Comments to the Commodity Futures Trading Commission in Response to the Request for Input on Crypto-asset Mechanics and Markets

Peter Van Valkenburgh
February 11, 2019

Introduction

Coin Center is a non-profit research and advocacy center focused on the public policy issues facing open and decentralized blockchain technologies. Our mission is to build a better understanding of these technologies and to promote a regulatory climate that preserves the freedom to innovate using them. We do this by producing and publishing policy research from respected academics and experts, educating policymakers and the media about decentralized blockchain technology, and by engaging in advocacy for sound public policy. In that spirit, please find below our response to the Commission's Request for Input on Crypto-asset Mechanics and Markets.[1]

We welcome this opportunity to offer the Commission information on Ethereum as per its questions, and thank the Commission for its open-minded approach to new digital commodities generally. We also applaud the Commission's evident commitment to continued education on these matters through the Technical Advisory Committee and LabCFTC.

As a perfunctory matter, going forward we do not believe that the Commission needs to engage in an RFI process specific to each and every cryptocurrency that may come to underlie a derivative contract. While different cryptocurrencies certainly do have technical variability, the fundamental issues facing derivatives market participants and regulators likely do not vary so substantially from cryptocurrency to cryptocurrency as to warrant individual RFIs. We will illustrate why we believe this to be the case throughout our responses to the Commission's specific questions about Ethereum.

In general, the particular risks or eccentricities of any given cryptocurrency will be best addressed in the derivatives context through clear and carefully spelled-out policies within derivative contracts themselves and at organizations involved in offering or trading cryptocurrency derivatives. While these policies warrant further discussion beyond this RFI process, we will attempt to highlight the need for some of these policies throughout our responses as we address the Commission's questions in turn.

[1] 83 FR 64563, *available at* https://www.cftc.gov/sites/default/files/2018-12/2018-27167a.pdf

The Commission's Questions Regarding Ethereum

Purpose and Functionality

1. What was the impetus for developing Ether and the Ethereum Network, especially relative to Bitcoin?

As with Bitcoin, Ethereum is a technological innovation with many contributors across a diverse community of software developers, entrepreneurs, and enthusiasts. Each contributor will bring her own unique motivations and expectations to the project and each may contribute at varying levels. The end product does not have a unified impetus or purpose, much as a city would also not have a monolithic purpose or impetus.

That being said, many of the earliest developers of Ethereum appear to have had two primary motivations in mind: (1) build a cryptocurrency (Ether) and associated network (Ethereum) that is similarly decentralized and censorship resistant as Bitcoin, but make it capable of executing arbitrarily complex transactions (*i.e.* smart contracts) and (2) reduce the dependence on costly proof-of-work consensus mechanisms by developing and implementing a proof-of-stake mechanism for the new cryptocurrency and network.

As the technology developed, two further motivations clearly emerged within the community: (3) use smart contracts executed by the network to build decentralized web applications (Dapps) that could replace popular centralized web applications such as Twitter or Uber, and (4) allow ethereum users to easily create their own provably scarce, peer-to-peer tradable digital property, which may be either fungible (*i.e.* digital tokens) or unique (*i.e.* digital collectables).

Arbitrarily Complex Transactions or Smart Contracts

All cryptocurrencies are programmable money. The primary impetus for developing Ether and the Ethereum Network was to make a new cryptocurrency that would be more easily programmable and capable of executing transactions of arbitrary complexity (*i.e.* if you can imagine it in logic, then you can code it as an ethereum transaction and the blockchain will execute it). These complex transactions are often referred to as *smart contracts* because they may involve similar logic to traditional legal contracts: *if one party performs, the other is paid the negotiated price.* However, this terminology can be confusing given that a smart contract may not necessarily be a legally binding contract (depending on the circumstances) and given that several poorly written smart contracts, whose bugs or aberrant behavior have earned them some infamy, hardly warrant the adjective "smart."

