Gus P. Coldebella
EVP, Chief Legal Officer, and Secretary
gcoldebella@circle.com
617-951-1887

February 15, 2019

VIA ELECTRONIC SUBMISSION

Mr. Christopher Kirkpatrick
Secretary of the Commission
Commodity Futures Trading Commission
Three Lafayette Centre
1155 21st Street, N.W.
Washington, DC 20581

RE: ***Request for Input on Crypto-asset Mechanics and Markets***

Dear Commissioners and Staff:

Circle Internet Financial Limited thanks the Commodity Futures Trading Commission for providing the opportunity to comment on the Commission's RFI regarding Ether and its use on the Ethereum Network. Circle (www.circle.com) is a global crypto finance company, dedicated to helping people and institutions create and share value globally. With our suite of products, we enable our customers to send and receive money around the world easily, as well as invest in and trade crypto assets.

Derivatives markets are essential to the virtual currency industry, and we fully support the agency's efforts to enhance legal certainty in the markets through informed policymaking. We believe that public input on matters integral to the functioning of the virtual currency markets like the subject of this RFI and on proposals affecting our industry such as the interpretation of "actual delivery" is vital to implementing regulation that allows innovation.[1] To assist in that regard, we are pleased to provide responses to the questions posed.

[1] *See* Retail Commodity Transactions Involving Virtual Currency, 82 Fed. Reg. 60335 (proposed Dec. 20, 2017) (proposing amendment of 17 C.F.R. pt. 1), https://www.gpo.gov/fdsys/pkg/FR-2017-12-20/pdf/2017-27421.pdf.

Purpose and Functionality

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

The impetus for developing Ethereum as a separate protocol was the cryptocurrency community's desire to extend Bitcoin functionality beyond value exchange. At the time, projects like Namecoin and other protocols based on Bitcoin were developed in order to fill needs such as a decentralized Domain Name System,[2] but the Bitcoin community did not want to implement features like tracking the state[3] of variables unassociated with transactions on-chain. There was a fear that implementing support for smart contracts would detract from one of Bitcoin's core competencies as digital cash. As a result, many who saw potential for tokenizing other assets worked to build complex programmability into Ethereum so that complex operations like "smart contracts" (on-chain programs that can execute functions or actions based on specified conditions) could function on-chain. Among other things, smart contracts are able to call and track the state of variables within them, which can potentially unlock complex and previously-inaccessible forms of value transfer.

With smart contracts and "tokenization" -- which is the ability to create new tokens that run on the Ethereum network -- we believe that communities will be able to tokenize more forms of value and make them accessible online and internationally, similar to how the Internet made information transfer accessible and easier over time.

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

Bitcoin and Ether differ in a number of ways. In Ether, new coins are rewarded to proof-of-work miners that calculate a block with the correct hash, but there's also an

---

[2] Domain Name System or DNS converts domain names into IP addresses.

[3] In the case of cryptocurrencies, their respective ledgers are viewed as "state transition systems," meaning that a given ledger records the location ("state") of all balances through transaction histories. In the case of Bitcoin, the "state" is "the collection of all coins (technically, 'unspent transaction outputs' or UTXO[s]) that have been mined and not yet spent." In the case of Ethereum, the "state" is "made up of objects called 'accounts', with each account having a 20-byte address and ['state transitions'] being direct transfers of value and information between accounts." *See* A Next-Generation Smart Contract and Decentralized Application Platform, https://github.com/ethereum/wiki/wiki/White-Paper#bitcoin-as-a-state-transition-system.

"uncle reward,"[4] which grants a partial reward to miners who mine the correct block slightly after the first miner. This "consolation prize" promotes decentralization, because mining a block becomes less zero-sum, and individuals can mine in smaller pools while still having a chance to receive compensation.

There is also a difference in how balances are recorded and calculated. With Bitcoin, coins are a "chain of electronic signatures" with specific values called unspent transaction outputs (UTXOs). Functionally, this is analogous to dollars and coins in one's pocket; transferring value is accomplished through transferring UTXOs from one address to another. If, say, Alice with 0.05 BTC wants to send 0.03 BTC to Bob, the protocol would "make change" in the form of breaking the 0.05 BTC into two new UTXOs worth 0.02 and 0.03 BTC, with the former being returned to Alice. Ethereum uses an accounts-based architecture, meaning that balances show up based on the total number of each token belonging to an address, as opposed to the sum of the values of UTXOs belonging to an address, as seen in Bitcoin.

