GAUNTLET

CFTC RFI on Crypto-asset Mechanics and Markets

Authors: Rei Chiang, Tarun Chitra, John Morrow and Aseem Sood
Date: 2/14/2019

This response is jointly written by the team at Gauntlet. We build tools and infrastructure to test the stability and security of decentralized networks. Based on our experience building High Frequency Trading models at designated CFTC-regulated market makers, we created agent-based adversarial models that can rapidly simulate thousands of network scenarios in real-world conditions. We evaluate results in two areas: 1) code security - does the code do what it says it will? - and 2) financial security - is the code statistically indistinguishable from the idea that it is supposed to execute?

We are writing today to share what we have learned working with various networks. We believe decentralized networks provide a useful economic and societal benefit - the Internet is an excellent recent example. That being said, it's still early in their evolution and we have much to learn about their capabilities, risks and security guarantees, especially as it relates to establishing a healthy, stable and dynamic financial market on top of these networks.

A few of the questions required more research and/or lead time than we had available before the deadline. We would happily work with the Commission beyond this RFI to facilitate further research into remaining (or additional) questions.

Thank you for giving us an opportunity to share our thoughts. Please direct additional questions to: tarun@gauntlet.network.

Questions

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

Bitcoin was primarily built as a decentralized payment mechanism. It's a trustless public ledger that tracks how much Bitcoin is owned by a wallet (aka an address).

After Bitcoin's success, it became clear that decentralized systems could be expanded to other use cases like financial derivatives, contracts, and even whole decentralized organizations. Instead of building a separate system for each use case, what if we could codify them into a general computer? And that's how the idea of a generalized, decentralized computing platform was born. Essentially, a system that could support arbitrarily complex contracts - any use case currently supported via traditional computing.

Initial efforts evaluated existing blockchains to identify ones that could be extended. Ultimately, it was decided (for technical and governance reasons) to build a new blockchain from scratch. This new blockchain, eventually called Ethereum, was to be Turing-complete. In theory, anything one can compute on one's own personal computer could be computed in a decentralized manner on the Ethereum blockchain. In practice, there are real-world limitations on capacity, storage, speed, reading external data, generating randomness, etc. that are actively being addressed by the community.

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

In general, Ether supports everything that Bitcoin supports as well as numerous additional use cases.

Bitcoin's primary purpose is payment transactions and store of value. Its ledger tracks only one type of entry: an address and how much unspent bitcoin is currently held by that address. It also supports a simple scripting language (without loops) for advanced payment use cases like multi-signature wallets - meaning one can require more than one private key to unlock the wallet.

Ethereum blockchain contains two types of entries: 1) accounts and 2) contracts. Accounts on Ethereum provide all the same functionality as Bitcoin addresses. Contracts (usually referred to as "Smart Contracts") are the generalized computing containers that enable new use-cases beyond payment transactions and store of value.

We highlight the biggest differences between Bitcoin and Ethereum.

Ethereum smart contracts are Turing-complete and:

- contain long-term, easily accessible storage.
    - Bitcoin accounting is called UTXO - it only tracks Unspent Outputs. We can use the history encoded in the ledger to reconstruct the previous outputs, however it only cares about what's available in an Unspent state right now.
    - Ethereum has proper accounts similar to a bank account displaying the total holdings in one's account. This means a particular contract can issue a custom token and maintain an account of the owners and their corresponding tokens.

- communication with the outside world
    - Both Bitcoin and Ethereum support encoding arbitrary information into their blockchains, so one can easily input information from the outside world. However, due to Bitcoin's limiting scripting language, it's difficult to process this data.
    - Ethereum, on the other hand, has several workarounds to trigger the outside world to provide information that can be processed and become available to the entire blockchain. This is mostly useful to date for small amounts of data like price feeds.
- support increased computing capacity
    - Support for loops, which significantly increase the amount of computation and flexibility
    - One downside of a Turing-complete system is that it can be programmed to run in an infinite loop. Thus someone could program all computers on the Ethereum network to run aimlessly in an infinite loop and stall the entire system. Ethereum addresses this issue by requiring users to pay "gas" (denominated in Ether) up front for computing capacity *of the entire network*. One can think of gas as the fuel to run a computation. Each operation in a smart contract costs gas, anywhere from a few units to several thousand units and the protocol limits the max gas allowed for a single contract. The current gas limit is 8M units.
    - Some examples of gas and dollar costs for common operations that show the disparity of costs:

