**Response comment for CFTC Request for Input on Crypto-asset Mechanics and Markets**

Invention of digital decentralization started with Bitcoin and was followed by other projects using those design principles that make it possible. A lot of opportunists followed seeking profit using the same buzzwords but with none of the actual design principles. Ethereum and other similar fake cryptocurrencies are perfect examples of such profit seeking opportunists that quite literally deceive innocent people into using unsecure technology by pretending to be part of the decentralization movement solely for personal profit. This comment will clarify how Ethereum is a malicious, dishonest, and highly unsecure project with none of the principles and not even relevant to cryptocurrencies. As such, it should never be supported by any United States government agency in any manner and its promotion should be treated as fraud. All of their promoters should be prosecuted for fraud. Most of the other comments are by people with financial interest in seeing this specific fraud succeed and are typically factually incorrect. This comment will answer all the questions while pointing out the misinformation present in other misleading responses.

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

Profit and lack of ethics, using decentralization hype and buzzwords but none of the principles that make decentralization possible resulting in highly unsecure and centralized project with all success purely due to fraud.

First of all, Ethereum has nothing to do with decentralized technology or decentralized cryptocurrencies, only their marketing claims so. From the start it was a for profit venture unlike Bitcoin. Instead of designing for decentralized distribution of coins and thus control, the most important aspect of cryptocurrencies, they centrally printed 72 million Ether for personal profit, 70%+ of the entire supply. They use all the same terminology as Bitcoin, but follow none of the principles, and are wildly unpopular among the ethical cryptocurrency experts.

Everything there is to know about Ethereum fraud, easily verifiable:

- https://medium.com/@nextlevelcrypto/ethereum-is-not-a-decentralized-trust-minimized-blockchain-ccff48c08b8b
- https://www.reddit.com/r/ethereumfraud/
- https://medium.com/@WhalePanda/ethereum-chain-of-liars-thieves-b04aaa0762cb

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

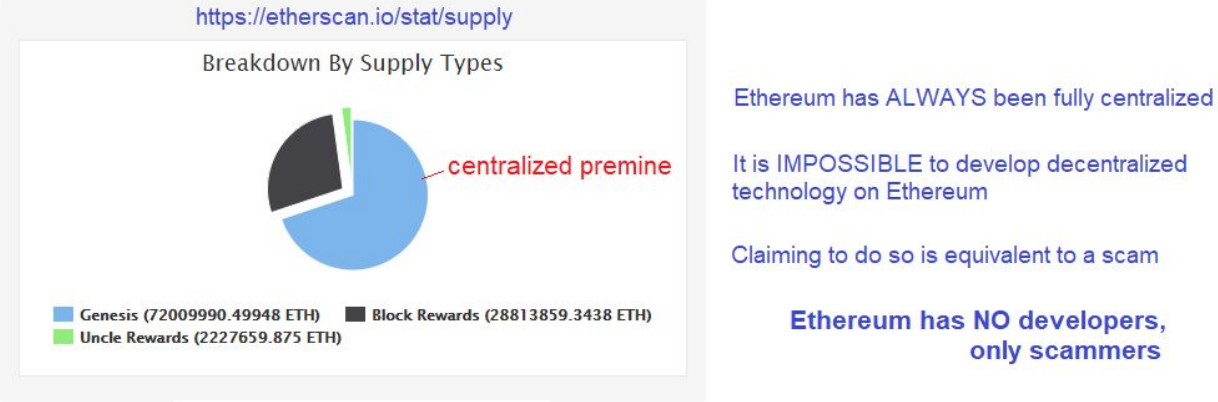
Centralized Ethereum cannot do anything decentralized like Bitcoin due to its centralization via premine by design, but Bitcoin can do everything Ethereum can directly, via layers like Counterparty, and via sidechains like Rootstock, currently supported by more than 40% of

Bitcoin's hash power. After Nick Szabo and Bitcoin invented a concept known as smart contracts where custom scripts can be put on top of the chain to do various logic, Ethereum tried to take credit for that and succeeded purely through marketing despite its perfect centralization and irrelevance to decentralized technology. As it is right now there's not a single thing Ethereum can't do that you can't do with a simple server design before Bitcoin era. As they learned nothing from what makes Bitcoin decentralized, they have only added layers of complexity to old technology and made it more expensive. The low quality of developers incompetent enough to not understand basic principles (like that centrally printing stake is not decentralized) are sadly unfit to comment on this.

