February 15, 2019

Re: ***Comments to the Commodities Future Trading Commission in Response to the Request for Input on Crypto-Asset Mechanics and Markets***

Introduction

Blockchains, LLC appreciates the Commission's dedication to gaining further insight into the Ethereum Network and the Ether token through its Request for Input on Crypto-Asset Mechanics and Markets (RFI). Our responses to the questions in the RFI are set forth below. We look forward to participating in the continuing dialog regarding appropriate regulation of the Ether token and the Ethereum Network.

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

The creators of Ethereum were inspired by Bitcoin's ability to offer an ordered ledger of transactions that does not require trust in a central entity, but instead, incentivizes a decentralized network of individuals to use their computers to maintain a verifiable, true record of transactions. They saw the potential for the technology behind Bitcoin – blockchain – to facilitate more advanced applications, such as Executable Distributed Code Contracts (EDCCs) (sometimes referred to as smart contracts). EDCCs are self-executing code contracts that operate according to arbitrary programmed specifications, allowing for the automation of certain processes. For example, an EDCC could be programmed to transfer ownership of assets between parties on a specified date, or upon being triggered by whatever catalyst to which it is programmed to respond. A blockchain enables trustworthy execution of these processes, because if the EDCC is programmed to respond to information stored on the blockchain, then users interacting with that contract can verify the validity of the execution-triggering data.

EDCCs can be programmed such that many of them interact with each other to facilitate complex applications, which means that a blockchain capable of supporting EDCCs is also capable of supporting complex applications. It should be noted that complex applications require Turing completeness, and this was the vision for Ethereum: a blockchain capable of facilitating trustless applications stored across a network of computers. This is sometimes called the "world computer," because instead of storing information related to an application on a central server that individual computers access remotely, in the Ethereum network, that information would be stored across a worldwide network of computers, which is collectively owned and maintained by the network participants.

However, there must be a way to incentivize honesty of the participating computers in maintaining a true ledger of transactions. The Bitcoin network uses bitcoin – a virtual currency that is produced and issued to participating computers to reward their honest collaboration. For the Ethereum network, the incentivizing mechanism is Ether. These digital currencies do not function identically. Bitcoin is primarily a currency and derives its value because it functions as a medium of exchange. For Ethereum, it is only necessary that Ether has enough value to incentivize individuals to use their computers to support the network. Ether, then, while it can be used by individuals as a medium of exchange – and in fact must have value to incentivize honest behavior of network participants – has as its main purpose to pay those running the Ethereum network (also known as miners or nodes) for transaction costs within the network.

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

The most obvious differentiation is that Ethereum is host to EDCC-based applications, whereas Bitcoin continues to serve only as a virtual currency. Using EDCCs, Ethereum hosts video games, blockchain-native businesses (such as Blockchains' planned Distributed Collaborative Entity), virtual currency exchanges, social media platforms, and a range of other applications.
Further, these distributed applications, typically referred to as "DApps," are capable of issuing their own digital tokens, which are used for a wide range of functions. Some uses of these DApp-specific tokens include game tokens, currency, shares of an asset, unique digital collectibles, tools for voting, and other governance-related functions.

Ethereum has a virtual machine (the Ethereum Virtual Machine, or EVM), which is Turing complete (or at least quasi-Turing complete), while Bitcoin does not have a virtual machine and is not Turing-complete. Turing completeness allows for much greater functionality and flexibility, which Bitcoin does not need because it is only a virtual currency. Turing completeness allows for the computation of any imaginable algorithm (given the necessary memory resources and transaction fees), making it almost infinitely flexible to new applications.

The Bitcoin network takes much longer to create new blocks, and there is a maximum possible size for every block. Ethereum has no block size limit and blocks are created much faster. It is also generally true that Ethereum can process more transactions per second than Bitcoin. However, the particulars of how long it takes to create a new block, and how many transactions can be processed per second by each network vary considerably. It is generally quoted that Bitcoin has 10-minute block times, and that it can process roughly 3-7 transactions per second, but sometimes blocks are created much faster. With Ethereum, blocks are generally created roughly every 13 seconds and transactions per second range from 4-20.

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?

There is not necessarily a clear relationship between what the developer community is building on Ethereum and the applications for which end users are using the network. A significant amount of developer talent is currently building the base level protocol of Ethereum and what are called "layer two scalability solutions." All of this development is focused on improving the capacity of the Ethereum network such that it might be capable of more widespread adoption and use for applications with heavy traffic. Much improvement is needed to the base level protocol before many applications built on Ethereum will be particularly attractive to end users, though there are some existing DApps with fairly significant (though still very limited) user interest. Generally, the most used DApps are games and financial services applications, though there are some DApps that do not necessarily have a high level of traffic, but which are more respected, talked about, or which have more Ether (or DApp-specific tokens) locked in their EDCCs. Another use case that gets a lot of attention are Decentralized Autonomous Organizations (DAOs), or blockchain-native organizations that allow people who do not know or trust each other to coordinate around a common purpose, across borders and time zones.

Financial product providers, such as decentralized currency exchanges, loan issuers, securities issuers, and companies tokenizing real world assets currently represent a significant amount of use cases. One prominent DApp is MakerDAO, a platform that allows individuals to use EDCCs developed by MakerDAO to issue Ether-collateralized loans in a stable coin called Dai, which is pegged to the price of the US dollar. MakerDAO represents a significant feat of engineering, as the price of the Dai has remained very close to the U.S. Dollar, despite drastic volatility in the price of Ether. Further, MakerDAO accomplishes all of this through a combination of complex programmed mechanisms and participation by MakerDAO community members. MakerDAO is innovative not just for its ability to offer cryptocurrency-backed stable coin loans, but also in its governance structure, which is increasingly decentralized. MakerDAO token holders govern the loan interest rates and help control price volatility.

Other financial service applications include platforms to fractionalize ownership of assets, like art or housing. Sometimes these are used simply to sell these assets to multiple people, but sometimes it's more about governing the use of objects or resources. For example, one company, Mattereum, is fractionalizing ownership of a very old and expensive violin. The original owner of the violin is fractionalizing ownership of the violin and selling it to investors so that she can gain liquidity, but she is able to maintain ownership of a portion of the violin and stipulate the rules of its use, e.g., that the violin remain unaltered, and that it be played some minimum or maximum number of times per year.

Games are another popular use case. Ethereum allows for the creation of non-fungible assets, which are often used in games as characters or in-game purchases. For example, one of the most popular games (still less than 500 users per day) is called HyperDragons, where people buy unique digital tokens associated with a correspondingly unique digital image of a dragon. Each dragon is encoded with certain traits and capabilities, and then the dragons can battle each other. This works

essentially in the same way as Pokemon or other game cards, except that every dragon is perfectly unique and owned by the person who possesses it.

DAOs are another big potential use case. As discussed above, DAOs are blockchain-native organizations that allow some significant portion of operations to be completed on-chain. This allows for anonymous individuals in a global community to coordinate to complete tasks. Some platforms, like DAOstack and Aragon, allow organizations to facilitate payroll and fund management on-chain, and have DAO members participate in decision making through on-chain voting. This voting can even be used to trigger EDCCs to automatically execute based on member votes. DAOs do not require any one individual make any decisions, but instead rely upon participation and coordination between members. Further, because DAOs are based on EDCCs, DAO members can trust that outcomes will execute exactly as coded.