Operations	Gas Used	Estimated price in USD (1 Eth = ~$107)***
Arithmetic: Add, Subtract, Multiply and Divide	3-5 units	$0.0000006
Modifying a 256-bit word*	5k units	$0.0006
Storing a 256-bit word*	20k units	$0.0023
Creating a contract**	32k units	$0.0037
Max limit	8M units	$0.915

* Storage is expensive. That's why Ethereum 2.0 is planning to introduce a "Storage Rent"
** Creating a contract is the most expensive operation on the Ethereum blockchain
*** This is assuming Gas price of 1.1 GWei based on current conditions. Also worth noting that the Ethereum price is currently low. When it's 5x or 10x more, gas costs become pretty significant.

Block reward mechanism differs in several ways.

Bitcoin blocks are generated every ~10 minutes. This has two downsides:

- Wait times can be long for small use cases
- Significant wastage of mining power, as lots of hashpower (computers mining to be first to find the hash that completes the next block) is racing to find the next block simultaneously. However, the winner takes the entire reward and everyone else must start again with the new block. Network congestion or delayed packets can further exacerbate this problem.

Ethereum addresses these issues:

- It targets block generation time to be ~15 seconds, giving a much faster turnaround.
- It also reduces wasted mining power by rewarding competing chains that were not found first, known as “uncles”. By rewarding uncles, it incentivizes people to mine on other forks and converges mining power quicker, reducing the time to probabilistic finality. It’s worth noting that supporting uncles is possible due to the GHOST algorithm, which required serious academic and algorithmic advances to overcome some of Bitcoin’s flaws

Monetary Policy

Bitcoin is intentionally built to be deflationary. At some point (currently estimated to be in year 2140), all of the 21M bitcoins will have been mined and then the network is expected to run on transaction fees alone.

Ethereum is currently operating as an inflationary system. Miners will continue to receive a block rewards forever, though the rewards reduce over time. There have been proposals to cap Ether at 120M or even 144M tokens, though none have been accepted.

There’s one other consideration when thinking about Monetary policy: lost coins. While we can’t know for sure, estimates of lost bitcoins (meaning the private key is no longer known, effectively blocking use of those bitcoins *forever*) range as high as 4M bitcoins (out of currently 17M issued).

We don’t have an estimate for lost Ether, though based on stories like these, it’s probable that a significant percentage is lost as well. By the nature of these public/private key logistics, it’s likely that some will get lost each year and if block rewards continue to reduce, we may reach a point in the future where newly mined Ether is less than the normal attrition due to lost coins, thus making Ethereum network effectively deflationary.

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?

Current utilization of the Ethereum network mostly consists of financial transactions and services, but other types of usage is growing quickly. We include a list of these cases below, along with their similar offerings in traditional computing and finance.

Ethereum Use Cases (decentralized)	**Traditional (centralized) alternative**
Prediction Network: Augur	PredictIt, OddsChecker
Initial Coin Offerings (tracker)	Venture Capital Funding or Initial Public Offerings
Censorship resistant video transcoding: LivePeer	Amazon Web Services, Wowza, etc.
Stablecoins: MakerDAO	Fiat currencies like USD
On-chain, jurisdiction-less legal entities: Aragon	C corps, LLC, 501c3, etc
Subscriptions: Unlock	Stripe, in-house solutions, etc.
Gaming/Unique digital goods: Cryptokitties	World of Warcraft items
Decentralized Exchanges: Radar Relay, Oasis, etc	Coinbase, Gemini, etc
Financial Derivatives: dYdX, Compound, Set, Dharma	ETrade, Schwab, etc
Gambling apps: Wagerr	?

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 a few businesses that accept Ether as a form of payment for goods and services today, however it is not widely used in this fashion. We contacted a few commercial enterprises on how they record Ether for accounting purposes. Most were still figuring this out and at this time, we don't have any concrete methods to share.

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 few issues to keep in mind when estimating these factors.

- Cryptocurrencies' supply and demand is extremely fragmented. There isn't a single central source with complete information. Instead, there are dozens of worldwide exchanges, often following rules of their own jurisdiction or even arbitrarily modifying them in certain cases.
- This fragmentation leads to sharp interexchange price deviations. Arbitrageurs attempting to close the gaps between exchanges are slowed down by block generation times in the underlying chain, long confirmation wait times, and sometimes due to capital controls from illiquid stablecoin assets (like Bitfinex removing Tether).
- No standardization of exchange data, formats or pricing (e.g. FIX post-Reg NMS)
- No regulations against wash trading -- hard to know how much liquidity is "real". There have been allegations in the past that exchanges were trading within their own systems to "create" liquidity.

