CONSENSYS

February 15, 2019

Mr. Christopher Kirkpatrick
Secretary of the Commission
Commodity Futures Trading Commission

Three Lafayette Centre
1155 21st Street, NW
Washington, DC 20581

Re: Request for Input on Crypto-Asset Mechanics and Markets

Dear Mr. Kirkpatrick:

ConsenSys appreciates the opportunity to submit this letter in response to the CFTC's request for input on crypto-asset mechanics and markets. ConsenSys was founded by Joseph Lubin, who was one of the co-founders of the Ethereum Network, and the company is a leader in the Ethereum ecosystem. ConsenSys is a global blockchain innovator, transforming our present digital architecture toward a more open, inclusive, and secure internet of value, commonly called "Web3." With a more trustworthy internet architecture, we are helping enterprises and governments unlock new business models and value, gain efficiencies through a shared IT infrastructure, and utilize modern cryptographic methods to safeguard private user data. We accomplish this through our unique global business network comprised of a startup incubator, enterprise and government consulting arm, education academy, protocol engineering team, and venture capital fund.

We are encouraged by the CFTC's thoughtful and inviting approach to these issues and its ongoing support for innovation in the blockchain technology and cryptoasset industry. We believe that the introduction of a regulated futures contract on ether would support the industry by providing a reliable method for projects and companies to hedge exposure, as well as providing the industry in the United States with a regulated alternative for futures positions on ether. This response was informed in part by open industry collaborations through The Brooklyn Project (https://theBKP.com), which is an open source-style industry initiative to help engage and give a voice to all members of the blockchain technology and cryptoasset industry on important regulatory, legal, and public policy issues.

Purpose and Functionality

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

The Ethereum Network and ether, its "crypto-fuel," were originally conceived by Vitalik Buterin and brought to life by a large and dispersed ecosystem of developers, miners, academics, and innovators.

Ethereum Network. Buterin began formulating his vision for Ethereum after Bitcoin became the first successful "crypto-currency." Bitcoin proved that an open, decentralized network could transfer and keep track of value through an open "consensus" algorithm.[1] In late 2013, Vitalik began envisioning an improved platform for

[1] *See* https://github.com/ethereum/wiki/wiki/White-Paper.

building “programmable money,” where parties could enter blockchain-based “contracts” holding digital assets and transfer those assets according to pre-set rules.[2]

Buterin first published his vision for Ethereum in December 2013. Many people all around the world were inspired by and began collaborating with Vitalik on his vision. These collaborations led to expanding, modifying and refining the specifics of the Ethereum “protocol,” as well as transitioning Ethereum from a platform for “programmable money” to one for general computation – *i.e.*, allowing anyone to create and run any type of code through “smart contracts” on the Ethereum blockchain, similar to a shared world computer.[3]

Ether. From the start, the Ethereum protocol was designed to rely heavily upon ether as a “cryptofuel” native to the Ethereum blockchain for accomplishing two necessary objectives: (1) to serve as fuel in order to pay for resources on the Ethereum blockchain; and (2) to serve as the “reward” in the Ethereum Network’s crypto-economic system.

Ether was designed as a “fuel” for paying fees in order to allocate resources efficiently across the Ethereum Network. The Ethereum protocol requires every computational step of a transaction or smart contract to pay a dynamic and variable fee – called “gas” – that is payable only with ether.[4] This was a “crucial” aspect of the Ethereum protocol, because without these gas fees, “members of the network could choke the network with spurious requests including infinite loops that would prevent smart contracts from executing.”[5]

Ether’s role as the cornerstone of a crypto-economic system was designed to enable the Ethereum Network to operate even though it would require coordination and cooperation of an unlimited number of actors who would not know or necessarily trust each other. In short, “cryptoeconomics is the use of incentives and cryptography to design new kinds of systems, applications, and networks.”[6] The Ethereum protocol was designed to distribute ether to miners as a reward for them adding new blocks of transactions to the blockchain.

(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?

The best source of data for many of these issues is the Ethereum blockchain itself. Because the blockchain is open and transparent, it is a rich source of data for analysis. A ConsenSys project, Alethio (https://aleth.io/), provides an advanced Ethereum blockchain analytics platform (https://ethstats.io) with rich analysis of this on-chain data.

This data reflects, as depicted in Figure 1, that the most common on-chain activities are calls to and interactions with smart contracts, which surpasses other activities such as smart contract creation and simple value transfers. In addition, as illustrated in Figure 2, the complexity of function calls within smart contracts is expanding as more use cases emerge. Currently, the most common function call is “transfer”, which is a common function that is used both for transfering value and also using tokens for their intended purpose. For example, consider “FOAM,” a decentralized network that utilizes an open protocol to empower users anywhere in the world to help build a map that can be trusted and is not owned by any central authority.[7] The “FOAM” token functions similar to a software license -- users need to own the token in order, among other things, to help curate “points of interest” (or locations) on the map. Users stake their FOAM tokens to curate the points of interest. This “staking” functionality is implemented, in part, by calling the “transfer” function within the FOAM token’s smart contract.

[2] *See* https://vitalik.ca/2017-09-15-prehistory.html.
[3] *Id.*
[4] *See* https://blockgeeks.com/guides/ethereum-gas-step-by-step-guide/.
[5] *See* Jonathan Rohr and Aaron Wright, *Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets*, Cardozo Legal Studies Research Paper No. 527, (March 28, 2018), https://ssrn.com/abstract=3048104, at 19.
[6] *See* https://medium.com/l4-media/making-sense-of-cryptoeconomics-c6455776669.
[7] *See* https://blog.foam.space/introducing-the-foam-protocol-2598d2f71417