It is possible to make some complex transactions using bitcoin and the Bitcoin network.[2] However, all bitcoin transactions must be written in a particular scripting language, called Script, in order to be interpreted and verified by miners and ultimately executed on the blockchain. Bitcoin Script has been intentionally designed to be limited in its expressiveness as a security measure.[3]

Ethereum's transactions are written in a new computer language called Solidity rather than Bitcoin's Script and this language is capable of expressing any series of logical operations one might imagine within a transaction or computation.[4] For example, an Ethereum transaction could include a loop, such as: *X=0; While X is less than 26, check if Peter is still listed as an employee at Coin Center and, if he is, pay Peter $1.50, wait 14 days, add 1 to X, and repeat.* This transaction will loop for a year and pay Peter every two weeks as long as he remains employed. Bitcoin script does not have the ability to describe such a loop within a transaction, but Solidity could describe this or any other logically coherent arrangement. This versatility is sometimes described as Ethereum having a "Turing complete" scripting language.[5] That terminology is technical and its appropriateness has been subject of debate; the simple description is that Ethereum allows for more complex transactions than Bitcoin.

Ethereum users can write transactions that will allow for future and repeat interaction from multiple other Ethereum users. For example, a transaction could have a rule set such as: *for every 1 ether sent to address X, send a message to an array of internet-connected light bulbs that will make their hue more red, and for every 1 ether sent to address Y, send a message to the light bulbs that will make their hue more blue.* Once developed, a smart contract can be instantiated on the Ethereum blockchain by the developer or a third party. Once instantiated, the contract will live at a unique contract address where it will be accessible (for interaction or payment) to any

---

[2] For example, a holder of bitcoin can write a transaction with associated rules that would cause 1 bitcoin to be sent to the recipient 18 years in the future (say on the birthday of a presently newborn baby). Upon inclusion into the blockchain, these funds will be permanently locked away from the sender, and the recipient will only be able to spend them once 18 years have passed. Any attempt to violate these rules will be recognized as fraudulent by computers run by miners and node operators on the network and will be ignored. This is known as a Timelock transaction because it is scripted to take advantage of the nLockTime field in bitcoin's transaction scripting language known as Script. *See generally,* Andreas Antonopoulos, *Mastering Bitcoin* (2014) *available at* https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch05.html.

[3] *See generally* "The Best Step-by-Step Bitcoin Script Guide Part 1," *Blockgeeks*, https://blockgeeks.com/guides/best-bitcoin-script-guide/ ("Script is a Forth-like, stack-based, reverse-polish, Turing Incomplete language. … Bitcoin Script doesn't need to be as complicated as an Ethereum smart contract. In fact, if a script was Turing Complete, it would have given malicious parties the freedom to create complicated transactions and eat up the hash-rate of the Bitcoin Network and slow down the entire system.").

[4] *See generally* "Solidity 0.5.3 documentation" *Github.com* (*last accessed* Feb 2019) https://github.com/ethereum/solidity/blob/v0.5.3/docs/index.rst ("Solidity is an object-oriented, high-level language for implementing smart contracts. Smart contracts are programs which govern the behaviour of accounts within the Ethereum state.").

[5] Kyle Wang, "Ethereum: Turing-Completeness and Rich Statefulness Explained" *Hackernoon.com* (July 2017) https://hackernoon.com/ethereum-turing-completeness-and-rich-statefulness-explained-e650db7fc1fb.

Ethereum user. In our simple example, the author could now install her lightbulbs on a famous building, say the Empire State Building, and direct the world to the particular contract address, urging them to pay it in ether in order to vote for the iconic building's color in real time.

Note that a similar smart contract could exist off-chain (*e.g.* logic on a computer chip that lives with the lightbulb rather than logic that lives on the Ethereum blockchain). This off-chain smart contract would merely monitor two payment addresses (they could be Bitcoin addresses) and adjust the lights accordingly. Ethereum, however, allows the developer to credibly signal to the community that the code will do what it says because the code itself lives on the Ethereum blockchain and is executed by the Ethereum network, leaving an auditable and immutable record of all of its interactions with all of its users. This transparency is sometimes referred to as Rich Statefulness and debate continues over whether it is a valuable feature of Ethereum or merely unnecessary complexity.[6]

Alternatives to Proof-of-Work

A long stated goal of several Ethereum developers has been the adoption of a proof-of-stake consensus mechanism.[7] The proposed mechanism has been named Casper the Friendly Finality Gadget.[8] It combines elements of proof-of-stake systems (*i.e.* one's relative power in consensus participation is proportional to the amount of valuable digital property one has or is willing to pledge) and more traditional Byzantine Fault Tolerant (BFT) consensus mechanisms which have been in development for decades.[9]

The network launched with a proof-of-work mechanism (Ethash) that remains in place to this day.[10] Early estimates of when the switch to proof-of-stake would happen have proven overly optimistic.[11] However, many in the community still anticipate a transition later in 2019.[12] The

