Comment on Commodity Futures Trading Commission Notice of Meeting: *Technology Advisory Committee,* 84 FR 4,449 (Feb. 15, 2019).

Authors:[1] John Hamilton, Daniel Kennedy, and Kelly Todd

Date: April 3, 2019

<div align="center">

Executive Summary

</div>

The Commodity Futures Trading Commission's ("CFTC") Technology Advisory Committee ("TAC") held a public meeting March 27, 2019.[2] At this meeting, the TAC received reports and recommendations from various TAC subcommittees including significant contributions from both the Distributed Ledger Technology and the Virtual Currencies Subcommittees.[3] This Comment responds to a public request for comment in connection with this meeting. We comment to suggest that the CFTC revisit the scope of its self-certification process for approving virtual currency futures.

Specifically, this Comment suggests that the CFTC should consider issues in the underlying spot market when approving virtual currency futures. In support of this position this Comment 1) provides evidence of manipulability of virtual currency spot markets and points to past manipulation; 2) questions virtual currency futures contracts' ability to account for the effect of "hard forks" on settlement prices; and 3) points to textual and parol evidence that indicates these futures contracts are themselves capable of manipulation. Additionally, this Comment provides a primer on blockchain and virtual currencies, as well as an in-depth treatment of little-discussed facets of these technologies that the CFTC may wish to consider in formulating future policy.

---

[1] The authors are graduate students in the Duke Science Regulation Lab, an interdisciplinary course offered through the Duke Law and Graduate Schools. Michael B. Waitzkin, JD, J. H. Pate Skene, JD, PhD, and Sarah Rispin Sedlak, JD, are the faculty members who lead the SciReg Lab. We would also like to thank Lee Reiners, Executive Director of the Duke Law Global Financial Markets Center, for providing valuable technical assistance.

[2] Notice of Meeting, 84 Fed. Reg. 4,449 (Feb. 15, 2019).

[3] *Id.*

Table of Contents

I. INTRODUCTION

A. Who We Are

The Duke Science Regulation Lab ("SciReg Lab") is composed of graduate students from a variety of disciplines at Duke University, including science, law, ethics, and policy. The Science Regulation Lab was originally inspired by the traditional role of *amicus curiae*: to provide a court with unbiased information necessary to reach a binding decision. As an extension of that concept, we now provide government agencies with the scientific and technical information necessary to undertake effective rulemaking.

Modern society requires our government to handle increasingly complex issues when deciding cases or making policy. We, the Duke Science Regulation Lab, believe that the general public benefits from judgments that are based on sound scientific and technical knowledge. To assist decision makers in understanding a scientific or technical matter at hand, the students of the Science Regulation Lab combine their expertise to offer a non-partisan, accurate, and accessible explanatory brief or comment.

The members of the Duke Science Regulation Lab vary in their academic backgrounds. **John Hamilton** is a 2019 JD candidate. **Daniel Kennedy** is a 2019 JD candidate. **Kelly Todd** is a 2019 JD candidate who is jointly pursuing a Master's in Bioethics & Science Policy.

B. CFTC Technology Advisory Committee Notice of Meeting

On February 15, 2019, the Commodity Futures Trading Commission ("CFTC") published a Notice of Meeting informing the public that the CFTC's Technology Advisory Committee ("TAC") would hold a public meeting at the CFTC headquarters in Washington, DC on March 27, 2019.[4] The meeting included presentations and recommendations from the TAC

---

[4] Notice of Meeting, 84 Fed. Reg. 4,449 (Feb. 15, 2019).

subcommittees on Automated and Modern Trading Markets, Distributed Ledger Technology,

Virtual Currencies, and Cyber Security.[5] A significant portion of the meeting was devoted to

virtual currencies and distributed ledger technology.[6] The Notice of Meeting asks for public

comments pertaining to any topics discussed during the meeting.[7]

This comment responds to this request to suggest that the CFTC should consider issues in

the underlying spot market when approving virtual currency futures. Specifically, this comment

1) provides evidence of manipulability of virtual currency spot markets and points to past

manipulation; 2) questions virtual currency futures contracts' ability to account for the effect of

"hard forks" on settlement prices; and 3) points to textual and parol evidence that indicates these

futures contracts are themselves capable of manipulation.

II.   BACKGROUND

A. CTFC & The Technology Advisory Committee

1. CFTC Regulatory Authority and the Role of the TAC

The Commodity Futures Trading Commission ("CFTC") is an independent federal

agency that regulates the commodities futures and options markets and strives to promote

competitive and efficient futures markets while protecting investors against abusive trade

practices.[8] The CFTC has five committees, each headed by a presidentially-appointed and

Senate-confirmed commissioner.[9] The committees focus on agriculture, global markets, energy

---

[5] CFTC, TECHNOLOGY ADVISORY COMMITTEE AGENDA (Mar. 27, 2019), https://www.cftc.gov/sites/default/files/2019-03/tac_032719agenda.pdf.

[6] *See id.*

[7] Notice of Meeting, 84 Fed. Reg. at 4,449.

[8] COMMODITY FUTURES TRADING COMM'N., *Mission & Responsibilities*, CFTC.GOV, https://www.cftc.gov/About/MissionResponsibilities/index.htm (last visited Apr. 3, 2019).

[9] COMMODITY FUTURES TRADING COMM'N., *CFTC Committees*, CFTC.GOV, https://www.cftc.gov/About/CFTCCommittees/index.htm (last visited Apr. 3, 2019).