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?

There are existing and developing[1] commercial enterprises[2] that are using Ether[3] to power economic transactions.[4]

The use of Ether by commercial enterprises for economic transactions has been recorded in accordance with existing guidelines applicable to intangible assets generally. For instance, a commercial enterprise should report use of Ether according to the IRS Property tax guidelines[5] and use the comprehensive financial statements[6] that are standard for its accounting method.[7] Any transaction that takes places on the Ethereum Network requires the use of gas, a fractional measure of Ether, to take place, which can be recorded as an expense.

Footnotes:

1. Existing and Developing Commercial Enterprises
   The Enterprise Ethereum Alliance (EEA) has a list of members organizations around the globe passionate about evolving Ethereum-based enterprise-grade technology through research and development in a range of areas, including: privacy, confidentiality, scalability, and security. https://entethalliance.org.

2. Commercial Enterprise
   Commercial enterprise means any for-profit activity formed for the ongoing conduct of lawful business including, but not limited to:
   - A sole proprietorship
   - Partnership (whether limited or general)
   - Holding company
   - Joint venture
   - Corporation
   - Business trust, or
   - Other entity, which may be publicly or privately owned.

   This definition includes a commercial enterprise consisting of a holding company and its wholly owned subsidiaries, provided that each such subsidiary is engaged in a for-profit activity formed for the ongoing conduct of a lawful business.
   Note: This definition does not include noncommercial activity such as owning and operating a personal residence.
   https://www.uscis.gov/working-united-states/permanent-workers/employment-based-immigration-fifth-preference-eb-5/about-eb-5-visa-classification.

3. Ether
   https://ethereum.github.io/yellowpaper/paper.pdf.
   In order to incentivize computation within the network, there needs to be an agreed method for transmitting value. To address this issue, Ethereum has an intrinsic currency, Ether,

known also as ETH. The smallest sub denomination of Ether, and thus the one in which all integer values of the currency are counted, is the Wei. One Ether is defined as being 1018 Wei. In general, Ether is used to purchase gas. Gas is the fundamental network cost unit, which is paid for exclusively in Ether, which is converted freely to and from Gas as required. Gas does not exist outside of the internal Ethereum computation engine; its price is set by the individual initiating the transaction and miners are free to ignore transactions whose Gas price is too low.

4. Economic Transactions:

   IMF Balance of Payments Manual - Two categories of Economic Transactions:

   - Transactions involving a quid pro quo (two-way transactions)
     - Sales of goods or the rendering of services against payment in money, other credit instruments, or titles to investments, or capital items
     - Barter
     - The interchange of capital items, such as sales of securities against money, sales of one currency against another currency, the discharge of previously incurred commercial debt, etc.
   - Transactions involving no quid pro quo (one-way transactions)
     - Gifts in kind, i.e., in the form of goods and services
     - Gifts of money and other capital items

   https://irows.ucr.edu/research/globres/definitions/imfcncpt.html.

5. Internal Revenue Service Tax Guidance:

   The Internal Revenue Service has issued guidance on the tax treatment of transactions using virtual currencies, such as Ether or bitcoin. For federal tax purposes, virtual currency is treated as property. General tax principles applicable to property transactions apply to transactions using virtual currency.
   https://www.irs.gov/businesses/small-businesses-self-employed/virtual-currenciesTranslating foreign currency into U.S. dollars
   https://www.irs.gov/pub/irs-drop/n-14-21.pdf.

6. Comprehensive set of financial statements:

   GAAP Financial Statements

   - Balance Sheet
   - Income Statement
   - Statement of Cash Flows
   - Statement of Shareholder Equity
   - Notes to Financial Statements

   https://accountinginfo.com/financial-accounting-standards/asc-200/205-financial-statements.htm.

   IFRS Reposting Standard

   - Significance of financial instruments, for performance and financial position
     - Statement of financial position
       - Categories of financial assets and financial liabilities
       - Financial assets and financial liabilities at fair value

        - Reclassification
        - Derecognition
        - Collateral
        - Allowance for credit losses
        - Compound financial instruments
        - Defaults and breaches
    - Statement of comprehensive income
        - Income, expense, gains or losses
    - Other disclosures
        - Accounting policies
        - Hedge accounting
        - Fair value
- Nature and extent of risks, from financial instruments
    - Quantitative Disclosures
        - Credit risk
        - Liquidity risk
        - Market risk
    - Qualitative Disclosures
        - Exposures to risk
        - How to measure and manage the risk

https://cpaclass.com/gaap/ifrs/ifrs-07.htm.

7. Accounting Method:

Generally Accepted Accounting Principles (GAAP or U.S. GAAP) is the accounting standard adopted by the U.S. Securities and Exchange Commission (SEC). While the SEC previously stated that it intends to move from U.S. GAAP to the International Financial Reporting Standards (IFRS), they considerably different. The SEC has acknowledged that there is no longer a push to move more U.S companies to IFRS so the two sets of standards will coexist for the foreseeable future.
https://www.journalofaccountancy.com/news/2013/jan/20137119.html.

Generally Accepted Accounting Principles (GAAP) refer to a common set of accepted accounting principles, standards, and procedures that companies and their accountants must follow when they compile their financial statements. GAAP is a combination of authoritative standards (set by policy boards) and the commonly accepted ways of recording and reporting accounting information. GAAP improves the clarity of the communication of financial information. GAAP may be contrasted with pro forma accounting and with the IFRS standards, which are both considered to be non-GAAP. https://www.investopedia.com/terms/g/gaap.asp.

The U.S. is moving toward IFRS, as re-emphasized by the recent SEC proposal, one wonders what the potential impacts of the differences between these two frameworks on the financial statements will be? And how financial executives can anticipate the adoption of IFRS in order to minimize the last-minute adjustments?
https://www.ifrs.com/overview/General/differences.html.

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?

Market participants can generally exist in one or several of the following groups:

- Miners
- Developers
- Exchanges
- End Users
    - Market Makers
    - EDCC Users

Market participants consider a multitude of factors to gather information about the Ethereum Network. Each of these market participants will be slightly more concerned with certain metrics related to the performance of Ethereum Network. However, all market participants will be interested one metric in particular: the price of ETH.

The price of ETH is a determined by supply and demand. If there is a real or perceived lack of support for Ethereum, market makers will begin selling off their assets causing the price to fall. A decrease in the price of ETH may disincentivize miners from supporting the network. A robust number of miners is what produces a highly secure blockchain network. If miners leave the network, developers and EDCC users will also decrease or stop their activity on the chain due to a lack of security. Healthy price action of ETH helps increase the confidence of market participants and increase the overall security of the network.

Ether transactions on the Ethereum blockchain, as well as on-chain EDCC transactions, are publicly visible and accessible by anyone via a blockchain explorer such as the ones provided below. With respect to liquidity and trade volume, there are third-party data aggregators that collect and publicly disclose such information. Many exchanges also disclose trading volume information to their users. On the other hand, transactions conducted off-chain, such as within applications, are not publicly visible.