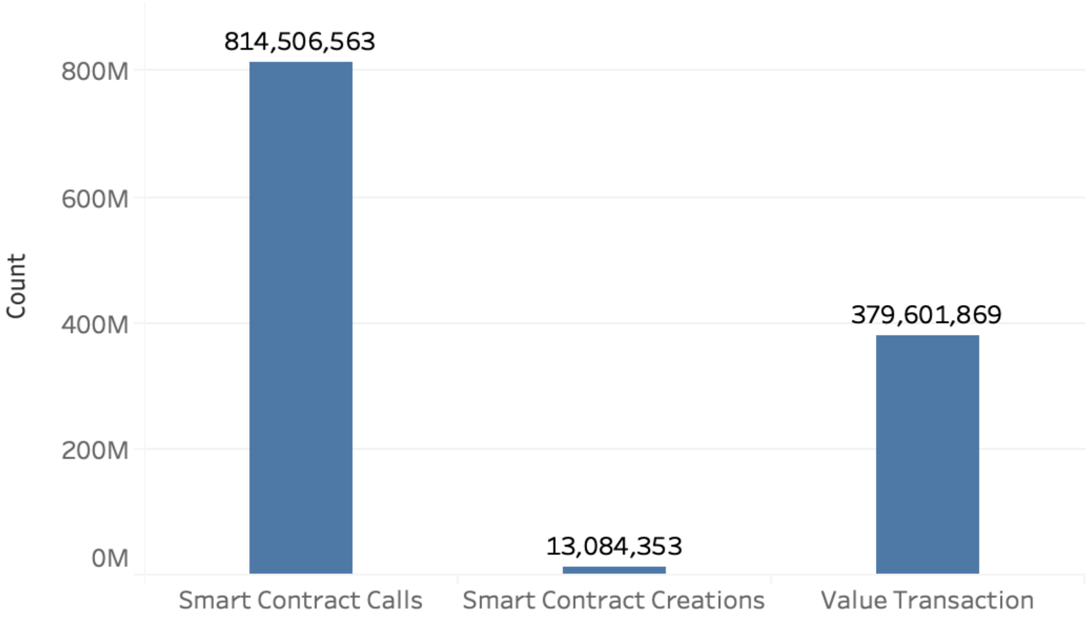

Fig 1. Network Traffic Segmented by Transaction, Contract Calls or Creation (Feb 13, 2019)

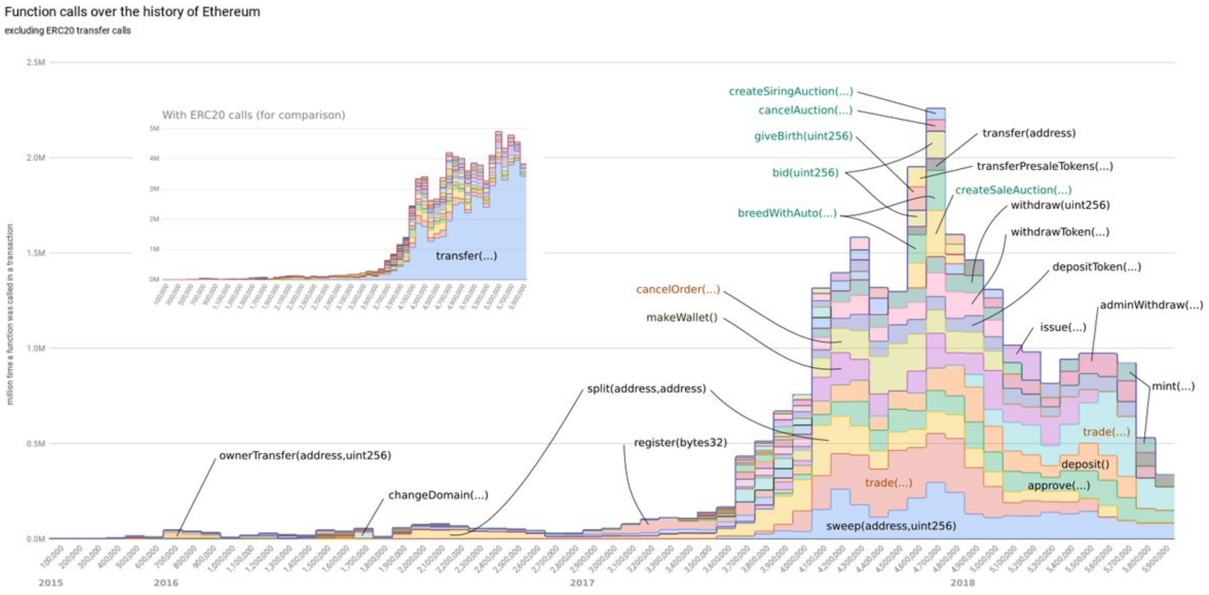

Fig 2. Function Calls Distribution on Ethereum (updated to ~6m blocks, August 2018)

Question 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.

This question is addressed in more detail below in response to Question 15. In short, under the current proof-of-stake plans for the Ethereum Network, the risk of a party successfully and materially manipulating the Ethereum Protocol is low. In particular, any party that stakes ether to validate blocks on the Ethereum Network will have less of an ability to directly impact the network, even relative to their proportional "staked wealth," than miners on proof-of-work protocols relative to their proportional hash power. In fact, as explained more fully below, under the Ethereum Network's planned proof-of-stake protocol, even if a validator controlled ⅓ of the entire ether staked in the protocol, the validator's probability of obtaining enough control to do damage is **less than one in one trillion**.

Governance

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

Governance of the Ethereum Network is similar to that of the Bitcoin Network: Both networks involve networks of people coordinating around ideas, principles and code through various communications channels and open source software practices.

Since October 2015, the Ethereum Network has collaborated on updating Ethereum protocol specifications, client APIs, and smart contract standards, through a process known as the Ethereum Improvement Proposal Process.[8] As part of this process, the community uses Ethereum Improvement Proposals (EIPs), derived from the Bitcoin Improvement Proposal (BIPs) process, as "the primary mechanisms for proposing new features, for collecting community input on an issue, and for documenting the design decisions that have gone into Ethereum."[9]

The EIP process can best be described as a merit-based proposal process whereby anyone can submit an EIP or a less formal "ERC," which stands for Ethereum Request for Comment, but the Ethereum Network only adopts the proposals that gain consensus by the broader decentralized Ethereum community. This is because no single person or company controls the Ethereum Network and its software. As a result, the Network must take action collectively. If an unfavorable EIP is proposed, the end result will be rejection by developers, users, and, if the proposal requires a change at the consensus protocol level, such as in the DAO Attack example, miners.