4

and environmental markets, cooperation between the CFTC and SEC, and technology.[10] The

committees are composed of representatives from different segments of industries, markets, and

consumers. [11]

The CFTC's Technology Advisory Committee ("TAC") is a discretionary advisory

committee. Its activities include holding public meetings, presenting recommendations and

reports to the CFTC, and in general helping the agency to address the implications of new

technology in the financial sectors under its purview.[12] The TAC offers "advice on the

application and utilization of new technologies in financial services and commodity markets, as

well as by market professionals and market users."[13] Moreover, the TAC advises the CFTC to

what extent the agency itself should invest in new technologies in order to competently carry out

its duties. [14]

The advent of financial technology ("FinTech") and virtual currencies are increasingly

pushing the CFTC away from its initial role as a regulator of traditional commodities-related

futures. The CFTC believes that these two technologies are propelling innovation throughout the

global financial community, but also presenting novel challenges for agencies. This makes sense,

considering that the type of innovation the CFTC is facing is quite eclectic in scope, including

cloud computing, lightning-fast algorithmic trading, distributed ledgers, and even AI and

machine learning. These technologies have the potential to transform CFTC-regulated markets

---

[10] *Id.*

[11] James Chen, *Commodity Futures Trading Commission – CFTC*, INVESTOPEDIA,
https://www.investopedia.com/terms/c/cftc.asp (last updated Mar. 6, 2018).

[12] COMMODITY FUTURES TRADING COMM'N, RENEWAL CHARTER OF THE TECHNOLOGY ADVISORY COMMITTEE,
(Oct 14, 2016), https://www.cftc.gov/sites/default/files/idc/groups/public/@aboutcftc/documents/file/tac_charter.pdf.

[13] *Id.*

[14] *Id.*

and the agency itself. The agency, thus, plans to actively keep abreast of, and play a role in the regulation of, these new technologies.[15]

2. *CFTC Regulation of Virtual Currencies*

In 2015, the CFTC labeled bitcoin and other virtual currencies "commodities," as defined by the Commodities Exchange Act ("CEA").[16] Per the CEA, a commodity can be physical, like an agricultural product, a natural resource, like oil, or a currency.[17] The definition also includes "all services, rights, and interests . . . in which contracts for future delivery are presently or in the future dealt in." Because the CFTC possesses the authority to regulate options, futures, and derivative contracts, the agency's jurisdiction is implicated when virtual currencies are used in such derivative contracts, or in connection with a manipulation or fraud involving virtual currencies in interstate commerce. Beyond these instances, the CFTC generally does not oversee "spot"[18] or cash market exchanges that make up the majority of virtual currency trading.[19]

Since designating cryptocurrencies as commodities in 2015, the CFTC has taken several enforcement actions. These include sanctioning unregistered bitcoin futures exchanges, enforcing laws prohibiting "wash trading[20] and prearranged trades on a derivatives platform,"

---

[15] Chen, *supra* note 11.
[16] *See* In re Coinflip, Inc., CFTC No. 15-29 (Sept. 17, 2015), https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcoin-fliprorder09172015.pdf.
[17] Commodities Exchange Act, 17 C.F.R. § 40.2 (2018).
[18] In this case, the market for virtual currencies is the spot market. The value of virtual currency futures contracts is largely derived from the market price of virtual currencies in the spot market. *See Tim Smith, Spot Market*, INVESTOPEDIA https://www.investopedia.com/terms/s/spotmarket.asp (last updated Mar. 11, 2019) (explaining that "the spot market is where financial instruments, such as commodities, currencies and securities, are traded for immediate delivery. Delivery is the exchange of cash for the financial instrument. A futures contract, on the other hand, is based on the delivery of the underlying asset at a future date.").
[19] *A CFTC Primer on Virtual Currencies*, LABCFTC (Oct. 17, 2017), https://www.cftc.gov/sites/default/files/idc/groups/public/%40customerprotection/documents/file/labcftc_primercurrencies100417.pdf.
[20] Wash trading is the selling or buying of a security for the express purpose of introducing misleading information into the market. *See* James Chen, *Wash Trading*, INVESTOPEDIA (Feb. 25, 2019), https://www.investopedia.com/terms/w/washtrading.asp.

publishing guidance on the distinction between spot and derivatives markets in the virtual

currency context, and confronting a cryptocurrency Ponzi scheme.[21]

Additionally, the CFTC has permitted the listing of two bitcoin futures products. The

Chicago Mercantile Exchange (CME) and Chicago Board of Options Futures Exchange (CBOE)

both self-certified contracts for cash-settled bitcoin futures products in 2017.[22] Under the

CFTC's self-certification process, an exchange may list a new futures contract one day after it

submits a certification to the CFTC that the futures contract complies with the CEA, unless the

CFTC objects to the listing within that 24-hour period.[23]

Prompted by questions and concerns about the use of self-certification for virtual

currency products,[24] the CFTC published a "Backgrounder on Oversight of and Approach to

Virtual Currency Markets."[25] In this backgrounder, the CFTC argues that it has limited

jurisdiction to stay a self-certification.[26] Specifically, the CFTC asserts that its authority over

self-certified futures contracts is limited to reviewing the contracts themselves, and that it is not

appropriate for the CFTC to consider the underlying virtual currency spot market when a request

for self-certification is made.

---

[21] COMMODITY FUTURES TRADING COMM'N., CFTC BACKGROUNDER ON OVERSIGHT OF AND APPROACH TO VIRTUAL CURRENCY MARKETS (Jan. 4, 2018), https://www.cftc.gov/sites/default/files/idc/groups/public/%40custom erprotection/documents/file/backgrounder_virtualcurrency01.pdf.

