15* (2015), <http://santanderinnoventures.com/wp-content/uploads/2015/06/The-Fintech-2-0-Paper.pdf>.

²⁸ Telis Demos, *Bitcoin's Blockchain Technology Proves Itself in Wall Street Test*, Apr. 7, 2016, *The Wall Street Journal*, <http://www.wsj.com/articles/bitcoins-blockchain-technology-proves-itself-in-wall-street-test-1460021421>.

²⁹ Based on conversations with R3 CEV, <http://r3cev.com/>.

³⁰ Emiko Terazono, *Commodities trader Louis Dreyfus turns to blockchain*<https://www.ft.com/content/22b2ac1e-fd1a-11e7-a492-2c9be7f3120a>, *Financial Times*, Jan. 22, 2018.

³¹ Frisco d'Anconia, *IOTA Blockchain to Help Trace Families of Refugees During and After Conflicts*, *Cointelegraph.com*, Aug. 8, 2017, <https://cointelegraph.com/news/iota-blockchain-to-help-trace-families-of-refugees-during-and-after-conflicts>.

³² See *supra* note 22.

VII. Policy Considerations

Two decades ago, as the Internet was entering a phase of rapid growth and expansion, a Republican Congress and the Clinton administration established a set of enlightened foundational principles: the Internet was to progress through human social interaction; voluntary contractual relations and free markets; and governments and regulators were to act in a thoughtful manner not to harm the Internet's continuing evolution.³³

This simple approach is well-recognized as the enlightened regulatory underpinning of the Internet that brought about such profound changes to human society. During the almost 20 years of “do no harm” regulation, a massive amount of investment was made in the Internet's infrastructure. It yielded a rapid expansion in access that supported swift deployment and mass adoption of Internet-based technologies. Internet-based innovations have revolutionized nearly every aspect of American life, from telecommunications to commerce, transportation and research and development. This robust Internet economy has created jobs, increased productivity and fostered innovation and consumer choice.

“Do no harm” was unquestionably the right approach to development of the Internet. Similarly, I believe that “do no harm” is the right overarching approach for distributed ledger technology.

Virtual currencies, however, likely require more attentive regulatory oversight in key areas, especially to the extent that retail investors are attracted to this space. SEC Chairman Clayton and I recently stated in a joint op-ed, that:

“Our task, as market regulators, is to set and enforce rules that foster innovation while promoting market integrity and confidence. In recent months, we have seen a wide range of market participants, including retail investors, seeking to invest in DLT initiatives, including through cryptocurrencies and so-called ICOs—initial coin offerings. Experience tells us that while some market participants may make fortunes, the risks to all investors are high. Caution is merited.

“A key issue before market regulators is whether our historic approach to the regulation of currency transactions is appropriate for the cryptocurrency markets. Check-cashing and money-transmission services that operate in the U.S. are primarily state-regulated. Many of the internet-based cryptocurrency trading platforms have registered as payment services and are not subject to

³³ The Telecommunications Act of 1996 (*See* Telecommunications Act of 1996 (Pub. L. No. 104-104, 110 Stat. 56 (1996))) and the ensuing Clinton administration “Framework for Global Electronic Commerce” (*See* Clinton administration, Framework for Global Electronic Commerce, <http://clinton4.nara.gov/WH/New/Commerce/>) established a simple and sensible framework: a) the private sector should play the leading role in innovation, development and financing; and b) governments and regulators should “do no harm” by avoiding undue restrictions, supporting a predictable, consistent and simple legal environment and respecting the “bottom-up” nature of the technology and its deployment in a global marketplace.

direct oversight by the SEC or the CFTC. We would support policy efforts to revisit these frameworks and ensure they are effective and efficient for the digital era.”³⁴

As the Senate Banking Committee, the Senate Agriculture Committee and other Congressional policy makers consider the current state of regulatory oversight of cash or “spot” transactions in virtual currencies and trading platforms, consideration should be given to shortcomings of the current approach of state-by-state money transmitter licensure that leaves gaps in protection for virtual currency traders and investors. Any proposed Federal regulation of virtual currency platforms should be carefully tailored to the risks posed by relevant trading activity and enhancing efforts to prosecute fraud and manipulation. Appropriate Federal oversight may include: data reporting, capital requirements, cyber security standards, measures to prevent fraud and price manipulation and anti-money laundering and “know your customer” protections. Overall, a rationalized federal framework may be more effective and efficient in ensuring the integrity of the underlying market.