Market Size, Liquidity, Trade Volume

Sites like CoinMarketCap or OnChainFX provide an estimate of current Ether issued, projected supply in the future and current ETH-USD prices (averaged across several exchanges).

Since it's expensive to publish to the blockchain, most trades aren't encoded on-chain. They are generally contained within an exchange. We could use statistical sampling: pick a few exchanges and estimate total trade volume based on their trading data. Sites mentioned above that track market cap also provide an estimate of trading volume, based on public information released by different exchanges.

We believe that as institutional players are joining the fray to consolidate liquidity, institution-focused broker dealers (such as Tagomi) will provide consolidated data feeds that give a more precise measurement of market size, liquidity and trading volume.

Types of Traders

These can be characterized in different ways: institutions vs retail, active vs passive, etc. We aren't sure what the Commission is specifically looking for.

We expect most institutions to enter the market via centralized brokers (e.g. Goldman Sachs, Tagomi, etc) and thus centralized brokers should be a good source of information about institutional traders.

OTC market must also be considered - estimates for Bitcoin trades in the OTC market range from 2x-3x the volume of centralized exchanges.

Active versus passive traders can be inferred for decentralized exchanges and sort of estimated for centralized exchanges, by trying to model how interexchange transfers correspond to active traders, e.g. pair trade arbitrageurs.

Ownership Concentration

One benefit of a public blockchain is that ownership (identified by an address) is publicly known. However, that data can also be misleading. Any person can spread their holdings across as many wallets as they want, which would make things look *less* concentrated than they are. Many people also hold their coins on exchanges, which can pool resources into a single address, which make things look *more* concentrated than they are.

Ideally, we'll need to cluster addresses to find out true ownership stakes of an individual or an institution. For example, Chainalysis recently shared their work identifying only a small number of parties behind most BTC heists.

Another way to measure ownership concentration is looking at active wallets. Number of wallets with transactions in the last 30 days, 90 days, 1 year or ever. We tried to compare Bitcoin and Ethereum holdings but were unable to find reliable data for Ethereum in this short timeframe. Here's one data point for Bitcoin.

Principal Ways Ethereum is Used

This is public and on the blockchain. One could look at transactions in each block to see Ether transfers. More than that, the contracts are also public and one can infer a lot of information with minimal analysis. Things like whether new tokens were issued, how they were used, were they sent to a contract that pools Ether (like MakerDAO) to receive DAI (stablecoin).

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?

There is no commonly agreed upon number. It's a tradeoff between probabilistic security and settlement latency and is often picked based on the use case. For example:

- Ethereum White Paper recommends waiting for 7 confirmations (~2 minutes)
- Exchanges can vary: Kraken, for example, requires 30 confirmations (~8 minutes)
- Mining nodes must check parameters for the last 250 blocks, so they often wait for 250 confirmations (~1 hour)

One could also determine the statistical likelihood of a transaction ending up in an invalid block for any number of confirmations by looking at the distribution of orphaned chain lengths. This would allow one to target a number of confirmations to any level of certainty, e.g. there is a 99% chance that a message is confirmed after 4 blocks, 99.9% after 7, etc.

Technology

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

Ethereum was developed when it was realized that Bitcoin couldn't be extended successfully to support the generalized computing use case. As such, Ethereum attempts to improve on many of Bitcoin's features and capabilities (and it's worth noting that not everyone agrees that all the changes in Ethereum are improvements).

	Bitcoin	**Ethereum**
Mining method	Proof of work (PoW)	PoW (planned transition to Proof of Stake in next release)
Hashing Algorithm	SHA-256	Ethhash
Miner Hardware	Custom ASICs	GPU (ASIC resistant)
Memory	Allows storage within blocks	Allows storage and supports data structures for easier retrieving
Programming language	Bitcoin Script	Solidity
Block structure	Merkle Tree and transactions	Lots of additional info like logs, bloom filters, etc
Transaction model	UTXO - only tracks unspent output	Account model

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?

Yes, Ethereum (and most blockchains) are facing major scalability challenges.