[6] *Id.*
[7] *See, e.g.*, Vitalik Buterin, "A Proof of Stake Design Philosophy" *Medium* (Dec. 2016) https://medium.com/@VitalikButerin/a-proof-of-stake-design-philosophy-506585978d51.
[8] Vitalik Buterin, Virgil Griffith, "Casper the Friendly Finality Gadget v4" *arXiv.org* (Jan. 2019) https://arxiv.org/abs/1710.09437.
[9] *Id.*
[10] Belavadi Prahalad, "Proof of Work, Proof of Stake and Proof of Burn" *Hackernoon* (Mar. 2018) https://hackernoon.com/proof-of-work-proof-of-stake-and-proof-of-burn-6823eac2776e.
[11] *See, e.g.*, Shawn Dexter, "Ethereum Roadmap Update [2019]: Casper & Sharding Release Date" *mangoresearch* (Jan. 2019) https://www.mangoresearch.co/ethereum-roadmap-update/
[12] *Id.*

motivation for this transition is to reduce the energy costs associated with proof-of-work[13] as well as to increase the scalability of the network.[14]

2. What are the current functionalities and capabilities of Ether and the Ethereum Network as compared to the functionalities and capabilities of Bitcoin?

The primary functional difference between Ethereum and Bitcoin is the ability to execute transactions of arbitrary complexity as described earlier. Ethereum has yet to adopt a proof-of-stake-based consensus mechanism and, like Bitcoin, remains driven by proof-of-work.[15] Other differences are likely of lesser importance but a few may be worth noting: Ethereum has a faster block propagation time; it averages new blocks every 15 seconds as compared with Bitcoin's average of 10 minutes. Ethereum addresses have balances describing the total amount of Ether they have received and have yet to spend; Bitcoin, by comparison uses a UTXO scheme instead of balances.[16]

3. How is the developer community currently utilizing the Ethereum Network? More specifically, what are prominent use cases or examples that demonstrate the functionalities and capabilities of the Ethereum Network?

As noted in Answer 1, two general usage trends have emerged since Ethereum's launch: community members are utilizing smart contracts to build decentralized web applications (DAPPs) that could replace popular centralized web applications such as Twitter or Uber, and they are utilizing smart contracts to create their own provably scarce, peer-to-peer tradable digital property, which may be either fungible (*i.e.* digital tokens) or unique (*i.e.* digital collectables).

---

[13] *See,* Peter Fairley, "Ethereum Plans to Cut Its Absurd Energy Consumption by 99 Percent" *IEEE Spectrum* (Jan. 2019) https://spectrum.ieee.org/computing/networks/ethereum-plans-to-cut-its-absurd-energy-consumption-by-99-percent (quoting Vitalik Buterin, "That's just a huge waste of resources, even if you don't believe that pollution and carbon dioxide are an issue. There are real consumers—real people—whose need for electricity is being displaced by this stuff,").

[14] *See* Shawn Dexter, "Ethereum Roadmap Update [2019]: Casper & Sharding Release Date" *mangoresearch* (Jan. 2019) https://www.mangoresearch.co/ethereum-roadmap-update/

[15] *See id.*

[16] UTXO stands for unspent transaction output. Bitcoin addresses do not have associated 'balances' listed on the blockchain. Instead, several previously received amounts that have yet to be used in a new transaction belong to an address. These unspent transactions must be combined to send bitcoin onward, the inputs to the transaction must together be larger than the newly created transaction output, and any extra must be either returned to the sender in the form of a change transaction or else it will go to the miner as a fee; an Ethereum transaction, by contrast, merely adjusts the relevant balances of two or more addresses on the blockchain. *See generally,* Andreas Antonopoulos, *Mastering Bitcoin* (2014) *available at* https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch05.html.

Dapps

The ability to enforce arbitrarily complex transaction rules has led to the emergence of various use cases. For example, Ethereum's network powers a decentralized Domain Name System (DNS) registry where users can participate in fully automated auctions to purchase domain names that will be recorded onto the Ethereum blockchain.[17] If widely adopted, such a tool would obviate the need to trust centralized DNS registries that are arguably inefficient and vulnerable to hacking.[18]

The transaction rules (smart contract) in that use case are effectively: *if user voices interest in owning [insert user-selected domain name] and commits more ether than anyone else after a two week bidding period, then write to the blockchain that [user-selected domain name] belongs to user's ethereum address*. The rules also allow for peer-to-peer buying and selling of the domain after the initial auction.