Conclusion

We are entering a new digital era in world financial markets. As we saw with the development of the Internet, we cannot put the technology genie back in the bottle. Virtual currencies mark a paradigm shift in how we think about payments, traditional financial processes, and engaging in economic activity. Ignoring these developments will not make them go away, nor is it a responsible regulatory response. The evolution of these assets, their volatility, and the interest they attract from a rising global millennial population demand serious examination.

With the proper balance of sound policy, regulatory oversight and private sector innovation, new technologies will allow American markets to evolve in responsible ways and continue to grow our economy and increase prosperity. This hearing is an important part of finding that balance.

Thank you for inviting me to participate.

#####

³⁴ See *supra* note 5.

Appendix A

CFTC Enforcement Activities: Fiscal Year (FY) 2017 Year Through the Present

Overview of FY 2017

In the fiscal year that ended September 30, 2017, the CFTC brought 49 enforcement-related actions, which included significant actions to root out manipulation and spoofing and to protect retail investors from fraud. The CFTC also pursued significant and complex litigation, including cases charging manipulation, spoofing, and unlawful use of customer funds. The CFTC obtained orders totaling \$412,726,307 in restitution, disgorgement and penalties. Specifically, in the fiscal year, the CFTC obtained \$333,830,145 in civil monetary penalties and \$78,896,162 million in restitution and disgorgement orders. Of the civil monetary penalties imposed, the CFTC collected and deposited at the U.S. Treasury more than \$265 million.

Retail Fraud

The CFTC brought a significant number of retail fraud actions in FY 2017 (20 out of the 49). For example, in February 2017, the CFTC filed and settled charges against Forex Capital Markets LLC for \$7 million for defrauding retail foreign exchange customers over a five year time period by concealing its relationship with its most important market maker and misrepresenting that its platform had no conflicts of interests with its customers. That month the CFTC also brought an action charging Carlos Javier Ramirez, Gold Chasers, Inc., and Royal Leisure International, Inc. with misappropriating millions in customer funds and engaging in fraudulent sales solicitations in connection with a Ponzi scheme involving the purported purchase of physical gold.

In May 2017, the CFTC filed charges against an individual and his company with defrauding 40 investors out of at least \$13 million in connection with a commodity pool they operated; investors included family members and members of his church. In June 2017, the CFTC filed charges against two individuals and their company with fraudulently soliciting customers, including at a church gathering, and defrauding them out of more than \$11 million. The pair was also arrested by the Federal Bureau of Investigation (FBI) on related criminal charges.

In September 2017, the CFTC filed one of the largest precious metals fraud cases in the history of the Commission. As alleged, the Defendants defrauded thousands of retail customers—many of whom are elderly—out of hundreds of millions of dollars as part of a multi-year scheme in connection with illegal, off-exchange leveraged precious metal transactions.

Market Manipulation

In February 2017, the CFTC settled with RBS for \$85 million for attempted manipulation of ISDAFIX, a leading global benchmark for interest rate swaps and related derivatives. The CFTC

also brought actions against The Royal Bank of Scotland plc and Goldman Sachs Group, Inc. and Goldman, Sachs & Co. for attempted manipulation of the ISDAFIX, resulting in \$85 million and \$120 million in penalties, respectively. In February 2018, the CFTC settled with Deutsche Bank Securities Inc. for \$70 million for attempted manipulation of ISDAFIX.

Since 2012, the CFTC has imposed over \$5 billion in penalties against banks and brokers with respect to benchmark manipulation settlements.