Commonly Consulted Ethereum Sources:

- Etherscan.io

    The leading BlockExplorer for the Ethereum Blockchain. A BlockExplorer is basically a search engine that allows users to easily lookup, confirm and validate transactions that have taken place on the Ethereum Blockchain. It is independently operated and developed by a team of individuals who are truly passionate and excited about the decentralized information and infrastructure applications that Ethereum makes possible.
    https://etherscan.io/aboutus.

- Ethernode.org

  The Ethereum Node Explorer. tries to estimate the number of nodes, or validating miners, on the Ethereum network. The estimation is based on an active crawling process that recursively connects to a node and asks for its known peers. https://www.ethernodes.org.

- Ethereum Improvement Proposals (EIPs)

  Describe standards for the Ethereum platform, including core protocol specifications, client APIs, and contract standards.
  https://eips.ethereum.org/.

Etherdocs.org

Contains the Homestead Documentation Initiative. It is a guide that should serve to be an entry level for all Ethereum users and developers. The goal is to create documentation with information, short tutorials, and examples that will cover the basic and intermediate functionality of using Ethereum to interact with DApps or develop a DApp.
http://ethdocs.org.

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?

This concept is referred to as block finality. As it stands, there is no guarantee of finality for Ethereum blocks – it just becomes increasingly less likely over time that a block will revert. Under current specifications and network hash power, after 6 blocks, the likelihood that a block will be reverted is about .02 percent, and by 10 blocks the chance is .002 percent. As the hash power of the network grows, the likelihood of reversion can be further reduced. It has become accepted in the industry that "assumed finality" is reached at 6 or 10 blocks. With block times at roughly 13 seconds, this translates to roughly two minutes after block creation.

When Ethereum switches to proof-of-stake in its next proposed upgrade, there will be built-in finality, which will occur periodically – though the exact amount of time is not yet specified.

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

Below is a side-by-side comparison of the technologies:

Ethereum	Bitcoin
• Ethereum blocks are mined in seconds (usually 10-17 seconds on average). This allows for faster transaction times and Ethereum does it by using the "Ghost" Protocol	• Bitcoin transactions are confirmed in around 10 minutes on average
• Ethereum releases the same amount of Ether each year • Ethereum rewards miners with 3 Ether (current reward) for each block mined. (Reward is slated to be reduced to 2 Ether per block by the end of February 2019). There is no maximum cap on the number of Ethers.	• Bitcoin block rewards halve every 4 years • Bitcoin is currently valued at 12.5 million bitcoins, meaning the total supply of bitcoins will eventually reach 21 million and stop (it has higher holding than spending value)
• Ethereum has a different method for costing transactions depending on their computational complexity, bandwidth use, and storage needs, which is measured by "Gas" and is limited per block, meaning, higher gas transactions take up a larger chunk of the block	• Bitcoin transactions compete equally with each other and are limited by block size
• Ethereum is a Virtual Machine with its own Turing complete internal code. Turing-complete code means that if the machine is given enough computing power, time, and memory (RAM), anything can be calculated or computed. Turing-complete code of Ethereum is what allows it to host and run DApps.	• The Bitcoin Network uses code that is intentionally Turing-incomplete. The Bitcoin Network has one primary computational function – sending payments. Therefore, the Bitcoin Network does not benefit or require a Turing complete computing environment to run.
• Ethereum discourages centralized pool mining through its Ghost protocol rewarding stale blocks	• There is no advantage to being in a pool in terms of Bitcoin block propagation
• Ethereum uses a memory hard hashing algorithm called Ethash that mitigates against the use of ASICS and encourages decentralized mining by individuals using their GPU's	• Bitcoin doesn't have any such algorithm

• Maintains a global ledger of accounts that is associated with an address and a state, such as the number of Ether held.	• Does not maintain a state ledger. Instead, Bitcoin uses a transaction-based ledger.

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?

As currently implemented, similar to many other blockchain networks, scalability is a concern due to security concerns. Because public blockchains handle value transfers, security is paramount, and the algorithms and techniques used to achieve the necessary security prevent the blockchain from scaling up quickly.

Ethereum uses a combination of technical innovations and incentives to ensure that the network accurately records who owns what without the need for a central authority. This is accomplished, in the current design, by each full node processing every single transaction in the network. This ensures that the network is highly secure but at the cost of scalability.

The problem is that it becomes difficult to maintain the balance between increasing the number of network users and adding more users to the chain. This is because Ethereum depends on a network of "nodes," each of which stores the entire Ethereum transaction history and the current "state" of account balances, contracts, and storage.

This is obviously a cumbersome task, especially since the total number of transactions is increasing approximately every 10–12 seconds with each new block. The Gas limit is an estimate that regulates the block size and every transaction requires a certain amount of Gas. The concern is that if developers raise the size of each block to fit more transactions, the data that a node will need to store will grow larger – effectively kicking people off the network. If each node grows too large, only a few large companies will have the resources to run them. In other words, decentralization and scalability are currently at odds, but developers are looking for ways around this.

Several potential solutions that are being developed by Ethereum developers to solve the scalability challenge include:

- **Sharding** - The main idea behind sharding is to break down the network into smaller groups (each, a shard) without sacrificing security and decentralization and achieve unlimited scalability. However, sharding does not work with the current proof-of-work (PoW) consensus mechanism. With the release of "Casper", where Ethereum would be implementing a new algorithm, proof-of-stake (PoS), sharding would potentially solve the scaling issue.

- **Off-chaining** - Borrowing from Bitcoin's Lightning Network, this is a proposed top-layer to the blockchain that mirrors how the multi-layered internet works. According to this vision, most transactions will occur on off-chain micropayment channels, lifting the burden from the underlying blockchain. The reason that this works is that either party can send the transaction back to the blockchain anytime they want, giving both parties the ability to end the interaction. With this add-on, Ethereum's computational limit doesn't need to increase

too much, and the hope is that it will still be reasonable for regular Ethereum enthusiasts to run a full node. Raiden is Ethereum's version of the Lightning Network designed to handle micropayments at a fraction of the current transaction cost. The network will allow for secure transfer of value off-chain using ETH and any ERC20 compliant token. It's like set of channels that allows two parties to exchange unlimited transactions at a fraction of the current cost and in near real-time.

Several solutions are being developed to solve the scalability challenges:

Layer 1 Scaling Solutions

ETH 2.0, formerly known as Serentity, is a long-term research and development project for the Ethereum Network's platform, incorporating fundamental base-layer upgrades like proof-of-stake (PoS) and Sharding. The main idea behind sharding is to break down the network into smaller, more manageable groups (each, a shard) without sacrificing security and decentralization and ultimately achieving unlimited scalability. However, sharding does not work with the current proof-of-work (PoW) consensus mechanism. ETH 2.0 has been, and remains, a difficult work in progress, but has a relatively clear road map in the developer community.

Casper FFG, an eagerly awaited upgrade to the Ethereum platform, launched its testnet in January 2018. A few months later, the developer community shifted its research and development focus away from FFG and towards a plan that would see Casper and Sharding implemented together, which led to the Ethereum 2.0 Specifications: https://github.com/ethereum/eth2.0-specs.

