It is a delight to see the CTFC exploring Ethereum and reaching out to the industry for information to assist in that process. As an outspoken advocate for cryptocurrencies and blockchain technology for many years, I felt compelled to contribute what I could to your process.

I first wrote about the benefits of derivatives in the crypto markets in 2013.[1] Since then, I have co-founded two companies, including TradeBlock – the world's leading provider of institutional trading tools and data services for digital currencies, and Axoni – a capital markets technology company working in partnership with many of the world's leading financial institutions, including our engagement with the DTCC to replatform the post-trade infrastructure for the global credit derivatives market onto our blockchain technology.

Please feel free to reach out to me directly with any questions.

Greg Schvey

[1] Hedging Bitcoin Mining Investments with Network Difficulty Futures – Aug 2013 https://tradeblock.com/blog/hedging-bitcoin-mining-investments-with-network-difficulty-futures-part-1-hedging-shipment-delay/

1 & 2. What was the impetus for developing Ether and the Ethereum Network, especially relative to Bitcoin? What are the current functionalities and capabilities of Ether and the Ethereum Network as compared to the functionalities and capabilities of Bitcoin?

Bitcoin established reliable peer-to-peer record keeping with the stated purpose of facilitating electronic payments. It achieves that objective by focusing on its core functionality: updating the balances of accounts on the network via validated debits and credits. While there is a handful of additional functions that can be facilitated natively on the bitcoin network, they are oriented around the facilitation of payments (i.e. require sign-off from multiple parties to send money, escrow, etc.).

Ethereum leveraged many of the technical concepts of bitcoin related to security and verifiability, but used those as a foundation not only for payments, but also for the synchronized processing of any data. Whereas messages stored on the bitcoin ledger are oriented around adjusting account balances, messages on the Ethereum network can also contain executable computer code (i.e. applications). The underlying software in Ethereum coordinates with other nodes not only on the contents of the message that was sent, but also the latest state of all applications on the ledger.

Bitcoin (and the many similar network before Ethereum) were "all too concerned about specific applications and not being sufficiently general - hence the birth of Ethereum,"[2] which instead seeks to provide a distributed, reliable computer with open access to anyone in the world.

3 & 4. 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? 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?

The best-known applications of Ethereum tend to be oriented around asset transfer for speculative purposes. However, a long list of innovative applications has arisen over the past few years.

DNS Alternative - The Domain Name System (DNS) serves as the global directory of the internet today. DNS is effectively a lookup of human-readable domain names (e.g. "google.com"), which are then used by DNS to route to the actual internet address of the target servers. While DNS is generally reliable, the lookup system is based on the trust of a small handful of centralized parties, which enables a handful of attack vectors if end users cannot trust the servers they're using for that lookup process. Even Google has been the victim of such

[2] Quote from the personal blog of Ethereum found Vitalik Buterin: https://about.me/vitalik_buterin

attacks.[3] Projects like EthDNS[4] seek to leverage the distributed Ethereum network to store and process domain name lookups, enabling end-user verification of accuracy.

Moreover, the benefits of a permanently-up network with thousands of distributed servers globally provides redundancy and resiliency that can improve the technical infrastructure on which our economy relies.[5]

Authentication of Digital Art - Bitcoin gave the world a reliable way to prove digital uniqueness, however, the application of that utility is limited to tracking the network's native currency.[6] Projects like R.A.R.E. leverage the Ethereum blockchain[7] to track authenticity of digital creations.

Insurance Automation - AXA, the world's second largest insurance company, built an automated, transparent insurance product[8] leveraging the Ethereum network. Insurance agreements related to travel delays are recorded as applications on the Ethereum blockchain. Third party data related to flight delays is also printed to the network, which in turn updates the state of the insurance contracts and triggers payments as relevant[9]. All parties involved benefit from the transparency of seeing that the contracts were executed appropriately and automatically.

Gaming - One would be remiss to discuss Ethereum applications without mentioning gaming, particularly CryptoKitties.[10] The game uses applications on the Ethereum network to represent "kittens" with different attributes, as well as provable uniqueness and ownership. Kittens can then be bred with other kittens, creating offspring that have a randomized blend of the attributes of the parent kittens. Given the native functionality of the Ethereum network, these kittens are tradeable, and anyone in the world can build a user interface on top of them.

The concept may sound absurd or pointless (and as a first generation endeavor, it very well may be), but it would be naïve to dismiss the potential that this application has proven. The global games market is approaching $150 billion in annual revenue and, for the first time, there

---

[3] More info: https://www.pcworld.com/article/2889392/like-google-in-vietnam-lenovo-tripped-up-by-a-dns-attack.html

[4] More info: https://medium.com/@jgm.orinoco/ethdns-an-ethereum-backend-for-the-domain-name-system-d52dabd904b3

[5] On Feb 1, 2019, Microsoft lost customer data due to an outage at their DNS provider: https://nakedsecurity.sophos.com/2019/02/01/dns-outage-turns-tables-on-azure-database-users/

[6] Note: additional data can be added to bitcoin transactions. However, it is a cumbersome and limiting process relative to Ethereum, which is designed for generalized information and processes

[7] Note: files are stored on IPFS (InterPlanetary File System), a blockchain designed for file storage and transfer. Digital prints of those pieces are tracked as provably unique assets on the Ethereum blockchain.

