

**Comments to the U.S. Commodity Futures Trading Commission in Response to the Request for Input on Crypto-Asset Mechanics and Markets**

February 15, 2019

**Introduction**

The Ethereum Foundation appreciates the opportunity to respond to the Commission’s Request for Input on Crypto-Asset Mechanics and Markets. We have set out below our comments to the questions which lie within our areas of expertise.

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

The Bitcoin network was designed to perform, and was limited to performing, one specific task: processing spot transfers of money (more specifically, transfers of the Bitcoin’s network’s own internal cryptocurrency, also called the “bitcoin”).

However, the blockchain technology underlying the Bitcoin network can be applied for many more purposes than just simple spot currency transfers. The Ethereum network was first conceived at a time when there was increasing interest in building other blockchains customized for other categories of applications. Instead of a future with a variety of single-use-specific blockchains, the intention for the Ethereum network was to provide a single blockchain that could be usable for a maximally wide class of applications, by allowing users to upload a specialized form of computer code that could be executed by 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?**

In the Bitcoin network, each “account” (called a UTXO) stores a quantity of bitcoins as well as a script in an ultra-minimal programming language that determines how to verify who has the right to spend these bitcoins. This allows users to store bitcoins and specify simple conditions for when those bitcoins can be spent (eg. one might want to require a valid digital signature from a specific cryptographic key, or two of a specified three cryptographic keys).

In the Ethereum network, there is also a built-in cryptocurrency that users can transfer to each other, called “ether”, but in addition to this there is a special class of account called a “contract” that also have access to an internal memory (“storage”) as well as a much more expressive programming language that has the ability to read and write to storage.

This type of account can be used to implement smart contracts and other applications involving complex interactions between multiple participants, including applications that are not financial in nature but simply use the blockchain as a source of high-assurance computation and data storage.

Ether is then used as fuel, to allocate the computational resources on the Ethereum network necessary to execute such transactions and applications.

**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 a variety of use cases now, some in the financial space akin to Bitcoin, and some completely non-financial in nature.

Some examples of financial use cases include:

* Issuance of fungible digital assets (ie. currencies or “tokens”). This includes (i) tokens associated with some utility in some application on the platform (eg. REP, MKR), (ii) “stablecoins” which aim to provide digitized versions of real-world assets such as dollars (two of which were recently [authorized by the New York Department of Financial Services](https://www.dfs.ny.gov/about/press/pr1809101.htm)), as well as other miscellaneous types of assets
* Smart contracts being used to implement financial contracts (eg. [HurricaneGuard](http://hurricaneguard.io/) is doing this for weather insurance)

Some examples of non-financial use cases include:

* Decentralized alternatives to internet infrastructure such as DNS (in this case, the “Ethereum Name System” (ENS))
* Issuance of non-fungible digital assets, so far mostly virtual world and game assets and collectibles (most famously [Cryptokitties](https://www.cryptokitties.co/))
* Proof of publication of data (eg. [Acronis’s timestamping service](https://www.ccn.com/backup-software-provider-acronis-reveals-ethereum-blockchain-secured-storage-offering/))
* Management of data associated with access control for identities (eg. uPort)

**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?**

Data related to the Ethereum network itself can be found on [http://etherscan.io](http://etherscan.io/), [http://etherchain.org](http://etherchain.org/), [http://amberdata.io](http://amberdata.io/) among other sources. All of these websites are simply frontends for public data which one can also download and analyze oneself by running an Ethereum full node (the two most popular software packages for this being [Geth](https://github.com/ethereum/go-ethereum/wiki/geth) and [Parity Ethereum](https://github.com/paritytech/parity-ethereum)).