While all roadmaps are subject to change and projections are uncertain, the beacon chain, a mechanism for relaying messages between nodes on the blockchain, is expected to go live in 2019. One of the main functions of the beacon chain is to manage the PoS protocol for itself and all of the shard chains. Despite the roadmap's clarity, there are still unsolved problems in blockchain sharding. For example, while the first few phases of the roadmap are relatively clear, and no significant unsolved theoretical problems remain, plenty of interesting research and implementation issues do remain for future phases so that we get to a truly scalable layer 1 of Ethereum.

Layer 2 Scaling Solutions

Borrowing from Bitcoin's Lightning Network, layer 2 is a proposed top-layer to the blockchain that mirrors how the multi-layered Internet works. According to this vision, most transactions will occur on off-chain micropayment channels, lifting the burden from the underlying blockchain. This works so that either party can send the transaction back to the blockchain anytime they want, giving both parties the ability to end the interaction. With this add-on, Ethereum's computational limit does not need to increase significantly. Instead, the hope is that it will still be reasonable for Ethereum enthusiasts to run a full node. Raiden is Ethereum's version of the Lightning Network designed to handle

micropayments at a fraction of the current transaction cost. The network allows for the secure transfer of value off-chain using ETH and any ERC20 compliant token. It is akin to a set of channels that permit two parties to exchange unlimited transactions at a fraction of the current cost and in near real-time.

Layer 2 solutions off-load computation from Ethereum to “off chain”. In 2018, we saw an incredible leap in the development of layer 2 scaling solutions for Ethereum. These off-chain systems can process transactions faster and more efficiently than the Ethereum main-chain, leading to more scalable payments and smart-contracts. Examples of existing layer 2 solutions include state channels and plasma sidechains. State channels are a very broad and simple way to think about blockchain interactions that could occur on the blockchain, but instead are conducted off of the blockchain without significantly increasing the risk of any participant. Plasma is a scaling technique where operations are moved off-chain into a secondary blockchain, where they can be performed faster and at lower cost. zkSTARKs zero-knowledge proofs, commonly used in cryptography for privacy, are being explored as a potential scaling solution. Zero-knowledge proofs can prove an operation happened, without having to share the transaction’s underlying data.

.

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?

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.

The following response applies to questions 9 & 10:

The proof-of-stake consensus mechanism, which attempts to solve the energy consumption problem inherent in proof-of-work, requires the user to show ownership of a certain number of cryptocurrency units (32, which is called the Stake). The creator of a new block is chosen in a pseudo-random way, depending on the user's wealth. In the proof-of-stake system, blocks are said to be "forged" or "minted," not mined.

In order to validate transactions and create blocks, a forger must first stake their own tokens. This can be thought of as the staker placing his/her holdings in an escrow account: if they validate a fraudulent transaction, they lose their holdings and their rights to participate as a forger in the future. Once the forger puts his/her stake up, he/she can partake in the forging process, and because he/she has staked his/her own money, he/she, in theory, is now incentivized to validate transactions.

Potential Problems with the Proof-of-Stake Consensus Mechanism:

The "nothing at stake" problem is grounded in the fact that voting on a particular version of a proof-of-stake blockchain requires no resources and therefore has no opportunity cost:

- Unlike proof-of-work, where miners must choose at which chain to point their mining power, to the exclusion of other chains, miners can stake their coins on every version of a proof-of-stake blockchain that exists
- Since there's no opportunity cost to mining on a particular chain, the miners have nothing at stake. So rational miners should simply mine on every competing chain that they can access, so as to maximize their mining returns.

In his essay, "On Stake", Vitalik Buterin identified here two ways of addressing the nothing at stake problem:

- Introduce into the protocol a way to penalize those who "equivocated" on a given block, i.e., voted on two different versions of it.
- Introduce into the protocol a way to penalize those who voted on the wrong block, regardless of whether or not they double-voted.

A penalization "slasher" mechanism will be incorporated into the Constantinople upgrade to address this "nothing at stake" problem.

Long Range Attacks

Another widely known, albeit less frequently seen problem is that of long-range attacks, described below.

- In the early stages of proof-of-stake blockchains, there will be a relatively small group of miners with staked tokens. As more and more users join the chain and obtain the underlying asset, the pool of miners, i.e., the users who have staked tokens, becomes larger.
- However, after the fact, the original, small group of miners can get together and decide to go back and "revive" that early version of the chain, and since in the ensuing stages they would be the only ones who could mine blocks, they would soon hold a large share of the assets on that chain.
- And since there isn't a limit on the growth-rate of proof-of-stake chains, only how long it takes each chosen miner to mine the next block, these chains can suddenly become extremely long.

Most blockchains, for example Casper and NXT, address this in a roundabout way, by requiring, in their protocols, that only blocks with a certain range of prior blocks (720 in NXT's case) can be disputed, while the rest are a part of the "main chain". However, this simply changes the scope of the problem. Under this protocol, nodes will have undefined behavior when they come back online after more than the amount of time in the 'window' given by the client, or they come online for the first time.

These two cases lead to something called 'Weak Subjectivity' (all proof-of-stake blockchains have this issue). There are different methods for dealing with this issue:

- Peercoin, for example, gets around it by broadcasting daily the hash of the "legitimate" chain.
- NXT ignores the problem, saying in its wiki that since nodes automatically reject any changes more than 720 blocks in the past, they are not susceptible to long-range attacks. However, they do acknowledge the existence of the problem.
- Vitalik Buterin has acknowledged that Casper will need to depend on trusted nodes to broadcast the correct block hash.

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?

The disagreements in the Ethereum community between proof-of-work (PoW) and proof-of-stake (PoS) are not as prominent as those outside of the community believe. In fact, the majority of the community acknowledges the advantages that PoS offers, such as cutting out the energy-intensive mining process of PoW, the heightened security since bad actors would need to stake assets in order to attempt a 51% attack, preventing large mining-pools from transforming the Ethereum Network into a centralized network, and paving the way for methods that increase transaction speed (e.g., sharding).

Should parties in the community not want to transition to PoS, there is the option of forking to stay on the PoW chain. However, it is unlikely that many parties would choose that route, because of the benefits of PoS. Any disagreements on the transition, outside of the transition setbacks, are minimal, and there is a low probability of such disagreements impacting the Ether market.

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

Ethereum currently hosts a large ecosystem of developers around the world. As of right now, developers can easily program a DApp on the Ethereum blockchain using EDCCs– a simple program that would automatically execute an action as soon as a specific criterion was fulfilled. There are plenty of great projects already demonstrating how DApps can improve user experience. For instance, ENS (Ethereum Name Service) is a solution that allows users to turn their hexadecimal wallet address into a unique domain name instead. Projects like these encourage ideas that might lead to developers making DApps to appeal to the general public.

The open sourced Ethereum clients being developed for different programming languages makes the network more decentralized, robust, and secure.

"Constantinople," a significant upgrade to the Ethereum chain, features small, yet highly technical, improvements to network efficiency and the fee structure, as well as, upgrades that pave the way for Ethereum's highly anticipated scaling roadmap.