Successful examples of this decentralized governance format and the resulting contribution to the progress of the Ethereum Network are the ERC-20 and ERC-721 standards. The ERC-20 standard[10] set the community recognized parameters for fungible digital tokens on Ethereum, allowing all tokens that conform with the ERC-20 standard to be compatible with software built to handle such tokens, including, for example, wallets and exchanges. The ERC-721 standard[11] does something similar for non-fungible tokens. Both the ERC-20 and -721 standards began as drafts soliciting comment from the community, and then both gained widespread support and were implemented by many unaffiliated projects and developers. As a result, both standards were "adopted" by the community and moved to "final" status in the EIP process.[12]

Proposals that implicate the core, underlying protocol of the Ethereum Network are handled separately[13] than other proposals and are always evaluated at "All Core Devs Meetings," which are "technical meeting[s] intended to bring together various Ethereum teams who play major roles in determining the direction of the

[8] https://eips.ethereum.org/; *see* also https://eips.ethereum.org/EIPS/eip-1 (dated October 27, 2015 and describing the EIP process).
[9] https://eips.ethereum.org/EIPS/eip-1
[10] https://eips.ethereum.org/EIPS/eip-20
[11] https://eips.ethereum.org/EIPS/eip-721
[12] *See* https://eips.ethereum.org/erc
[13] https://eips.ethereum.org/core

protocol."[14] The agendas, notes, and recordings of All Core Devs Meetings are posted online.[15] Anyone can add an agenda item to these meetings, or join the meetings themselves.[16]

This EIP process is still highly fluid and continues to evolve. Often it is not clear whether and when a proposal receives sufficiently broad community adoption. Further, many ideas and proposals, before being formally posted to the EIP process, are evaluated and discussed by the community through the "Fellowship of Ethereum Magicians,"[17] which is a "self-organized Fellowship within the Ethereum community to maximize technical opportunities, share ideas, and work together effectively across national, organizational and other boundaries."[18]

Although much of the original work on the Ethereum Network was done by individuals that participated in putting together the "Ethereum Foundation," and the Foundation offers technical leadership, it is not an official controlling authority within the Ethereum Network.[19] The Foundation's express and only remit, as required by the laws of Switzerland, where it is organized, is to "promote and support Ethereum platform and base layer research, development and education to bring decentralized protocols and tools to the world that empower developers to produce next generation decentralized applications (sometimes called dapps), and together build a more globally accessible, more free and more trustworthy Internet."[20]

In furtherance of its mission, the Foundation focuses on research and development and improving the core protocol and software, while leaving to the wider community other aspects of the Ethereum Network ecosystem.[21] The Foundation publishes open-source code online and maintains a blog that issues security alerts, among other posts such as educational pieces and updates about the Ethereum Network.[22]

Increasingly, the Foundation also plays the role of encouraging further development of the Ethereum Network by developers from around the world. For example, in January 2018, the Foundation started a grant program to award developers and projects that aim to increase scalability of the Ethereum Nework.[23] The Foundation also organizes the annual Ethereum Developer Conference that brings together the decentralized development community to discuss technical evolutions pertaining to the Ethereum Network.

Markets, Oversight and Regulation

Question 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?

[14] https://github.com/ethereum/pm

[15] https://github.com/ethereum/pm

[16] *See* EIP0 - A Review of the Current Ethereum Governance Processes (EIPs & All Devs Call), https://www.youtube.com/watch?v=VJ3r52T7HV8 (

[17] https://ethereum-magicians.org/

[18] https://ethereum-magicians.org/about

[19] Much as there is a standard setting body (several in fact—the Internet Engineering Task Force, The Internet Architecture Board, the World Wide Web Consortium, The Linux Foundation, etc.) for the protocols that govern much of the internet, the Foundation considers whether to propose amendments to the Ethereum Network's underlying code for consideration and adoption by the broader user community. But no proposals of the Foundation are binding or even more likely to be adopted than proposals that any user, interested person, or group of users and interested persons may put forth regarding the Ethereum Network. All changes require adoption by the majority of the user community, which do not vote to accept or reject the changes but instead opt to devote/send computing or mining power to the amended version of the network. If they disagree, they keep sending/devoting computing or mining power to the original, un-amended network. *See* Patrick Murck, Who Controls the Blockchain?, Harv. Bus. Rev., April 19, 2017, https://hbr.org/2017/04/who-controls-the-blockchain.

[20] *Mission and Vision Statement*, Ethereum Foundation (last visited May 25, 2018), https://ethereum.org/foundation; *see also* Taylor Gerring, *Cut and Try: Building a Dream*, Ethereum Blog (Feb. 9, 2016), https://blog.ethereum.org/2016/02/09/cut-and-try-building-a-dream/ .

[21] Vitalik Buterin, *Ethereum Foundation Internal Update*, Ethereum Blog (Jan. 7, 2016), https://blog.ethereum.org/2016/01/07/2394/. The core group of developers creating and proposing updates to the Bitcoin blockchain network operate in a similar fashion: "Bitcoin Core is an open source project which maintains and releases Bitcoin client software called 'Bitcoin Core'. . . . The Bitcoin Core project has a large open source developer community with many casual contributors to the codebase. . . . Everyone is free to propose code changes and to test, review and comment on open [proposals]." *See* https://bitcoincore.org/en/about/ and https://bitcoincore.org/en/team/.

[22] *See generally* Ethereum Blog (last visited February 15, 2019) https://blog.ethereum.org/.

[23] Vitalik Buterin*, Ethereum Scalability Research and Development Subsidy Programs*, Ethereum Blog (Jan. 2, 2018), https://blog.ethereum.org/2018/01/02/ethereum-scalability-research-development-subsidy-programs/.

The Ethereum Network will not be vulnerable, even if there are future hard forks or splintering. As with the Bitcoin Network, the ability of network participants to “fork” and create another chain is a feature -- not a bug -- of the network. It ensures that the protocol is developed and operated in a way that meets the needs of participants and the market. As set forth below, this “forkability” is an important component of open, permissionless, and decentralized networks like Bitcoin and Ethereum.[24] To the extent commercial risks arise related to hard forks and splintering, market participants can deal with them through legal agreements specifying fork choice rules (e.g., choosing the branch with the most “hash power” or “market capitalization”).