Most of the challenges involve improving the transaction rate to be closer to that of a computer. Since Ethereum is trying to emulate a general computer, one would hope that its performance (given the number of resources it is using) is "close" to that of a single computer. However, it is

currently 7-8 orders of magnitude slower than a 1Ghz chip (~15 sec/tx), which drastically limits the types of computations that people can do.

There are a variety of solutions under development:

- Sidechain solutions like Plasma. These allow sidechains - similar blockchains like Ethereum that are rooted in the main chain but operate independently, perhaps periodically syncing with the main chain. Sidechains could significantly increase parallel processing of transactions.
- Sharding solutions, similar to the methods used by traditional databases
- Consensus experiments like Casper and proof of stake (PoS)

There are also a large number of heavily funded *non-Ethereum* versions of these projects. Some of them may have an easier time experimenting than Ethereum because they get to learn from Ethereum's mistakes and they don't need to be backwards compatible, which significantly reduces the amount of development work.

Specific data sources that can be used to estimate network congestion:

- Ethereum Pending Transactions indicate high volumes. Longer list indicates network bottleneck.
- Gas prices are another indicator. As network congestion increases, gas prices rise. Miner's generally choose transactions based on highest gas price. Shorter list of pending transactions, generally means lower gas prices.
- Financial data providers are likely aggregating across different private mempools and could be a good source of information.
- One can use NLP sentiment analysis of major projects' Twitter accounts (and those of their founders and top users) to gauge general consensus. Mentions of scaling are likely increasing.

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?

It's early to claim any PoS chain has been tested or validated at scale. Most of the largest PoS blockchains (by market cap) have launched within the last year:

- EOS launched on June 10, 2018
    - Daily transactions are increasing significantly
    - Still a major concern that only ~21 block producers isn't enough for being decentralized
- Tezos launched mainnet on Sept 17, 2018
    - Transactions per second maxed out at ~40; still too low for large scale adoption
    - Limited developer community and number of dApps available
    - Decentralized governance still not battle tested

Some of the other PoS chains that launched but haven't found major traction: NXT, Peercoin, Blackcoin, and Decred.

Compared to a decade of PoW history for Bitcoin and a few years for Ethereum, we don't have enough data or experience with PoS to claim success at scale.

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.

Proof of work (PoW) can be viewed as "collateralizing a probabilistic reward with energy", whereas proof of stake (PoS) is "collateralizing a probabilistic reward with a digital asset". In order to collateralize energy, you have to prove that you spent it - an irreversible, entropy increasing action. On the other hand, PoS requires careful engineering and threat analysis to cover all the edge cases to prevent "reversing" the ownership of a digital asset while it is staked.

One can view all of the complications of PoS --- having to account for asynchrony [which has been proven to be *not* necessary for Bitcoin] and forcing validators to stay online, figuring out how much to slash to prevent collusive and/or manipulative behavior, providing a delegation mechanism --- as a direct consequence of the fact that it is "cheap" to revert possession of a digital asset. This means that one has to be very careful and thorough while designing PoS systems, because there are many more failure modes and many more states that one has to inspect to prove security.

There is also another way of looking at PoS: it emulates the security properties of PoW by *financializing* a digital asset. It creates mechanisms for validators to earn yield (turning the asset into a bond), it provides penalties for bad behavior that get redistributed to other holders (similar to a self-regulatory agency, e.g. FINRA), and it gives an asset with no intrinsic value some value by agreeing that it can be used for transfer. Just as one has to do with financial products such as derivatives, options, and swaps, one needs to provide risk assessment tools in order for users of these financial assets to figure out how to manage their portfolios. PoW does not require this, but PoS intrinsically requires this. The only way to provide these risk estimates --- the Black-Scholes equations of the staking world, if you will --- is through simulation.

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?

Transition to PoS is not a backwards-compatible, seamless upgrade. It requires an active migration - ETH holders and dApps need to explicitly convert and move to the new fork. This could cause fragmentation or major dislocations in market prices for the tokens involved.

Ethereum has anticipated this outcome and tried to minimize its chances by building in a difficulty bomb. Once switch to PoS happens, a difficulty bomb would increase the amount of hashing power needed for PoW, making it economically unviable for miners to sustain the chain. It's also possible that once the chains split, the PoW supporters postpone the difficulty bomb or remove it altogether and keep both chains active.