[22] *Id.*

[23] *Id.*

[24] *See, e.g.*, Gabriel T. Rubin, *Rise of Bitcoin Futures Prompts Regulator to Revisit Hands-Off Approach*, WALL ST. J. (Jan. 31, 2018), https://www.wsj.com/articles/rise-of-bitcoin-futures-prompts-regulator-to-revisit-hands-off-approach-1517394600.

[25] COMMODITY FUTURES TRADING COMM'N., *supra* note 21.

[26] *Id.* at 2.

B. Blockchain Technology

Blockchain technology is the backbone of bitcoin and other virtual currencies and was invented to serve as the public transaction ledger of bitcoin.[27]

A blockchain is essentially a distributed public ledger of all transactions that have been "executed and shared among participating parties."[28] Each transaction in this ledger is verified by a majority of the participants in the system, and information cannot be erased once entered.[29] Blockchain technology is revolutionary because it allows a system to operate as a decentralized network that does not require a central server, meaning the network does not have a single point of failure.[30] Further, blockchain transactions cannot be reversed, and any changes to the blockchain are visible by all parties within the system, making blockchain systems inherently transparent.[31] For virtual currencies, these features solve the "double-spend" problem by ensuring a unit of currency can only be transferred to one person at a time without needing to a central depository to confirm that specific unit of currency is only being used in one transaction.[32]

At its basic level, blockchain is quite literally a chain of blocks. Each "block" is a block of digital information. Blocks contains three types of information: 1) information about transactions such as the date, time and amount of the transaction; 2) information about the parties participating in the transaction, and 3) information unique to that particular block, such as its

---

[27] Marco Iansiti & Karim R. Lakhani, *The Truth About Blockchain*, HARV. BUS. REV. (Feb. 2017), *available at* https://hbr.org/2017/01/the-truth-about-blockchain (citing Satoshi Nakamoto, *BitCoin: A Peer-to-Peer Electronic Cash System*, https://bitcoin.org/bitcoin.pdf.).

[28] Michael Crosby et al., *Blockchain Technology: Beyond Bitcoin*, 2 APPLIED INNOVATION REV. 6, 8 (June 2016), *available at* https://j2-capital.com/wp-content/uploads/2017/11/AIR-2016-Blockchain.pdf.

[29] *Id.*

[30] Mark Pilkington, *Blockchain Technology: Principles and Applications, in* RESEARCH HANDBOOK ON DIGITAL TRANSFORMATIONS 226 (F. Xavier Olleros & Majlinda Zhegu, eds. 2016).

[31] *Id.* at 226–27.

[32] *Id.*

"hash" value[33] and the hash of its "parent block". [34] Importantly, each block can contain information of type 1) and 2) relating to multiple transactions.

Each time a transaction occurs, that transaction is timestamped and must be verified. Blockchain transactions are verified by a network of millions of computers that voluntarily connect to a virtual currency's network. These computers are commonly referred to in blockchain parlance as "nodes." The actual verification process is somewhat of a race among these nodes to perform a cryptographic calculation. First, multiple transactions occurring around the same time are placed into a single block. Then, the nodes run programs in an attempt to be the first to successfully perform a cryptographic "hash" calculation, which will derive a hash value unique to that block.[35] For bitcoin, it takes an average of ten minutes to solve such a calculation and successfully hash a block.[36] When a block is successfully hashed, the transactions in that block are verified and the block is broadcast to the rest of the network.[37]

Once a block is successfully verified through the hashing process, it is added as the newest block in the blockchain – it is connected to the end of the "chain".[38] When a new block is added it becomes publicly available and is chained to the preceding block by incorporating that blocks hash value.[39] Because any change to the data in a block would also change its hash value,

---

[33] A hash code is a block's unique identifier. Each has code is created by a mathematical function that takes the digital information of that block and generates a string of letters and numbers from it. Any change to the digital information stored inside of a block would change its hash value. Because blocks are linked by their hash value, such a change would be a red flag within the blockchain.

[34] Crosby et al., *supra* note 28 at 9. A "parent block" is the block immediately preceding the block in the chain.

[35] *See supra* note 33 for a discussion of the implications of the hash calculation. *Id.*

[36] Crosby et al., *supra* note 28 at 9–10.

[37] This race to be the first computer to hash a transaction is what is commonly known as bitcoin "mining" and the computer who successfully hashes a block first is rewarded with bitcoin.

[38] Crosby et al., *supra* note 28 at 10.

[39] *Id*. at 11.

the chaining of blocks by reference to hash value ensures that any change to a previous block would be noticed.[40]

Accordingly, to successfully hack a single transaction, one would need to change the block in which that transaction was recorded and every block following it in the blockchain. This would take an enormous amount of computing power and time, making a successful attack on data stored in a blockchain improbable.[41] Thus, once a block is added to the blockchain, it becomes almost impossible to edit or delete the transactions in that block.

C. **Introduction to Cryptocurrencies and other Virtual Currencies**

Cryptocurrencies are digital assets that use cryptography, an encryption technique "that converts data into a format that is unreadable for an unauthorized user, allowing it to be transmitted without unauthorized entities decoding it back into a readable format," and blockchain technology.[42] Initially, there was only one cryptocurrency, bitcoin, which came into being in 2008.[43] The impetus for the creation of bitcoin, and virtually all other virtual currencies that followed, was to remedy three of the primary perceived flaws in the financial system and fiat currencies, which are discussed below.[44]

The first, and perhaps most significant, advantage of cryptocurrencies over traditional currencies is that they are decentralized, meaning there is no central hub within which transaction data is stored. Instead, information regarding any cryptocurrency is stored on hard drives and servers all over the world. This arrangement is designed to ensure that no individual

---

[40] *See id.*

[41] *See id* at 11–12.