A. The Conceptual and Philosophical Importance of “Decentralization”

A core philosophical principle underlying the design and creation of the Ethereum Network was ensuring that the network was open and permissionless protocol layer.[25] A critical component of ensuring an open network was to design the Ethereum protocol so that no single entity or even small group of people could actually or effectively control or exercise “market power” over the Ethereum Network. A market dominant actor or actors would raise the cost of verifying transactions on the Ethereum blockchain[26] and, more importantly, lead to higher privacy and censorship risks.[27]

As a result, the Ethereum Network was designed to achieve the same type of openness as the Bitcoin Network, where nobody has control or “market power” over the operation or governance of the network. In other words, the network is “decentralized.” This can conceptually be understood from the following dimensions:

- **Logically Centralized**:[28] Both the Ethereum and Bitcoin blockchains are “logically centralized” in the sense that they each present and logically seem like a single monolithic system. In other words, people generally think about interacting with a single “Ethereum” or “Bitcoin” blockchain.

- **Operationally and Architecturally Decentralized**:[29] Despite the “feel” of a single system, there is no single computer or operational architecture for either the Bitcoin or Ethereum blockchains. There is no infrastructural or operational single point of failure. Specifically, the Ethereum Network was designed to depend on the following architectural and operational layers:

    ○ The Ethereum protocol - The protocol defines the “rules” of the network, such as how network participants communicate and the “consensus” algorithms that allow people who do not know or trust each other to agree (or reach consensus) on the state or data of the blockchain. The current protocol was and is reflected in the Ethereum “yellow paper.”[30]

    ○ Software “clients” - A “client” is a piece of software that enables anyone running it to interact with the Ethereum “blockchain” by facilitating communication with and between other clients. These clients are open-sourced and freely available to anyone. In addition, anyone is capable of developing a new client with any capable programming language, so long as the created software conforms to the standards set forth in the yellow paper. From the earliest days of the Ethereum Network, there have always been multiple competing client implementations, in multiple different programming languages.

    ○ Nodes - A “node” is a computer that is connected to the Ethereum Network by virtue of running a software client. The “logically centralized” Ethereum blockchain is simply the result of the communication and “consensus” reached by nodes on the network. Anyone can run a node anywhere

[24] *See* https://vitalik.ca/general/2017/03/14/forks_and_markets.html.
[25] https://github.com/ethereum/wiki/wiki/White-Paper, Philosophy.
[26] Christian Catalini and Joshua S. Gans, “Some Simple Economics of the Blockchain,” MIT Sloan Research Paper No. 5191-16, September 21, 2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2874598 (last visited 6 June 2018), at 5.
[27] *Id.* At 15.
[28] https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274
[29] https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274
[30] https://github.com/ethereum/yellowpaper

in the world by running a software client so long as they have sufficient internet and computer resources available.

  - Miners - A “miner” is a person or organization that validates new blocks, which consist of a group of transactions, for addition to the blockchain. Miners choose to run clients as well as specialized mining software, and perform computationally intensive “work” on the Ethereum blockchain solving an arbitrary mathematical problem (a hashing algorithm). The goal is to generate a unique fingerprint in the form of a cryptographic hash for the group of transactions within that block. This fingerprint is generated according to predefined rules set by the software client as necessary in order to successfully add a block to the blockchain. The Ethereum Network adopted a different algorithm for arriving at these digital fingerprints than the Bitcoin blockchain, in part to make it more difficult to centralize mining power on the Ethereum Network.[31]

    Each of these layers was designed as “open” in the sense that anyone and everyone is permitted to participate, and “necessary” in the sense that the Ethereum Network ultimately would fail without the voluntary participation of the actors at each layer.

- **Politically Decentralized**:[32] The Ethereum Network was designed like the Bitcoin Network in that no single group of individuals or organizations would ultimately control the computers or operations of the network. This contrasts with traditional software networks that are controlled by a single corporation and alternative platforms such as EOS or tez0s, which rely on delegated consortia of hand-picked entities to control portions of the network. Moreover, the Ethereum protocol and its related software components were designed to be “open-sourced.”

  This is significant from a governance perspective, because it enables anyone who disagrees with the governance decisions made by the network to “fork” the network and start a competing network. The concept of “forking” as well as current network governance are discussed in more detail below.

B. Overview of “Forking”

As discussed above, because the Ethereum Network is open-sourced and politically and architecturally “decentralized,” changes to the network cannot be forced upon users in the same way that Microsoft can force all users of Microsoft Word to install updates. With the Ethereum Network, anyone can make changes to the underlying protocol or software by “forking” the project. In the open-source software community, “forking” means that “developers take a copy of source code from one software package and start independent development on it, creating a distinct and separate piece of software.”[33]

In the case of blockchains, including the Ethereum Network, these “forks” can result in different versions of the blockchain. Because there is no single, authoritative copy of the Ethereum blockchain, and the version of the blockchain that we associate as being the blockchain exists only by virtue of thousands of nodes running software clients that allow them to agree on the “correct” blockchain. Thus, it is important what version of the software these nodes are running, including forks.

At the highest level, there are at least two types of blockchain “forks” -- soft and hard. A “soft fork” involves software upgrades that are backwards compatible with older versions, so that participants who did not upgrade to the new software are still able to participate in validating and verifying transactions.[34] More specifically, “soft forks change the rules of a protocol by strictly reducing the set of transactions that is valid, so nodes following the old rules will still get on the new chain (provided that the majority of miners/validators implements the fork).”

[31] https://vitalik.ca/2017-09-15-prehistory.html; *see* also https://media.consensys.net/are-miners-centralized-a-look-into-mining-pools-b594425411dc (describing the extent to people can contribute their computing resources to “mining pools”).
[32] https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274
[33] https://en.wikipedia.org/wiki/Fork_(software_development); *see* also https://lopp.net/pdf/princeton_bitcoin_book.pdf.
[34] https://masterthecrypto.com/guide-to-forks-hard-fork-soft-fork/.