**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?**

The question of how many confirmations are safe depends on what kinds of issues one is attempting to protect oneself against; possible reasons why a very small number of confirmations is not sufficient could include (i) risk of a short-range “chain reorganization” due to very high network latency, (ii) a large percentage of miners attempting to attack the network, (iii) software glitches leading to a chain split or denial-of-service attacks, and other issues. Different attempts to calculate the level of safety that would be equivalent to the usual standard of “six confirmations” used by Bitcoin services include:

* <https://blog.ethereum.org/2015/09/14/on-slow-and-fast-block-times/> : 10 confirmations
* <https://dl.acm.org/citation.cfm?id=2978341>: 37 confirmations
* Kraken’s deposit acceptance threshold (<https://support.kraken.com/hc/en-us/articles/203325283-How-long-do-digital-assets-cryptocurrency-deposits-take-> ): 30 confirmations
* Coinbase’s deposit acceptance threshold (<https://support.coinbase.com/customer/en/portal/articles/593836-why-is-my-transaction-pending->): 35 confirmations

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

At present, Ethereum and Bitcoin both use a similar blockchain structure, using proof of work for consensus, although the way the blockchain is processed differs in key ways. In Bitcoin, processing a block is a relatively simple operation, for each transaction in the block verifying that each account (“UTXO”) used in the transaction is still available, then removing the spent accounts and introducing new accounts containing new outputs. In Ethereum, processing a block involves executing more complex computer code that is contained in the accounts that are touched by each transaction in the block. There are other technical differences, for example, each Ethereum block contains a “state root”, a kind of cryptographic hash of the contents of all accounts after processing that block, allowing not just transactions as in Bitcoin but also account state to be verified given a small piece of block data called the “header”.

In the future, the two chains’ technologies are expected to diverge much more significantly with the introduction of proof of stake and sharding (see below).

**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?**

At present, the Ethereum blockchain has a “gas limit” of 8 million, meaning that the transactions in one block all together cannot consume more than 8 million gas (where “gas” is essentially a unit of computational resources; when reading “gas” one can think “CPU cycles” as an approximation). The smallest possible transaction type consumes 21000 gas; however, many Ethereum applications use more complex smart contracts, and so on average a transaction at present consumes ~67000 gas [footnote: this can be calculated by dividing the values for “daily gas used” by the “transaction count” from the charts at<http://etherscan.io/charts>]; given a block time of 14 seconds this implies a maximum rate of ~8.5 transactions per second, though this value may increase if smaller transactions start to become more popular relative to larger transactions.

Data about transactions and gas consumption can be found at [http://etherscan.io](http://etherscan.io/).

There are two kinds of strategies that the Ethereum community is exploring to increase scalability. The first is upgrades to the Ethereum blockchain itself that allows the blockchain to run in such a way that each node in the network needs to only process a small portion of transactions. This is typically called “sharding”; for more info on this see the FAQ at<https://github.com/ethereum/wiki/wiki/Sharding-FAQs> and the ETH 2.0 Specs at<https://github.com/ethereum/eth2.0-specs/blob/master/specs/core/0_beacon-chain.md>.

The second involves modifications to existing uses of the blockchain that allow them to use the blockchain less often, either by compressing transactions through cryptographic means (eg.<https://ethresear.ch/t/on-chain-scaling-to-potentially-500-tx-sec-through-mass-tx-validation/3477>) or by only using the blockchain in the case where there is a dispute between different users of a system (eg. as in “[state channels](https://counterfactual.com/statechannels/)” or “[Plasma](http://plasma.io/)”).

**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?**

Proof of stake is used in multiple blockchains running today, including NXT, QTUM and Tezos, generally without issue. However, the form of proof of stake used in these blockchains is much simpler than the form that Ethereum aims to eventually use (Casper), as Casper provides much stronger properties, including much faster confirmations and the concept of “finality”. Such more advanced forms of proof of stake have not yet been tested on live public networks. The relatively untested nature of more advanced forms of proof of stake is a key reason why the Ethereum roadmap for upgrading to Casper aims to roll out over time in stages so that the functioning of the network is not dependent on the new proof of stake system until its stability is proven.