Disruptive Trading

In November 2016, the CFTC entered into a consent order with Navinder Singh Sarao and Nav Sarao Futures Limited PLC to settle allegations related to the 2010 flash crash for \$25.7 million in monetary sanctions, \$12.9 million in disgorgement, and a permanent trading and registration ban. In December 2016, the CFTC settled with trading company 3Red and trader Igor Oystacher imposing a \$2.5 million penalty, a monitor for three years, and requiring the use of certain trading compliance tools for intentionally and repeatedly engaging in a manipulative and deceptive spoofing scheme while placing orders for and trading futures contracts on multiple registered entities.

In January 2017, the CFTC fined Citigroup \$25 million for failing to diligently supervise the activities of its employees and agents in conjunction with spoofing orders in the U.S. Treasury futures markets. Later that year, in July 2017, the CFTC entered into its first non-prosecution agreements (NPA) with three former Citigroup traders who admitted to spoofing in the U.S. Treasury futures markets in 2011 and 2012. The NPAs emphasize the traders' timely and substantial cooperation, immediate willingness to accept responsibility for their misconduct, material assistance provided to the CFTC's investigation of Citigroup, and the absence of a history of prior misconduct.

In January 2018, in conjunction with the Department of Justice (DOJ) and FBI, the CFTC announced criminal and civil enforcement actions against three banks and six individuals involved in commodities fraud and spoofing schemes. The banks were fined \$45.6 million in penalties.

Virtual Currency

In September 2017, as part of its work to identify and root out bad actors in the virtual currency markets, the CFTC brought its first virtual currency anti-fraud enforcement action in Gelfman Blueprint, Inc., which charged an individual and his corporation with fraud, misappropriation, and issuing false account statements in connection with operating a Bitcoin Ponzi scheme.

In January 2018, the CFTC brought three virtual currency enforcement actions: (i) My Big Coin Pay Inc., which charged the defendants with commodity fraud and misappropriation related to

the ongoing solicitation of customers for a virtual currency known as My Big Coin; (ii) The Entrepreneurs Headquarters Limited, which charged the defendants with a fraudulent scheme to solicit Bitcoin from members of the public, misrepresenting that customers' funds would be pooled and invested in products including binary options, making Ponzi-style payments to commodity pool participants from other participants' funds, misappropriating pool participants' funds, and failing to register as a Commodity Pool Operator; and (iii) CabbageTech, Corp., which charged the defendants with fraud and misappropriation in connection with purchases and trading of Bitcoin and Litecoin.

APPENDIX B

Virtual Currency Educational Materials and Outreach Activities

CFTC's Bitcoin web page Resources

Launched on December 15, 2017, the CFTC now has a dedicated web page, www.cftc.gov/bitcoin, where the public can access educational materials on the CFTC's regulatory oversight authority of virtual currencies and ways to avoid fraud in the virtual currency space.

Current resources available on www.cftc.gov/bitcoin :

- “CFTC Backgrounder on Oversight of and Approach to Virtual Currency Futures Markets”
- LabCFTC's Virtual Currency Primer
- *CFTC Talks* Virtual Currency Podcast, “Roundtable with CFTC leaders on Bitcoin”;
- Self-Certification Fact Sheet
- Customer Advisories on “Understand the Risks of Virtual Currency Trading” and “Beware ‘IRS Approved’ Virtual Currency IRAs”

Forthcoming resources to be featured on www.cftc.gov/bitcoin:

- Customer Advisories (under development; issuance expected in February 2018)
 - Bitcoin pump-and-dump schemes
 - Avoiding fraud in Bitcoin-to-gold trades
- Brochures (available digitally and printed in mid-February 2018):
 - “Virtual Currency”
 - 6-paneled brochure on the definition of virtual currencies, the risks associated with them, and ways to avoid fraud
 - “Bitcoin Basics”
 - 2-sided Bitcoin brochure that speaks about the currency's distinct traits, that fact that it is a commodity, and recommendations for spotting fraud

