EthHub – Ethereum Information Hub

CFTC RFI on Crypto-asset Mechanics and Markets

Authors: Eric Conner, Anthony Sassano and over 20 Ethereum community members
Date: 2/15/2019

Introduction

EthHub is a fundamentals-focused, open source, community-driven Ethereum research and resources hub. The website provides in-depth information about Ethereum, the applications built on top of it, and hosts a weekly newsletter & podcast.

We would like to thank the Commission for the opportunity to provide answers to the questions posed and believe that we have produced a relevant and comprehensive document.

The responses below have been prepared by various Ethereum community members in a completely open-source way on the EthHub Github repository. Over 20 individual contributors worked together to produce this document.

Please direct additional questions to: info@ethhub.io

Purpose and Functionality

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

It's first vitally important to distinguish between Ether and Ethereum. Ethereum is an open-source, blockchain-based distributed ledger with decentralized control that supports general computing and economic activities. Anyone is able to build and deploy decentralized products and services that run on top of Ethereum by creating highly flexible programmable transactions, called 'smart contracts'. This smart contract technology has proven to be attractive to developers since it enables them to create programs and business logic that run exactly as coded, trustlessly and with no down time.

Ether is the native cryptocurrency used on the Ethereum network and is used to compensate miners who secure transactions. A planned upgrade to the Ethereum protocol in 2019-2021 would replace mining with a less computationally expensive Proof of Stake mechanism which will be secured by validators, who are also expected to receive a proportional compensation in Ether. Ether also has many current use cases, such as a store of value (e.g. in lending collateral), a medium of exchange (e.g. in trade and payments), and a unit of account (e.g. in digital marketplaces).

The underlying impetus to develop Ethereum and consequently Ether was to utilize aspects of the technology initially developed as part of the Bitcoin blockchain and combine it with the capabilities of smart contract technology. The idea was that this marriage would lead to a platform that could sustain not only the money or medium of exchange use case, but also to add programmability to money, introducing conditional logic to the equation that would open up a world of possibilities with regards to decentralized financial applications and products, and additional decentralized applications. Contrary to the singular purpose vision for Bitcoin as a simple store of value (pivoting more recently from the original peer-to-peer electronic cash vision championed by Satoshi Nakamoto) and ultimately made necessary by a lack of flexibility in the Bitcoin protocol's scripting language, Ethereum was created in response to the aversion to adding new features by the core maintainers of the Bitcoin protocol, such as those required to enable Ethereum-like functionality on Bitcoin.

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

The Bitcoin and Ethereum blockchains are currently both secured by a Proof of Work transaction ordering, Sybil-control mechanisms, and Byzantine Fault Tolerance (BFT) consensus. However, the core difference is that Ethereum offers smart contract functionality enabled by its flexible scripting languages and the Ethereum Virtual Machine (EVM), which is a quasi-Turing Complete virtual machine that compiles smart contract code and enables the execution of that code. These smart contracts allow the incorporation of logic-based programs that can create unique conditions to the transfer and settlement of Ether transactions amongst counterparties. Because of its ability to support smart contracts, Ethereum enables the development and deployment of digital decentralized products and services that can incorporate complex computational logic.

The functionality of the native asset Ether is actually similar to Bitcoin in many ways:

1. Miners who perform computationally intensive work that is crucial to provide secure transaction ordering, block creation which prevents a wide array of failures (e.g. double spending, transaction censorship), are rewarded with Ether issued by the Ethereum network protocol as a compensation for each block found and added to the blockchain; when Proof of Stake is launched in 2019-2021, Stakers who will take the role of securing the network, will also be incentivized through Ether to secure the network in a somewhat similar mechanism.

2. Ether is used to pay for transaction fees on the network. This serves as a Sybil-resistance mechanism, and prevents forged identity-based attacks, as well as spam and denial of service attack protection. The transaction fees on Ethereum are dynamic, and user-adjustable, which creates an interesting fee market that aids in preventing network congestion.

3. Ether is also used to interact or trigger actions by smart contracts deployed on the Ethereum blockchain.

4. Ether is also traded on several secondary markets.

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?

The simplest use case of the Ethereum network is value transfer by sending Ether (which has an attached value) from one person to the other, or by programming value transfers through more complex tools and applications. The amount of decentralized applications being built on top of the Ethereum blockchain is growing at a rapid pace, and the most notable use cases for now are:

1. Decentralized Finance: Currently, the most active applications are those related to "Decentralized Finance". As of 12/11/18, there is currently $120,000,000 worth of Ether being used in decentralized finance applications like Stablecoins such as DAI, tokenized debt such as Dharma, margin trading and derivatives dYdX and decentralised exchanges like the 0x.