As with Bitcoin, Ether can be used to pay for transactions and can be used for payments. Unlike Bitcoin, tokens on the Ethereum Network can be generated using smart contracts and can be used in smart contracts and transfers.

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

The Ethereum developer community is using Ethereum to streamline and reduce the cost of traditional modes of value transfer. The first step is tokenizing forms of value that end-users of technology have already been exchanging, directly or indirectly. By manifesting value as tokens, the community intends to create robust marketplaces, and networks with programmable forms of value accessible to the underserved.

---

[4] The "uncle reward" is found in Ethereum, but not Bitcoin. Since Ethereum has lower block times than Bitcoin, there's a higher rate of valid blocks that are not on the main chain and do not receive a direct reward. To counter this, the Ethereum network pays rewards for these valid blocks, thereby adding to the security of the main chain. *See* StackExchange, https://ethereum.stackexchange.com/questions/34/what-is-an-uncle-ommer-block.

For instance, Ethereum users are exchanging value through decentralized markets on platforms,[5] increasing access to credit through decentralized lending platforms,[6] and using the wisdom of crowds through prediction markets.[7] People are sidestepping the squatting behaviors seen with DNS domains through ENS (Ethereum Naming Service), storing files in a decentralized manner,[8] and accessing Ethereum-based websites (colloquially referred to as decentralized apps, or dApps) through mobile browsers.[9]

"Stablecoins" -- tokens pegged to the price of fiat currencies, like CENTRE's USDC[10] Gemini's GUSD, and itBit's PAX -- allow individuals to transact on-chain without worrying about price volatility. Non-fungible tokens allow holders, owners, and others to issue and track ownership of art and other collectibles on-chain.

Communities are also restructuring incentives pertaining to quality posts on social media platforms[11] and curating data on decentralized maps using open protocols.[12] There are also platforms working on identity, gaming, shipping, and the tokenization of ownership of other forms of value (including equity, real estate, and other real-world assets).

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?

As noted in Question 3, the dApp ecosystem is comprised of commercial enterprises using Ether to facilitate both familiar and nuanced types of value transfer. Commercial enterprises include lending markets, crowdsourcing knowledge through prediction markets, and marketplaces for collectibles and in-game items like OpenSea and CryptoKitties. UNICEF has also ventured into experiments using Ethereum to pay out and track payments made to refugees, indicating that non-profits and NGOs are also exploring the benefits of using Ethereum to facilitate and measure value traction.[13] These efforts all benefit from being on Ethereum because the Ethereum network supports

[5] *See, e.g.*, Paradex, https://paradex.io/ and IDEX, https://idex.market.
[6] *See, e.g.*, Dharma Lever, http://lever.dharma.io/ and Compound, https://compound.finance/.
[7] *See, e.g.*, Augur, https://www.augur.net/.
[8] *See, e.g.*, STORJ, https://storj.io/ and IPFS, https://ipfs.io/.
[9] *See, e.g.*, MetaMask, https://metamask.io/ and Opera, https://www.opera.com/crypto.
[10] Circle is affiliated with CENTRE.
[11] *See, e.g.*,Peepeth, https://peepeth.com/welcome and Cent, https://beta.cent.co/.
[12] See, e.g., FOAM, https://www.foam.space/.
[13] *See* UNICEF, https://www.unicef.org/innovation/blockchain.

programmable variables on-chain through smart contracts, allows users to read, update, and remove variables in smart contracts, and through these functions allows for computations in a distributed manner. Additionally, average block times for Ethereum are calculated in seconds instead of minutes, making it easier for people and companies using the Ethereum network to process more transactions on-chain.

Accounting for digital assets such as Ethereum is a complex and nuanced topic. Miners, exchanges, trading desks, and other services interacting with digital assets book said assets in different ways. Those methods can differ depending on the business model and geographic accounting framework. As of yet, US GAAP hasn't specifically addressed how to account for virtual assets, adding more uncertainty to the proper way to record Ethereum on one's books.