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

Ethereum was architected to function as a generalized computer. While it's limited by processing power, memory and certain operations today, its core structure is well designed to improve on all those shortcomings. Additional computing power and memory are being addressed with various initiatives mentioned above. New operations are easily supported technically in both the byte code as well as the Solidity programming language.

In order to be a mature development platform, Ethereum also needs developer tools that allow users to experiment, build and test quickly. These can be built by the community at large, independent of the core team. Given security issues with Solidity, it likely needs a strongly typed language with higher security guarantees as well.

Other ideas that Ethereum is already considering in anticipation of future growth:

- Charging state rent to directly pay for space to compensate contributors (blockchain is getting very big and taking up a lot of disk space).
- Centralized node hosts like Infura provide a valuable service but if everyone uses them, it defeats the idea of a decentralized blockchain. How to discourage centralization?
- Exploring zero-knowledge proofs to mitigate privacy concerns.
- Ethereum Web Assembly (eWASM) could supplant Solidity by allowing developers to use more powerful and typed languages like C/C++/Rust/Go.

Many of the upcoming challenges will be more governance-related than technical. We'll cover that in the next section.

Governance

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

Bitcoin's original creator is still unknown. It's largely run by its developer community, as well as the large miners who weigh in on big proposals.

Ethereum, on the other hand, has well known and active creators: Vitalik Buterin, Gavin Wood, and Joe Lubin (to name just a few). Further, Ethereum Foundation is officially tasked for maintaining the protocol. Bitcoin is decentralized, but fairly uncoordinated. Ethereum is decentralized yet highly coordinated, mostly as a result of the its stronger leadership and community.

As such, it's sometimes easier to make progress in the Ethereum world, while Bitcoin requires consensus from a lot of different players.

In terms of similarities, both have had hard forks before due to community disagreements. Neither supports or plans to support self-amending onchain governance mechanisms.

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?

We believe that Ethereum difficulty bomb and planned hard forks (like migration to PoS) suggest that Ethereum has a less cautious approach and accepts hard forks as a potential outcome.

This isn't meant as a negative assessment of Ethereum or its foundation. We believe that Ethereum's grand vision of a decentralized, general computer is still limited in practice in many ways and it needs to take bold steps (and risk hard forks) to fulfill its mission.

Compared to Bitcoin, with its mission to become a payment mechanism and a store of value, Ethereum has more "cliffs" to cross and thus higher risk of hard forks and splintering.

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?

Yes, a few:

- Enough decentralization such that no single actor wields enough has power to perform a selfish mining attack or a 51% attack for any long period of time
- A relatively ASIC-unfriendly mining algorithm called EthHash, especially in comparison to Bitcoin's SHA-256. EthHash and other algorithms like it are memory hard and thus resistant to being sped up with additional computing power through ASICs.
- A weak derivatives market (transaction fees at venues with liquidity, such as Bitmex, can be thousands to tens of thousands of times as expensive as what they are on regulated derivatives exchanges)
- A lot of long-term "HODLers", who will hold onto the asset forever. (ETH's inflation schedule is not too severe until we get closer to the difficulty bomb that is the on-ramp to PoS)

However, when Ethereum transfers to PoS (in reality, a PoW/PoS hybrid, at least at the bootstrapping stage), it will be particularly vulnerable to plutocratic behavior (e.g. the Gini coefficient of the Beacon Chain in ETH 2.0 might be extremely high - current estimates of the Gini coefficient of Ether are already 80+) and it will be easier to underwrite derivatives transactions.

We believe further economic stress testing is needed in PoS scenarios, since cost and availability of levered Ether could be used to disproportionately influence staking. Emergent phenomena (e.g. Gini coefficients) are important to simulate in wide variety of scenarios as well.

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?

For starters, KYC/AML checks are difficult to verify on Ethereum holdings. One would need to show proof of fiat to cryptocurrency transaction and then the complete flow of crypto assets to the current address, including all passthrough addresses. If regulators were to require a provable source of funds to participate in derivative markets, it could remove a large amount of Ether from the available supply. Increased adoption of privacy tech like zero-knowledge proofs could further limit the amount of supply available that complies with KYC/AML checks.

Given that the Ethereum chain crosses jurisdictions, any conversion to legal tender will need to account for fiat capital controls and local regulations, as these can have an impact on settlement prices.

In addition, there are various other trade-offs around latency, fees, collateral and overall security. Perhaps depending on size of transaction and risk appetite, one can select an appropriate path.