[42] Jeffrey Mazer, *Demystifying Cryptocurrencies, Blockchains, and ICOs*, TOPTAL, https://www.toptal.com/finance/market-research-analysts/cryptocurrency-market.

[43] *An Abridged History of Bitcoin*, N.Y. TIMES (Nov. 19, 2013), http://www.nytimes.com/interactive/technology/bitcoin-timeline.html#/#time284_8156.

[44] Sean Williams, *Cryptocurrencies Explained, in Plain English*, MOTLEY FOOL (Jan. 2, 2018), https://www.fool.com/investing/2018/01/02/cryptocurrencies-explained-in-plain-english.aspx.

10

or institution retains control of the currency; it also safeguards against cyber-attacks and theft. The lack of a central authority issuing a cryptocurrency ensures that there is no "middleman" in cryptocurrency transactions, meaning the costs associated with the transactions will be lower. Moreover, blockchain-based currencies have the potential to allow their users to settle transactions significantly faster than banks currently do, as transactions are processed almost instantaneously.[45]

Cryptocurrencies, unlike many other currencies, are not backed by an asset—like gold— or a guarantee from a government. Nor are they pegged to any other metric. Instead, they exist entirely digitally across a decentralized network of thousands of computers. Cryptocurrencies are passed between individuals, making them "peer-to-peer" in important ways traditional currencies are not; there is no need to place trust in a central intermediary, like a bank, in order to ensure payment. Payments are verified by a host of individuals and the underlying blockchain itself, rather than an institution.[46]

Verification of many crypto transactions falls on a group of individuals known as "miners" that possess powerful computers and compete with other miners to solve extremely complex mathematical equations that are designed to protect data on the cryptocurrency's ledger. The first miner that solves these equations—which verify the transactions on the ledger— receives a reward in the form of a cryptocurrency. This process is known as "proof of work." The mining process produces new cryptocurrency each time a transaction is verified.

One of the most significant differences between cryptocurrencies and traditional investments is that, unlike buying a share of a public company, which grants you a fractional

---

[45] *Id.*
[46] Ray King, *What is Cryptocurrency? Your Complete Crypto ABC*, BIT DEGREE, https://www.bitdegree.org/tutorials/what-is-cryptocurrency/#Crypto_Definition (last updated Jan. 2, 2019).

ownership of the underlying company, buying a cryptocurrency does not grant you ownership of the underlying ledger.

Virtual currency exchanges allow individuals to buy and sell cryptocurrencies for other types of virtual currency or traditional forms of currency. These exchanges are subject to government regulation, and individuals are required to provide proof of identity before opening an account. However, individuals can also engage in peer-to-peer trading of currencies, akin to over the counter derivative exchanges, which are more anonymous and less subject to regulation.

Virtual currency "wallets" are a requirement for sending and receiving virtual currencies, such as bitcoins. These wallets can be either software or hardware. Hardware wallets tend to be more secure since they allow a user's private keys to be stored offline. A wallet is not used to store cryptocurrency. Instead, ownership of bitcoin is evidenced in the blockchain.[47]

Importantly, while the transactions of a cryptocurrency are recorded on its underlying blockchain, the "key" that is needed to authorize new transactions is located within an individual wallet. When an individual tries to create a new transaction, this key must be entered before the blockchain can authorize it. Losing this key results in losing access to the cryptocurrency associated with it forever.

In spite of popular opinion to the contrary, most cryptocurrencies are not as anonymous as one would think. While no personal information is required to engage in a crypto-transaction, each and every transaction is recorded on the underlying ledger, and often can be traced to the individual. Moreover, the IRS recently successfully sued Coinbase, the largest virtual currency exchange, to turn over the information of thousands of its users that the agency suspected had

---

[47] Gerald P. Dwyer & Norbert J. Michel, *Bits and Pieces: The Digital World of Bitcoin Currency*, HERITAGE FOUND'N (Sept. 16, 2015), http://www.heritage.org/research/reports/2015/09/bits-and-pieces-the-digital-world-of-bitcoin-currency.

evaded capital gains tax. That said, there are specialized "privacy coins," whose sole purpose is to protect the identity of their users.

D. Types of Virtual Currencies

1. Bitcoin

Bitcoin was conceived by an individual—or potentially individuals—using the alias Satoshi Nakamoto in 2009.[48] It is the oldest cryptocurrency and the most stable, though this may not be saying much, as will be discussed *infra.* An individual bitcoin can be purchased in incredibly small increments, as small as 0.00000001 BTC per transaction.[49] The supply of bitcoins is finite and the system was designed so that the mining process produces fewer bitcoins as the years go on.[50] The maximum number of bitcoins is capped at 21 million.[51]

2. Litecoin

Litecoin makes use of the Scrypt encryption algorithm, as opposed to the SHA-256 algorithm that bitcoin uses.[52] This algorithm is simpler and should allow transactions to be confirmed at a higher speed than bitcoin. The amount of Litecoin that is available for mining and circulation is four times the quantity of bitcoin, meaning there will be quadruple the quantity of Litecoin that is accessible compared to bitcoin.[53]

---

[48] *Different Types of Cryptocurrency*, EMPIRICA, http://empirica.io/blog/different-types-cryptocurrency; *An Abridged History of Bitcoin*, *supra* note 43.
[49] Arjun Kharpal, *All You Need to Know About the Top 5 Cryptocurrencies*, CNBC: MARKETS (Dec. 14, 2017), https://www.cnbc.com/2017/12/14/bitcoin-ether-litecoin-ripple-differences-between-cryptocurrencies.html.
[50] Dwyer & Michel, *supra* note 47.
[51] *Id*.
[52] Kharpal, *supra* note 49.
[53] *Id*.