The five Ethereum Improvement Proposals (EIPs) set to be released in Constantinople are:

- EIP 145: A technical upgrade written by two Ethereum developers, Alex Beregszaszi and Pawel Bylica, which details a more efficient method of information processing on Ethereum known as bitwise shifting.
- EIP 1052: Authored by core developer Nick Johnson and Bylica, which offers a means of optimizing large-scale code execution on Ethereum.
- EIP 1283: Based on EIP 1087, which was written by Johnson, mainly benefits EDCC developers by introducing a more equitable pricing method for changes made to data storage.
- EIP 1014: Created by Ethereum founder Vitalik Buterin, the purpose of this upgrade is to better facilitate a certain type of scaling solution based upon state channels and "off-chain" transactions.
- EIP 1234: Championed by Afri Schoedon, release manager for major Ethereum client Parity, this upgrade is the most contentious of the batch. It reduces the block mining reward issuance from 3 ETH to 2 ETH and delays the implementation of the "difficulty bomb," an exponential increase in the difficulty of the mining algorithm to force miners to transition to proof-of-stake, for a period of 12 months.

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

Fundamental vs. Surface-Level Upgrades

Broadly speaking, the Bitcoin community prefers minimal upgrades or changes to the Bitcoin protocol, though they do face some significant scalability challenges. It was designed to be peer-to-peer digital cash, and it has performed that function – or been capable of performing it – from the genesis block. Ethereum, on the other hand, has not been – and still is not – the "world computer" it aspires to be. It is too slow, and hardly capable of handling the relatively minimal transaction throughput it currently faces. Upgrades and changes, though often wrought with conflict over specifics, are much needed and anticipated in the Ethereum community. Whereas any potential upgrades to Bitcoin are generally optimizing in nature and (arguably) rarely change any fundamental aspects of the codebase, the Ethereum community members anticipate and are working toward major, fundamental changes: Ethereum is slated to replace its virtual machine, its mechanism for creating new blocks (from proof-of-work to proof-of-stake), and the chain's architecture (a linear chain to a sharded network of chains). The Ethereum community hopes that within the next few years, if all goes according to plan, that Ethereum will be an essentially different blockchain. A new proof-of-stake blockchain will be created that is rooted in the Ethereum proof-of-work chain, and it will eventually become a sharded blockchain. In time, even the existing proof-of-work chain is expected to become a proof-of-stake chain.

Client Coordination

This shift will require massive protocol changes that will require extensive coordination between software companies and independent developers, which brings up another significant difference between Bitcoin and Ethereum: the vast majority of the Bitcoin network is comprised of computers running software made by the same entity, while Ethereum is comprised largely of computers running software made by two different entities – though both networks also include a small number of computers running software created by various other software entities. This software is often referred to as a "client." Clients are the software that allows blocks to be created and validated on the blockchain, and which store the blockchain on individual computers. When protocol changes are agreed upon, it is the clients that must code the changes. When there are a number of software entities making clients for a particular blockchain, they must coordinate to ensure that they all make the same changes. If they fail to coordinate and one client implements changes to its code, but the other clients do not, then instead of working together to create and validate blocks in a chain, the chain splits in half – one chain following the encoded rules of one software and the other chain following the other set of un-upgraded encoded rules.

Because the vast majority of Bitcoin clients (roughly 96 percent) are all made by the same entity (Bitcoin Core), minimal coordination is required to implement changes. If Bitcoin Core developers decide to change the software, they can do so. All they need to do is then convince all of the individuals running the software to also upgrade (though this may be a significant coordination game).

Decentralized Coordination Across Multiple Channels

In the Ethereum network, all development must be coordinated between clients such that all clients fit the same agreed-upon specifications. This coordination takes place in a very public and decentralized fashion, with some de facto leaders, but no official or enforced hierarchy. Specifications are open source and posted on GitHub, and the leading developers of these specifications meet every couple of weeks by public conference call to discuss and debate proposed developments. These protocol changes are discussed across a number of forums, including Gitter, GitHub, Reddit, and encrypted messaging apps. Eventually, decisions are made by rough consensus.

Ethereum's EIP Process

A central part of Ethereum governance is its EIP, or Ethereum Improvement Proposal, process. The EIP process allows anyone to submit a proposal for a new specification or standard that would affect all Ethereum network participants and specifies a process by which these proposals will be refined, denied, or accepted. Many client-level upgrades are initially suggested through the EIP process, but not all. For example, the proof-of-stake and sharding specification is not being completed through an EIP process, since it is an enormous and hugely complicated feat of development requiring significant cross-client and network participation to define from the start. In comparison, smaller changes, such as a proposal to increase or decrease the cost for some specific transaction types, could just be proposed by an individual, and then debated and refined by the community.

Still, while not every change is determined through the EIP process, it does cover an immensely diverse set of decisions – from base level protocol changes, to second layer scaling solutions, to token standards. Because Ethereum is not just a base level protocol with a single currency, but rather a network host to wide-ranging applications some with their own tokens, there is significant coordination necessary to ensure some level of interoperability between contracts and wallets. For example, developers of a gaming application must make sure that the token their application uses is compatible with user wallets, or else no one will be able to store, spend, or buy the application's token. To ensure compatibility, everyone in the community agrees to certain standards for token specification.

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?

Not everyone would agree with the premise that Ether is an "outgrowth from the Ethereum Classic blockchain." The vast majority of the developer and enterprise community (estimates are over 95%), as well as the nonprofit Ethereum foundation, forked the original Ethereum code to fix an error, with the un-fixed chain becoming Ethereum Classic. Ethereum Classic has nothing to do with Ethereum's potential to hard fork or "splinter" in the future.

To further answer the question, a brief explanation of forks is helpful. A soft fork is a backwards compatible software upgrade to the clients storing and building the blockchain. After a soft fork, clients pre- and post-upgrade can still communicate and there is a single blockchain.
A hard fork is a non-backwards compatible software upgrade to clients storing and building the blockchain. Hard forks happen periodically to the Ethereum blockchain and other blockchains when significant protocol changes are made. There is one currently scheduled for the end of February called Constantinople, and there will be another, in probably 8-18 months, called Istanbul. At the time of a hard fork, all of the computers in the network must upgrade their software to maintain a single chain. Both Constantinople and Istanbul are upgrades that have been widely adopted by the community, and it is expected that most, if not all, of the Ethereum community will complete the upgrade.

A chain split happens when not all of the individuals in the network upgrade their software, or choose a different version of software upgrades, and then both groups of people continue to mine new blocks with incompatible software.

All public blockchains can split at any time; the ability to fork in this way is a central value premise to blockchains. While it is highly unlikely that Ethereum would split given the current state of the community, if there are two widely differing, essential and unresolvable disagreements about the direction of software development, or the methods of governance, or any other issue relating to a blockchain, the participants running the nodes can choose to fork the chain and create a blockchain that reflects their needs and values, while allowing for the continuation of the other chain if it is desirable to another group. This is democracy and freedom in action -- public blockchains allow for free collaboration between individuals, not opaque and distant systems or services outside of the control of the people using them. Admittedly, this creates potential market instability, which makes regulation challenging. The potential to fork can create risk for market actors, such as Dapp developers and users, who are exposed to the Ether price. The ability to hedge this risk through financial instruments could reduce the disruptive effect of forks in the marketplace.

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?

Note: The following answer was developed on EthHub, an open source, community-run information hub for the Ethereum community.
EthHub.io. "EthHub CFTC Response." *EthHub*, docs.ethhub.io/other/ethhub-cftc-response/.