	Latency	Fees	Collateral	Security
Centralized Derivative & underlying Exchange	Low	High	None	Low
Inter-blockchain*	Medium	Medium	Low	Medium
Atomic swap	High	High	High	High
Decentralized Derivatives markets	High	Vary	High	High

* Inter-blockchain refers to protocols such as Cosmos or Polkadot.

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?

We believe that availability of levered Ether, especially when it's recorded on-chain, can disproportionately affect the underlying PoS consensus model and it is hard to reason about these from first principles. Given the complexity, it's difficult to enumerate all such scenarios and thus we believe that a simulation is a necessary tool when assessing network resilience and security.

Here are a few scenarios/conditions that could be problematic:

Use of staked Ether in a derivatives market
How is staked Ether is treated by the derivatives market? Can it be offered as collateral? If so, we could imagine scenarios where one can stake on forks to try to destabilize the system and benefit from previously bought put options in the derivatives market. Locking out staked Ether from the derivatives market could significantly reduce risk.

On-chain derivatives
MakerDAO is a good example of an on-chain derivative. Currently, it allows one to create a levered long Ether position. One can lock up Ether in a MakerDAO contract and receive DAI (a stablecoin pegged to USD) worth 66% of the Ether value. Then, one could use that DAI to purchase more Ether and repeat the process to reach a ~3x leveraged position on Ether.

MakerDAO is run by Maker token holders. Those holders can vote on various network parameters as well as overall direction of the project. What if Maker holders decide to use some of that position to stake? In theory, users would withdraw their deposits if they disagreed with this direction. In practice, some could have financial limitations, liquidity issues, etc that could prevent them from withdrawing. Intuitively, two parties enter a margin trading agreement and

expect that the terms are constant over the duration of the contract. However, Maker voters could change the terms and upend collateral risk and yields.

Currently, ~2% of Ether is locked into a single MakerDAO contract. That's a large position and as it grows, it also becomes a bigger target of re-entracy vector attack (similar to the DAO hack that drained Ether from the DAO contract and led to Ethereum Classic hard fork).

51% attack
There may be scenarios under which an external derivatives market for Ether could make a 51% attack on Ethereum more profitable. Typically, a 51% attack is profitable through double spending. In PoW, one can double spend a couple of times at most and the profit is commensurate to the amount of Ether one had to begin with.

However, there is a disincentive against this behavior because a 51% attack will also reduce faith in the overall chain and likely cause value of Ether to drop, as markets panic and dump the currency. So, an attacker's Ether is going to lose value as well. Now this doesn't make all 51% attacks unprofitable, but it might explain why there are not more of these attacks on Ethereum or other coins given that the hash power costs to complete one do not appear to be that high.

A large enough external derivatives market could change this balance. One could take out a short position (or buy an out-of-the-money put option) on Ether to hedge against any losses one might incur as a result of a 51% attack, guaranteeing a profitable outcome in such an attack. In fact, this makes all sorts of "griefing" attacks (e.g. DDoS) on Ethereum profitable as long as they create a large enough downward pressure on the price.

This effect is independent of the consensus models - it applies to both PoW and PoS. However, in a PoS system one may need to hold a long position equal to 51% of the total network value (or some sizeable fraction if you are able to borrow a lot of coins to stake). Almost any downward pressure on price would offset profit from a double spend. One would need a large options market in relation to the total value of Ether being staked, but even in the unlikely case that 100% of ether was actively staking, it's not unheard of for someone to amass a derivative position larger than the total value of the underlying market.

Another double spend scenario: Suppose that we have prediction markets (such as Veil/Augur/Gnosis) that allow people to bet on whether a double spend will happen in the next *n* blocks. If there is enough liquidity in this market (perhaps due to algorithmic malfeasance), can this incentivize stakers to double spend? This presupposes that the derivative is itself on the chain. There maybe a gas-cost argument against this vector, although the ChainSecurity bug that delayed Constantinople release suggests that it is extremely hard to reason about this type of attack.

These are just few of the scenarios. Our larger point being that these types of scenarios are difficult to enumerate and reason about from first principles. We believe that an agent-based adversarial model could potentially reveal edge cases much more thoroughly.

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?