3. Ethereum

Ethereum is backed by a blockchain, much like bitcoin, but the technology is geared more specifically for the development of smart contracts.[54] A smart contract is coded into a blockchain such that "once the terms of the contract are met by each party, a deal will be executed." *Id.* While bitcoin is designed to take third parties out of the payment process, Ethereum can be thought of as trying to eliminate intermediaries that ensure the performance of contractual obligations, like the transfer of title.[55] Many organizations, including Microsoft and JPMorgan have been experimenting with Ether applications.[56]

4. Ripple (RXP)

Ripple is a real-time worldwide settlement network that allows for instant and low-cost international payments.[57] Ripple does not require mining, which distinguishes it from bitcoin.[58] One can only obtain Ripple from registered exchanges, and it is backed by many banks and financial institutions.[59] Importantly, Ripple is distinctive from other virtual currencies in that it was launched by a for-profit corporation in order to "use the concepts behind bitcoin to build a cross-border, interbank payments and settlement network."[60]

E. Futures Contracts

Futures contracts, commonly referred to as futures, are contracts to buy or sell an asset at a pre-determined price at a specified time in the future.[61] The purchaser of a futures contract

---

[54] *Id.*

[55] Alyssa Hertig, *What is Ethereum?*, COINDESK, https://www.coindesk.com/information/what-is-ethereum.

[56] Kharpal, *supra* note 49.

[57] *Different Types of Cryptocurrency*, *supra* note 48.

[58] *Id.*

[59] *Id.*

[60] Paul Vigna, *Meet Ripple, the Currency that is Running Laps Around Bitcoin*, WALL ST. J. (Dec. 29, 2018), https://blogs.wsj.com/moneybeat/2017/12/29/meet-ripple-the-currency-thats-running-laps-around-bitcoin/.

[61] Richard Heckinger, *Derivatives Overview, in* UNDERSTANDING DERIVATIVES: MARKETS AND INFRASTRUCTURE 3–4 (FED. RES. BANK CHI. ed. 2015), *available at* https://www.chicagofed.org/publications/understanding-derivatives/index.

agrees to buy the underlying asset at the date the futures contract expires, while the seller of the futures contract agrees to provide the underlying asset on that date.[62]

Futures trading in the United States began in the mid-19th century with central grain markets that allowed farmers to sell the rights to delivery of agricultural products at a future time.[63] Futures contracts gradually expanded to include non-agricultural commodities such as oil, metals, and energy.[64] Beginning in the 1970's, futures contracts expanded to include currencies, equity indexes, and interest rate products.[65]

As the assets subject to futures contracts evolved over time, so did the use of futures. Futures were originally devised as a way to hedge against risk.[66] A traditional hedger is someone with a business interest in the underlying asset who uses futures to manage pricing risk, typically producer or purchaser of the underlying asset.[67] For example, a cereal manufacturer may buy rice and sugar futures to protect themselves from the possibility of a price increase in their two principal ingredients. Currently, speculators represent a large portion of the futures market. These speculators willingly accept the pricing risk that futures attempt to hedge against in an attempt to profit from favorable price movement.[68] Most of these speculators are professional traders, but anyone can buy and sell futures.[69] Speculators are important to the futures market because they provide market liquidity, allowing hedgers to buy and sell futures quickly when need.[70]

---

[62] *See id.*
[63] CME GROUP, A TRADER'S GUIDE TO FUTURES 4 (2013), https://www.cmegroup.com/education/files/a-traders-guide-to-futures.pdf.
[64] *Id.* at 5
[65] *Id.*
[66] *Id.* at 6
[67] *See id.*
[68] *Id.*
[69] *Id.*
[70] *Id.*

Futures contracts can be settled either through physical delivery of the asset, or by cash payment.[71] Today, most futures contracts are settled through cash payment to avoid the transaction costs associated with physical delivery.[72] In a cash settlement, a payment will be made based on the difference between the contract price and the contractually provided for "reference rate", typically the market price of the asset at the time the futures contract comes due.[73] Accordingly, the individual with a loss pays cash to the individual with a gain. For example, imagine two individuals enter into a futures contract for oil at $50 per barrel, and that oil is trading at $45 per barrel on the settlement date. The purchaser of the futures contract is contractually obligated to buy oil from the seller at $50, which is $5 above the market price, representing a $5 loss to the buyer. On the other side of the transaction, the seller is obtaining $50 for oil that he could sell for only $45 on the open market, representing a $5 gain from entering into the futures contract. Here, the purchaser will pay the seller $5 in cash to settle the contract. If the seller is a speculator, he will simply pocket that $5 gain. If the seller is an oil manufacturer, that $5 will offset the reduced price at which he must sell his oil.[74]

III.   COMMENTS

A. The Manipulability of Virtual Currency Spot Markets

The CFTC should consider issues systemic to virtual currency spot markets when considering the approval of virtual currency futures through the self-certification process. We acknowledge that such a policy change would involve a a two-part decision. First, the CFTC needs to determine whether it has the legal authority to stay a futures contract certification based

---

[71] *See id*. at 12

[72] *Id.*

[73] *See id.*

[74] This assumes the oil manufacturer has a separate contractual obligation to provide oil on the settlement date, a common fact pattern that would cause a hedger to enter into a futures contact.

on issues in the spot market. Second, the CFTC would need to determine that 1) as a factual matter, virtual currency spot markets are particularly susceptible to manipulation and 2) the degree of this susceptibility warrants a policy decision to treat virtual currency futures contracts differently than other futures contracts.