Virtual Currency Outreach Activities by Audience

- Reaching retail investors and industry professionals via in-person presentations at industry events, conferences and trade shows
- Targeting seniors, vulnerable populations and those who serve them:
 - Connecting national non-profits who serve seniors and vulnerable populations to relevant CFTC virtual currency materials to use for their constituent outreach and communications
 - Distribution of both digital and print virtual currency materials to state regulators for their fraud prevention outreach
 - Participation in trainings for intermediaries, such as library staff, to educate them on the CFTC's fraud prevention resources to protect and assist their constituencies

- Outreach to key virtual currency demographics, such as Millennials, through digital communications designed to engage these demographics through channels and in forums they are predisposed to engage
- Engaging the general public through institutional partnerships and direct communication:
 - Working with other federal financial regulators and self-regulatory organizations to hold joint outreach activities, such as webinars, educational campaigns and community-level outreach, to build public awareness of the CFTC’s virtual currency resources
 - Utilizing print and radio features to reach the public through media placements

Appendix C

October 17, 2017



A CFTC Primer on Virtual Currencies



CFTC

Please note that LabCFTC cannot and will not provide legal advice. If you have specific questions regarding your activities and whether they conform to legal or regulatory requirements, you should consult with a qualified lawyer or appropriate expert. LabCFTC has no independent authority or decision-making power, and cannot independently provide, or create an expectation for, legal or regulatory relief. Communications from LabCFTC shall not create estoppel against CFTC or other enforcement actions. Any formal requests for relief must be addressed by relevant CFTC staff or, as necessary, by the Commission. LabCFTC will work with entities on such requests with the appropriate offices through established processes.

1



Contents

This primer format is intended to be an educational tool regarding emerging FinTech innovations. It is not intended to describe the official policy or position of the CFTC, or to limit the CFTC's current or future positions or actions. The CFTC does not endorse the use or effectiveness of any of the financial products in this presentation. It is organized as follows:

- **Overview**
 - What is a Virtual Currency?
 - Bitcoin and Related Technologies
 - Potential Uses of Virtual Currencies and Blockchain Technologies
 - **The Role of the CFTC**
 - The CFTC's Mission
 - Sample Permitted and Prohibited Activities
 - ICOs, Virtual Tokens, and CFTC Oversight
 - **Risks of Virtual Currencies**
 - Operational Risks
 - Speculative Risks
 - Cybersecurity Risks
 - Fraud and Manipulation Risks
-



OVERVIEW OF VIRTUAL CURRENCIES



What is a Virtual Currency?

- Although precise definitions offered by others are varied, an IRS definition provides us with a general idea:
 - “Virtual currency is a digital representation of value that functions as a **medium of exchange, a unit of account, and/or a store of value.**
 - In some environments, it operates like ‘real’ currency . . . but it **does not have legal tender status** [in the U.S.].
 - Virtual currency that has an equivalent value in real currency, or that acts as a substitute for real currency, is referred to as ‘convertible’ virtual currency. **Bitcoin is one example of a convertible virtual currency.**
 - Bitcoin can be digitally traded between users and can be purchased for, or exchanged into, U.S. dollars, Euros, and other real or virtual currencies.”[†]

[†]IRS Notice 2014-21, available at <https://www.irs.gov/businesses/small-businesses-self-employed/virtual-currencies> (emphasis added). Please note that this definition is not a statement of the Commission’s view, and is instead offered as an aid to enhance public understanding of virtual currencies. We further note that one prominent type of virtual currency is cryptocurrency. Cryptocurrency has been described as “an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.” Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (Oct. 31, 2008), available at <https://bitcoin.org/bitcoin.pdf>.



What is Bitcoin?