Ethereum currently secures billions of dollars in value using open-source code, so the security of the platform is an utmost concern to both developers and the general community. This vigilance has been warranted, given that the platform has experienced availability attacks, smart contract bugs, and ideological disagreements in governance. Through these challenges, the Ethereum platform has demonstrated that its multiple layers of protection can effectively secure value.
Ethereum's defenses can be broadly categorized into four layers: well-written code, security-optimized system design, cautiously implemented crypto-economics, and effective governance.
Well-written code serves as the first line of defense. Ethereum developers have taken many steps to write secure code such as using battle-tested encryption methods, sharing secure design patterns, and implementing rigorous reviews and testing processes. Their efforts are not perfect, and mistakes have sometimes led to significant consequences, such as mistakenly locking up Ether forever or having Ether stolen due to security bugs. Even so, the uninterrupted operation of Ethereum since the Frontier launch in 2015 has shown that the system can remain operational despite these flaws.

Beneath the code, Ethereum's security-optimized system design provides a second line of defense. The pieces of Ethereum work together in a way that minimizes the chance that a fault in one area will have systemic consequences. For example, the application layer is separated from the base protocol layer such that, if a smart contract proves faulty, it will not jeopardize the safety of the network. The well-publicized DAO attack is one great example. Even though an attacker had hacked a smart contract holding about a sixth of all available Ether, a sizeable minority argued that the platform did not need to make a protocol-level change to fix the issue. This position would not have been viable if the application layer was at all connected to protocol functionalities.

Another important system design decision is the encouragement of multiple clients with multiple versions that all sync to the same Ethereum blockchain. There have been numerous examples of how bugs in a blockchain's client software can cause potentially critical failures in the system. Unlike Bitcoin, Ethereum has two major clients (Geth and Parity) for its proof-of-work system that prevent bugs in one client from becoming systemic issues. The ecosystem's security is expected to improve further in this regard under proof-of-stake, where 8 new clients are under development.

After system design, a cautious implementation of crypto-economics serves as a third line of defense for Ethereum. Crypto-economics is defined as the usage of economics, cryptography, and game theory to design systems that generate predictable outcomes given certain assumptions. Ethereum's code and system design use crypto-economics to ensure the network's security. Bitcoin's proof-of-work system pioneered this type of design (which Ethereum largely uses), while

Ethereum's new proof-of-stake system offers significant improvements. Proof-of-work likely needs no introduction; in the 10 years since the introduction of the Bitcoin Network, no one has successfully broken the system. Ethereum's proof-of-stake improves on security by introducing new concepts such as staking and slashing, which increases the economic cost of attacking the network as compared to proof-of-work.

As explained elsewhere, making a switch in consensus system entails significant risks. A failure within the code or the system design might provide short or medium-term inconveniences to the network, but a failure of crypto-economics in the consensus system potentially threatens the network's survival. To mitigate this risk, Ethereum researchers have designed a conservative, staged approach that migrates network activity to the new system without jeopardizing the old system. This approach minimizes the chances that flaws within the proof-of-stake system that may otherwise make the Ethereum platform unusable.

The final and most enduring source of resilience for Ethereum is its effective governance. Since the Ethereum yellow paper was first published in 2014, the community has grown from a small group of visionaries to a network of hundreds of thousands of technologists and enthusiasts around the world. During that time, it has only improved in its ability to act as effective custodians to the value secured by the network.

An example of the community's growth comes from how it handled a broken smart contract written by Parity. On November 6, 2017, a bug in Parity's wallet smart contract caused it to permanently lock away $300 million of community funds. While this bug did not affect as many people as the DAO hack, it directly impacted Parity, a development group which was responsible for the second biggest client that runs Ethereum. When Parity proposed a solution somewhat similar to how DAO hack was resolved (a fix submitted through a hard fork), the community quickly concluded that such a solution was not in the best long-term interests of the network. Right or wrong, the community showed the ability to decide quickly on a potentially controversial topic. As a result, this incident ended up causing little visible impact to the value of Ether.

Within the community, the Ethereum protocol developers have shown an exemplary capacity to put the long-term interests of the network ahead of short-term goals and personal ambitions. The recent decision to combine the development of proof-of-stake and Sharding illustrates this ongoing commitment. Originally, developers of proof-of-stake and Sharding had been working separately to design their respective solutions. Through the course of their research, it quickly became clear that a combined solution would be more secure and less complex. Of course, working together would come with the inevitable result of scrapping their existing work and delaying the timelines for release, but the developers quickly aligned on the new approach with minimal disagreements. Their willingness to change course exemplifies the community ethos to subordinate short-term rewards to long-term value-creation.

Ethereum has operated uninterrupted for three years as a decentralized blockchain. With continued improvements to coding practices, system design, crypto-economics, and governance, the community looks to keep the network running for decades to come.

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 consumers?

As with all virtual currencies, the conversion of Ether into fiat carries multiple risks. First, there is no guarantee that existing exchanges will continue to offer conversion services or that other businesses will fill the void if the exchanges exit this market. Second, substantial volatility makes transacting in Ether difficult. With such volatility, it may be necessary to determine the value of a transaction or what collateral needs to be staked using USD instead of Ether. This will ensure that both parties receive the amount originally agreed upon. Additionally, since Ether is a global virtual currency, any transaction that encompasses a conversion from fiat to Ether back to fiat will have conversion issues due to the rapid price fluctuations. The lack of easily available financial products to hedge this risk may be an impediment to the adoption of Ether by commercial entities.

The infancy of Ether and the exchanges it is offered on, makes custody of virtual currency difficult. Due to the virtual currency being represented in digital form, there has been significant exchange hacks that have cumulative losses in the hundreds of millions of dollars. Without consumer protection mechanisms, investors could lose an entire investment if the exchange experiences a hack.

The exchanges that trade Ether derivative contracts may have custody issues in the context of physically settled futures contracts. Custody has been and remains an issue since asset custody in the spot virtual currency market is less regulated than in the securities or futures markets. However, many U.S.-based virtual currency exchanges have voluntarily sought licenses that subject their custody activities to regulation by State banking authorities, and best practices for custody are beginning to emerge.

Throughout the history of virtual currencies, there has been numerous hacks on exchanges. The most recent is New Zealand-based cryptocurrency exchange Cryptopia. Hackers have stolen over $180,000 and are believed to have the private keys of the Cryptopia users and can withdraw funds from any Cryptopia wallet at will. Without controls, there may be theft of the Ether in custody of the exchanges or the escrow account it is being held in. This issue is highlighted with the bitcoin futures. No exchanges are currently offering the physical delivery futures contracts in part because of custody risks.

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?

This question implies that the individual staker has an interest in the underlying asset or the Ether that the individual has staked in order to become a staker in the Ethereum network. Additionally, a staker is compensated for validating transactions in Ether, and as such, may wish to hedge against price volatility for the Ether earned as a staker. Therefore, the derivative products available to hedge against risk for this individual are derivatives that manage risk. As such, speculative derivative products are not included in this discussion.

One risk for a staker when he or she stakes Ether on the Ethereum network is that the price of that underlying asset becomes volatile. The staker may want to protect against these price fluctuations in the Ether derivative markets. If a potential staker does not have the ability to hedge against price risk for staked Ether, the potential staker may not want to participate in the Ethereum network as a staker at all. Less stakers means less distribution over validation of transactions, which as a policy, the Ethereum network would like to avoid.