[8] More info: https://group.axa.com/en/newsroom/news/axa-goes-blockchain-with-fizzy

[9] Payments are handled via traditional payment methods, rather than automated on the Ethereum network with ether, though AXA has announced their intent to eventually facilitate payments in the network's native token. More info: https://medium.com/@laurentbenichou/fizzy-axa-reaches-a-new-milestone-fadd41f20e11

[10] More info: https://www.cryptokitties.co/

is a way to create and track unique digital game pieces that can be accessed by anyone seeking to build a unique experience on top of the underlying data.

Funding Open Source Contributions - Monetary rewards for contributions to software projects, commonly referred to as “bounties,” are common in the software developer ecosystem. Projects like Gitcoin[11] leverage applications on the Ethereum blockchain to automate payments to developers for their contributions, reducing risk of non-payment.

Transparent Funding of Research Grants - The National Research Council of Canada has begun publishing grant and contribution data to the Ethereum blockchain, with nearly $800M of grant data now publicly accessible to the world in an immutable record since the project’s inception. In the council’s own words, “This technology offers unprecedented levels of transparency and trust allowing public records to be searched, verified and audited at a level the world hasn’t seen before.”[12]

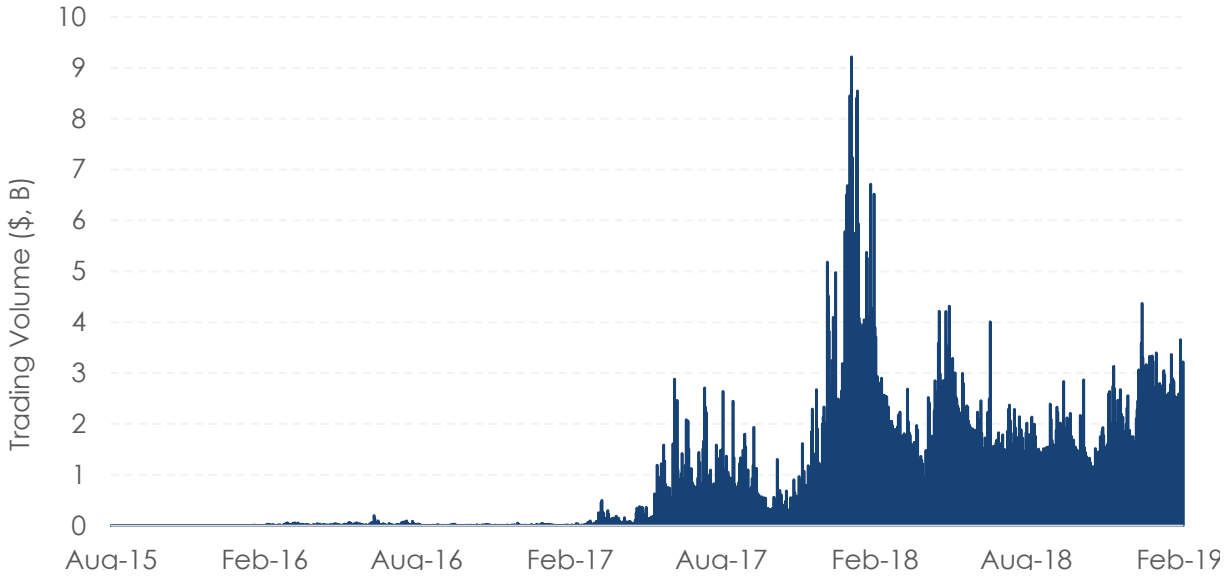
Digital Real Estate & Assets - With the provable uniqueness of digital objects on the network, combined with transparent ownership and easy transfer, some projects are building entire virtual worlds on top of Ethereum. For example, Decentraland[13] is leveraging the Ethereum blockchain to manage ownership rights of virtual real estate, which can then be used to build entire virtual experiences, including economic activity, in virtual reality. Whether or not Decentraland itself takes hold, it is proving that real estate for entire regions can be tracked on a globally accessible network.

Optimizing Energy Markets - Multiple projects[14] looking to directly connect buyers and sellers of electricity have leveraged Ethereum’s blockchain to provide a distributed, openly-accessible marketplace for energy. By cutting out middle parties in the energy distribution process, these projects are looking to bring greater efficiency and lower costs to end users.

[11] More info: https://gitcoin.co/
[12] More info: https://nrc-cnrc.explorecatena.com/en
[13] More info: https://decentraland.org/
[14] Examples: https://gridplus.io/ , https://www.lition.io/p2p-platform, https://lo3energy.com/