- Bitcoin is currently the largest convertible virtual currency by market capitalization (close to \$72 billion in August 2017)[†]
- Bitcoin was created in 2008 by a person or group that used the name “Satoshi Nakamoto,” with the belief that:
“[w]hat is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.”
- Bitcoin:
 - Is “pseudonymous” (or partially anonymous) in that an individual is identified by an alpha-numeric public key/address;
 - Relies on cryptography (and unique digital signatures) for security based on public and private keys and complex mathematical algorithms;
 - Runs on a decentralized peer-to-peer network of computers and “miners” that operate on open-source software and do “work” to validate and irrevocably log transactions on a permanent public distributed ledger visible to the entire network;
 - Solves the lack of trust between participants who may be strangers to each other on a public ledger through the transaction validation work noted in the sub-bullet above; and
 - Enables the transfer of ownership without the need for a trusted, central intermediary.

[†] Paul Vigna, *Bitcoin, Valued Like a Cool Blue Chip, Trading Like a Hot Small Cap*, Wall Street Journal (Aug. 29, 2017), available at <https://blogs.wsj.com/moneybeat/2017/08/28/bitcoin-valued-like-a-blue-chip-trading-like-a-small-cap/>. It is important to note that there are many other virtual currencies with sizeable market capitalizations that are built upon various Blockchain technologies, but may have different characteristics or functionalities than Bitcoin, including Ethereum (or Ether), Litecoin, and Ripple.



What is the Difference between Public and Private Ledger Systems?

- Certain virtual currencies operate on public distributed ledger systems that capture “blocks” of transactions – there is no inherent trust in this decentralized system.
 - Virtual currencies create an economic incentive for dispersed, independent, computers, or groups of computers, around the world to confirm transactions and perform verifiable “work” (that creates consensus) to publish a new block of transactions on the public ledger in exchange for a payment of the applicable virtual currency.

 - Private / permissioned distributed ledger networks typically have some degree of trust between participants.
 - Private ledger systems allow a network of known participants to share transaction information between themselves more efficiently.
 - While cryptography and consensus may still be involved in private ledger systems, these systems do not necessarily involve a virtual currency that may serve as the economic incentive for miner or validator participation in public networks.
-



Sample Potential Use Cases of Virtual Currencies

- **Store of Value**
 - Like precious metals, many virtual currencies are a “non-yielding” asset (meaning they do not pay dividends or interest), but they may be more fungible, divisible, and portable
 - Limited or finite supply of virtual currencies may contrast with ‘real’ (fiat) currencies
 - **Trading**
 - Trading in virtual currencies may result in capital gains or losses
 - Note that trading in virtual currencies may involve significant speculation and volatility risk (see Virtual Currency Risks section below)
 - **Payments and Transactions**
 - Some merchants and online stores are accepting virtual currencies in exchange for physical and digital goods (i.e., payments)
 - Some public Blockchain systems rely on the payment of fees in virtual currency form in order to power the network and underlying transactions
 - **Transfer / Move Money**
 - Domestic and international money transfer (e.g., remittances) in order to increase efficiencies and potentially reduce related fees
-



Sample Potential Use Cases of Blockchain/DLT Technology

Blockchain, or distributed ledger technology,* underpins many virtual currencies, but can also be used within private, permissioned ledger systems – versions of public and private systems may be used by:

- **Financial Institutions**
 - Trading & Payment Platforms / Clearing and Settlement
 - Regulatory Reporting, Compliance & Audit
 - Know Your Customer (KYC) / Anti-Money Laundering (AML)
 - Repurchase Agreement Transactions (“Repos,” i.e., short-term borrowing of securities)
- **Governments**
 - General Records Management
 - Title & Ownership Records Management (e.g., real property deeds and title transfer)
 - Regulatory Reporting and Oversight
- **Cross-Industry**
 - Smart Contracts (i.e., self executing agreements)
 - Resource / Asset Sharing Agreements (e.g., allowing rental of a personal car left behind during a vacation or allowing rental of excess computer or data storage)
 - Digital Identity (e.g., proof of identity when entering into a contract)

* See generally Marco Iansiti and Karim R. Lakhani, *The Truth About Blockchain*, Harvard Business Review (Jan-Feb 2017), available at <https://hbr.org/2017/01/the-truth-about-blockchain> (for a general overview of how a public Blockchain works).