Several such Dapps are in development. A website called State of the Dapps maintains one of the more comprehensive lists of Dapps as well as descriptions of their functionality and current state of development.[19]

Tokens and Collectables

Smart contracts can be deployed to the Ethereum blockchain that allow their authors to dispense fungible tokens or non-fungible collectables to interested users. The transaction rules of the contract can describe and guarantee a variety of attributes for these newly created digital assets. For example the transaction rules could cap the number of tokens available, credibly signaling to prospective token purchasers that the tokens are economically scarce. Alternatively, the rules could dispense a single digital collectable to the user who paid the largest sum to the contract address within a set period as a thank you gift for donating to a charitable cause. Again, Ethereum allows for transactions of arbitrary complexity, so these are merely two of an endless list of possible examples.

A notable example of the community's use of fungible tokens would be the several so-called initial coin offerings (ICOs) occuring on the Ethereum platform over the last two years. In a typical Ethereum-based ICO, a promoter:

1. Pitches an idea for some future technology to the general public (often it is a proposal for a new Dapp that could replace an existing centralized service),

---

[17] *Ethereum Name Service* (last accessed Jan. 2019) https://ens.domains/ ("ENS offers a secure & decentralised way to address resources both on and off the blockchain using simple, human-readable names.").
[18] *See, e.g.*, Catalin Cimpanu, "Iranian hackers suspected in worldwide DNS hijacking campaign" *ZDNet* (Jan. 2019) https://www.zdnet.com/article/iranian-hackers-suspected-in-worldwide-dns-hijacking-campaign/.
[19] *State of the DApps* (last accessed Jan. 2019) https://www.stateofthedapps.com/.

2. Promises that the future technology will eventually be available to the general public but only in exchange for a newly created fungible token on Ethereum,
3. Creates an Ethereum smart contract that will disperse a set number of these tokens to anyone who pays the contract address in Ether, and then
4. Proceeds to build the new technology using the raised funds as capital (hopefully).

Estimates vary, but in 2017 and 2018 some $15 billion, remarkably, was invested in ICOs. Many of these ICOs were powered by Ethereum-based smart contracts.[20]

4. Are there any existing or developing commercial enterprises that are using Ether to power economic transactions? If so, how is Ether recorded for accounting purposes in a comprehensive set of financial statements?

Several commercial enterprises have received ether in an ICO or use ether in order to power DappS that they have developed. We do not have expertise in the accounting practices used by these entities.

5. What data sources, analyses, calculations, variables, or other factors could be used to determine Ether's market size, liquidity, trade volume, types of traders, ownership concentration, and/or principal ways in which the Ethereum Network is currently being used by market participants?

There is nothing fundamentally different between Ether and Bitcoin that would necessitate an alternative approach to determining market size, liquidity, or any of the other factors mentioned in this question. As with Bitcoin, sources should include public data on the blockchain as well as trading data from secondary markets and other trading data aggregators.[21]

6. How many confirmations on the Ethereum blockchain are sufficient to wait to ensure that the transaction will not end up on an invalid block?

Informal analysis of a handful of exchanges indicates that between 30 and 50 confirmations appears to be an emergent best practice.[22] For enhanced safety, as many as 240 (which should be about an hour given an average block propagation time of 15 seconds) may be prudent.

Technology

7. How is the technology underlying Ethereum similar to and different from the technology underlying Bitcoin?

See answers 1 and 2.

---

[20] *See* "Funds raised in 2018" *ICOData.io* (last accessed Jan. 2019) https://www.icodata.io/stats/2018.
[21] *See, e.g.*, Tradeblock (last accessed Jan. 2019) https://tradeblock.com/home.
[22] *See, e.g.*, "How long do digital assets/cryptocurrency deposits take?" *Kraken* (last accessed Jan. 2019) https://support.kraken.com/hc/en-us/articles/203325283-How-long-do-digital-assets-cryptocurrency-deposits-take- ("Ether (ETH) 30 Confirmations, 6 Minutes").

8. Does the Ethereum Network face scalability challenges? If so, please describe such challenges and any potential solutions. What analyses or data sources could be used to assess concerns regarding the scalability of the underlying Ethereum Network, and in particular, concerns about the network's ability to support the growth and adoption of additional smart contracts?