We believe that the introduction of derivative contracts on Ether can potentially change and modify the incentive structures for stakers in a positive manner. Having the ability to hedge against price volatility encourages more people to stake Ether since they will be protected against price fluctuations while the Ether is locked up in a staking protocol.

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?

In 2018, the Ether cash market was extremely volatile with the virtual currency at one point losing 94% of its value from its January 2018 peak. With such volatility, it may be necessary for the Commission to implement additional safeguards to ensure that bad actors are not using the underlying cash market of Ether to manipulate derivative contracts market.

In addition to the existing risk management practices governing derivative contracts, the Commission may need to take a more aggressive role in monitoring the collateral/margin staked to deal with market volatility risks and counterparty risks. For example, the Commission could mandate that exchanges and dealers in OTC markets take additional collateral, or even full collateral, before the investor is permitted to trade derivatives. The Commission could also require capping the losses/gains, so that the parties understand from the outset the best-and worst-case scenario. Further, if a transaction is materially amended, or if the margin spread becomes greater than the initial margin/collateral posted, the short seller may be required to post additional collateral/margin. Requiring additional collateral and constantly monitoring the spread of the current margin and the initial margin may deter bad actors who own Ether in the underlying market from manipulating Ether's price to gain a more favorable settlement in a derivative contract as it nears its expiration. Alternatively, the Commission could require exchanges to adjust an investor's margin account balance for profits and losses on daily basis. For even greater protection, it may be necessary for cash to be used for the initial margin and any future settlement amounts instead of other assets, like Ether.

The illiquidity of the Ether market also creates risk management issues. The price of Ether is provided by exchanges. However, with so many exchanges that operate in different global markets, it will need to be determined which exchanges can be relied upon. For this analysis, the size of the exchange, the exchange's vulnerability to financial and cybersecurity hazards, and the KYC requirements of the exchange all must be considered to ensure the stability of the exchange.

The Commission may also need to take measures to ensure exchanges are offering both vehicles associated with futures: the physical delivery of the underlying asset futures and speculative futures. Over the past two years, the bitcoin futures market only encompassed cash settled futures. This permitted bitcoin holders to hedge their exposure. Cash-settled derivatives require an index to settle against, with no consensus on what the "true" price of Ether is or if the inputs forming the index become prone to manipulation and influence by those with vested interests. Given that a cash-settled future involves no transaction of the underlying asset itself, anyone with a large enough position in the underlying asset can impact the price in the futures market by buying and selling in the physical market. Bad actors with large positions in Ether could create activity in the price of Ether prior to the expiration date of the futures contract. This is especially true because the virtual currency market thus far is highly unregulated. Mandating exchanges participate in the physical delivery of Ether futures will require participants to use futures in the manner they were intended. The shorting investor should be required to place the Ether to be delivered in storage to send to the buyer on the expiration of the contract. Thus, prohibiting that short seller from using

that Ether to separately create buying pressure in the physical market. Despite such safeguards, with the market volatility there is a high likelihood that one of the investors will always lose a large amount in the transaction, but regulations cannot substitute for investors' own judgment and due diligence.

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.

Listing or trading of derivative contracts on Ether may drive the Ether market further into a bear market. As alluded to in Request No. 18, many believe that bitcoin futures were instrumental in the rapid bitcoin price decline. The Ether market is currently unregulated. Without oversight of the underlying asset in a derivative contract, the Ether market is subject to manipulation by dishonest investors and traders.

Further, Ether is still a volatile asset and the market will take time to stabilize. Many question whether introducing new players into the market via derivative contracts will benefit or harm the market. In fact, there is already substantial speculative investing in Ether, which is evidenced by significant price swings.

The additional regulations surrounding listing or trading derivative contracts on Ether may also be an issue for the Ethereum community, which is split on the issue of whether virtual currency should be regulated. The decentralized nature of blockchain technology goes against having centralized authorities create rules and regulations. While most agree some regulation is necessary for virtual currency, there is also a strong fear of overregulation by governmental entities. The Commission may consider working closely with the Ethereum Community on any regulations. For example, the Ethereum Community may be willing to adopt guidelines and regulations itself to safeguard against some of the risks mentioned, which would prevent the Commission from having to mandate all regulations for Ether and the Ethereum Network. In exchange, the Commission should only regulate what is necessary to ensure consumer protection versus the entire Ethereum Network ecosystem.

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?

Some unregulated international exchanges may be in a position to manipulate the Ether derivative markets due to information asymmetry with its customers. Certain exchanges have visibility into transactions that customers do not have with little protections in place to ensure the customers have access to such information. To the extent these exchanges offer services to US citizens, they should be monitored and regulated by the appropriate agencies.

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.

Solvency risks could impact the Commission's ability to oversee trading of Ether derivative contracts. For example, Ether prices still have a propensity to rise or fall rapidly without much warning. If a large amount of Ether derivative contracts is sold and a rapid price increase occurs, brokers may not be able to recover the funds from investors going short but will still be obligated to payout the money to investors who went long. This instability has the potential to threaten the solvency of brokers. In the bitcoin arena, many brokers are addressing this issue by creating separate legal entities for bitcoin futures in the event of bankruptcy.

Most of the tradable supply of Ether is not on an exchange but in off-exchange wallets, in order to prevent hacking of exchanges. In stark contrast, the vast majority of all tradable stock for publicly listed companies is transacted on a single exchange. Large market order can drastically impact an exchanges order book causing "slippage." Because of the capacity for large traders to move the market in either direction and employ tactics to encourage this, volatility goes up.

The privacy and anonymous features of the Ethereum Network may also impact the Commission's oversight because transactions can be completely private. Thus, there will be features of transactions in the Ether cash market that the Commission will be unable to examine, including the identity of the parties involved. Such privacy is vital to the success of the Ethereum Network, however it will prevent the Commission from being able to regulate the transaction, unless and until the Ether involved in the transaction is converted to fiat. In order to foster the relationship between the Commission and the Ethereum community, the Commission should consider mechanisms that continue to protect the anonymity of the Ethereum Network as much as possible. For example, many transactions involving Ether or the Ethereum Network are irrelevant to the Commission or any governmental agency. Therefore, these transactions should still be permitted to continue with anonymity. For those transactions that the Commission may need additional information, there potentially could be a standard that the Commission must demonstrate a need for the information and institute guidelines that safeguard the information from only being released to those on a "need-to-know" basis, similar to trade secret protections.

The amount of Ether that can exist is limitless. On the other hand, Bitcoin has a limited number of bitcoins that can ever exist, 21 million. Many argue that having a market cap provides slightly more stability and that Ether by its underlying structure will always be more volatile. Having a market cap allegedly makes an asset scarcer. The theory being that the scarcer an asset is, the more valuable it becomes. With such scarcity comes a level of stability. If there is a finite supply of a token, the value of the coin is likely to increase over time, which will protect the integrity and value of the underlying network. Many critics of Ether's lack of cap, claim that the market will become diluted, causing the value of Ether to constantly rise and fall.