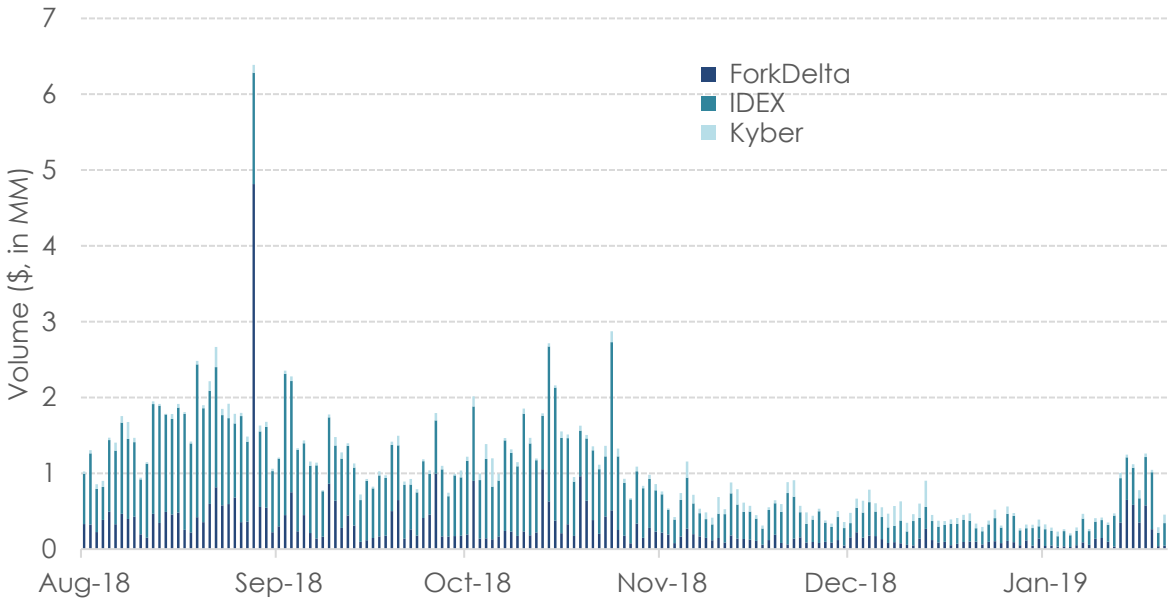
5. What data sources, analyses, calculations, variables, or other factors could be used to determine Ether's market size, liquidity, trade volume, types of traders, ownership concentration, and/or principal ways in which the Ethereum Network is currently being used by market participants?

Ethereum Daily Trading Volume (Centralized Exchanges)



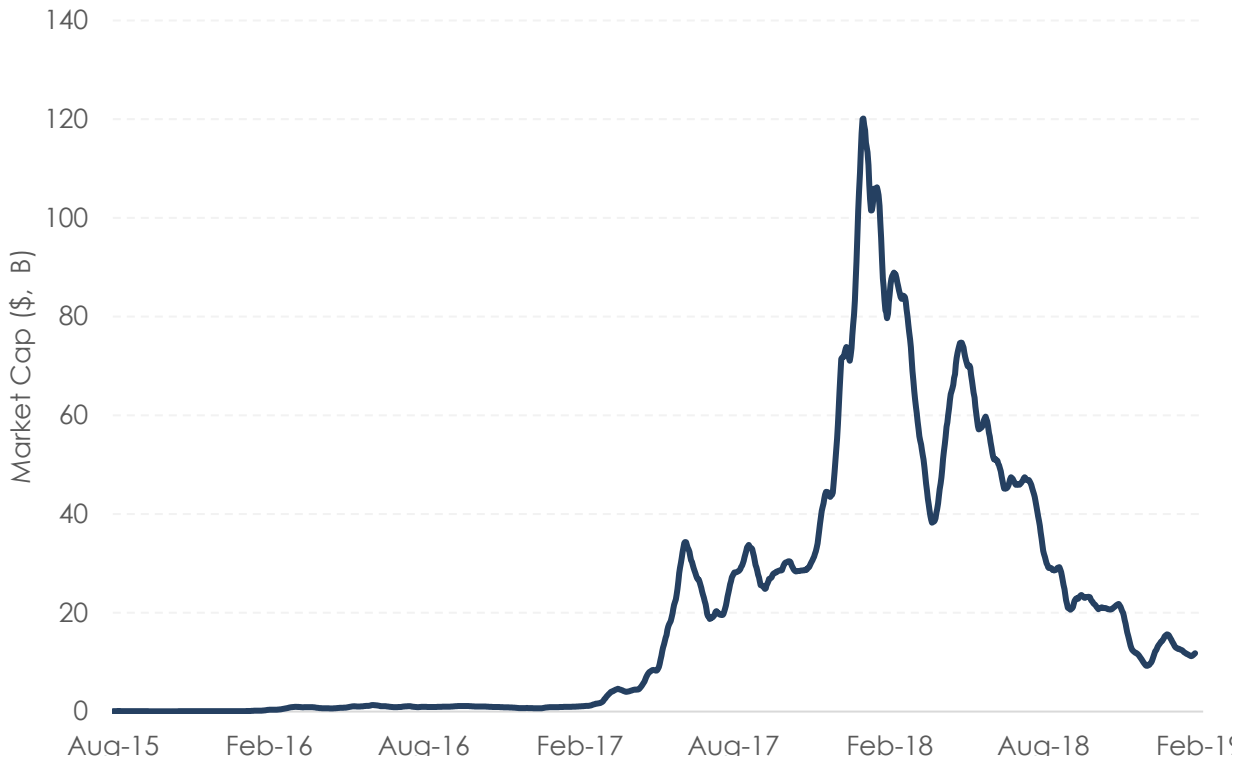
Source: TradeBlock

Ethereum Daily Trading Volume (Decentralized Exchanges)



Source: Dappradar.com, TradeBlock

Ethereum Market Capitalization



Source: Dappradar.com, TradeBlock

Ethereum Ownership Concentration (Top 100 Addresses)

Entity	Balance (in ETH, MM)	% of Supply
Exchange	6.3	6.0%
Bitfinex	*1.9*	*1.8%*
Binance	*1.4*	*1.4%*
Huobi	*0.9*	*0.8%*
Kraken	*1.4*	*1.4%*
Bittrex	*0.3*	*0.3%*
Okex	*0.2*	*0.2%*
Gate.io	*0.2*	*0.2%*
Wrapped Ether	2.2	2.1%
ICO Wallet	1.8	1.7%
DigixDAO	*0.4*	*0.4%*
Golem	*0.4*	*0.4%*
Polkadot	*0.3*	*0.3%*
Gnosis	*0.2*	*0.2%*
Aragon	*0.2*	*0.2%*
Status	*0.2*	*0.2%*
SingularDTV	*0.2*	*0.1%*
EthDev (Dev Foundation)	0.6	0.6%
Vitalik Buterin	0.4	0.3%
Unknown	22.9	21.8%
Grand Total	**34.1**	**32.6%**

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?