2. Games: Smart contracts can be programmed in a way to reflect not only units of account, but also digital representation of game items, such as collectibles like Cryptokitties, cards like in Zombie Battleground or even digital (VR) property such as Decentraland. The fact that items exist on the Ethereum blockchain, and not on the siloed databases of each individual games, makes them more exchangeable, and guarantees the right of ownership of such items regardless of the existence of the actual game/project developers.

Noting that the above are just examples of many others and were just listed here for illustrative purposes.

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 commercial start-ups currently using Ether as a medium of exchange and unit of account in their existing business model. For example, Fuel Games is presently charging some 4200 customers a fixed price in Ether to purchase its unique playable digital trading cards, which upon final sale become provably owned by the customer in a cryptographically verifiable way. At present, over 11,000 Ether has been paid to Fuel Games in exchange for these products. The digital cards, while being collectible and tradable, are primarily intended for use as in-game assets within Fuel Games' video game called Gods Unchained, currently in closed beta. As part of their business model, Fuel Games plans to release new playable card sets 3-4 times a year and charge for them in Ether. While the pricing for these products is currently denominated in Ether, Fuel has announced plans to have the price pegged to a fixed price in dollars. To incentivize consumers to play with the cards, the business has promised that 10% of sales will go towards the US dollar prize pool of an international tournament event they are organizing in 2019. To limit their forex risk, Fuel Games has reported that they regularly convert a portion of their Ether holdings into a stable currency.

The above example demonstrates some of the economic transactions produced by a start-up. In just this one case, a business is collecting payments in exchange for a digital product they are making, where 10% of that payment is being tracked and liquidated for use in another financial obligation.

It has not been divulged how private businesses like Fuel Games might be managing their internal accounting, but there are standards which one might reasonably assume they are following. For example, the Financial Accounting Standards Board classifies native cryptocurrencies, including Ether as indefinite-lived intangible assets under ASC 350 in their report titled *Financial Reporting Alert 18-9 — Classification of cryptocurrency holdings*. Ether, like other cryptocurrencies, meets the definition of an indefinite-lived intangible asset. Using the intangible-asset model results in holdings of cryptocurrencies being recorded at the cost of acquisition, subject to impairment. That is, the model should only capture declines in the value of the cryptocurrency, not increases. When Ether is purchased, the intangible asset would be measured at the price paid or consideration given to obtain the cryptocurrency. However, the question for miners in Proof of Work or validators in Ethereum's proposed Proof of Stake design is more complicated. Unlike a direct purchase, miners and staked validators are awarded Ether as a reward for ordering transactions and securing the network, but they incur costs of computing equipment, electricity, dev-ops and other expenses. At issue for the miners or staked validators is whether the associated costs should be capitalized as an intangible asset or expensed.

While Ether may fit into the existing model for intangible assets and appear as such in the company's balance sheets, a simpler, and potentially better model for representing the economics associated with holding or using Ether is the fair value measurement model, with both realized and unrealized changes reflected currently in the income statement.

It can also be noted that the Enterprise Ethereum Alliance (EEA) is a large group of commercial enterprises dedicated to developing enterprise use cases and building out standards frameworks for Enterprise Ethereum. Additionally, though non-commercial, the United Nations International Children's Emergency Fund's Kazakhstan branch and the UNICEF Innovation Fund is piloting an effort utilizing the Ethereum blockchain to provide tracking and traceability for transactions between UNICEF and partners to enhance transparency and efficiency of how UNICEF deals with its implementing partners on the ground.

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

There are a plethora of publicly available tools, websites, and APIs that this type of information can be obtained from. Exchanges such as Coinbase aggregate trading data and metrics for each blockchain whose native cryptocurrency they have listed. Additionally, free and open source tools such as those provided by coinmetrics.io, etherscan.io, and Santiment, or paid tools such as coinfi.com, Diar Newsletter, and other Ethereum blockchain tools and services monitor and provide metrics. These metrics include the concentration of wealth in Ethereum by wallet address, individual account information including all send and receive transactions (and in some cases available ownership information), daily transaction volume measured in total Ether and USD value equivalent, average block time, average block size, number of nodes connected to the network, current network transaction fees, most active addresses and smart contracts, smart contract internal transaction monitoring, amount of Ether or USD value equivalent stored or transferred by decentralized applications and associated smart contracts, subjective user activity metrics, and more market focused metrics tracking price trends, market cap, total and available supply, liquidity, etc.

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?