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?

Block explorers, including sites like EtherScan (https://etherscan.io/), Etherchain (https://www.etherchain.org/), and BlockScout (https://blockscout.com/eth/mainnet), are industry-trusted sources for transaction history, transactional data, ownership concentration, and other general information. Market data including market size, trade volume, and other data can be gleaned from aggregators including OnchainFX (https://messari.io/onchainfx/), Coinmetrics (https://coinmetrics.io/), CoinMarketBook (https://coinmarketbook.cc), and CoinMarketCap (https://coinmarketcap.com/). Due to the nature of dApps, there are many uncharted smart contracts and addresses that may be associated with popular services, but Ethereum block explorers may not have that information available. For dApps and other Ethereum smart contracts, services including DappRadar (https://dappradar.com/), NonFungible (https://nonfungible.com/), CuriousGiraffe (https://www.curiousgiraffe.io/) present user metrics for popular dApps through dashboards.

6. How many confirmations on the Ethereum blockchain are sufficient to wait to ensure that the transaction will not end up on an invalid block?

The number of confirmations varies from platform to platform, and is dependent on the amount of trust a service places on its users; too many confirmations will impede the user experience, whereas not enough confirmations for a transaction exposes the recipient to invalid transactions. The industry has deemed 30 minimum confirmations for Ethereum and ERC20 token deposits to be a safe standard. This protects both traders and our company from deposits being deemed invalid after a customer's balance has been updated and exchanged for another token.

Technology

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

Both the Ethereum and Bitcoin Networks are similar in that they both use proof-of-work consensus mechanisms to generate new blocks, are conventionally known as "public blockchains," and have native tokens used for payments.

Where Ethereum differs from Bitcoin is in Ethereum's ability to perform smart contracts, and its developers' desire to iterate upon its current consensus mechanism and governance structures. In the future, the Ethereum network plans to implement features like proof-of-stake consensus (instead of miners expending huge amounts of electricity for proof of work), and sharding[14] in a way that facilitates smart contract functionality at scale.

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?

---

[14] "Sharding" helps the Ethereum network scale. Through sharding, the network assigns different nodes the task of validating different transactions, so a node can validate a transaction without storing the entire transactional history. This allows increased scalability (transaction output) without compromising on decentralization or security. *See* Sharding FAQs, https://github.com/ethereum/wiki/wiki/Sharding-FAQs#what-is-the-basic-idea-behind-sharding.

The scalability challenges faced by the Ethereum network are fundamentally different from those involving Bitcoin. While the Bitcoin network has support for some scripting functionality, the Ethereum network tracks the "state" of variables within a smart contract, increasing the computational burden necessary to run a full node (a node being a computer or server saving the entire history of Ethereum transactions; full nodes are important to the network as they increase decentralization and facilitate access and participation in validating the network).

There are numerous proposed scaling solutions to Ethereum:

- Plasma. This involves "sharding" the network into smaller blockchains with similar protocol rules. Transactional and computational data would live on different nodes, so that more transactions can be processed.
- State channels. Off-chain transactions that are settled on-chain once the parties involved agree upon a specific sequence of transactions.
- Sidechains. Different blockchains can protocol rules similar or different from the parent chain. This includes a "bridge" allowing people to move funds to or from a parent chain onto the sidechain.

There are also a number of proposed scaling solutions actively being researched and developed. These solutions include:

- Serenity (Casper and sharding)
- Polkadot (an interchain protocol)
- Loom (a Plasma sidechain)
- Raiden Network (state channels)
- Connext Network and Spankchain's app-specific state channel solution

To analyze scalability concerns, one could use block explorers like EtherScan or BlockScout (both noted previously) to determine average block times. One could also also analyze the average gas limit of a block over time. Gas limits are a hard cap to the amount of computations a given block can hold, so as smart contract activity increases on Ethereum, the chance that the gas limit is reached on a given block increases. One can view this data on Etherscan (https://etherscan.io/blocks; https://etherscan.io/chart/gaslimit) or BlockScout (https://blockscout.com/eth/mainnet/blocks).

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?