[35] In contrast, "hard forks" involve software upgrades that are not compatible with older versions.[36] In the case of hard forks:

> *"All participants must upgrade to the new software to continue participating and validating new transactions. Those who didn't upgrade would be separated from the network and cannot validate the new transactions. This separation results in a permanent divergence of the blockchain. As long as there is support in the minority chain – in the form of participants mining in the chain – the two chains will concurrently exist."*[37]

In short, soft forks are more like minor updates to the operating software of a blockchain, and hard forks require affirmative "opt-in" by network participants and can result in splits in the blockchain if the fork is contentious.[38]

The Ethereum Network has experienced several "forks" since the Genesis Block. Most of have been soft or planned, non-contentious hard forks. For example, the Ethereum Network has long included a roadmap of planned upgrades involving issues such as privacy and scalability of the network. Those upgrades have been implemented in non-contentious hard forks known as "Frontier Thawing" on September 7, 2015; Homestead on March 14, 2016; and Byzantium on October 16, 2017.[39]

However, as with the Bitcoin Network, there has been a contentious hard fork that led to the creation of a new blockchain.[40] On the Bitcoin Network, the most high-profile and contentious hard fork was Bitcoin Cash.[41] On the Ethereum Network, the most high-profile contentious hard fork was the DAO Fork, which, as with Bitcoin Cash, resulted in two blockchain networks: Ethereum and Ethereum Classic. The DAO Fork resulted from an attack that was launched against a project commonly referred to as "The DAO," which was an early example of a Decentralized Autonomous Organization -- *i.e.*, a "virtual" organization embodied in computer code and executed on a distributed ledger or blockchain.[42] On June 17, 2016, an unknown individual or group (the "Attacker") began rapidly diverting ETH from The DAO, causing approximately 3.6 million ETH—1/3 of the DAO's total ETH—to move from The DAO's Ethereum Blockchain address to an Ethereum Blockchain address controlled by the Attacker (the "DAO Attack").[43] The diverted ETH was held in an address controlled by the Attacker, but the Attacker was prevented by The DAO's code from moving the ETH from that address for 27 days.[44] The Ethereum community put forth various proposals to "rescue" these funds during the 27-day waiting period. One proposal ultimately gained significant support for adoption, and it involved hard-forking the Ethereum blockchain to restore the diverted funds. Some people within the Ethereum Network objected to this solution, typically arguing that the blockchain should be truly "immutable" and never changed.

Nevertheless, many in the community implemented the proposed solution to the DAO Attack. This created a new "fork" of the Ethereum blockchain, where the state of the blockchain no longer reflected the Attack. However, some within the Ethereum Network who opposed the solution chose to run software clients that did not implement the solution's code, and they continued mining and operating on the original Ethereum blockchain. Since this time, the Ethereum blockchain fork that includes the Attack is referred to as "Ethereum Classic," and the other fork of the chain, which reverts the Attack, is known as "Ethereum."[45]

Both of the Bitcoin and Ethereum networks have remained strong following their hard forks. And the potential for more forks continues to play an important role in the governance and development of both networks.

Question 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?

[35] https://vitalik.ca/general/2017/03/14/forks_and_markets.htm.
[36] https://masterthecrypto.com/guide-to-forks-hard-fork-soft-fork/.
[37] Id.
[38] https://vitalik.ca/general/2017/03/14/forks_and_markets.html.
[39] https://www.etherchain.org/hardForks.
[40] *See* https://www.etherchain.org/hardForks; http://list.wiki/Ethereum_Forks.
[41] https://www.technologyreview.com/the-download/609485/bitcoin-cash-had-a-big-day-hinting-at-a-deep-conflict-in-the-cryptocurrency/
[42] *See* SEC DAO Report at 1.
[43] Securities and Exchange Commission, Release No. 81207, https://www.sec.gov/litigation/investreport/34-81207.pdf ("SEC DAO Report") at 9.
[44] Id.
[45] *See* https://en.wikipedia.org/wiki/Ethereum_Classic; https://www.etherchain.org/hardForks.

Like the Bitcoin Network, the Ethereum Network protocol involves several protections against disruptions to the normal function of the network. In addition, there exist substantial impediments to predictably impacting the spot price of ether by attacking or disrupting the Network.

As explained below, attempts to disrupt ether markets by directly disrupting on-chain ethereum transactions are likely to fail. Moreover, while attacks could theoretically shake confidence in the Ethereum Network and have an indirect impact on ether markets, the Ethereum Network protocol contains several protections against such attacks that make them unlikely to succeed or materially and predictably impact ether markets.

A. Disruptions to the Ethereum Network are Unlikely to Directly and Materially Impact Ether Markets in a Predictable Manner.

As an initial matter, notwithstanding the protocol-level protections to prevent attacks and disruptions of the Ethereum Network, a practical impediment to impacting the ether market exists: Specifically, the "Ether market," as it likely relates to futures contracts, is not directly susceptible to attacks on or disruptions of the Ethereum Network. These futures markets are typically based on spot prices from one or more centralized exchanges. The transactions on these exchanges occur "off-chain" — *i.e.*, the transactions execute and settle on the exchange's systems; they are not sent to or settled on the Ethereum Network.

As such, these spot prices will not directly reflect or incorporate disruptions to on-chain activity on the Ethereum Network. For example, consider a hypothetical attacker who holds and wants to make money on a large futures position by delaying or preventing the Ethereum Network from mining a large transaction. Specifically, imagine the attacker holds a short position and wants to delay a large on-chain "buy" of ether on the theory that doing so could help the value of his short. This strategy would fail, among other reasons, because the on-chain transaction likely would not impact the ether spot quotations used by his futures contract(s). In fact, it is theoretically possible that centralized exchanges could continue facilitating ether trades even if the Ethereum Network itself was down.