In Ethereum and other blockchains with similar consensus mechanisms, one cannot ever be absolutely sure a transaction won't end up in an invalid block; transacting requires a degree of comfort with probability. It is possible for a malicious miner with substantial hashing power to pick a past block and begin rewriting history from that point forward. This would require more hashing power than the rest of the network combined.

That said, the probability of a transaction once viewed as valid becoming invalid decreases with every new block built on top of the block in question. Due to the implementation of the GHOST protocol in Ethereum (described below), blocks can be confirmed faster and are generally considered sufficiently reliable in a shorter amount of time than bitcoin. A detailed analysis of this can be found on the Ethereum website.[15]

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

Ledger Accounting

Bitcoin uses an unspent transaction output (UTXO) accounting model.[16] In this construct, all newly issued bitcoin start as a transaction[17] from no one to the miner of a given block, creating the first transaction output. When that miner sends that bitcoin to another address, the entirety of that transaction is reassigned to the recipient's address for the intended amount. If the intended amount to spend to the recipient is less than the original transaction that is being re-spent, the original input is split into two outputs, one with the correct amount going to the recipient, and the other sending the remainder (less fees) to a "change" address of the sender.

This system allows for the heritage of every bitcoin - down to the eighth decimal point - to be accounted for all the way back to its original issuance. The balance of each network address / identity is then simply the sum total of the unspent transactions that are assigned to them.

As an example, if Alice received a transaction for five bitcoin and wants to send 3.2 bitcoin to Bob, her wallet software would turn that unspent five bitcoin output into two new outputs. Bill would receive an output for 3.2 bitcoin and Alice would receive a change output for 1.8 bitcoin. Alice now has an unspent output for 1.8 bitcoin and Bill has an unspent transaction for 3.2 bitcoin, both of which can be re-spent at will.

Notably, unspent transactions can be combined. For example, if Alice still wanted to send Bob 3.2 bitcoin, but had two unspent transactions of three bitcoin and two bitcoin, her wallet software

---

[15] More info: https://blog.ethereum.org/2015/09/14/on-slow-and-fast-block-times/
[16] https://bitcoin.org/bitcoin.pdf
[17] Transaction values for newly minted bitcoin sent to miners are for a pre-determined amount of bitcoin based on rules coded into the bitcoin protocol

would combine them in a single blockchain message for five bitcoin to Bob, who would then return a single change transaction for 1.8 bitcoin.

Ethereum uses an account based model that is much more similar to what one might expect to see on a traditional financial ledger. In this system, the balance is the sum of all the unspent Ether sent to that address, but the Ether is then indistinguishable when being re-spent to a new recipient. This fungibility and ease of record keeping makes it much simpler to build applications into the network with arbitrary state that could impact the way Ether moves between accounts.

Programmable State Modification

The fundamental advantage of Ethereum computation model is that it has persistent state which can be modified by code to generate an arbitrary state, which in turn affects how future transactions are processed. Said simply, you can code any set of instructions into the network (frequently referred to as a “turing complete” system) which are then broadly validated based on the consensus rules. This allows sophisticated[18] applications to direct monetary flows in a manner that is validated, transparent, and perfectly synchronized across parties on the network. Ethereum ensures that all programs avoid an infinite loop eventually reach either completion or an error by introducing a “gas” pricing model. All operations require the payment of ethereum, and when the payment runs out or the gas limit is hit then the program halts.

Bitcoin does have some degree of programmability, but it is highly limited by design[19]. Functionality to drive movement of assets on the network that is not available in the scripts provided in the bitcoin protocol must be done in an off-chain process, meaning the transparency and synchronization of the calculations or other processes to drive that asset movement is greatly reduced or wholly diminished.

Block Architecture

Both bitcoin and ethereum synchronize the list and order of transactions stored on the ledger through use of a Merkle Tree,[20] which is a succinctly summarized representation of many pieces of data.

Ethereum, given its ability to also execute user-defined code to derive an arbitrary state, also uses Merkle Tree implementations to verify the data storage of all accounts on the network. This, combined with the transaction list synchronization, ensures not only that all nodes on the network have the same inputs, but also have reached the same outputs.

In order to allow for faster block times, Ethereum implements ideas proposed in the GHOST protocol[21], wherein block headers also include references to ‘uncle’ blocks. Uncle blocks are

[18] Subject to the economic incentives provided to miners to process the transaction
[19] More info: https://en.bitcoin.it/wiki/Script
[20] More info: https://en.bitcoin.it/wiki/Protocol_documentation#Merkle_Trees
[21] More info: https://eprint.iacr.org/2013/881.pdf

mathematically valid, but are not part of the main chain and are instead related to the parent block of the current block. New Ether is also issued to miners of uncle blocks as an incentive to align competitive blocks to the main chain, as a reduction of splintering chains enables greater consistency with faster block time.