A user must only wait 1 block confirmation for their transaction to be validated and confirmed. However, there is a risk of hash power related attacks to the network (e.g. 51% attacks) that could potentially result in double spends or the block a transaction was originally included in being orphaned (abandoned in its own version of the chain that is not accepted by the network) and thus censored by a large hash-rate owning miner or group of miners attacking the network. However, because Ethereum, like Bitcoin, is probabilistic by nature, the probability of such an attack decreases with every block confirmation, as the cost to acquire the hash-rate necessary to attack the network increases substantially until it becomes economically infeasible. Because of this, some merchants may wait a pre-selected amount of confirmations, such as 6 block confirmations for Bitcoin with its 10-minute block time (~1 Hour) or 30 for Ethereum with its 12-14 second block time (~6 mins) in order to avoid this risk. "An analysis by Vitalik Buterin on PoW block times and their effects on transaction finality and security can be found here: https://blog.ethereum.org/2015/09/14/on-slow-and-fast-block-times/."

Technology

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

From a high level, Ethereum is similar to Bitcoin in that it uses a 'blockchain' and uses 'Proof of Work' to achieve consensus and secure the network. Both blockchains have a native digital asset - Ether (ETH) for Ethereum and Bitcoin (BTC) for Bitcoin.

The Ethereum network is a turing-complete blockchain. This means that it is capable of executing arbitrary code - known as smart contracts. The ability to run code on the Ethereum blockchain means that developers can build applications on top of it. One such application, MakerDAO, allows users to use their ETH as collateral to take out a loan denominated in a USD-pegged stablecoin (known as DAI). Applications are all interoperable within the confines of the Ethereum network. Ethereum acts as a common protocol for all decentralized applications built atop, similar to the way that TCP/IP acts as a common protocol for all public web-based applications. It is not strictly limited to being used as a settlement layer as Bitcoin has become.

Ethereum 2.0 (Serenity) is a substantial upgrade for the Ethereum network being deployed in multiple phases. The main features in this upgrade include a move to a novel Proof of Stake system known as Casper (for securing the network), sharding (for scaling the network) and eWASM (a new virtual machine for the network). These upgrades and new features are developed by a decentralized network of core developers spanning 8 individual Ethereum software client teams, the non-profit Ethereum Foundation, and additional volunteer developers and researchers from around the globe.

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?

The Ethereum network faces scalability problems similar to Bitcoin and other decentralized blockchains. Where some other blockchains have traded off decentralization, trust minimization, and security in favor of throughput (transactions per second) both Ethereum and Bitcoin were created on the principle of maximum decentralization and security above all. It is a trade-off as identified in Vitalik Buterin's trilemma for blockchain scalability.

It's important to understand the basics of how the Ethereum blockchain functions before diving into scaling. Every transaction cost a certain amount of "gas", which is the cost, in computational power, to execute a transaction (denominated in Ether). Every block processed on the network has a cap on the amount of gas it can hold (the "gas limit"). This is because if blocks get too large, there are issues with the way they propagate across the network which increases the likelihood of an incidental fork (chain split) as well as storage and initial synchronization issues. Currently, the Ethereum network sits at max capacity in terms of gas used every day, though recent optimizations in the most widely used clients, Parity Ethereum and Go Ethereum, now enable the block gas limit (and by extension the computational throughput of the network) to be increased safely if the mining nodes, and researchers so agree.

This is how Ethereum plans to tackle the scalability issue beyond just the block gas limit:

'Layer 1' refers to the main Ethereum network/blockchain.

'Layer 2' refers to technologies built on top of (or above) the main Ethereum network/blockchain. 'Interoperability' refers to the use of other blockchains.

A decentralized network of open source developers is addressing Ethereum's Layer 1 scalability challenges by introducing a mechanism borrowed from traditional databases - 'sharding'. Sharding takes the blockchain and splits it up into multiple blockchains (that can communicate with each other) so that transactions and computations can be processed in parallel, and then finalized to one larger ledger of record (known as the beacon chain).

An ecosystem of project teams, decentralized application teams, traditional companies, and open source developers are addressing Layer 2 scalability challenges on Ethereum through the use of multiple technologies. These technologies include sidechains or child chains(such as Plasma), state channels, and interoperability chains and bridges that outsource some transacting to other, compatible blockchains and utilize Ethereum strictly as a settlement layer.

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 (and Proof of Work) aren't consensus mechanisms - they are sybil-control mechanisms. They need to be coupled with a protocol such as BFT (byzantine fault tolerance) to achieve consensus.

There are different types of Proof of Stake (PoS).

- DPoS - Delegated Proof of Stake
- LPoS - Liquid Proof of Stake
- Casper FFG (friendly finality gadget)

DPoS has inherent flaws as it tends to centralize the system over time (to what is commonly referred to as a plutocracy). Unfortunately, DPoS suffers from poor distribution of coins and small holder voter apathy, and thus is a honeypot for cartel formation. Additionally, DPoS chains rely heavily on extra-protocol social and political mechanisms to promote "honesty" such as a constitution or block producer agreements which are not enforceable under any jurisdiction and are instead good faith agreements or handshake agreements to operate in the best interest of the network.