Derivative contracts need to be benchmarked to an Ether cash price index that

- aggregates liquidity across exchanges,
- is not overly dependent on any single exchange, and
- can be updated as the underlying market structure changes

Some of this depends on market structure of Ether derivative:

	Fiat Settlement	**Cryptocurrency Settlement**
Traditional Centralized Exchange	• Counterparty risk • Reserves for margin calls	• Custody and security risk
Decentralized Exchange	• n/a	• Exchange availability is dependent on underlying blockchain • Order latency and liquidity issues • Transaction ordering and frontrunning
Inter-blockchain	• n/a	• Free option
Atomic swaps	• n/a	• Free option when across different currencies

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.

There's a risk of price manipulation on Ether cash markets, especially since many of those markets lack regulation.

Also risk of manipulation or Distributed Denial of Service (DDOS) attack on Ethereum network itself. This is particularly a weak point if the derivatives are being traded on a decentralized

exchange running on Ethereum. Real (or manipulated) network congestion could slow down or prevent trades from completing. Frontrunning of trades also remains a risk.

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?

We'll need to put controls in place to monitor for flash crashes - we have already seen them on major venues like Coinbase.

We'll also need to monitor for large and continuous arbitrage opportunities between crypto/fiat pairs (e.g. BTC/USD vs BTC/KRW, KRW/USD) as these can be indicative of a deeper issue.

Ultimately, we need to wary of derivatives trade that lead to on-chain transactions, which can lead to feedback loops like a derivatives trade clogs the main chain, which changes underlying token price and affects the derivatives price.

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?

As mentioned above, there's massive supply and demand fragmentation making it difficult to completely monitor all corners of the market. Fiat exchange fragmentation, capital controls and inconsistent regulatory frameworks will make it hard to agree on consistent price feeds and opens the door for manipulations, which can impact derivatives markets.

There's also significant volume in OTC markets that transpires without much visibility.

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

Currently, the best statistical data comes from projects like FALCON and companies like bloXRoute.

In decentralized systems, one can only make a small number of point measurements (e.g. by running a full node in different locations around the world) to estimate how the overall system is performing and what offerings like Service Level Agreements might look like.

The only way to gain increasing certainty in one's monitoring estimates over time is to collect data, simulate outcomes, measure expected outcomes, predict futures outcomes, and then

adjust the simulation to better match all observed predictions. This type of loop is necessary to train a simulation to become better at finding outlier behavior.

Cyber Security and Custody

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

Ethereum's primary development language is Solidity. It's an easy language to pick up but one that makes it hard to guarantee a secure contract. There have been number of attacks in the wild:

- The DAO hack, which led to a hard fork
- Delay of the Constantinople upgrade on Jan 15, 2019 due to a security bug
- And a more comprehensive list

We believe that a combination of smart contract auditing, fuzzing, concolic testing and incentive simulation testing is necessary to ensure that Ethereum contracts provide their users with the guarantees that are claimed by the creators.

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?

For individuals, we suggest using hardware wallets (like Trezor or Ledger) as "cold storage" for maximum security. One of the biggest risks is an attacker gaining access to your machine (through malware for example) and stealing your private key. With hardware wallets, your private key never leaves the secure device. However, there are trade-off in terms of accessing those funds, so in some cases a combination of hardware wallet and a trusted exchange (like Coinbase) might make sense as well. Additionally, we recommend that users write the 24-word recovery phrase on a piece of paper and store it in a different physical location than their hardware wallet to safeguard against physical disasters like fires.

For institutions where multiple people are involved, it's a much more complicated scenario. Not many institutions share their practices, fearing greater scrutiny may expose weaknesses in their setup. A hardware vault (like Hashicorp's Vault) is one solution for high end enterprise wallets.

Recent news about QuadrigaCX is a good example of needing best practices. The young founder of the company died unexpectedly and no one can access the funds in "cold storage",

effectively wasting $100M+ of cryptocurrency forever. Needless to say, a comprehensive process should ensure that access to stored cryptocurrency is never lost to the world.

It's worth noting that much of this will change with the PoS transition. For instance, signature schemes are likely to change as Ethereum tries to aggregate signatures in order to handle more signatures per block (which can be needed for PoS). Ethereum Research also appears to have a variety of complex key generation schemes that are necessary and will impact the way we construct and secure wallets.

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

We aren't sure what the Commission means by this question. If it's a matter of verifying Ether at a specific address, one can spin up an Ethereum node, sync to the network and query the address to verify deposits.

We would also like to thank Peteris Erins, Yi Sun and Phin Barnes for reviewing and commenting on our earlier drafts.