Light Client Support

Bitcoin and Ethereum both support the use of "light clients," software that is able to verify the accuracy of the data it's receiving without having to download and process the entire blockchain. This requires trust that the server sending the data is reliable, but does not require trust to know if the data received is valid. Light client servers can censor data (i.e. selectively not share), but cannot crate fraudulent information.

Mining

In a proof of work consensus model,[22] a valid block is found when a miner generates a valid hash that includes various fields such as: a reference to the transactions in the block, a reference to the previous block header, and a random number (nonce). The range of valid hashes is automatically increased or reduced in order to keep consistent average time between blocks based on parameters set in each of the blockchain protocols. This model is currently used in both Bitcoin and Ethereum.

However, Ethereum uses a different hashing algorithm in an effort to be resistant to specialized hardware designed to generate guesses for valid hashes more quickly, a dynamic that has become prolific on the bitcoin network. While that decision for the Ethereum network has proven effective at resisting the specialized hardware to date, rumors began circulating towards the end of 2018 that such specialized hardware may soon be available.

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?

Blockchain Size

The first consideration in scaling is the raw size of the Ethereum blockchain, which currently stands at approximately 129 GB with 390 M transactions stored on the ledger. Notably, the full disk space used for all historical Ethereum processing to date is approx 1 TB, including storage of states, though the later versions of the most popular Ethereum clients automatically prune much of that data. For comparison, the bitcoin blockchain is currently at ~200 GB with nearly 382 M transactions stored on the ledger.

[22] More info: https://en.bitcoin.it/wiki/Proof_of_work

As noted earlier, Ethereum nodes store all historical state, which adds to the amount of disk required. Individual network participants do have options to reduce their disk requirements, including running a node that supports pruning[23] or running a light client, as described earlier. The downside of these options is that if they become widely adopted, fewer people will be running full nodes, which means greater centralization as less parties have the entire data set, and less network resiliency.

Network Throughput

A variety of solutions are in development to address the volume of transactions the network can support, including:

- Pegged side chains - This concept enables a group of nodes to share data directly between each other, signing each transaction and building blocks between them, but only transmitting those transactions and blocks to relevant parties. Over time, these chains can be 'anchored' by publishing their state root to the Ethereum blockchain. The parties on the side chain can establish rules to govern their activity on the side chain by encoding those rules in a smart contract on the public Ethereum chain. Similarly, they can also lock assets on the Ethereum chain that can only be unlocked when certain conditions on the side chain have been met. More information about this can be found in the Plasma[24] whitepaper.

- Sharding - This concept divides the main Ethereum blockchain into multiple independent chains, enabling for parallelization of transaction processing. Network nodes can have different roles on different shards, potentially validating transactions on one shard and observing as a light client on others.[25] The main challenge currently is allowing transfer of assets and information across these shards

- Channels - With channels, predetermined groups of nodes transmit transactions directly to each other, signing them as if they were going to the public Ethereum network. These transaction lists build up between the parties over time to generate a net payment amount or series up updates to the state of a smart contract - all of which only they can see. Similar to side chains, these transaction lists can be periodically printed to the public Ethereum ledger.

- Off-Chain Computations - Individual users can always choose to run complex calculations independently and submit the output to the Ethereum chain for synchronization on the resulting data or state. This will save gas costs, but inherently

[23] More info: https://medium.com/coinmonks/analyzing-the-hardware-requirements-to-be-an-ethereum-full-validated-node-dc064f167902
[24] More info: https://plasma.io/plasma.pdf
[25] More info: https://blockonomi.com/sharding/

prohibit the automated calculation validation offered by processing data in the node's native virtual machine.

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?

NXT, Peercoin, Bitshares, and others have been running various versions of proof of stake (PoS) for years. NXT, for example, has been operational and fully functional since its launch in November 2013.

Since the concept was announced, a number of variations on the PoS concept have arisen. Among the most popular is Delegated Proof of Stake (DPoS), in which network participants vote their coins to elect 'delegates' to maintain the blockchain and 'witnesses' to add blocks to the chain, similar to the way miners would in a proof of work (PoW) model. This model is generally viewed as more efficient, as relying on a limited number of witnesses reduces the validation complexity and increases transaction speed. Witnesses are responsible for maintaining a good reputation through good behavior, including validating blocks appropriately and not missing a turn to submit blocks to the chain, as they can also be voted out by network token holders.

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.

Risk Concentration

In the abstract, perhaps the most notable concern with proof of stake is the potential concentration of risk. Proof of work systems, through their requirement for activity that happens outside of the network (i.e. physical machines processing calculations), separates the progression of the ledger from the activity on the ledger itself. In a PoS system, those concepts are intertwined by design in order to align incentives of large cryptocurrency holders to operate the network properly. However, the inverse could work against the security of the network.

In the simplest example, the ability for a party who steals a large amount of funds to maliciously impact the network would go up substantially and immediately. However, you will notice the theme of risk concentration throughout the more detailed attack vectors outlined below.

Centralization

The likelihood of all parties staking all of their coin is exceptionally low, given the conscious action required to do so. This means that new ether will be unevenly distributed (albeit not necessarily more than the concentration in PoW as a result of the economies of scale). This would presumably be exacerbated in a delegated system, or potentially by infrastructure

providers who hold large volumes of ether (i.e. exchanges, custodians) presumably reap some share of the returns from their clients' holdings.

Long Range Attacks

In long range attacks, the attacker starts forks off of the genesis block and creates an alternative chain with same length. These attacks are mainly targeted towards new nodes or nodes that have been offline. There are few different manifestations of this attack vector:

- Stake Bleeding[26] - If a coalition of malicious miners started from the genesis block and replayed all of the old transactions, they would receive the block rewards for all transactions and, when they caught up to the valid chain, would be the most heavily rewarded and dominate the PoS validation process going forward.