We take no position on the CFTC's legal authority other than to note that 1) CFTC Commissioners have made statements suggesting the self-certification process needs changes,[75] 2) commentators argue that failure to consider issues in the underlying spot market could actually violate the CFTC's statutory mandate that it "…shall list on the contract market only contracts that are not readily susceptible to manipulation,"[76] and 3) the Securities and Exchange Commission ("SEC") has refused to approve the listing of virtual currency Exchange-traded Funds ("ETFs") due to concerns about virtual currency's susceptibility to manipulation while operating under a similar statutory mandate.[77] Rather, in this section we seek to 1) point out characteristics of virtual currency markets that make them susceptible to manipulation, and 2) provide evidence of past manipulation of virtual currency markets. We believe the evidence presented below suggests a more rigorous review of virtual currency futures contracts is warranted.

1. Susceptibility to Manipulation

Because all virtual currency futures to date are cash settled, they can be manipulated by manipulating the reference rate that is used to price the contract. A standard futures manipulation

---

[75] *See, e.g*., Rubin, *supra* note 14 ("'The commission must reconsider its historical regulatory approach to new products,' [a] CFTC Commissioner . . . said Wednesday at a public meeting he chaired that focused on the self-certification process.").

[76] Core Principle 3, 17 C.F.R. § 38.200; *see, e.g.*, Lee Reiners, *Bitcoin Futures: From Self-Certification to Systemic Risk*, 23 N.C. BANKING INST. 61 (2019).

[77] *See, e.g.*, Order Disapproving a Proposed Rule Change to BZX Rule 14.11(e)(4), Exchange Act Release No. 34-80206, 116 S.E.C. Dockets 2746 (Mar. 10, 2017), https://www.sec.gov/rules/sro/batsbzx/2017/34-80206.pdf, at 2.

technique based on reference rate is "banging the close."[78] In this scheme, a trader who is long on bitcoin futures may try to push the price of bitcoin up on the date his futures contract settles.[79] For example, the final value of CBOE bitcoin futures is based on the 4pm daily auction held on the bitcoin exchange Gemini.[80] If a trader held a long position in CBOE bitcoin futures, he could offer abnormally high prices during the Gemini auction in an attempt to artificially inflate the value of bitcoin on Gemini that day.[81] If successful, this would skew the benchmark price for the day and inflate the price of the bitcoin futures the trader holds.[82]

Banging the close is incredibly difficult to execute if there are many participants in the spot market auction, because a large volume of bitcoin would need to be purchased to move the benchmark price.[83] However, virtual currency exchanges have incredibly low volume, making such a scheme viable. For example, the Gemini 4pm auction used as the basis for the CBOE future settlement price sometimes fails to clear a single bitcoin.[84] Further, many bitcoin exchanges are completely anonymous and are operated beyond U.S. jurisdiction, meaning an individual can attempt to manipulate those exchanges with very little chance of being punished.[85]

Additionally, bitcoin exchanges often lack adequate cybersecurity. Between January of 2011 and July of 2018, there were approximately fifty-six virtual currency exchange

---

[78] *See* Alexander Osipovich, *Bitcoin Futures Manipulation 101: How 'Banging the Close' Works*, WALL ST. J. (Dec. 16, 2017), https://www.wsj.com/articles/bitcoin-futures-manipulation-101-how-banging-the-close-works-1513425600.

[79] *Id.*

[80] *Id.*

[81] *See id.*

[82] *See id.*

[83] *See* Reiners, *supra* note 76 (noting, however, that banging the close has been done successfully in a few large-scale conspiracies, such as frauds perpetrated on the foreign exchange market and LIBOR).

[84] *Id.* (citing Gemini's Daily Auction Data, GEMINI, https://gemini.com/auction-data/?cur-rentPage=2&startIndex=1&filter=4PM-BTC-USD#auctionData (last visited Nov. 8, 2018).

[85] *See* Osipovich, *supra* note 78.

cyberattacks, causing $1.63 billion in losses.[86] The price of bitcoin declined swiftly after each of these successful hacks.[87] Accordingly, an individual could take a short position on a virtual currency future and then conduct a cyberattack near the settlement date in order to push the virtual currency's price down. Successful hacks of bitcoin exchanges often lead a virtual currency to initiate a "hard fork,"[88] meaning a futures contract holder could benefit from a cyber attack if the provisions in that contract surrounding hard forks benefit him.[89]

2. *Instances of Manipulation*

There are numerous recorded instances of manipulation of virtual currency markets. For example, a research paper from John Griffin and Adam Shams at the University of Texas analyzed data from bitcoin market Bitfinex and virtual currency Tether and found overwhelming evidence that Tether had been used by individuals associated with Bitfinex to artificially inflate the price of bitcoin.[90] Grffin and Shams analyzed blockchain data to find that bitcoin purchases with Tether were timed to follow bitcoin market downturns and resulted in "sizable increases" to bitcoin prices.[91] Griffin and Shams found that about 1% of Tether trading could explain approximately 50% of the rise in bitcoin prices in 2017 and approximately 64% of the rise in other virtual currency prices.[92] Accordingly, the report suggest that the majority of bitcoin's

---

[86] Steven Russolillo & Eun-Young Jeong, *Cryptocurrency Exchanges are Getting Hacked Because it's Easy*, WALL ST. J. (July 16, 2018), https://www.wsj.com/articles/why-cryptocurrency-exchange-hacks-keep-happening-1531656000.