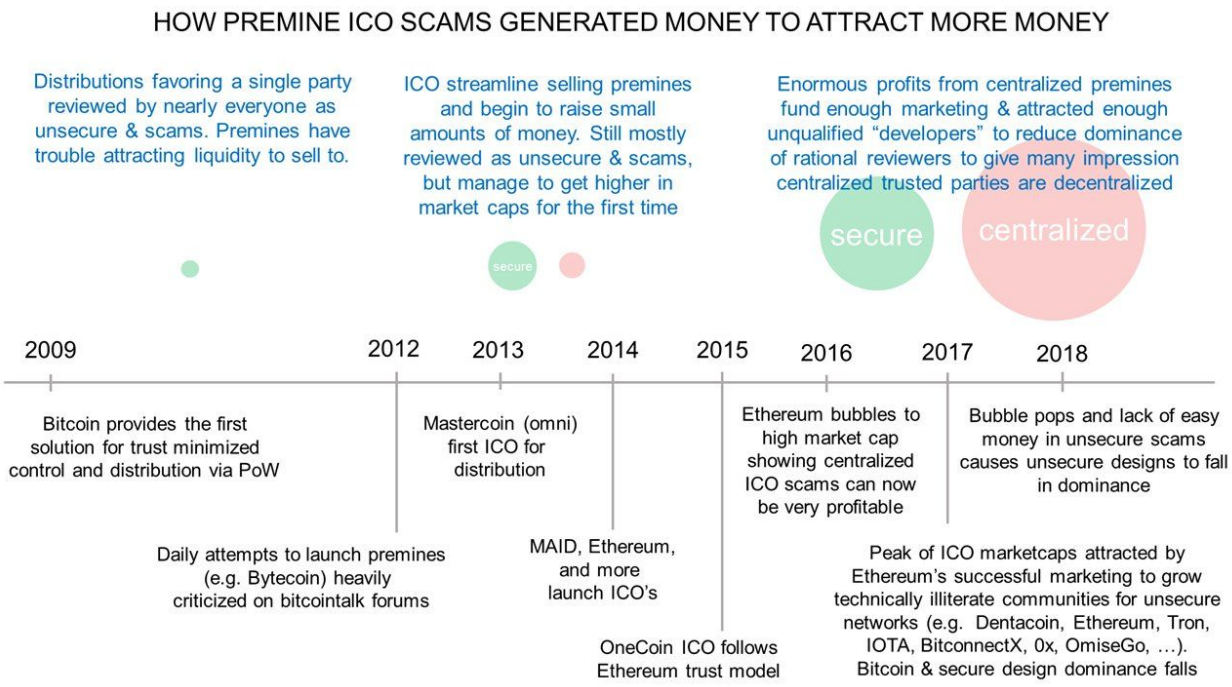
- https://medium.com/@nextlevelcrypto/whats-the-story-with-smart-contracts-and-ethereum-c0d771fd9eb9

**3. How is the developer community currently utilizing the Ethereum Network? More specifically, what are prominent use cases or examples that demonstrate the functionalities and capabilities of the Ethereum Network?**

There are no competent developers on Ethereum, only scammers, as it's a well known fraudulent project considered centralized by all non-Ethereum communities. It's not utilized in any manner different from any other blockchain, but with the downside it offers no advantages of a decentralized blockchain. As such, the people and developers promoting or utilizing Ethereum are more accurately referred to as scammers. Ironically, Ethereum famously called "chain of liars and thieves" lives up to its name.