THE ROLE OF THE CFTC



The CFTC's Mission

- The mission of the CFTC is to foster open, transparent, competitive, and financially sound markets. By working to avoid systemic risk, the Commission aims to protect market users and their funds, consumers, and the public from fraud, manipulation, and abusive practices related to derivatives and other products that are subject to the Commodity Exchange Act (CEA).
 - To foster the public interest and fulfill its mission, the CFTC will act:
 - To deter and prevent price manipulation or any other disruptions to market integrity;
 - To ensure the financial integrity of all transactions subject to the CEA and the avoidance of systemic risk;
 - To protect all market participants from fraudulent or other abusive sales practices and misuse of customer assets; and
 - To promote responsible innovation and fair competition among boards of trade, other markets, and market participants.
 - Responsible innovation is market-enhancing.
-



Virtual Currencies are Commodities

- The definition of “commodity” in the CEA is broad.
 - It can mean a physical commodity, such as an agricultural product (e.g., wheat, cotton) or natural resource (e.g., gold, oil).
 - It can mean a currency or interest rate.
 - The CEA definition of “commodity” also includes “all services, rights, and interests . . . in which contracts for future delivery are presently or in the future dealt in.”
- The CFTC first found that Bitcoin and other virtual currencies are properly defined as commodities in 2015.‡
- The CFTC has oversight over futures, options, and derivatives contracts.
- The CFTC’s jurisdiction is implicated when a virtual currency is used in a derivatives contract, or if there is fraud or manipulation involving a virtual currency traded in interstate commerce.
 - Beyond instances of fraud or manipulation, the CFTC generally does not oversee “spot” or cash market exchanges and transactions involving virtual currencies that do not utilize margin, leverage, or financing.

‡ See, In the Matter of: Coinflip, Inc., d/b/a Derivabit, and Francisco Riordan, CFTC Docket No. 15-29, available at <http://www.cftc.gov/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcoinfliporder09172015.pdf>.



Examples of Permitted Activities

- TeraExchange, LLC, a Swap Execution Facility (“SEF”) registered with the CFTC, entered in to the virtual currency market in 2014 by listing a Bitcoin swap for trading. Trading on a SEF platform is limited to “eligible contract participants,” a type of sophisticated trader, which includes various financial institutions and persons, with assets above specified statutory minimums.
 - North American Derivatives Exchange Inc. (“NADEX”), a designated contract market (“DCM”), listed binary options based on the Tera Bitcoin Price Index from November 2014 to December 2016. Retail customers may trade on NADEX.
 - LedgerX, LLC (“LedgerX”) registered with the CFTC as a SEF and Derivative Clearing Organization (“DCO”) in July 2017. It plans to list digital currency options.
-



Examples of Prohibited Activities[‡]

- Price manipulation of a virtual currency traded in interstate commerce.
- Pre-arranged or wash trading in an exchange-traded virtual currency swap or futures contract.
- A virtual currency futures or option contract or swap traded on a domestic platform or facility that has not registered with the CFTC as a SEF or DCM.
- Certain schemes involving virtual currency marketed to retail customers, such as off-exchange financed commodity transactions with persons who fail to register with the CFTC.

[‡]Please note that this is not an exhaustive list of prohibited activities.



ICOs, Virtual Tokens, and CFTC Oversight

- The Securities and Exchange Commission (“SEC”) recently released a report about an Initial Coin Offering or “ICO” (the “DAO Report”).[‡]
- The DAO Report explains that “The DAO” is an example of a “Decentralized Autonomous Organization,” which is a “virtual” organization embodied in computer code and executed on a distributed ledger or blockchain.
- Investors exchanged Ether, a virtual currency, for virtual DAO “Tokens” to fund projects in which the investors would share in anticipated earnings. DAO Tokens could be resold on web-based platforms.
- Based on the facts and circumstances, the SEC determined that DAO Tokens are “securities” under the federal securities laws.
- There is no inconsistency between the SEC’s analysis and the CFTC’s determination that virtual currencies are commodities and that virtual tokens may be commodities or derivatives contracts depending on the particular facts and circumstances.
 - The CFTC looks beyond form and considers the actual substance and purpose of an activity when applying the federal commodities laws and CFTC regulations

[‡] See Release No. 81207, Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO, available at <https://www.sec.gov/litigation/investreport/34-81207.pdf>.