[87] *Id.*

[88] *See* Nathaniel Popper, *A Hacking of More Than $50 Million Dashes Hopes in the World of Virtual Currency*, NY TIMES (June 17, 2016), https://www.nytimes.com/2016/06/18/business/dealbook/hacker-may-have-removed-more-than-50-million-from-experimental-cybercurrency-project.html (discussing the successful hack of a virtual currency "hedge fund" and the resulting hard fork in cryptocurrency Ether).

[89] We discuss the issue of hard forks more thoroughly in Part III.B, *infra*.

[90] John M. Griffin & Amin Shams, *Is Bitcoin Really Un-Tethered?* (June 13, 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3195066.

[91] *Id.*

[92] *Id. See also* Kate Rooney, *Much of Bitcoin's 2017 Boom was Market Manipulation, Research Says*, CNBC (June 13, 2018), https://www.cnbc.com/2018/06/13/much-of-bitcoins-2017-boom-was-market-manipulation-researcher-says.html.

price increase in 2017 was likely attributable to fraudulent transactions.[93] The U.S. Department of Justice launched a formal investigation into Tether and Bitfinex in 2018.[94]

In a more recent study, Bitwise, a virtual currency asset management firm with its own exchanges and funds, found that approximately 95% of bitcoin trading volume has been faked by exchanges.[95] To collect this data, Bitwise created a program which examined trading data across 81 bitcoin exchanges.[96] The program analyzed trading patterns in an effort to separate genuine trading from artificial trading. Bitwise concluded that 71 of the 81 exchanges it analyzed exhibited overall trading patterns that appear manufactured.[97] The fake trading trends included 1) wash sales[98], 2) trading patterns where the average spread between bid and ask prices was closer than would be typical in a market of human traders, and 3) trade volume that dwarfed the volume of legitimate exchanges.[99] Bitwise concluded that only $273 million of the roughly $6 billion in reported daily trading volume during a four day period in March of 2019 was actually legitimate.[100]

B. A Fork in the Road for Regulation

A further reason that the CFTC should be wary of certifying virtual currency futures is the constant possibility of a "hard fork" occurring during the term of the contract. A hard fork is

---

[93] *Id. See also* Matt Robinson & Tom Schoenberg, *Bitcoin-Rigging Criminal Probe Focused on Tie to Tether*, BLOOMBERG (Nov. 20, 2018), https://www.bloomberg.com/news/articles/2018-11-20/bitcoin-rigging-criminal-probe-is-said-to-focus-on-tie-to-tether.

[94] Robinson & Schoenberg, *supra* note 93.

[95] BITWISE ASSET MGMT., PRESENTATION TO U.S. SECURITIES EXCHANGE COMM. (Mar. 19, 2019), https://www.sec.gov/comments/sr-nysearca-2019-01/srnysearca201901-5164833-183434.pdf.

[96] *See id. See also* Paul Vigna, *Most Bitcoin Trading Faked by Unregulated Exchanges, Study Finds*, WALL ST. J. https://www.wsj.com/articles/most-bitcoin-trading-faked-by-unregulated-exchanges-study-finds-11553259600?shareToken=ste90e80f8d18f47cb896491914f06cea3

[97] *See id.*

[98] A wash sale is when offsetting buy and sell orders are entered almost simultaneously. These neutralize one another, creating no economic value but generating transaction fees and the appearance of volume on the exchange.

[99] *See* Viga, *supra* note 96.

[100] *See* BITWISE ASSET MGMT., *supra* note 95.

20

a permanent break from the previous blockchain, where the blockchain is divided into two distinct entities.[101] This occurs when a cryptocurrencies' code is changed, making the old and new version of the currency incompatible.[102] Hard forks involve a significant alteration to the underlying blockchain that fundamentally alter its operation and can do everything from undoing previous transactions to modifying the mining process.[103] Hard forks require all the nodes—all the computers connected to the blockchain network—to adapt to the new protocol if they want to utilize this new blockchain. Hard forks can retain the same coin or create a new one.[104]

Creating a hard fork requires consensus of a majority of nodes, which can in practice come from a small group of individuals—typically miners—that control a large number of nodes.[105] Successful forks can be created for any reason, provided there is enough support for them to become a viable alternative to the underlying currency. Generally, hard forks occur when miners are unable to agree on software updates for the virtual currency.

Already throughout bitcoin's short life, it has undergone several hard forks, the most notable of which created Bitcoin Cash in 2017.[106] If another hard fork occurs during the life of a future's contract, determining the appropriate reference price, let alone if the reference asset has been converted to a new blockchain, could be incredibly costly and difficult. CME and CFE outline their policies in the event of a hard fork, but their contingency planning is vague and unsatisfying.[107] CME's policy states that "the exchange shall have the *discretion* to take action

---

[101] Nathan Reiff, *A History of Bitcoin Hard Forks*, INVESTOPEDIA (Apr. 25, 2018), https://www.investopedia.com/tech/history-bitcoin-hard-forks/.

[102] *See Understanding Hard Forks in Cryptocurrency,* CRYPTOCURRENCY FACTS https://cryptocurrencyfacts.com/understanding-hard-forks-cryptocurrency/ (last visited Jan. 29, 2019). This stands in contrast to a "soft fork" where the two versions of the currency remain compatible.

[103] *Id.*

[104] *Id.*

[105] *Id.*

[106] Reiners, *supra* note 76.