Moreover, the likely success of such an attack would remain low even if we assume for the sake of argument that the spot price directly incorporated on-chain transactions. Again, setting aside the protocol-level protections against such an attack, the total volume of ether traded on-chain pales in comparison to the off-chain activity through so-called "centralized" exchanges, as depicted in this chart:

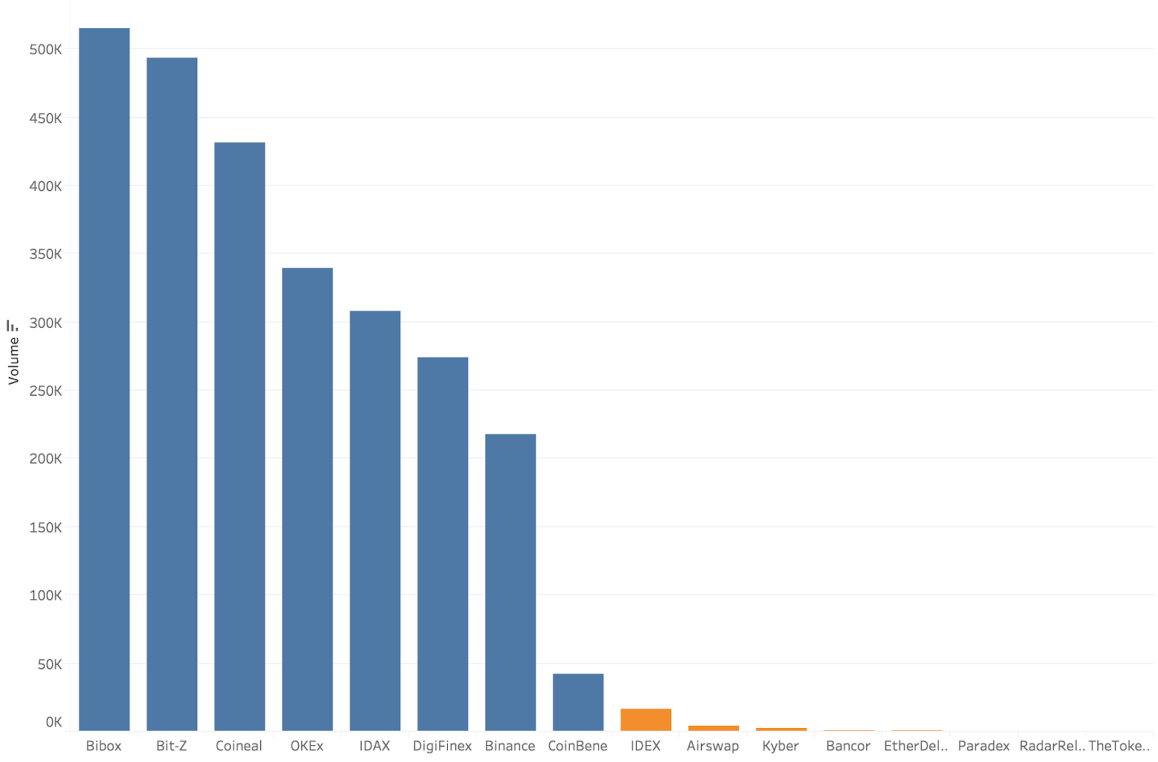

Fig 1. Comparison of 24h Trading Volume of ETH on DEXes and CEXes (Feb 6, 2019)[46]

[46] Data from Coinmarketcap.com and includes the top 8 centralized and decentralized exchanges by volume for the period in question. Note, however, that Coinbase was not part of the data and therefore is not reflected in the chart.

As a result, for pricing purposes, the off-chain transaction activity would almost certainly outweigh the on-chain activity that the attacker would be targeting in this example, and the attack would again fail.

B. An Attacker Could Not Reasonably Expect to Reliably Impact the Ether Market by Attacking the Ethereum Network.

Of course, it remains possible that an attacker could attempt to influence ether markets by shaking confidence in the Network. For example, an attacker could attempt to lock the network in an infinite loop, censor transactions, or carry out 51% attacks, all with the goal of shaking confidence in the Network and impacting ether markets.

Like the Bitcoin Network, however, the Ethereum Network protocol protects against these types of disruptions. It requires payment of gas to protect against infinite loops, and it implements "proof-of-work" and, soon, "proof-of-stake" protocols to protect the reliability of on-chain transactions and assets. Moreover, even if the network's protections do not succeed, any successful network attack or disruption would not necessarily result in a material or predictable impact on ether markets.

i. The Ethereum Network Protects Against Infinite Loop Disruptions by Requiring "Gas" Payments for Computational Resources.

One important potential disruption to the Ethereum Network that could impact confidence and, as a result, indirectly impact the ether market would be locking the network in an infinite loop. An accidental or hostile infinite loop inserted into a smart contract could effectively seize the Ethereum Network.

The Ethereum Network protocol effectively protects against this type of disruption. The fundamental unit of computation on the Ethereum Network is referred to as "gas," and each transaction on the Ethereum Network is required to (1) specify its maximum number of computational steps, and (2) pay for each computational step. In short, the "intent of the fee system is to require an attacker to pay proportionately for every resource that they consume, including computation, bandwidth and storage; hence, any transaction that leads to the network consuming a greater amount of any of these resources must have a gas fee roughly proportional to the increment."[47]

Thus, an attacker could not reasonably expect to seize the Ethereum Network with an infinite loop. The most he or she could accomplish is paying the Ethereum Network to carry out computational steps, which is exactly how the Ethereum Network is designed to operate. As a result, this is not a likely path for an attacker to disrupt ether markets.

ii. Like the Bitcoin Network, the Ethereum Network Currently Uses "Proof of Work" to Protect the Reliability of On-Chain Transactions and Assets.

Like the Bitcoin Network, the Ethereum Network currently uses a "proof of work" protocol to secure the network and prevent disruptions around transactions and ownership of cryptoassets.[48]

For both networks, the proof-of-work system requires that a computer repeatedly execute a hashing algorithm until the algorithm outputs a hash that meets specified conditions--e.g., it contains a sufficient number of leading zeros.[49] This is, effectively, a guessing game that requires participants -- so-called "miners" -- to expend computational resources for a chance to receive the reward of newly minted digital tokens: on the Bitcoin Network, bitcoin; on the Ethereum Network, ether.