None of the projects on Ethereum are new, interesting, or relevant. Everyone promoting Ethereum is well aware they are literally lying to people about the security properties of the system they are selling to innocent americans, but they don't care because they can profit of it. There are no ethical or intelligent people working on Ethereum, and all of them belong in prisons. The lack of litigation against them has lead to countless more equally centralized copies appear like TRON, Bitconnect, Onecoin, and so on that have been preying on innocent Americans. These are not good people, these are not innovative developers, only scammers.




**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?**

It's possible some were tricked into using it through the marketing of it being called "decentralized" or "secure" when a history suggests only security failures. Ethereum use in various companies efforts would appear no different than any other cryptocurrency use.

**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?**

Ethereum has no dependable metrics to use. The central group behind the project kept at least 12m Ether. The other 60m Ether was sold in a sale where they alone could buy in for free with absolutely no way to see if they refused free money due to how addresses on blockchains are pseudo anonymous and anyone can create as many as they want. As such, any metrics can be easily faked or abused by the enormous stash in the hands of the central group that is more concerned with marketing and appearance than working on anything resembling decentralized technology. Ethereum has become the best tool for fraud in the history of technology. Its community is the least technically literate community of users and developers in this space that lacks the ability to process how trusting somebody with money doesn't mean they will return

something back. This is demonstrated in their willingness to trust money in ICO's and automated twitter accounts promising returns on twitter.

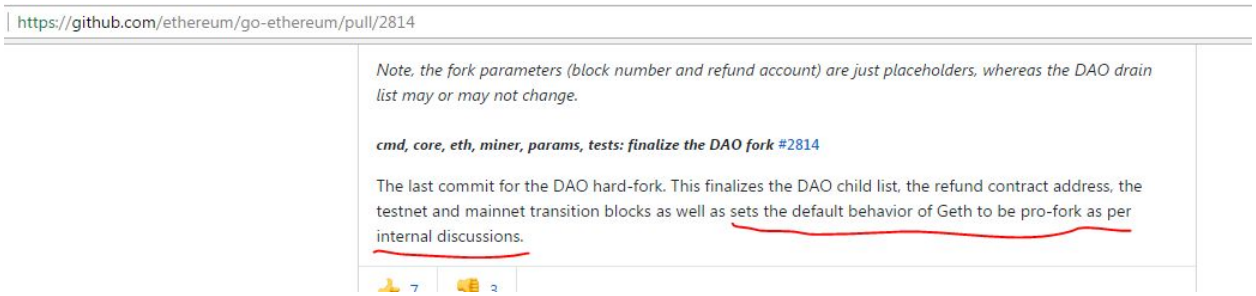
Their worst possible design of Ethereum distribution are reviewed often:

- https://prestonbyrne.com/2018/04/23/on-ethereum-security/
- https://medium.com/@hasufly/ethereum-presale-dynamics-revisited-c1b70ac38448

**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?**

Infinity is not enough and you can never be sure. PoW can add more cost to revert transactions via mining, but they can't stop reverting transactions via forks. Ethereum has a history of confiscating money from anyone a central authority decides deserves it at any time and have enough central control via premining (centrally printing) coins to force it through.

This is an example of how easy it was for them to revert transactions:




More examples on this:

- https://elaineou.com/2016/07/18/stick-a-fork-in-ethereum/
- https://www.reddit.com/r/ethereumfraud/comments/6bgvqv/faq_what_exactly_is_the_fraud_in_ethereum/
- https://www.youtube.com/watch?v=u4NMuBK9s_Q&t=1183

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

Protocol alone, it's a modified version of Bitcoin with more flexibility in scripting on base layer instead of Bitcoin's sidechain and 2nd layers. However, Ethereum main chain implementation ruined the protocol by centrally printing the entire supply and depending entirely on a single trusted party behavior, completely open to capturing the entire supply for profit with no way for anyone else to detect it or stop them. The ethereum developers lack understanding of writing secure code and Ethereum has always been known for enormous numbers of security and technical failures, down to becoming a best known examples of terrible quality of people and developers. After failing at decentralization, they created countless chain breaking vulnerabilities

that were exploited on the live chain due to their incompetence. They had to hard fork several times to fix it after the chain became unusable. Sometimes the global forks even happened accidentally as they didn't listen to basic principles the creator of Bitcoin suggested, like limiting the number of incompatible implementations to avoid those specific scenarios. But Ethereum developers treat their project like it's a $1 game and not a global platform, make edits hours before going live, and use designs all the experts warn them not to.