- In a PoS system, malicious parties could purchase keys for addresses that no longer hold ether, but held large volumes in the past. What this would allow them to do is replay history starting from a given point in the past, staking coins that belonged to the purchased address to vote for the newly-manipulated record.

- A number of solutions have been proposed to address this, including checkpointing to introduce transactional finality, key-evolving cryptography, and others.

Nothing-at-stake Problem

If competing blocks create a fork in a PoW blockchain, miners have to choose which block to build on top of, as each hash generated comes at a cost to the miner. If there are competing blocks in a PoS system, validators are arguably incentivized to stake on both chains[27] as it comes at no marginal cost to them. This creates a potential problem of never reaching consensus even if all parties are acting honestly, as both sides of the fork could maintain sufficient consensus to continue generating blocks. The leading proposal against this is to punish validators who stake on both chains (or alternative, punish for building on the wrong chain) by deducting a sufficient amount of ether from their accounts to disincentivize this behavior. This is a longstanding discussion in the community.[28]

Potential Lower Threshold for Malice

The proposed threshold for a block to be validated in Ethereum's Casper PoS system requires two thirds of staked coins be honest. Depending on the number of coins staked for mining, the threshold of malicious voters could be substantially less than 67% of the total amount of ether.

---

[26] Stake-Bleeding Attacks on Proof-of-Stake Blockchains: https://eprint.iacr.org/2018/248.pdf

[27] It could be argued that validators would choose a single block on top of which to continue validating for the good of the network, on which the value of their stake coins are based

[28] More info: https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQs#what-is-the-nothing-at-stake-problem-and-how-can-it-be-fixed

This could be further manipulated by a malicious party preventing honest stakers from participating. For example, targeted denial of service attacks against honest stakers could prevent them from voting their coins, reducing the threshold for malice to prevail. Moreover, once a party has the requisite two thirds of coins staked to continue progressing the blockchain, they could disallow honest stakers from rejoining the network.[29]

Validator Privacy

There is a decrease in privacy to the parties participating in the consensus process relative to PoW systems. In bitcoin, for example, miners can use different addresses for every block reward.[30] In PoS systems, validators must stake their wealth, which means publicly announcing the wealth held by those earning block rewards.

Stake Grinding

PoS algorithms frequently have information in the current block to randomly select the validator in the next block. If this is not computationally expensive, then validators can generate a large set of random data for their designated block and select one that increases the probability of their selection as a validator in the next block. This would manifest as a validator or set of validators having a larger percentage of blocks than their staking percentage would expect. Since it is random data, it can be difficult to identify this outside of luck.

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?

It seems more likely than not that the consensus switch *will* result in a fragmented market, just as fundamental changes to the protocol rules have historically created such a result. Bitcoin Cash, Ethereum Classic, and a slew of others serve as examples of this. In this case, miners that have invested in hardware have an economic incentive to disagree with the new protocol.

With regards to diminishing the market, chain splits - at least in the case of Bitcoin Cash and Ethereum Classic - have historically not diminished the use or price of those networks beyond an initial market reaction, be it in price or developer activity.

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

---

[29] Joining the consensus process requires sending a transaction announcing your intentions to the network, which must be accepted by the current validators

[30] It should be noted that mining pools generally make their addresses public, so the impact of this privacy benefit is largely muted in reality

With regards to scaling to process more sophisticated applications, I would refer you to the response to question eight above. However, it should also be noted that the use of WebAssembly (WASM) as the virtual machine for Ethereum has been in discussion for years. WASM not only supports compilation from multiple programming languages, but is expected to be more efficient both in its processing and mapping to various CPU architectures.

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

Technically, Bitcoin and Ethereum have similar governance structures. Both rely on distributed decision making, with decisions decided by miners and full nodes. While miners have the ability to update the ledger, they still must follow the protocol rules or honest nodes will reject their blocks.

That said, the practical differences between Bitcoin and Ethereum governance is quite tangible. Both communities are vocal, but Ethereum tends to be more organized, thanks to groups like the Ethereum Foundation[31] and the Enterprise Ethereum Alliance,[32] and conferences like DevCon,[33] which provide structured platforms for community discussion and cohesion. In a similar vein, Ethereum has informal-but-broadly recognized leaders, such as founder Vitalik Buterin, who remains a vocal part of the community and active contributor to the technical roadmap. Satoshi Nakamoto's anonymity and eventual absence led to a leadership vacuum that ultimately led to many competing voices vying unsuccessfully to gain sustained authority in Bitcoin.

Cohesion, however, can have both benefits and costs. For example, when the Distributed Autonomous Organization (DAO) was drained of tens of millions of dollars worth of ether,[34] the Ethereum community quickly rallied to build and implement protocol changes to freeze the funds of the actor who withdrew them. Some would argue that level of cohesion is a positive force and demonstrates the ability to mobilize with high efficiency. Others would argue that the protocol update driven by influential voices - many of whom were vocal investors in the DAO and stood to lose millions when the funds were drained - created a moral hazard that manifested in changing the rules of the network post hoc.

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?