[47] Vitalik Buterin, The Ethereum Whitepaper (2013); *see also* Jonathan Rohr and Aaron Wright, *Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets*, Cardozo Legal Studies Research Paper No. 527, (March 28, 2018), https://ssrn.com/abstract=3048104, at 19..

[48] Ethereum uses a different consensus algorithm called "Ethash." This algorithm requires maintaining a large, frequently accessed data structure, which is intended to make it more difficult to mine Ethash with application-specific integrated circuits (ASIC). The rationale for this approach was that "Ethereum's founders wanted to avoid centralization in PoW mining, where those with access to specialized silicon fabrication factories and big budgets could dominate the mining infrastructure and undermine the security of the consensus algorithm." Antonopoulos, Andreas M.,D., Gavin Wood Ph.. Mastering Ethereum (Kindle Locations 7637-7640). O'Reilly Media. Kindle Edition ("Mastering Ethereum").

[49] Mastering Ethereum, *supra*; Vitalik Buterin, The Ethereum Whitepaper (2013); *see also* Jonathan Rohr and Aaron Wright, *Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets*, Cardozo Legal Studies Research Paper No. 527, (March 28, 2018), https://ssrn.com/abstract=3048104, at 19.

The system is designed as "a careful balance of risk and reward that drives participants to behave honestly out of self-interest."[50] The reward, of course, is receiving newly minted digital tokens. The risk derives from "punishment" in the form of the cost of energy required to participate in mining. "If participants do not follow the rules and earn the reward, they risk the funds they have already spent on electricity to mine."[51]

These proof-of-work protocols mitigate disruptions that otherwise would arise from disputes or uncertainty around ownership and transfers of cryptoassets. For example, a common problem that proof-of-work addresses is "double spend." When Person A transfers $100,000 of BTC or ETH to Merchant B in order to buy goods and services, proof-of-work seeks to ensure that Person A cannot turn around and send the same $100,000 of BTC or ETH to someone else.

One important limitation of proof-of-work is that it does not provide transaction finality at the protocol layer. This means that an attacker, in theory, could attempt to disrupt the networks by changing any transaction history. For example, in the previous example, Person A could wait until he receives his purchased goods and services from Merchant B, and then he could attempt to go back and change the on-chain transaction history to regain his $100,000 of BTC or ETH to spend elsewhere.

This type of attack is expensive, at least on the Bitcoin and Ethereum Networks, because the attacker must control at least 51% of the network's mining hash power to rewrite transaction history. For networks other than Ethereum and Bitcoin, a 51% attack may be less expensive to execute, especially for networks where hashpower is easily rented and their proof-of-work algorithms are shared by other larger networks. This is because the cost to rent hash power on these networks for a short period of time is much less expensive than the cost of purchasing all of the mining equipment needed to capture that level of hash power.

Ultimately, proof-of-work provides "probabilistic" finality — *i.e.*, network participants can determine the probability that an attacker could reverse a prior transaction. In general, the deeper embedded a transaction is on the blockchain — *i.e.*, the greater the number of subsequent blocks added on top of the transaction's block — the greater the probability that the transaction will not be reversed. However, as the Bank of International Settlements recently noted, attackers could still have sufficient economic motivations to reverse older blocks, and the risks of such attacks may increase with decreases in mining rewards and hash power to market capitalization ratio.[52] To combat these risks, recipients of high-value transactions may need to wait more blocks before relying on them.[53]

Even a successful 51% attack that rewrites network history may not have a predictable or material impact on ether markets. For example, the Ethereum Classic network recently suffered a 51% attack that enabled an attacker to execute a "double-spend" of $100,000 worth of ETC. The Ethereum Classic network is more susceptible to such attacks than the Ethereum or Bitcoin networks, because it has a lower market capitalization, it uses the same proof-of-work algorithm as the larger, more secure Ethereum Network, has a fraction of the hash power that is securing Ethereum and Bitcoin, and attackers can rent sufficient hash power for the ETC network for short periods of time. Nevertheless, despite the successful attack, there was a negligible impact on ETC spot prices.[54]

iii. The Ethereum Network's Planned Transition to a "Proof of Stake" Protocol Should Make it Even More Difficult to Reliably Disrupt Ether Markets by Introducing Finality, Better Punishment of Validator Misbehavior, Indirect Compensation for Legitimate Holders After Attacks, and Tools to More Quickly Detect and Recover From Attacks.

The Ethereum Network has long planned, and still plans, to transition to a "proof of stake" protocol for securing the network. This transition is expected to begin in 2019 and will occur in phases, including initially using both proof-of-work and proof-of-stake protocols.

The core idea of "proof of stake" is that participants in the block-verification process no longer "risk" only computational "hash power" and energy; instead, they risk their own assets that they "stake" directly with the protocol. These "staked" assets act as a deposit that enables participation in transaction verification but is subject to forfeiture for misconduct.

[50] Mastering Ethereum, *supra*.

[51] *Id.*

[52] Raphael Auer, *Beyond the Doomsday Economics of "Proof-of-Work" in Cryptocurrencies* (2019), www.bis.org/publ/work765.pdf.

[53] *See* Nick Szabo, *https://twitter.com/NickSzabo4/status/1092887225140834304* ("Bitcoin security would not be irreparably degraded if hash power decreased over the long run. The worst consequence of a gradually lower hash power / market cap ratio: it may require recipients of very-high-value transactions to wait more blocks before relying on them.").

[54] *See Here's Why 51% Attacks Don't Affect Price, https://bitcoinist.com/why-51-attacks-dont-affect-price/* .

There is no single proof-of-stake protocol, and so-called "Ethereum 2.0" has developed its own proof-of-stake protocol ("ETH POS"). This protocol is purportedly expected to lead to greater scalability of the Ethereum Network and an immense reduction in energy costs as compared to proof-of-work blockchains. In addition, ETH POS, as compared to proof-of-work, involves some notable additional protections against disruptions to the Ethereum Network.