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

Due to the transparency of blockchains, there are multiple services that provide monitoring, visualization and analytical tools for Ethereum and related applications that are built on top. Monitoring on the Ethereum mainnet can be done by various ways. The most common way of monitoring the past transactions, block details, and the status of the network is through:

1) **Block Explorers**, most of which are web applications like – Etherscan, EtherChain, Blockchair, and BlockScout. These block explorers are a group of tools which provide the users with the ability to view past transactions, details of the blocks mined, and a graphical representation of financial aspects related to the transactions. Things that can be explored with some of the block explorers are:
    - Contract Addresses
    - Non-Contract Addresses
    - Transactions
    - Blocks
    - Contract Code

2) **DApps monitoring**, is another way in which the apps running on the mainnet can be monitored to get information about number of users as well as the contract addresses for that applications. State of the DApps, DappRadar, are some of the applications that give extensive list of DApps running on the Ethereum mainnet.

3) There also have been a group of developers who came up with their own ways of depicting the transaction details along with block details, in an attempt to help the users visualize these transactions and block creations. Ethviewer and cryptolights are some of the attempts to depict Ethereum mainnet transactions and block creations in a visually appealing format.

There are various datasets available to download and analyze Ethereum data, collected by multiple organizations. Google released dataset from its BigQuery Public Data and a software system. The software system Google has built on its Cloud platform does several things: it synchronizes the Ethereum blockchain to computers running Parity; it pulls data from the Ethereum ledger on a daily basis, including the results of smart contract transactions; and it "de-normalizes and stores date-partitioned data to BigQuery for easy and cost-effective exploration". Google also adds visualization for accounts that conduct transactions over the mainnet.

As each transaction by definition involves two or more parties, the Ethereum network can be seen as a giant graph of financial interactions. Several projects allow viewing parts of this graph by choosing account or contract of interest. Observeth displays ether and token transfers in a given period of time. Ethtective focuses on showing accumulated graph of interactions for a given Ethereum account.

Firms like Gauntlet, are building a blockchain simulation and testing platform that leverages battle tested techniques from other industries to emulate interactions in crypto networks. Simulation

provides transparency and greatly reduces the cost of experimentation so that teams can rapidly design, launch, and scale new decentralized systems.

Finally, there are application-specific visualization and analytic tools. Most of these tools are focused on financial protocols. For example, MKR Tools provides an overview of the debt positions made via Maker DAO. However, these DApps can be monitored in depth by using DApps monitoring tools specified above.

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

Ethereum network relies mostly on deployment and execution of EDCCs which govern the transfer of Ether or ERC20 tokens over the network and that's why securing the EDCCs becomes the most important aspect in securing the blockchain. However, EDCCs, like any piece of code, suffer from the possibility of having vulnerabilities or bugs. There have been multiple attacks which resulted from exploiting these bugs or unhandled exceptions in the EDCCs. The biggest impact on the Ethereum network was caused by "TheDAO" attack, followed by attacks like King of the Ether Throne (KotET) , GovernMental, EtherPot, SmartBillions and TheRun. The main reason for these attacks were unhandled exceptions in the EDCC's code and the bugs which were exploited.

However, independent auditing and various tools preventing vulnerable EDCCs have been created.

- ZeppelinOS – "an open-source, distributed platform of tools and services on top of the EVM to develop and manage smart contract applications securely". Zeppelin introduces a novel approach in developing EDCCs by using already developed and secure EDCCs (i.e. libraries). Doing so, presumably will lead to mitigating severe vulnerabilities which are related to programming mistakes. Furthermore, the off-chain component provides numerous tools like debugging, testing, deployment and monitoring
- SolCover – a tool that measures and describes the degree of overall testing in an EDCC. Even though it does not serve as a mechanism to identify specific vulnerabilities, it could be argued that it creates a more secure environment with the philosophy that more tests = more secure.

Security audits are considered to be the most effective way of identifying vulnerabilities in a pre-deployment phase. Experienced blockchain developers, and specialized teams, carefully investigate the smart contract manually and automatically to identify possible vulnerabilities, and make sure that it follows best programming practices. Despite the fact that it might be the most secure method for preventing deployment of vulnerable EDCCs, it is not considered to be popular because of the high price range that security audit firms have.

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?

Note: The following answer was developed on EthHub, an open source, community-run information hub for the Ethereum community.
EthHub.io. "EthHub CFTC Response." *EthHub*, docs.ethhub.io/other/ethhub-cftc-response/.

There is a wide range of solutions tackling the problem of storing and managing Ethereum assets a.k.a. creating and using an Ethereum wallet. Solutions vary in the security, usability, and dependence on third-parties. All wallet products can be divided into two groups depending on who owns and controls the private key. First, there are centralized solutions that own the private keys and therefore the underlying assets. They can potentially censor user's actions and are vulnerable to hacks as they become honeypots, but can offer features like account recovery, shorter passphrases, and overall better user experience. Second, there are self-custody solutions where a user is in control of her private key, which is more secure and reliable, but at the same time, a user carries a risk of permanently losing her funds if she'll ever lose the private key. It's worth to mention that there're projects like Gnosis Safe aiming to deliver secure yet convenient and reliable wallet software where a user can be sure that funds will be recoverable even in the event of losing the private key by relying on a decentralized network of trusted third-party KYC providers.

Speaking about self-custody Ethereum wallets, there are implementations of multisignature wallets that are audited and battle-tested. Probably the biggest one in terms of adoption is MultiSigWallet. Another solution is Simple Multisig. To get some insight about the industry average in terms of the number of required keys to sign a transaction, one can look at the existing deployments of MultiSigWallet used by various Ethereum projects. For example, Aragon's multisig is 2-of-3, Bancor's wallet is 2-of-4, and Golem's contract is a 3-of-N multisig.

In terms of creating new EDCCs for safe custody and management of assets, one can look for the best practices in the ecosystem. Consensys' Ethereum Smart Contract Best Practices provide advice on what direction to follow when writing a contract, as well as highlight various caveats. ETHSecurity serves as a curated list of everything related to writing secure contracts including blogs, lectures, and tooling. Finally, there are tools designed to find potential vulnerabilities and bugs in the smart contract source code, including Mythril, Manticore, and Echidna.

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

By the virtue of blockchain technology, everything on the public blockchains is recorded in the public ledger which makes it open for anyone, who is connected to the blockchain, to verify balances of any account or smart contract without any interruptions. Alternatively, one can use a block explorer like Etherscan or Blockscout, which involves some trust in the honesty of the service provider but doesn't require from the user to run a node.

Many firms and organizations provide blockchain auditing services to provide track and trace for transactions from deposit/source to destination. Additionally, private sector CPA firms including PwC, Deloitte, EY, and Accenture now provide full-service forensics for cryptocurrencies and blockchains. However, a private blockchain, which does not reveal sensitive information about the transacting accounts, would need a different approach for auditing. There's a lot of research (Aztec, Enigma) directed towards general-purpose cryptographic schemes that will enable private transactions on Ethereum. In most cases, to audit the balance of a private account or smart contract, one would need to cooperate with the owner of such account in some way. The exact way of collaboration will largely depend on the privacy solution that will be used. One example might involve sharing "view keys" with the auditor, which will allow viewing the balance of the wallet, but not to move the funds. Another solution is to use zero-knowledge proofs that can reveal some properties of the underlying wallet (say, there are more than 10,000 ETH in that wallet) without revealing the exact amount of funds.