Before addressing the main question (and at the risk of being pedantic), it is worth noting that in proof-of-work blockchains, the chain with the most work is generally considered the valid chain. Since Ethereum has always maintained substantially more hashing power / work than Ethereum

[31] More info: https://www.ethereum.org/foundation
[32] More info: https://entethalliance.org/
[33] More info: https://devcon4.ethereum.org/
[34] More info: https://www.coindesk.com/understanding-dao-hack-journalists

Classic, Ethereum Classic would technically be considered an outgrowth, even though Ethereum updated its protocol rules at the time of the split.

There are a variety of situations that would likely be solved by a hard fork and could lead to another chain split, including:

Quantum Computing

If the protocol itself creates vulnerabilities, the parties involved may wish to implement a hard fork. One example of such a reason could include quantum computing diminishing the security of the cryptography currently used. If the ability to brute force Ethereum's private keys or block creation hashes became available through extreme computational power, quantum or otherwise, a protocol update would presumably be desirable.

ASIC Resistance

Similarly, indications of specialized hardware being made available for highly-optimized Ethereum mining,[35] which ultimately led to discussions in the Ethereum community about implementing a hard fork.[36] As an interesting case study of this, Monero updated their hashing function to increase ASIC resistance, which ultimately led to a split chain as some parties continued extending the ledger with the original hashing algorithm.[37]

Other Protocol Updates

In the case of Ethereum, it's conceivable that other protocol updates such as the change in consensus (to PoS), adjustment of gas calculations, or addition of new opcodes could lead to a similar forking scenario.

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?

The Ethereum protocol is designed to mitigate disruptions by aligning end user incentives with the network stability. This means that the cost of attacking the network should increase as the value of Ether increases (and vice versa). However, that may not always be the case, as outlined below.

[35] More info: https://coinjournal.net/bitmain-announces-1st-ethash-asic-for-ether-mining/
[36] Discussions of an ASIC-resistant hard fork died down substantially given the planned switch to PoS
[37] More info: https://medium.com/@kaykurokawa/forking-for-asic-resistance-a-monero-case-study-ecdfb6c9fba2

51% Attack

For example, a 51% / Majority Attack[38] would require collusion from parties (or a single party) who have invested heavily in mining equipment and stand to receive the majority of newly-minted ether, so they would be incentivized to keep the value of ether high by not disrupting the network.

It's worth noting that the cost of that attack would be substantial. As a *very* rough estimate:

- You can buy 1 megahash / second for ~$10.00[39] [40]
- The current Ethereum network hashrate is an estimated 150K TH / s
- 75.1K TH = 7.51e+7 MH
- >50% of current hashing power would cost $751 million

One interesting dynamic in the current market environment is that network hashing power used to be close to 300 TH/s. Much of it was presumably turned off as a result of the high power and operational costs that exceeded the value of returns in ether following the 80% decline in ETH / USD prices. This means that there is enough hashing power on the sidelines to majority attack the network that is not currently generating returns.

Given the above, one could argue - purely from an economic standpoint[41] - that if the price of ether falls below the threshold of generating positive ROI for miners to keep their hardware on, it would be more beneficial for those miners to threaten an attack on the network unless paid not to do so than it would be to productively mine. Actively mining costs money, threatening an attack costs almost nothing. I'm certainly not an attorney or regulator, but it would seem that it's not clear if this is even illegal. The network is explicitly designed to give control to those with hashing power over how the network will operate. If some party (or parties) with unused majority hashing power were to, for example, print empty blocks[42] until paid to release their grip on the network, it may be deemed antisocial behavior, but it's well within the protocol rules.

Legal Regulations

It should be noted that there are various attacks that would likely be outright illegal. For example, directly attacking someone else's servers, such as in the case of a denial of service attack, is against the Computer Fraud and Abuse Act in the U.S. Similar regulations exist around the world, however enforcement on a distributed network with open access and high incentive to disrupt in certain scenarios could prove particularly difficult.

---

[38] More info: https://en.bitcoin.it/wiki/Majority_attack
[39] More info: https://www.techradar.com/news/best-mining-gpu
[40] More info: Using a retail price is presumably not scalable in reality, as supply shortages would likely be realized before sufficient hash power was achieved
[41] This is not intended as a suggested course of action!
[42] This has already happened in the split Bitcoin Cash community: https://cryptoblockwire.com/bitcoin-sv-vs-bitcoin-abc/

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?

Thin Markets

Ethereum trading is thin relative to most institutional markets. Institutional-sized orders have eaten through order books in the past, creating flash crashes.[43]

Custody

We have just recently seen the introduction of institutional-grade custody solutions for ether. While many of the technical and security requirements are native to the protocol, services that offer the operational and reporting requirements have only become available within the last year.

Exchange Security

Similarly, exchanges where ethereum is traded continue to prove vulnerable to theft, with more than $1 B stolen to date[44] and $2.7M stolen per day on average in 2018.[45] Naturally, it would prove exceedingly difficult to liquidate an ether position if your money had been stolen from the trading venue.

Exchange Hacks

Year	Funds Stolen	Hacks
2011	8,800,000	2
2012	865,000	4
2013	3,290,000	3
2014	475,574,000	9
2015	7,180,000	3
2016	80,870,000	4
2017	6,300,000	2
2018	810,000,000	4
Total	**1,392,879,000**	**31**

(Source: CoinIQ)

[43] More info: https://www.cnbc.com/2017/06/22/ethereum-price-crash-10-cents-gdax-exchange-after-multimillion-dollar-trade.html
[44] More info: https://coiniq.com/cryptocurrency-exchange-hacks/
[45] More info: https://www.coindesk.com/2018-a-record-breaking-year-for-crypto-exchange-hacks

Network Disruption

When a hard fork occurs, it is common practice[46] for exchanges to halt trading until there is clarity on the outcome of the fork. Similarly, in the case of a network disruption of any kind, it could prove difficult to move ether to an exchange to liquidate holdings.