RISKS OF VIRTUAL CURRENCIES



Virtual Currencies Have Risks

- While virtual currencies have potential benefits, this emerging space also involves various risks, including:
 - Operational Risks
 - Cybersecurity Risks
 - Speculative Risks
 - Fraud and Manipulation Risks
 - Virtual currencies are relatively unproven and may not perform as expected (for example, some have questioned whether public distributed ledgers are in fact immutable).
 - Investors and users of virtual currencies should educate themselves about these and other risks before getting involved.
-



Virtual Currency: Operational Risk

- *Conduct extensive research before giving any money or personal information to a virtual currency platform.*
 - The virtual currency marketplace is comprised of many different platforms where you can convert one type of virtual currency into another or into real currency, if offered.
 - Many of these platforms are not subject to the supervision which applies to regulated exchanges. For example, if they engage in only certain spot or cash market transactions and do not utilize margin, leverage, or financing, they may be subject to federal and state money transmission and anti-money laundering laws, but they do not have to follow all the rules that regulated exchanges operate under.
 - Some virtual currency platforms may be missing critical system safeguards and customer protection related systems; without adequate safeguards, customers may lose some or all of their virtual assets.
-



Virtual Currency: Cybersecurity Risk

- *Keep your property in safe accounts and carefully verify digital wallet addresses.*
 - Some platforms may “commingle” (mix) customer assets in shared accounts (at a bank for real currency or a digital wallet for virtual currency). This may affect whether or how you can withdraw your currency.
 - Depending on the structure and security of the digital wallet, some may be vulnerable to hacks, resulting in the theft of virtual currency or loss of customer assets.
 - If a bad actor gains access to your private key, it can take your virtual currency with limited or no recourse
 - When transferring virtual currency, be sure to confirm the destination wallet address, even when using “copy and paste.” It is possible for hackers to change digital wallet addresses on your computer.
-



Virtual Currency: Speculative Risk

- *Only invest what you are willing and able to lose.*
- The virtual currency marketplace has been subject to substantial volatility and price swings.
- An individual or coordinated group trading a large amount of virtual currency at once could affect the price, depending on the overall amount of trading in the marketplace.
- Periods of high volatility with inadequate trade volume may create adverse market conditions, leading to harmful effects such as customer orders being filled at undesirable prices.
- Some advertisements promise guaranteed returns – this can be a common tactic with fraudulent schemes.



Virtual Currency: Fraud & Manipulation Risk

- *Carefully research the platform you want to use, and pay close attention to the fee structure and systems safeguards.*
 - Unregistered virtual currency platforms may not be able to adequately protect against market abuses by other traders.
 - For example, recent news articles discuss potential “spoofing” activity and other manipulative behavior that can negatively affect prices
 - Some virtual currency platforms may be selling you virtual currency directly from their own account – these types of transactions may give the platform unfair advantages and sometimes resemble fraudulent “bucket shop” schemes.
 - There is also a risk of Ponzi schemers and fraudsters seeking to capitalize on the current attention focused on virtual currencies.
-

Appendix D

Consumer and Market Advisories on Investing in Bitcoin and other virtual Currencies



Customer Advisory: Understand the Risks of Virtual Currency Trading

The U.S. Commodity Futures Trading Commission (CFTC) is issuing this customer advisory to inform the public of possible risks associated with investing or speculating in virtual currencies or recently launched Bitcoin futures and options.

Virtual currency is a digital representation of value that functions as a medium of exchange, a unit of account, or a store of value, but it does not have legal tender status. Virtual currencies are sometimes exchanged for U.S. dollars or other currencies around the world, but they are not currently backed nor supported by any government or central bank. Their value is completely derived by market forces of supply and demand, and they are more volatile than traditional fiat currencies. Profits and losses related to this volatility are amplified in margined futures contracts.