**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.**

Some particular challenges and concerns include:

* The risk that centralized exchanges will become the largest participants in proof of stake consensus, leading to the network being controlled by a small number of actors similar to the status quo of mining pool centralization today.
* The risk that proof of stake consensus participation will be dominated by explicit “stake pools” similar to mining pools today.
* The risk that people’s willingness to participate in the proof of stake mechanism without high rewards will be low. With low participation, a single very wealthy actor could quickly join the proof of stake mechanism, gain a majority share of the “validator set” (the set of active proof of stake participants), and use this position to launch 51% attacks.

In designing the proposed Ethereum proof of stake mechanisms, the developers are taking measures to ensure that proof of stake favors smaller and more decentralized participants; for example there is an “anti-correlation penalty” mechanism where participants that are detected by the protocol as unambiguously having violated the protocol’s rules get penalized an amount which is proportional to the number of other participants that were caught violating the protocol’s rules at close to the same time, one of the effects of which is to disincentivize participation in highly concentrated staking pools where all participants’ risk is highly correlated.

**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?**

If there is a critical mass of users that find a switch to proof of stake sufficiently disagreeable, a fork similar to Bitcoin Cash or Ethereum Classic is possible. However, it is our opinion that the risk of this is low, because proof of stake has been presented [as part of Ethereum’s roadmap since 2015](https://blog.ethereum.org/2015/03/03/ethereum-launch-process/) with general support from the community, and from our own observation, most Ethereum users who are fundamentally opposed to the proof of stake switch have already migrated to Ethereum Classic or other systems.

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

We anticipate the use of smart contracts will continue to develop and increase both the number of transactions and the variety of use cases. To support the increasing number of transactions, there is ongoing work on scalability solutions (see above). For variety of use cases, the Ethereum network was from inception intended to act as a single blockchain that could be usable for a maximally wide class of applications. This philosophy continues today and permeates the Ethereum community. Whenever the then-existing state of the Ethereum Network has been unable to provide certain features or capabilities which are needed, evolution and advancement of the network itself has been implemented through the use of Ethereum Improvement Protocols (see below).

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

Both Bitcoin and Ethereum networks follow a relatively similar process where changes to the protocol are first presented as ideas on technical forums (eg. the Bitcoin Wizards mailing list or <http://ethresear.ch>), and once the ideas are sufficiently formalized they are presented as formal proposals (“[Bitcoin Improvement Proposals](https://github.com/bitcoin/bips)” (BIPs) or “[Ethereum Improvement Proposals](http://github.com/ethereum/EIPs/)” (EIPs)), at which point protocol and client developers get consensus on which proposals to include, which then get implemented in code which users then download. In the case of Ethereum, community polling tools like [Carbonvote](http://carbonvote.com/) are sometimes used to gauge wider community opinion on relatively controversial EIPs.

Some key differences between the two communities are:

\* **Norms**. The Bitcoin developer community believes much more strongly in not changing the protocol unless absolutely necessary, whereas Ethereum developers are more likely to accept changes if they improve the platform in the long term. The Bitcoin developer community believes strongly that any upgrades should preserve specific guarantees (eg. that the total supply of bitcoins does not exceed 21 million); the Ethereum community also has highly valued core guarantees (eg. not breaking existing applications unless necessary for the survival of the platform) but they are different in the content and details.

\* **Type of fork**. Bitcoin upgrades are typically implemented via “soft fork”, meaning that any changes to rules are *strictly tightening*: any block that is valid under the new rules is also valid under the old rules, but not necessarily vice versa. This ensures that clients that do not upgrade to the new rules can continue to stay on the same chain, at least if the majority of miners support it, but also greatly limits what can be done with forks. Ethereum upgrades, on the other hand, use “hard forks”: blocks that were valid under the old rules may not be valid under the new rules. In addition to the greater technical simplicity of implementing any given change via a hard fork, hard forks are believed to have other benefits; see<https://vitalik.ca/general/2017/03/14/forks_and_markets.html> for a philosophical piece expanding on this theme.

**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?**

If the Ethereum community attempts to push through changes that some in the community find excessively disagreeable, then splintering is certainly possible. The only way to mitigate this is to have governance norms that discourage adopting changes to the protocol without broad consensus.