Ethereum faces similar scalability challenges as Bitcoin. If the use of Dapps becomes widespread, Ethereum's scalability problems may be more severe than Bitcoin's because of the sheer number of transactions potentially involved. The intuition here is that an average person makes perhaps three or four currency transactions every day. To scale to global payments Bitcoin must be able to accommodate this number of transactions multiplied by a reasonable portion of the world's population. By comparison an average person likely has several hundred transactional interactions with websites per day—everything from posting to social media, checking email, visiting websites and blogs, searching Google, etc. If the bulk of these services were to become Dapps and much of the users' interaction with the Dapp required adding data to the Ethereum blockchain, then the network would need to accommodate far more transactions per second than one limited only to payments.

As with Bitcoin, the blockchain is the authoritative source for information on the network's scale. Capacity or lack thereof can be inferred by the relative fees being paid by users in order to persuade miners to incorporate their transactions into blocks (high fees indicate that the network has reached saturation and users are paying a premium for priority). Similarly the current volume of transactions both in number and in dollar amount is observable on the chain. Various sources provide visualizations and exploration tools that can make it easier to consume and interpret this data.[23]

9. Has a proof of stake consensus mechanism been tested or validated at scale? If so, what lessons or insights can be learned from the experience?

Despite several running implementations of proof-of-stake, some researchers argue that—ultimately—these systems will not prove robust as compared with proof-of-work.[24] The heart of these concerns is as follows. Both proof-of-work and proof-of-stake mechanisms are designed to make participation in consensus costly such that sybil attacks are non-viable. In non-technical terms a sybil attack is when a single participant in a purportedly democratic process forges multiple identities in order to bias selection toward herself. Proof-of-work systems deter this attack because, in effect, each chance to create the next block comes at the cost of computing work and real energy expenditure. A participant is free to try to increase her odds of being selected by dedicating more computing power but she cannot do so without

[23] Jon Wood, "What's the best Ethereum block explorer? 10 Alternatives to Etherscan" *Medium* (Jan. 2019) https://medium.com/coinmonks/whats-the-best-ethereum-block-explorer-10-alternatives-to-etherscan-8eb5f2be263d.

[24] *See, e.g.*, Andrew Poelstra, "On Stake and Consensus" (*last accessed* Jan. 2019) https://download.wpsoftware.net/bitcoin/pos.pdf.

suffering real economic costs. Proof-of-stake systems attempt to impose the same costs on participants by requiring them to prove that they have obtained an amount of the valuable digital property described by the system's blockchain. Depending on the design of the system, the user may need to cryptographically sign a message with the same private key that is associated with an address that has the valuable digital property in it according to the blockchain, or she may need to lock her digital property out of her control for a period of blocks (*i.e.* bonded proof-of-stake) through something akin to Bitcoin's Timelock transaction type, or she may need to provably destroy some amount of the digital property by sending it to addresses with no possible associated private key (*i.e.* proof-of-burn), or there may be a variety of other requirements.

In all of these cases, however, the only evidence that the staker is actually suffering these costs is the record of her prior transactions within the blockchain's history (*e.g.* any past blocks wherein she was signing, bonding, burning, etc.). Because the staker is also securing that very blockchain, it's possible that she could forge past blocks (present the network with an alternative history) in order to include transactions that would make it appear as though she is presently permitted to write the next block. This is not possible in a proof-of-work scheme because the attacker would need to produce costly work for that past block and every block since in order to present a valid alternative history; it would be an impossibly large mountain of computing work even if we assume rapid advances in computing power. With proof-of-stake, however, effectively no costly computing work is needed to present the network with multiple alternative histories that fraudulently overstate the stake of the attacker. This attack has come to be known as the "nothing at stake" problem or "costless simulation."[25]

When the attacker presents her alternative history, however, her call to reorganize the blockchain is necessarily public and can be scrutinized. This presents potential solutions. For one, the rules of the blockchain can forbid block reorganizations that go back more than a certain number of blocks. Alternatively, participants who suggest deep reorganizations or who append their cryptographic signature to multiple inconsistent states of the blockchain can be punished, perhaps by having a protocol mechanism that would destroy an amount of digital property that they'd previously pledged.