[107] *Id.* at 100.

in consultation with market participants to align bitcoin futures position holder exposures with cash market exposures as appropriate."[108]

Professor Lee Reiners of Duke University points out that the possibility of a hard fork could significantly affect the complexity of these futures contracts because of the difficulty in determining a reference price.[109] Consequently, investors have no way of knowing what would happen to these contracts in the event of a hard fork. For this reason, if and when another hard fork occurs, it could trigger a "mass selling in the bitcoin spot market as well as the futures market."[110] While virtual currencies do not represent a significant portion of the global economy at this time, the introduction of bitcoin futures has tied the global markets to these volatile currencies in such a way that the spillover effects of such a selloff could become a source of systemic risk as these currencies continue to proliferate.

Nobel prize winning economist Robert Shiller has explained that hard forks threaten the very existence of bitcoin, arguing that the forks will result in a bitcoin that is no longer recognizable, and that it will "be a matter of dispute whether [bitcoin] exists or not."[111] The CFTC must put greater onus on virtual currency futures providers to spell out the exact protocols that will be taken in the event of a hard fork and require them to justify their selling of a derivative for which the underlying asset may no longer exist. This is a particularly important lesson learned from the 2008 financial crisis. Complex financial instruments were at the center of

---

[108] S*ee* Certification Letter from Christopher Bowen, Managing Director & Chief Reg. Couns., Chicago Exchange, Inc., to Christopher J. Kirkpatrick, CFTC Secretary, 5 (Dec. 1, 2017), https://www.cftc.gov/sites/default/files/filings/ptc/17/12/ptc120117cmedcm001.pdf; Product Certification Letter from Cboe to Christopher J. Kirkpatrick, CFTC Secretary 2 (Dec. 1, 2017), https://www.cftc.gov/sites/default/files/filings/ptc/17/12/ptc120117cfedcm001.pdf.
[109] Reiners, *supra* note 76.
[110] *Id.*
[111] Stephanie Landsman, *Bitcoin Could Be Extinct by 2118: Yale's Robert Shiller*, CNBC: MARKETS (May 30, 2018), https://www.cnbc.com/2018/05/30/bitcoin-could-be-extinct-by-2118-yales-robert-shiller.html.

the financial crisis, largely because the intricacy of these products made their risk difficult to evaluate.[112] While it is difficult to understand the exposure of a structured financial product like mortgage-backed security, ultimately there are physical assets from which cash flows can be derived. For virtual currency derivatives, however, net exposure could be far harder to judge. This is because the underlying asset is virtual, unique from other commodities in that it lacks economic utility, and capable of being fundamentally altered through hard forks by actors outside of the contract.

It appears, thus, that the CFTC was mistaken in not considering the ramifications of hard forks in their analysis of bitcoin futures, particularly as the agency purported to be subjecting CME and CFE to heightened scrutiny. Nothing in the record suggests that the CFTC addressed, let alone investigated, both organizations' proposed protocols for addressing potential forks. The vague "discretion" that CME retains to adjust a reference price is itself an indictment of the CFTC review process. When it refused to consider manipulation in the spot market, the "CFTC made clear that their sole focus was on the potential to manipulate the contracts in question."[113] It is shocking, then, that the agency failed to consider that the contracts, by definition, grant CME rather broad discretion to potentially manipulate the very contracts in question. The inconsistency in the agency's reasoning is apparent in the statement of Commissioner Zaidi, who notes that "contract design issues are so important [in order] to ensure that cash settlement process cannot be manipulated through . . . outside trades or other factors."[114] CME's contract

---

[112] *See, e.g.*, Heather Hughes, *Financial Product Complexity, Moral Hazard, and the Private Law,* 20 STAN. J.L. BUS. & FIN. 179 (2015)
[113] Reiners, *supra* note 76.
[114] *Transcript of Market Risk Advisory Committee Meeting*, COMMODITY FUTURES TRADING COMM'N., (Jan. 31 2018), https://www.cftc.gov/sites/default/files/2018-08/mrac_013118_transcript.pdf.

design is fundamentally unequipped to prevent manipulation that would create multiple and concurrent potential reference prices as a result hard forks.

The questionable logic of the CFTC's inquiry can partially be pegged to the fact that, by statute, it bears the burden of proving why these exchanges should *not* be certified. However, the record, particularly in its dearth of hard fork analysis and inconsistent logic, may betray the agency's consequentialist rationale. The CFTC's Chairman, Chris Giancarlo, "has earned the moniker Crypto Dad for his embrace of cryptocurrencies – a title which he apparently relishes considering his frequent use of #CryptoDad on Twitter."[115] One academic points out on the same social media platform that "this is quite stunning. Can you imagine if Alan Greenspan called himself 'subprime dad' circa 2005?"[116] It may be that in the agency's rush to hop on the crypto bandwagon, it failed to adequately prepare for the inevitable fork in the road ahead

IV.   CONCLUSION

The advent of virtual currencies and blockchain technology has sparked innovation in the global financial community. Virtual currencies and blockchain are exciting technologies, but they also present new challenges for the CFTC. We suggest that the CFTC revisit the scope of its self-certification process, as current policies surrounding self-certification of futures contracts are inadequate when applied to virtual currency futures. Specifically, the current approval process 1) does not adequately consider fraudulent trading in virtual currency spot markets and the potential effect of spot market manipulation on the futures market and 2) fails to consider futures contracts' inability to account for the effect of hard forks on settlement prices.

Thank you for considering this submission.

---

[115] Lee Reiners, *Reflections on NYC Cryptocurrency Conference*, FINREG BLOG (July 11, 2018), https://sites.duke.edu/thefinregblog/2018/06/11/reflections-on-my-first-cryptocurrency-conference/.
[116] @leereiners, TWITTER (Mar. 6, 2019, 5:01PM), https://twitter.com/leereiners/status/1103460586569023490.