Ethereum's Proof of Stake mechanism (known by the common name of Casper) is fundamentally different and intends to maximize decentralization by incentivizing hundreds of thousands of validators to participate in securing the network versus a small subset of voted on delegates.

There are currently multiple projects that employ the Proof of Stake consensus mechanism. There have been many lessons learned from these deployments including potential attack vectors, such as the "nothing at stake" problem. Ethereum researchers have taken these lessons learned and incorporated them into their design requirements. For example, Casper Proof of Stake addresses the nothing at stake problem by enforcing a set of pre-defined conditions and rules that if violated by a malicious party will result in the "slashing" of their staked Ether as a penalty. For example, if a validator proposed a different version of the blockchain versus what the remaining honest nodes have reached consensus on, that validator is slashed a portion of their staked Ether as a punitive measure. This discourages attacks as their stake becomes “skin in the game” or something at stake.

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.

Ethereum's Casper Proof of Stake will function on the basis of validators, each of which will stake 32 Ether. Users are able to run multiple validators but their computing cost will increase as well (it should be noted that there is a cost to running a validator in Casper Proof of Stake including the cost of computational resources, the cost of high availability and dev-ops, and the opportunity cost and risk of locking value in the stacking system when that wealth could be used elsewhere). A validator will be randomly chosen to propose a block and then a committee of users (at least 111) will attest that validator acted properly. If so, the block will be validated and the validator rewarded. If not, the validator's deposit will be slashed and be lost. If an attacker gained 51% of all Ether they could attempt to attack the network but mechanisms in place make it likely that they will still be slashed. At current Ether price, this attacker would be risking $4,300,000,000 to do so and if caught could lose it all. The cost to acquire 51% of the Bitcoin hash rate is much less.

As noted previously, Casper Proof of Stake addresses the "nothing at stake" problem suffered by previous Proof of Stake based blockchains by enforcing a set of pre-defined conditions and rules that if violated by a malicious party will result in the "slashing" of their staked Ether as a penalty.

Additionally, Ethereum enjoyed the benefit of initial Proof of Work based distribution versus other Proof of Stake based chains. This provides greater guarantees for wealth distribution and preventing a single entity from amassing a disproportionate amount of Ether which could grant them a supermajority of the stake weight and thus the block validity vote.

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 roadmap and community consensus is very clear when it comes to the switch to Proof of Stake. There are active conversations occurring about the logistics and mechanisms of the Proof of Stake transition but wanting to stay on Proof of Work is not something actively discussed by any significant portion of the Ethereum community. At any point, a user can attempt to fork or stay on the current Proof of Work chain but the incentive will be very little once Proof of Stake is live because the users of the network see many positive network effects from the updated Proof of Stake version of Ethereum. These include: scalability by also enabling sharding which requires the transition to Proof of Stake, a more solidified monetary policy, the ability to work as a validator securing the network and earn by using your stake as collateral for remaining an honest party, and a greater ecosystem of decentralized applications that can take advantage of both the economic state and scalable state of Ethereum.

It is worth mentioning that Ethereum has only seen one contentious fork in its lifetime following the "DAO hack" and subsequent recovery effort. This was driven partially by a split in the community based on values, which is a natural progression in blockchains /(see Bitcoin Cash, Bitcoin Cash ABC, Bitcoin Cash SV, Bitcoin Diamond, which are all community values driven forks of Bitcoin/).

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

Ethereum currently supports the most active and largest ecosystem of developers globally. In addition to the core protocol developers and the massive ecosystem of decentralized application developers building and testing on Ethereum, there are currently 8 client teams developing individual client implementations for Ethereum which makes the network more decentralized, robust, and secure. A network with a reliance on a single client implementation becomes a single point of attack or failure (see CVE-2018-17144, the Bitcoin Core client bug that represented a High risk vulnerability affecting Bitcoin's security and monetary policy, present in 95% of Bitcoin nodes due to the reliance mostly on the single client implementation).

Additionally, one only needs to visit sites such as edX.org or Udemy.com to view the incredible amount of Solidity and Vyper smart contract development courses enthusiasts have created, or to Indeed.com to see the increasing number of positions related to Ethereum and smart contract development.

Governance

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

The Ethereum governance process, at least in regards to software updates and development, is similar to Bitcoin's in that it uses a public Github repo to track development from proposal to implementation. In Bitcoin, this is referred to as the Bitcoin Improvement Proposal or BIP process, and in Ethereum it is the EIP process. Where the two differ is in the openness to feature additions, layer 1 improvements, and the way in which those updates are discussed, weighed, and proposed. Ethereum seeks to be an inclusive forum for all stakeholders, which would be defined as anyone who believes they would like to contribute to the governance or development of the Ethereum network (Ether holding not required!).