Peercoin was the first proof-of-stake-based protocol, but it suffered a spate of costless simulation attacks and the developers decided to impose a checkpointing process that involved the developer signing blocks at regular intervals with their private key in order to prevent reorganizations of the blockchain before those checkpoints. This prevents some attacks, but it depends on the trustworthiness of the developers.[26]

Subsequently, other networks have launched with proof-of-stake systems that were designed to prevent these attacks by using bonding and penalties as described above. One notable example is Tezos. Thus far there has been no observed successful attack on Tezos' proof-of-stake

[25] *Id.*
[26] *Id.*

scheme. Tezos's scheme has been identified by its developers as conceptually similar to Ethereum's still-in-development Casper protocol.[27]

10. Relative to a proof of work consensus mechanism does proof of stake have particular vulnerabilities, challenges, or features that make it prone to manipulation? In responding consider, for example, that under a proof of stake consensus mechanism, the chance of validating a block may be proportional to staked wealth.

Addressing the second part of the question first, the chance of validating a block *will* be proportional to staked wealth, but this is not a vulnerability *per se*; it is the intent of the protocol design. Some may be concerned about this given that it could promote wealth inequality.[28] However, that concern is orthogonal to market manipulation. Additionally, the same is true of proof-of-work systems given that computation is costly and those who can afford more computing power will, in turn, earn greater rewards.

We do not believe that the costless-simulation vulnerabilities discussed in the previous section bear any special relationship to the potential for manipulation beyond the simple fact that a newer and less-researched system could fail in unexpected ways. Those who might attack the network because of those vulnerabilities may be able to better profit from their attack if they can short the value of the associated cryptocurrency.

11. There are reports of disagreements within the Ether community over the proposed transition to a proof of stake consensus model. Could this transition from a proof of work to a proof of stake verification process result in a fragmented or diminished Ether market if the disagreements are not resolved?

As with all contentious decisions concerning the core consensus rules, the debate could ultimately result in a fork of the protocol.

12. What capability does the Ethereum Network have to support the continued development and increasing use of smart contracts?

See answer 8.

---

[27] *See* "Tezos Developer Resources" *tezos.gitlab.io* (*last accessed* Jan. 2019) https://tezos.gitlab.io/tezos/whitedoc/proof_of_stake.html *See also* https://twitter.com/tezos/status/815390767493644288.

[28] *See, e.g.*, Gert Rammeloo, "The economics of the Proof of Stake consensus algorithm" *Medium* (Oct. 2017) https://medium.com/@gertrammeloo/the-economics-of-the-proof-of-stake-consensus-algorithm-e28adf63e9db.

Governance

13. How is the governance of the Ethereum Network similar to and different from the governance of the Bitcoin network?

Ethereum's governance model is similar to Bitcoin in that it relies on informal discussion, public improvement proposals, open source software practices, and public participation in code creation and auditing through repositories like Github.[29] Unlike Bitcoin, much of the original work to build Ethereum's early versions was centralized amongst a community of developers who were funded through a public pre-sale of the cryptocurrency organized by a non-profit organization, the Ethereum Foundation.[30] Today, however, there are several independent organizations working on protocol design in addition to the Foundation[31] and several independently developed versions of the core software.[32]

Like Bitcoin, forking or the threat of forking is a major aspect of project governance. Notably, an unresolvable community-wide disagreement over how to respond to a bug in theDAO smart contract resulted in a fork in July of 2016.[33] The two factions went their separate ways and this is why Ethereum and Ethereum Classic are now separate networks with a common heritage. That fork is not dissimilar to the Bitcoin Cash fork from Bitcoin in August of 2017.[34] In both cases, intractable debates over governance led to a minority group choosing to exit the community and build an alternative network.

14. In light of Ether's origins as an outgrowth from the Ethereum Classic blockchain, are there potential issues that could make Ether's underlying blockchain vulnerable to future hard forks or splintering?

The wording of this question has proved amusing to some in the Ethereum community.[35] Metaphysically it is hard to argue with any certainty that either Ethereum or Ethereum Classic is an outgrowth from the other. Both share a common history but have no objective claim to primacy. All open consensus blockchain networks are vulnerable to hard forks, and this may be a feature rather than a bug. It enables communities who disagree with the majority view of protocol development to exit the network and develop their own alternative. This can lead to confusion but, with respect to traders and derivatives contracts at least, that confusion can be mitigated by developing clear policies for what to do in the event of a fork: These policies