Once again, Bitcoin can do everything Ethereum wishes it could do via its base and other layers, while Ethereum is not capable of sending even 1 centrally irreversible transaction, forget anything else. Any example they bring up, others have done it before them, others have done it better, and Bitcoin can do it better.

They plan to make the platform even worse via Ethereum 2.0 which will turn it entirely into a permissioned network using something called Proof of Stake, where 70% of stake is centralized as before, but now even trying to produce blocks requires permission of existing stake holders. A miner on Bitcoin can enter into creating blocks whenever and however he wants at any scale, but Ethereum is designing to remove that ability so the central premine controls block production more directly and has gatekeeper role over every aspect of the chain.

**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?**

It's not a decentralized network, so it shouldn't have any scalabilty challenges. However it's known for what's called "decentralization theater" where they pretend to have these challenges and copy other chains. The terrible designer behind their centralized premine called Vitalik came up with some more buzzwords like Plasma and Sharding, which are just another way of badly designing Lightning Network and Sidechains of Bitcoin. Ethereum developers simply don't have the technical literacy capable of creating any unique technology, so they copy others work without giving credit.


**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?**

Ethereum developers lack the technical understanding or ethics to understand proof of stake has been tested since 2012 by hundreds of cryptocurrencies. They created one of the least secure proof of stake algorithms ever seen in history of proof of stake called Casper that favors cartels and centralized premines above all else. With mechanisms like slashing they can literally use their giant centralized premine to cut other people's money for profit.

For example, Casper allows doing a denial of service attack on a node for its funds to be slashed (deleted).

Casper also allows abuse of censorship slashing where if one party has 99% of supply and another has 1% of supply, censorship slashing allows 1% cut of both, but by design that means the larger party now owns 100% of remaining supply, resulting in profit at same market cap.

Even when slashing only hurts the cartel or majority owner, the coins are deleted and made more scarce, thus canceling most of the slashing punishment.

The terrible design of Casper proof of stake comes from the same people who didn't realize (on purpose or not) a sale where the seller can buy from for free is not a secure and trust minimized way to distribute stake. Therefore, the incompetence is not surprising.

Instead of allowing selecting of nodes producing blocks based on merit or competence like some other proof of stake designs, they want it to be based purely on wealth (like the premine) and favor cartels and colluding parties.

Here is example of their lead developer, known for academic dishonesty, lying about other proof of stake mechanisms:

- https://medium.com/@nextlevelcrypto/vitalik-buterins-academic-dishonesty-on-other-projects-5a5d60967fe4

**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.**

All proof of stake (PoS) designs have same flaws.

Main issue is all of PoS designs require permission of existing coin holders to enter consensus, something proof of work chains never have to worry about as they are entirely permissionless and open for anyone to start mining at any scale. They have never and will never address this issue as it's fundamental to why proof of stake is not used by legitimate developers who care about decentralization. Permissionless entry, unlike premines and stake, is the main tool we have for decentralization or allowing entry of unlimited independent parties into consensus. Premines and proof of stake limit who gets to enter, by how much, and who controls the chain for the rest of time.

Another issue is being highly subjective about which blockchain is the real one with nothing preventing conflicting versions of blocks produced for the majority stake holder, and thus rely on subjective checkpoints and central coordination.

In both proof of work and proof of stake, the coin ownership is the dominant incentive for coin owners to do what is best for the blockchain, the value of those coins is what's at stake. Slashing in no way improves on that design, only makes it worse

**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?**

As all legitimate developers and users have left the Ethereum community after they demonstrated their centralization, even if premine alone wasn't enough, the very few things the left overs have figured out or disagree in pale in comparison to Ethereum's centralization issue that's not fixable. There are no possible usecases for Ethereum to exist as just a more expensive centralized distributed database.