Therefore, there are several different layers of governance in Ethereum. Ethereum utilizes rough consensus to gauge the greater community feedback and acceptance of proposals. Various tools are also used for signal measurement such as coin votes, polling, surveys, and general sentiment gauging attempts across a multitude of social media platforms.

There is not a central governing body for Ethereum, but rather an approach similar to the IETF in which various forums and working groups have been designed to review, discuss, and gauge general community sentiment for each proposal. These forums inform consensus amongst the core developers to inform whether changes should enter the EIP process for technical review, or if further discussions and consensus is needed. Ultimately, these processes are simply to guide development and improvements to the network, as the decision whether or not to approve or accept the updates and changes lies with the thousands of collective users running nodes on the network.

Nodes may choose to run or not to run code they agree or don't agree with. That is the node runners prerogative as the protocol's rules enforcers. If nodes choose not to update, the chain will continue without the added features or changes and is considered rejected by the community. If the nodes choose to update with no contention then the changes are considered accepted by the community. If the nodes are split by their beliefs and values, two chains may emerge if the differences cannot be reconciled. This is a natural expression of free will and decentralization in blockchains, as the communities are allowed to split and run the coded rules that support their interests. Finally, the market provides the final validation of these changes as the market and its participants will determine the value of each resulting blockchain, and its associated currency, if any.

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?

Ether was not an outgrowth of the Ethereum Classic blockchain. Ether, the cryptocurrency, was born out of the genesis block of the Frontier blockchain, the first iteration of the main-net Ethereum blockchain. In March 2016, the Ethereum blockchain hard forked again to add additional features and optimizations to the Homestead chain, the next iteration of the Ethereum blockchain. In July of 2016, following the exploit of a vulnerability found in a smart contract called "The DAO" which resulted in substantial loss of Ether to a bad actor. The Ethereum blockchain was hard forked again to include an "irregular state transition" that recovered the stolen Ether and returned it to the initial owners (it should be noted that the history of the blockchain remains 100% intact and no transactions were censored or removed. Funds were moved via irregular state transition from the hacked DAO child contracts and remaining DAO child contracts to a recovery contract that users could claim their Ether back from to undo the damages caused by the bad actor).

Most in the Ethereum community elected to support the hard-forked chain by upgrading their nodes. This chain became the chain we knew under the ticker ETH. A minority elected to remain on the unchanged chain in which the bad actor retained all of the stolen Ether under the ideological belief in 'code is law.' This chain was expected by the community to disappear over time like the old Frontier chain since only a small minority of nodes were supporting it still, and it had not received support from any exchanges, and thus had no value in the market. Poloniex (one of the largest exchanges at the time) listed the Ethereum Classic chain (the minority chain) and it gained a small share in the greater cryptocurrency market. It has continued on to this day under the ticker ETC building its own support from a small group of likeminded developers and community members operating the network under the ethos of 'code is law.'

As for predicting future hard forks or chain splits, each hard fork carries with it the possibility that the cast off, minority chain gains value in the market if listed by an exchange and raises some support because of it. Blockchains are not insulated or isolated from politics. Bitcoin is inherently political and relies on social contracts to ensure its system remains unchanged, which is what drove the Bitcoin Cash community away, and subsequently split that community into Bitcoin Cash ABC and Bitcoin SV. It is possible Ethereum will endure another contentious issue that could result in community members opting to go their separate ways by running the code that better promotes their interests, but this is not something to be feared. This is the value of decentralization and the freedom to choose the rules that support your values, interests, and opinions best.

Markets, Oversight and Regulation

15. Are there protections or impediments that would prevent market participants or other actors from intentionally disrupting the normal

function of the Ethereum network in an attempt to distort or disrupt the Ether market?

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 often lead to significant consequences such as mistakenly locking up Ether forever or having Ether stolen due to security bugs. These mistakes almost always occur within individual smart contracts, not on the protocol level. Even so, the uninterrupted operation of Ethereum since the Frontier launch in 2015 has shown that the system can remain operational despite these flaws. It should be noted that as industry standards continue to mature less mistakes are to be expected.

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 many clients written in several programming languages with 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 will 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 Bitcoin, 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 over 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 customers?

Ether can be converted to legal tender in two ways: directly via sale on an exchange or indirectly via a sale to another cryptocurrency and then to an exchange. Regarding a direct sale into fiat, Ether faces the same challenges as any other cryptocurrency: volatile price changes and immature exchanges that offer fiat-to-Ether conversion. Both factors contribute significant risk to the acquisition and holding of cryptocurrencies.