---

[29] Ethereum Github Repository (*last accessed* Jan. 2019) https://github.com/ethereum.
[30] Ethereum.org (*last accessed* Jan. 2019) https://www.ethereum.org/foundation.
[31] *See, e.g.,* Parity Technologies (*last accessed* Jan. 2019) https://www.parity.io/, and Consensys (*last accessed* Jan. 2019) https://consensys.net/.
[32] *See* Ethereum Homestead: Ethereum Clients (*last accessed* Jan. 2019) http://ethdocs.org/en/latest/ethereum-clients/.
[33] *See generally* Joon Ian Wong, Ian Kar, "Everything you need to know about the Ethereum 'hard fork'" *Quartz* (July 2016) https://qz.com/730004/everything-you-need-to-know-about-the-ethereum-hard-fork/.
[34] *See generally* Aaron van Wirdum, "The Birth of BCH: The First Crazy Days of "Bitcoin Cash" *Bitcoin Magazine* (Aug. 2017) https://bitcoinmagazine.com/articles/birth-bch-first-crazy-days-bitcoin-cash/.
[35] *See* https://twitter.com/koeppelmann/status/1072575570272247809.

should include a description of the process that will be used to decide which leg of the fork is the original commodity and which is something new. It should include clear statements of what will be done with any windfalls associated with the receipt of assets that have forked off of the original underlying commodity.

Markets, Oversight and Regulation

15. Are there protections or impediments that would prevent market participants or other actors from intentionally disrupting the normal function of the Ethereum Network in an attempt to distort or disrupt the Ether market?

Technical protections are largely the same as with Bitcoin—the network's transparency and its consensus mechanism prevent malicious behavior. Proof-of-stake, however, if adopted may create new vulnerabilities as discussed earlier in questions 9 and 10. Regulatory protections are also similar to Bitcoin. Retail spot markets are, by and large, regulated as money services businesses and money transmitters in the several states. With the exception of the New York BitLicense,[36] these are not anti-manipulation regulations *per se*, but requirements for customer identification, and associated safety and soundness requirements may make manipulation more difficult.

16. What impediments or risks exist to the reliable conversion of Ether to legal tender? How do these impediments or risks impact regulatory considerations for Commission registrants with respect to participating in any transactions in Ether, including the ability to obtain or demonstrate possession or control or otherwise hold Ether as collateral or on behalf of customers?

As with Bitcoin, to our knowledge there are few impediments. Several secondary markets and OTC markets for conversion are available. We do not, however, have expertise in secondary market activity.

Demonstration of possession or control is trivially easy from a technical perspective and identical to Bitcoin. One must cryptographically sign a message with a private key that corresponds to a public address with a positive balance.[37] Demonstration of exclusive control may be more difficult. Keys could, in theory, be shared although the practice puts both parties at risk that one of them will fail to secure their copy of the key or act maliciously against the other. Key sharing may therefore be unlikely, however there is no technical measure capable of preventing it and thereby guaranteeing exclusive possession. At this level, the institution will simply need to be trusted not to engage in such activity. This is little different than the possibility that a bank has made copies of its safe deposit box keys or that a debit card user has

[36] *See* Maria T. Vullo, "Guidance on Prevention of Market Manipulation and Other Wrongful Activity" *New York Department of Financial Services* (Feb. 2018) https://www.dfs.ny.gov/legal/industry/il180207.pdf.
[37] *See, e.g.*, Etherscan "Verify New Message Signature" (*last accessed* Jan. 2019) https://etherscan.io/verifySig.

given a friend a copy of her card number and secret pin, or that an unauthorized employee at a bank has obtained copies of the bank's SWIFT credentials.

17. How would the introduction of derivative contracts on Ether potentially change or modify the incentive structures that underlie a proof of stake consensus model?

Derivatives may introduce a risk to any open consensus model in that they create a means to profit from the price decreases that could result from a highly publicized attack on the network. As described in our answers to questions 9 and 10, we do not believe proof-of-stake creates any additional risk apart from it being generally less studied and tested.

18. Given the evolving nature of the Ether cash markets underlying potential Ether derivative contracts, what are the commercial risk management needs for a derivative contract on Ether?

We do not have expertise in studying these markets. However, to our knowledge, the Ether cash markets are sufficiently similar to Bitcoin's cash markets that differential risk management may not be necessary.

19. Please list any potential impacts on Ether and the Ethereum Network that may arise from the listing or trading of derivative contracts on Ether.

See answer 17.

20. Are there any types of trader or intermediary conduct that has occurred in the international Ether derivative markets that raise market risks or challenges and should be monitored closely by trading venues or regulators?