It's worth noting that not all disruptions are malicious. For example, enthusiasm for digital kittens once became so popular that they congested the network.[47] We also generally observe higher blockchain activity during particularly volatile periods, which could make moving ether to liquidity venues more difficult.

Risk of Data Compromise

It's possible that wallet providers or exchanges to have bad data. Whether it is the result of being attacked or broken software, it's feasible for a given party's view of the state of the blockchain to be incorrect if their software is not implemented properly or reliant on a third party that does not provide sufficient proofs. We are increasingly seeing institutional services providers (custodians / wallets, exchanges, trading desks) verifying all blockchain data against a second, independent blockchain data feed and /or node implementation before signing transactions.

Human Error

The risk of misplacing private keys or sending ether to the wrong account cannot be overlooked. It's estimated that four million bitcoin are lost forever[48] - history has proven that these types of mistakes can and do happen.

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?

Perhaps the most notable impact an institutional derivatives market could have on a PoS model is driven by the potential for notional value of derivatives to dwarf the spot market, as is the case in traditional foreign exchange.[49] The economic incentives in Ethereum, both in PoW and PoS, are wholly contained within the network. As external economics outweigh those incentives, the whole model becomes at risk.

In a world where total notional value of a derivative market outweighs the spot market, the cost of a 51% attack could become economically rational to take on if you can take a larger notional short position on futures, particularly if the advantage of leverage is available.

---

[46] Example: https://www.bitfinex.com/posts/313
[47] More info: https://www.coindesk.com/loveable-digital-kittens-clogging-ethereums-blockchain
[48] More info: http://fortune.com/2017/11/25/lost-bitcoins/
[49] Source: BIS - https://www.bis.org/statistics/d11_1.pdf

Ironically, one could argue the inverse of that is actually one of the fundamental reasons derivatives should exist in the first place. If honest farmers can use futures to hedge against a low crop yield, should not honest miners be able to use futures to hedge against a network disruption?

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?

While there are a large number of projects looking to leverage the Ethereum network for a variety of interesting purposes, as outlined earlier in this document, the actual economic productivity of those applications remains limited relative to speculative activity. That said, there is a case to be made that derivatives could actually encourage greater adoption of those applications that are currently beholden to substantial volatility in the underlying asset.
For example, if we consider the application of energy payments automated via smart contracts on the Ethereum network to reduce dependency on intermediaries and bring down the price of energy for consumers, it's likely that management of the price of ether could be a deterrent for energy producers. This in turn could hinder adoption and reduce the ability to deliver energy efficiently. Surely there are many other barriers to adoption for a distributed energy system, but standard corporate hedging programs are used heavily by companies receiving or making international payments - it seems reasonable to posit that parties transacting in ether inherently have the same needs.

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.

One could argue that the introduction of futures would increase overall liquidity, including in the spot market. Institutional traders who already have the infrastructure to trade regulated futures but have no infrastructure to trade ether spot would be able to participate in the market for the first time. This tends to drive liquidity providers to take the other side of the trade, who will presumably look to hedge their risk by trading in the spot markets.

There is also a case to be made for better price discovery in the ETH market following the introduction of futures. Taking a short position at scale on ether today is difficult, generally requiring a counterparty from whom to borrow spot or execute an OTC swap for institutions in the US market. The ability to take a short position using a liquid, regulated instrument, could help the market more readily find a reliable price over time.

It is worth noting, however, that derivatives on Ethereum are actively traded, albeit in non-US venues. Just a few weeks ago, Huobi, a Chinese exchange, reportedly reached more than $20 B in cumulative ETH futures trading volume.[50]

[50] More info: https://www.ccn.com/huobis-crypto-derivatives-market-has-already-passed-20-billion-in-trades

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?

It is worth noting that there is ETH derivative infrastructure being built, and derivatives being actively traded today. Projects like dYdX[51] and UMA[52] seek to build decentralized solutions.

However, there are also firms already trading OTC swaps on various crypto assets using modified ISDA documents. While it's comforting to see the adoption of widely-used foundational documents, the adjustments made to accommodate crypto are being done ad hoc, which can lead to a massive organizational issue as the market scales. The state of equity derivatives is a good example of this. That market evolved into every dealer using bespoke terms, creating substantial operational and risk management issues as the market grew. Now is the time to get organized and standardize trade terms for crypto derivatives and prevent the inevitable future that occurs if the market doesn't get organized. For example, blockchain network events are similar to corporate events - they may not all be exactly the same, but standardization on how to manage trade terms for those that are known (e.g. chain forks) can prevent a world of headache and systematic risk down the road.

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?

Global trading and distributed exchanges will inevitably make regulation difficult. Spot trading venues can be domiciled anywhere in the world and have access to the Ethereum network. Activity on these venues may not be sanctioned under future regulatory regimes in the U.S., but if they maintain a significant share of liquidity, activity in those markets will likely impact U.S.-based trading.

Ethereum, even more so than bitcoin, is suited to facilitate distributed derivative markets by virtue of the native applications that can be embedded within the network. Smart contracts that change state and / or distribute funds based on a predetermined agreement between parties is exactly the reason the network was conceived and designed.

[51] More info: https://dydx.exchange/
[52] More info: https://umaproject.org/