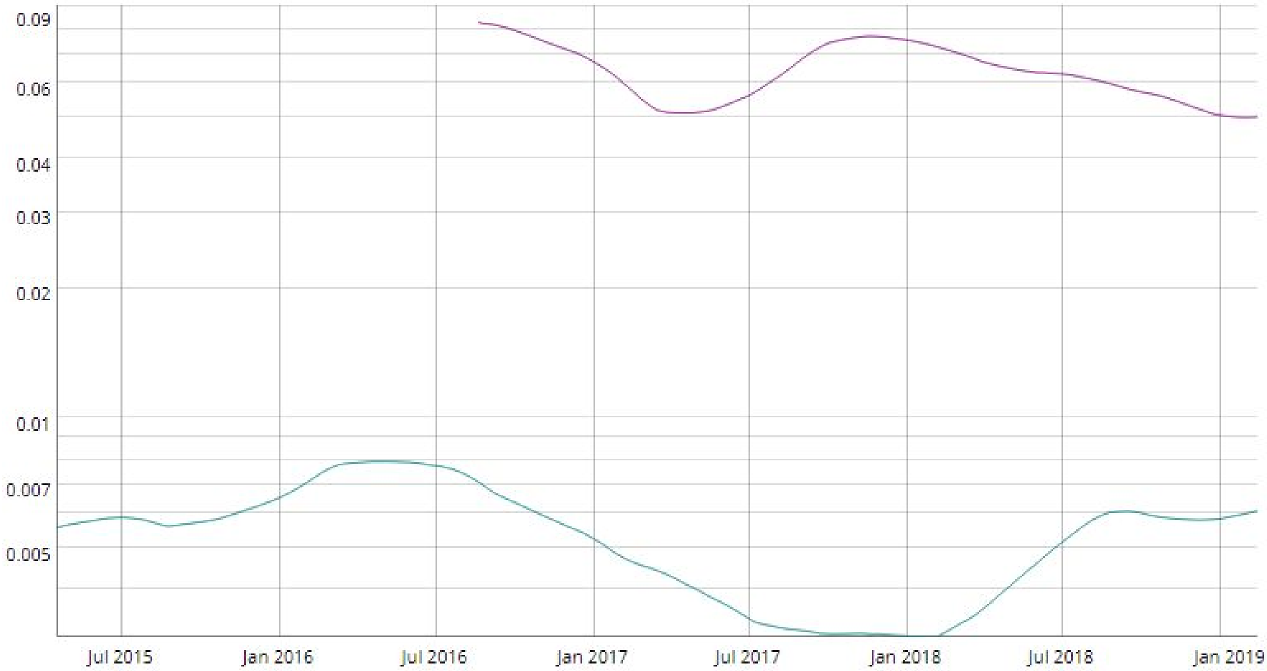

Exhibit 1: Purple = ETH, Turquoise = S&P500

As exhibit 1 shows, volatility in Ether far outstrips the S&P 500. Ether's volatility is not unique among cryptocurrencies as with any cryptocurrency Ether is volatile and markets illiquid and many exchanges unregulated, however there is no increased risk relative to bitcoin.

Beyond price volatility, Ether also must deal with a collection of exchanges that have limited operating experience, diversification, and liquidity. Five major platforms have the licenses to exchange USD with Ether: Coinbase, Kraken, Bittrex, Gemini, and Circle (operates an OTC market). The oldest of these exchanges is only seven years old (Kraken), and all of them entirely rely on revenue generated from cryptocurrency markets to operate. Furthermore, these exchanges have experienced “flash crashes” which cause forced liquidations for those on margin. On June 21, 2017, the price for Ether on Coinbase went down from $319 to 10 cents in a matter of minutes. Kraken has also faced a flash crash in May 2017, and it now faces a class action lawsuit for misconduct.

Given the nascent markets for cryptocurrencies and longstanding laws for KYC/AML, these exchanges play a vital role in allowing investors to legally exchange Ether with USD. Even so, until their performance is tested in more market cycles, an unexpected shutdown to their operations via technical problems or business insolvency remains a significant risk to the purchase and holding of Ether.

Granted, one significant caveat to the risks presented above is that investors can easily exchange Ether into other cryptocurrencies via an array of traditional exchanges, decentralized exchanges, and other services. The exchanges mentioned above all have ETH/BTC trading pairs as do crypto-to-crypto exchanges. In fact, the volume of ETH/BTC transactions on crypto-to-crypto exchanges often outstrip the volume of ETH/USD transactions on Coinbase, the largest US provider. Thus, when considering the liquidity of Ether, it’s important to account for the ability to exchange any cryptocurrency (particularly other liquid ones such as Bitcoin) to USD as a secondary source of liquidity.