None of which we are aware, but this is not our area of expertise.

21. What other factors could impact the Commission's ability to properly oversee or monitor trading in derivative contracts on Ether as well as the underlying Ether cash markets?

Again, underlying Ether cash markets are, to our knowledge, substantially similar to those for Bitcoin.

22. Are there any emerging best practices for monitoring the Ethereum Network and public blockchains more broadly?

Aside from using various public blockchain explorers,[38] several companies and institutions employ proprietary blockchain analysis tools as provided by several firms that specialize in analyzing and visualizing blockchain data.[39]

Cyber Security and Custody

23. Are there security issues peculiar to the Ethereum Network or Ethereum supported smart contracts that need to be addressed?

Every smart contract executed on the Ethereum blockchain is potentially unique and therefore should be independently audited to protect against bugs or malicious backdoors. Standards have formed describing best practices in creating certain commonly used smart contracts. These standards simplify smart contract auditing and encourage greater uniformity amongst a potentially boundless field of contract types. These standards are created and discussed by the Ethereum community in the form of Ethereum Requests for Comment (ERCs) and they may be formally approved as canonical to the Ethereum protocol by going through the Ethereum Improvement Proposal (EIP) process.[40] A well-known example of this standardization process is the ERC-20 Token standard, which describes standards for smart contracts that will generate fungible tokens capable of being transferred between Ethereum users.[41]

It is important to note that Ethereum implements multi-signature wallets through smart contracts rather than a uniform protocol-level process. Therefore, some smart contracts that generate multi-signature wallets may be better than others and some may even have bugs.[42] Any particular multi-signature contract should be carefully audited. Standardization of these contracts is an ongoing effort.

24. Are there any best practices for the construction and security of Ethereum wallets, including, but not limited to, the number of keys required to sign a transaction and how access to the keys should be segregated?

---

[38] Jon Wood, "What's the best Ethereum block explorer? 10 Alternatives to Etherscan" Medium (Jan. 2019) https://medium.com/coinmonks/whats-the-best-ethereum-block-explorer-10-alternatives-to-etherscan-8eb5f2be263d.
[39] *See, e.g.*, Elliptic (*last accessed* Jan. 2019) https://www.elliptic.co/, *and* Chainalysis (*last accessed* Jan. 2019) https://www.chainalysis.com/.
[40] EIP Process (*last accessed* Jan. 2019) https://github.com/ethereum/EIPs/issues/898#issuecomment-367942142.
[41] ERC20 Token Standard (last accessed Jan. 2019) https://eips.ethereum.org/EIPS/eip-20.
[42] *See, e.g.*, Sergey Petrov, "Another Parity Wallet hack explained" *Medium* (Nov. 2017). https://medium.com/@Pr0Ger/another-parity-wallet-hack-explained-847ca46a2e1c.

Generally speaking, established best practices for securing Bitcoin apply when securing Ethereum. These include:

- **Cold storage:** storing the bulk of the owner's ether in offline wallets or "cold" storage and keeping only the minimum amount of ether in online or "hot" wallets that is necessary for the particular purposes of the owner (*e.g.* an exchange may need ready access to a certain percentage of the total ether that they secure to guarantee sufficient liquidity for their traders).
- **Multi-sig:** using smart contracts the power to spend an amount of ether can be divided between several keys, some subset of which are required to transact. These keys can be distributed between multiple control persons within an institution in order to guarantee that there is never a single point of failure.[43]

Again, unlike Bitcoin, Ethereum multi-sig implementations may vary with the underlying smart contract and careful auditing of those contracts is essential.

25. Are there any best practices for conducting an independent audit of Ether deposits?

As discussed earlier in question 16, possession of Ethereum can be verified cryptographically. Aside from auditing general accounting practices, such cryptographic proofs may be valuable in an independent audit. We do not, however, have particular expertise in these matters and cannot offer further specifics regarding audits.

Conclusion

Again, we thank the Commission for this opportunity and its open minded approach to new digital commodities. Should anything in our responses be unclear or spur further questions, please do not hesitate to contact us for clarification or further discussion.

[43] *Cf.* Doug Alexander, "Crypto CEO Dies Holding Only Passwords That Can Unlock Millions in Customer Coins" (Feb. 2019) https://www.bloomberg.com/news/articles/2019-02-04/crypto-exchange-founder-dies-leaves-behind-200-million-problem.