For hedgers – those who own Bitcoin or other virtual currencies and who are looking to protect themselves against potential losses or looking to buy virtual currencies at some point in the future – futures contracts and options are intended to provide protection against this volatility. However, like all futures products, speculating in these markets should be considered a high-risk transaction.

Bitcoin is a Commodity

Bitcoin and other virtual currencies have been commodity under the Commodity Exchange Act (CEA). The CEA primarily regulates commodity derivatives contracts that are based on underlying commodities. While its regulatory oversight authority over commodity anti-fraud and manipulation enforcement authority over virtual currency cash markets as a commodity.

What makes virtual currency risky?

Purchasing virtual currencies on the cash market – spending dollars to purchase Bitcoin for your

personal wallet, for example – comes with a number of risks, including:

- most cash markets are not regulated or supervised by a government agency;
- platforms in the cash market may lack critical system safeguards, including customer protections;
- volatile cash market price swings or flash crashes;
- cash market manipulation;
- cyber risks, such as hacking customer wallets; and/or
- platforms selling from their own accounts and putting customers at an unfair disadvantage.

It's also important to note that market changes that affect the cash market price of a virtual currency may ultimately affect the price of virtual currency futures and options.

When customers purchase a virtual currency-based futures contract, they may not be entitled to receive the actual virtual currency, depending on the particular contract.

Under most futures contracts currently being offered, customers are buying the right to receive or pay the amount of an underlying commodity value in dollars at some point in the future. Such futures contracts are said to be “cash settled.” Customers will pay or receive (depending on which side of the contract they have taken –

long or short) the dollar equivalent of the virtual currency based on an index or auction price specified in the contract. Thus, customers should inform themselves as to how the index or auction prices used to settle the contract are determined.

Entering into futures contracts through leveraged accounts can amplify the risks of trading the product. Typically, participants only fund futures contracts at a fraction of the underlying commodity price when using a margin account. This creates “leverage,” and leverage amplifies the underlying risk, making a change in the cash price even more significant. When prices move in the customers’ favor, leverage provides them with more profit for a relatively small investment. But, when markets go against customers’ positions, they will be forced to refill their margin accounts or close out their positions, and in the end may lose more than their initial investments.

Beware of related fraud

Virtual currencies are commonly targeted by hackers and criminals who commit fraud. There is no assurance of recourse if your virtual currency is stolen. Be careful how and where you store your virtual currency. The CFTC has received complaints about virtual currency exchange scams, as well as Ponzi and “pyramid” schemes.

If you decide to buy virtual currencies or derivatives based on them, remember these tips:

- If someone tries to sell you an investment in options or futures on virtual currencies, including Bitcoin, verify they are registered with the CFTC. Visit [SmartCheck.gov](https://www.smartcheck.gov) to check registrations or learn more about common investment frauds.
- Remember—much of the virtual currency cash market operates through Internet-based trading platforms that may be unregulated and unsupervised.
- Do not invest in products or strategies you do not understand.
- Be sure you understand the risks and how the product can lose money, as well as the likelihood of loss. Only speculate with money you can afford to lose.
- There is no such thing as a guaranteed investment or trading strategy. If someone tells you there is no risk of losing money, do not invest.

- Investors should conduct extensive research into the legitimacy of virtual currency platforms and digital wallets before providing credit card information, wiring money, or offering sensitive personal information.
- The SEC has also warned that some token sales or initial coin offerings (ICOs) can be used to improperly entice investors with promises of high returns.¹

If you believe you may have been the victim of fraud, or to report suspicious activity, contact us at 866.366.2382 or visit [CFTC.gov/TipOrComplaint](https://www.cftc.gov/TipOrComplaint).

¹ See https://www.sec.gov/oiea/investor-alerts-and-bulletins/ib_coinofferings.

The CFTC has provided this information as a service to investors. It is neither a legal interpretation nor a statement of CFTC policy. If you have questions concerning the meaning or application of a particular law or rule, consult an attorney.