It’s also important to consider the risks that some of these providers represent to the ecosystem. Exchanges which don’t have regulated fiat on-ramps often are unaudited, lack proper licenses, and conduct questionable practices such as volume spoofing (An analysis of fake volume: https://medium.com/@sylvainartplayribes/chasing-fake-volume-a-crypto-plague-ea1a3c1e0b5e). These exchanges deserve further scrutiny to protect investors and institutions alike from potential misconduct.

The emergence of stablecoins offers an array of opportunities and risks as well. A stablecoin is a cryptocurrency that has a value pegged to a real-world asset such as USD. These coins facilitate the exchange of USD and Ether by ensuring transactions are easier to track, atomic (Ether only is received if USD is sent), and cheaper/faster to send via state channels. Coinbase and Circle, two prominent firms authorized to trade USD/ETH, have launched an Ethereum-based coin pegged to USD called USDC to achieve this purpose (https://www.centre.io/pdfs/centre-whitepaper.pdf). Gemini has a similar coin call the GUSD (https://gemini.com/dollar/). Separately, the MakerDAO group has released a token called DAI on Ethereum which achieves the USD peg via a decentralized system of smart contracts and collateralization (https://makerdao.com/whitepaper/).

The emergence of stablecoins has significant implications for regulatory considerations on Ether. On one hand, it offers opportunities for traditional cryptocurrency exchanges to increase liquidity, reduce volatility risks, and compliance to KYC/AML regulations via its transaction logging (e.g. all transactions exchanging USDC for ETH would be recorded on the Ethereum blockchain). It also opens the door to new types of decentralized exchanges which can facilitate these transactions without trusting a centralized exchange, thereby circumventing the risks enumerated above about both regulated and unregulated exchanges. On the other hand, stablecoins pose risks to effective regulation given that the main sources of Ether liquidity may not happen on venues where the US government has clear jurisdiction (e.g. decentralized exchanges). While the technologies behind stablecoins and decentralized exchanges are still nascent, it’s important to consider these possibilities when thinking about future regulations.

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?

A liquid and well-regulated derivative contracts market has the potential to improve the robustness of Proof of Stake incentive structures by removing unwanted risk from staking Ether.

To understand the impact of making more hedging options available for Ether holders, it helps to first understand how staking works. Holders of Ether can choose to lock up their Ether in a smart contract, which gives their node the ability to propose blocks of transactions and collect awards from those transactions. The locked-up Ether acts as a "stake" which can get taken away ("slashed") in the event that their node proposes invalid blocks or withholds information. Staked Ether comprises a critical part of the Proof of Stake consensus model, meaning that the network must pay stakeholders of Ether enough to merit a minimum amount staked and keep the network operational.

While network rewards stakeholders for performing a critical function, it also must compensate stakers for the market risks associated with holding a volatile asset. Given that the price of Ether can change significantly from day to day, it's reasonable that the average Ether holder values the ability to sell their holdings at will. This is not possible if they stake their Ether. Not only must the staked Ether stay within the contract for the duration that it's staked, the holder also must abide by a holding period upon deciding to withdraw. The inability to hedge these risks would reduce the number of entities/people willing to stake their Ether and penalize the network by requiring higher rewards for stakers.

Well-regulated derivative contracts on Ether would give Ether holders cheaper ways to hedge the risks of staking Ether. Currently, the only method to hedge these risks is to short-sell Ether on an exchange. Short-selling has limited utility because it relies on the availability of loaned Ether and the continued desire from the loaner to keep the Ether on loan. Derivatives such as futures and options have no such issues beyond the liquidity of the contract. Derivatives also provide new ways to hedge risks. Beyond selling futures instead of short-selling, they can also engage in more sophisticated strategies such as covered call writing or protective collars. Finally, and perhaps most importantly, derivatives require less capital lock-up than short-selling for hedging due to their implied leverage.

As such, the introduction of derivative contracts on Ether would decrease the risks of holding Ether for a given length of time, thereby increasing willingness in holders to stake Ether and decreasing the costs on the network to pay stakers.

Of course, introducing a derivatives market has certain risks as well. The biggest risk is encouraging undue speculation. Speculation makes hedging cheaper, but it also can cause the spot price of Ether to deviate from the fundamental growth rate of the ecosystem. Miners are incentivized to provide network security by receiving fees in Ether. Therefore, as with Bitcoin, if derivative markets could be used to manipulate markets and cause large decreases in price, mining security could be impacted.

While the jury is still out on whether the introduction of derivatives increases volatility and deviations from fundamental valuations on underlying assets, some measures could be implemented to control speculation, which are discussed in the following answer. Even so, given the practical needs for hedging the holding risk of Ether due to staking, the introduction of a well-regulated derivatives market would still augment the incentive structures in Proof of Stake despite the risks.

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?