Note that this same is true for Bitcoin (see e.g. Bitcoin Cash and Bitcoin Gold), and other decentralized networks.

**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?**

Disruption of the Ethereum network is difficult due to its decentralized nature and the fact that blockchain architectures are optimized for “Byzantine fault tolerance”, a technical term for a network’s ability to operate even when a large portion of the participants are actively trying to undermine its ability to function. However, due to failures of software implementation, attacks have happened before, the [DoS attacks in late 2016](https://www.ethnews.com/ethereum-continues-to-suffer-from-ddos-attacks) being a major example. Given the open nature of the network, the only possible way to prevent attacks from being possible is to continue to improve the security of the network.

**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?**

There are reports that [proof of work miners are already entering](https://news.bitcoin.com/chinese-miners-short-btc-markets-to-hedge-against-falling-prices/) into derivative contracts such as short sales. A wider availability of derivative contracts could make it easier to earn staking rewards without having exposure to the Ether price. It may also become easier to earn money from a hypothetical successful attack on the Ethereum network by shorting Ether. However, neither of these issues are unique to proof of stake; it is possible to profit from shorting a cryptocurrency before attacking it regardless of whether proof of work or proof of stake or something else is the underlying consensus.

**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?**

Cryptocurrency markets arguably face a heightened risk of traders seeking to profit from attacks on the cryptocurrency’s underlying blockchain network by shorting the cryptocurrency before starting an attack. While combining shorting with cyber attacks is not unique to the blockchain space, risk is certainly heightened compared to the other marketsbecause of the much higher damage that a successful attack could cause to the system.

Aside from attacks, in our historical experience there have been two types of events that can reliably cause large price shifts that could be used as the basis for profiting from a position on a derivatives market:

* A coin getting listed on an exchange
* An announcement or execution of a chain split à la Bitcoin Cash or Ethereum Classic

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

The higher complexity of applications that is possible to build on Ethereum relative to other platforms necessarily implies a heightened risk of bugs. The DAO hack from June 2016 is now by far the most well-known example of a smart contract bug taking place and leading to economic losses on a public network. After the DAO hack, the Ethereum community took various steps to improve smart contract security, including:

* Updating of the smart contract safety FAQ: <https://github.com/ethereum/wiki/wiki/Safety>
* Implementing a large number of safety-related improvements to the Solidity programming language, eg. see 0.4.0 here: <https://github.com/ethereum/solidity/blob/develop/Changelog.md>
* Developing new programming languages targeting Ethereum that are more explicitly safety-focused, eg. [Vyper](https://github.com/ethereum/vyper/) and [Bamboo](https://github.com/pirapira/bamboo)
* Working on formal verification of contracts
* Increasing emphasis on security audits

Many of these efforts are still ongoing. In general, we expect smart contract security to never be perfectly solved, much like safety in any other industry, but continue to steadily improve over time.

**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?**

As an example, the Ethereum Foundation cold wallet (publicly viewable at <https://etherscan.io/address/0xde0b295669a9fd93d5f28d9ec85e40f4cb697bae>) is controlled by a smart contract which specifies seven keys, with two rules for withdrawal:

* Any four of the seven keys can approve an operation to transfer any amount of ETH out of the wallet
* Any one of the seven keys can transfer up to 1000 ETH per day (~$90,000 at current prices) out of the wallet

The seven keys are controlled by different individuals that were approved by the Ethereum Foundation board of directors. Four of seven keys is also sufficient to authorize a replacement of any of the seven keys, which has been done to switch keyholders, usually when previous keyholders ceased working for the Ethereum Foundation.

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

To verify the quantity of Ether stored at a given address, the simplest method is to check that address on a public block explorer (eg. Etherscan, Etherchain). To verify that a given person controls a given address, one can either (i) watch them log into that account in person, or (ii) ask them to sign and publish a test transaction with a very small or zero value.

The above is sufficient to prove possession. Other details of treatment of Ether deposits in financial audits are application and jurisdiction-specific.