First, ETH POS involves in-protocol finality. The validation process is divided into "slots" and "epochs," with each epoch consisting of 64 slots and currently defined as 6.4 minutes.[55] After each epoch, finality is achieved for the block that is two epochs prior. With in-protocol finality, attackers cannot reverse previously finalized blocks and transactions regardless of how many validators they control. Even an attacker who controlled greater than 51% of all validators could not reverse finalized blocks. This is significantly different from proof-of-work, which, as discussed above, never finalizes blocks and can always involve transaction reversal given sufficient hash power. Moreover, this in-protocol finality will also enable the Ethereum Network to detect and more quickly recover from any attacks, including 51% attacks.[56]

Second, ETH POS utilizes a multi-step validation process that involves many validators and, compared to proof-of-work, reduces the influence of and potential disruption by even the largest stakeholders in the process. Specifically, block validation involves two categories of validators: proposers, who propose blocks, and attesters, who are organized in committees of at least 128 and vote on the validity of blocks. Proposers are randomly selected every 6 seconds, and attester committees are shuffled every epoch (6.4 minutes).[57] In short, "basically every protocol action is voted on by [large] committees of randomly selected set of members. These committees are constantly shuffled, in some cases as frequently as every 384 seconds."[58]

As alluded to in Question 10, the result of this validation process is that large validators or groups actually have less ability to directly impact (and thus disrupt) block validation than miners with large hash power in proof-of-work. Under proof-of-work, a miner who controls X% of the hash power will have an X% chance of mining the next block.[59] However, with ETH POS, a person or group that controls X% of validators has an X% chance only of proposing a block, which a committee of attesters must then still vote to approve.

In fact, even if a validator controlled ⅓ of the entire ether staked in the protocol, the validator's probability of also controlling enough of any particular committee to do damage -- namely, 2/3 of any particular committee -- is **less than one in one trillion**. Moreover, even if this occurred, the potential resulting damage is limited; this malicious validator cannot reverse previously finalized blocks, and would basically be limited to lying about the data availability of a block or exercising a limited influence on protocol randomness.[60]

Third, the deterrent and punishment costs imposed on misbehaving validators is greater and more narrowly tailored to securing the Ethereum Network than the same costs to miners in proof-of-work. As discussed above, in proof-of-work, miners who attempt to attack the network simply lose the cost of hash power, which often can be rented without needing to purchase expensive mining equipment, and, if the attack fails, the opportunity cost of missing the mining reward. In contrast, in proof-of-stake, the validator will irrevocably forfeit some or all of his staked ether.

This is a significant difference. A malicious miner in proof-of-work can continue mining whenever and however he or she pleases after an attack, because the protocol does not and cannot dictate how the miner uses his or her hash power. But a malicious validator in proof-of-stake loses his or her stake and can never again use those assets for any purpose, including validation. The equivalent in proof-of-work would be lighting on fire all of the mining equipment that is involved in any attack, which is obviously not possible.

Fourth, the ETH POS protocol actually burns (i.e., destroys) any staked ether that is forfeited due to validator misbehavior.[61] By burning this ether, not only does the protocol punish and deter misbehavior but it also reduces the overall supply of ether and indirectly compensates legitimate ether holders, which could help to

[55] https://github.com/ethereum/eth2.0-specs/blob/dev/specs/core/0_beacon-chain.md#slot_to_epoch; *see also* https://www.ethnews.com/clearing-up-casper-proof-of-stake-and-beacon-chain-confusion-once-and-for-all.

[56] Vitalik Buterin, https://notes.ethereum.org/9l707paQQEeI-GPzVK02lA#, "Very high cost of 51% attacks".

[57] https://github.com/ethereum/eth2.0-specs/blob/dev/specs/core/0_beacon-chain.md#justification-and-finalization; *see also* https://www.ethnews.com/clearing-up-casper-proof-of-stake-and-beacon-chain-confusion-once-and-for-all

[58] https://media.consensys.net/exploring-the-ethereum-2-0-design-goals-fd2d901b4c01

[59] https://www.radixdlt.com/post/what-is-proof-of-work

[60] https://vitalik.ca/files/Ithaca201807_Sharding.pdf

[61] Vitalik Buterin, https://notes.ethereum.org/9l707paQQEeI-GPzVK02lA#, "Very high cost of 51% attacks."

mitigate or eliminate any downward pressure on ether spot price that might otherwise result after an attack on the Network.

In sum, these combination of factors make it extremely unlikely that an actor could successfully manipulate the ether spot price by launching an attack on the Ethereum Network. Any 51% attack would be very expensive (likely hundreds of millions of dollars in ether) and would do minimal "damage" because the network could quickly recover. Moreover, the attack likely would result in slashing all of the ether staked by the attacking 51% of validators, causing a large reduction in ether supply that likely would counterbalance any decrease in ether price that might otherwise have resulted from the attack.

iv. Even Successful Attacks or Disruptions of the Ethereum Network May Not Lead to Material and Predictable Changes in the Ether Market.

An attacker may be able to profit from attacks on the Ethereum Network by extracting value directly from the network, but he or she may not be able to predictable profit from the indirect impact on ether markets that may result from that attack. Any direct impact on ether markets is too uncertain and unpredictable to incur the costs necessary to launch a successful attack. For example, as discussed above, the attacker in the ETC 51% attack successfully "double spent" $100,000, but the attack did not materially disrupt ETC spot markets. As the Ethereum Network transitions to proof-of-stake, the ability to profit from or impact ether markets with an attack -- directly or indirectly -- will likely become even less predictable and reliable.

Question 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?

The introduction of derivative contracts on ether would not materially change or modify the incentive structures of the Ethereum Network's planned proof-of-stake protocol. In theory, if an attacker could profit from a short position that would offset the cost of the attack, that could make an attack less expensive. However, as described above, ETH POS is designed to irrevocably burn the attacker's stake, therefore indirectly compensating all other ether holders who were not part of the attack through the reduction in total supply which could have the opposite impact someone taking a short position would seek, and allowing the Ethereum Network to recover quickly from any attack. As a result, as discussed in response to Question 15, the attack could be counterproductive and the attacker would lose both his or her stake as well as the cost of the futures position.

Best regards,

/s/ Patrick Berarducci

Patrick Berarducci
Deputy General Counsel, ConsenSys