Existing risk management practices governing commodity derivative markets provides a useful framework for Ether derivatives. In particular, stringent monitoring of position limits would be warranted. If an individual or entity can trade contracts with notional amounts that exceed the amount of staked Ether, they can theoretically profit from a 51% attack on the network, which the Proof of Stake consensus model is supposed to prevent. One recommendation is to tie position limits to a fraction of staked Ether. Such measures would mitigate the risk that parties could collude to successfully attack the network.

Another potential concern is the physical settlement of contracts with Ether. Given the developing nature of cash markets for Ether, there is a risk that the over reliance on physical settlement will cause artificial irregularities in the price of Ether. As explain in answer #17, the security of Ethereum does hinge on the price of Ether, so artificial irregularities in price can increase the risk of opening an attack vector on the network. As such, another recommendation is to keep settlements of Ether in cash.

Otherwise, existing measures to control risk for commodity contracts should prove sufficient for Ether derivative contracts. While Ether operates as a currency-like asset, its volatility and risk factors better reflect a commodity at current valuations. Exchanges would be prudent to apply similar limits to leverage and open interest accordingly.

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.

Market activity, including the trading of derivative contracts, that facilitate price discovery, hedging of risks, and increase liquidity are beneficial for Ether and the Ethereum network. In both Proof of Work and Proof of Stake models, network security is improved when free markets provide accurate price signals to miners and coin holders and enable them to trade and hedge risks appropriately. As described above in questions 17 and 18, derivative markets should take measures that limit the potential for large actors to unduly manipulate market prices as, similar to Bitcoin, market crashes can impact mining security incentives.

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?

The off-shore exchange BitMex, incorporated in the Seychelles, is in a position to engage in market manipulation through its proprietary trading desk that has direct advantages over customer traders. Additionally, BitMex introduced a perpetual swap product that allows customers to purchase ETHUSD perpetual swap contracts and take long or short positions. Bitcoin Quanto ETH/USD contract has a fixed Bitcoin multiplier regardless of the USD price of ETH. This allows the trader to go long or short the ETH/USD exchange rate without ever touching ETH or USD. This product disproportionately reduces the risk of either a long or short side play. Additionally, BitMex offers unchecked leverage up to 50x on the ETH/USD perpetual swap.

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?

The Ethereum Community views privacy as a fundamental human right and as a guarantor of individual human dignity. As such, privacy is one of the core features being worked on by multiple teams. The technology is expected to have profound effects on both the privacy of Ethereum and the scalability of the network.

Privacy technology on Ethereum already has working implementations being deployed to the Ethereum main network (https://medium.com/aztec-protocol/confidential-transactions-have-arrived-a-dive-into-the-aztec-protocol-a1794c00c009).

This privacy technology is unlikely to impede the Commission's ability to monitor, audit or oversee trading activity in the future.

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.

The first group of tools is so-called block explorers — applications that allow users to view past transactions and state of the network. Some Ethereum block explorers are Etherscan, BlockScout, and EthStats.

There are various datasets available to download and analyze Ethereum data, collected by multiple organizations. Different datasets have different content and format, and other tools might be required to get meaningful insights from the data. Google released dataset from its BigQuery Public Data and Alethio is working on the Ethereum Linked Data.

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.

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. 0x Tracker displays all token exchanges that go through the 0x Protocol. Loanscan gives insights into the lending activity facilitated by Dharma and other protocols.

Cyber Security and Custody

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

Smart contracts, like any piece of code, suffer from the possibility of having vulnerabilities or bugs. The security of smart contracts is paramount because they tend to interact with different financial apps and handle value transfer (such as the transfer of Ether or tokens)

Independent auditing and smart contract security firms exist such as Zeppelin, Trail of Bits, and others. These firms provide contract auditing and fuzzing services. Additionally, formal verification services have emerged to formally verify smart contract code. Runtime Verification is one of the leading providers of these services for Ethereum smart contracts.

Two well known custody providers are Gemini and Coinbase.

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?

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 are projects like Gnosis Safe aiming to deliver secure yet convenient and reliable wallet software where a user can be sure that funds will be safe even in the event of losing the private key without relying on a single service provider.

Speaking about self-custody Ethereum wallets, there are implementations of multi-signature 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 what is 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 multi-sig.

In terms of creating new smart contracts 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. To name a few, there are Mythril, Manticore, and Echidna.

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

The current design of Ethereum blockchain means that network state, as well as all transactions, are public. Anyone connected to the blockchain can verify balances of any account or smart contract without the need to ask permission of its owner. 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.

There's a lot of research (Aztec, Enigma) directed towards general-purpose cryptographic schemes that will enable private transactions on Ethereum. With the introduction of such protocols, some (or all) information of the accounts that decided to preserve privacy will be kept in secret. 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 Ether in that wallet) without revealing the exact amount of funds.

Many firms conducting audits utilize tools or forensics services such as Chainalysis to audit and 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.