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

Nothing unique. Bitcoin currently suports the most active and largest ecosystem of developers globally. Ethereum has a smaller but less intelligent community, but are completely irrelevant to decentralized technology and thus no point comparing them.

Bitcoin is the standard of security. Since bitcoin updates are backwards compatible, even introduction of a small bug would be filtered out by older compatible nodes until its fixed. The worst possible thing is to have more than one implementation, as mentioned by Satoshi, Bitcoin creator. The incompetent developers of Ethereum have created multiple implementations, all still forced to listen to the centralized Ethereum Foundation's premine control. The multiple implementations resulted in countless bugs including accidental forks where anyone's money could've been easily lost by sending it on the wrong chain, with absolutely no idea which node or user is on which chain.

Multiple client issue Bitcoin doesn't have:
https://cointelegraph.com/news/ethereum-issues-security-alert-after-fork-transactions-may-be-reverted

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

Exact opposite. Bitcoin has no premine, no profit seeking organization doing any sales, even miners are forced to sell virtually all coins to countless others as they have to put in money first for hardware and electricity. Ethereum instead gave the entire supply to a single trusted party for absolutely 0 cost, just profit.

Bitcoin governance is completely decentralized by anyone who wants can fork the codebase and offer changes. There is no economic force like the premine to force descisions. Ethereum is complete opposite, with a single central party dictating what the real chain should be, whose money should be confiscated, who should be censored, which contract should be changed, and so on - all of which they have done in the past already.

**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 is a fork out of the old Ethereum chain, now called Ethereum Classic. The central control of Ethereum Foundation over the codebase, up to 70% of supply on both chains, and thus control over incentives of everyone involved allowed them to use forks like that to confiscate money while trying to destroy all value of the other chain and its security. It's no surprise Ethereum Classic was successfully attacked via a 51% attack.

Virtually nobody supported the switch to a new chain in the votes before hand as only a few percent voted in short time given, but afterwards the central pressure, shelling factor of hard coding the change into the code base, forum censorship, and most of the supply by the foundation was used against the chain they disliked. Even though very few people participated in TheDAO, any members of the Ethereum Foundation lost funds, and thus have every incentive to only favor the chain where they get a bailout.

Using Ethereum means completely trusting their central Foundation for the rest of time as they can repeat that again and again on every fork for the rest of time.

**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?**

No, there are no protections against the Foundation using the premine from the random anonymous accounts against the network or any forks and chains that come out of it.

**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?**

Same as any other digital asset, minus the decentralization.

**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?**

It doesn't introduce anything that can't be done with a centralized server as is in fact equivalent in every way.

**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?**

The risks are the same as the risks of using any other centralized asset.

**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.**

It would validate fraud, associate CFTC with fraud, promote fraud, enspire countless copy cats, and hurt real innovation of decentralization where there's no centralized massive marketing funds by making it more profitable to centrally print supplies and call them decentralized for no technical reason and plenty for marketing.

**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?**

Since Ethereum is fully centralized, all of its success and value is attributed strictly to fraud, malicious unethical marketing, and lying to people about security they should expect for profit.

**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?**

There should be no reason to trade it on any government supported exchange, and a task force should be forced to find everyone involved with Ethereum and prosecure them for fraud.

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

There are countless explorers and node software, although they have limited use with centralized networks like Ethereum where changes and edits are trivial.

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

Yes, it's centralized and thus they have to entirely throw away the genesis block where the vulnerability is to make any of its code useful. Rootstock is one attempt at that by building everything Ethereum is on Bitcoin and thus using 10 years of trust minimized distribution for its security.

**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?**

It doesn't matter what private keys are as on Ethereum you depend entirely on a single trusted party to allow you to have a balance or do anything by design.

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

Have to understand addresses are not people and pseudoanonymous, same most other blockchains.