There has not been a digital asset with a proof of stake (PoS) consensus mechanism tested at the scale of the Ethereum Network, but EOS, another smart contract platform, uses delegated PoS (dPoS) as their consensus mechanism.

dPoS could present issues related to block producers. EOS's block producers are elected by the community, and have expended time and capital in maximizing their nodes' uptime and functionality. While they could attempt to collude with one another (or act as sole bad actors) in order to alter the protocol, there are economic incentives that impede a block producer from destroying the value of the token that allowed them to become a producer in the first place. This is also the case with Proof of Stake and Proof of Work (PoW); any one bad actor (or group of bad actors) that colluded to attack a given network would need to amass capital (in tokens for dPoS, and in hash power for PoW) to have the influence necessary to successfully attack the network. The moment the bad actors attacked the network, they would need to extract enough value to cover the costs of amassing the capital necessary to run the attack along with the value of the amassed capital, which would depreciate the moment other parties recognized there was an attack.

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.

It is arguably harder to gain the tokens necessary to conduct a majority attack[15] on a PoS-based network, compared to PoW. Since there are visible and liquid trading venues that would likely list the token, along with a plethora of blockchain analysis tools, websites, and social media bots, the price of the token would rapidly increase, and it would trigger a great deal of attention. Additionally, there may not be enough of a given PoS-based token's supply on exchanges, so sourcing the liquidity necessary to purchase a majority of tokens may not even be possible. Moreover, performing the attack will decimate the value of the tokens accumulated; in the case of PoW, since there is an unspoken rule to not create one's own cryptography, some PoW-based networks' coins

[15] An entity with a majority of the mining power on a network could exercise control over the chain, posing a security risk. A 51% attack is an example of a majority attack for PoS-based networks.

use the same hashing algorithms. This means that after a successful majority attack on a PoW protocol, one could reuse the miners for another protocol in the future, if the used miners are capable of efficiently mining another token.

11. There are reports of disagreements within the Ether community over the proposed transition to a proof of stake consensus model. Could this transition from a proof of work to a proof of stake verification process result in a fragmented or diminished Ether market if the disagreements are not resolved?

The future is uncertain, but we hold the view that the transition to PoS may be less contentious than the post-DAO hack fork that led to the creation of ETC. Additionally, we believe that the ability to "fork" a protocol is a feature of open source decentralized digital assets, and not a defect. If a participant, or group of participants, in a digital asset's network do not agree with decisions made, they may fork the protocol and apply changes that suit their fancy. The economic incentives of public blockchains keep things in check over time. If a fork has a value proposition, participants will join to reap the added value, and vice versa. As such, we're unsure if there will be a diminished Ether market, but if there was a contentious fork of Ethereum, we would eventually see if there was a unique value proposition found only in that fork.

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

Primarily, the Ethereum Network is the largest and most used smart contract platform within the digital asset space. While other networks may show higher transaction volume, many of those same networks also have no transaction fees, potentially skewing visibility into non-spam use of the network.

In the face of scaling issues, users and developers building on the Ethereum Network could use sidechains, or find gas-efficient methods to interact with smart contracts. It also helps that the upcoming Constantinople upgrade will add features that make interacting with smart contracts gas-efficient, as will other features over time.

Governance

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

We believe that the two networks' governance structures are similar in that they're both determined by the chain with the longest proof-of-work. Additionally, core network developers may feel beholden or at odds with different stakeholders using their respective networks.

A difference is that, with the Ethereum Network, the first set of core developers have been identified (unlike Satoshi Nakamoto). Over time, both networks have shown the ability and capacity for open discussions around the merits and detriments of specific features, indicating that both networks' governance focuses on obtaining and maintaining consensus while progressing the implementation of useful features.

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?

While we do acknowledge that the current Ethereum network was borne from a contentious fork following the DAO exploit, we do not believe that this is an inherent vulnerability. While hard forks can result from contentious disputes, the community's ability to resolve governance disputes through forking a protocol speaks to the freedom that cryptonetworks grant their participants. Ultimately, the market decides, and in the case of Ethereum Classic, values both ETH and ETC.

Looking ahead, there could be potential contention around proposed solutions to issues like scaling, or centralization. If a proposed solution puts Ethereum-based companies at odds with one another, this could lead to a contentious hard fork and two independent networks. That would arguably be a net positive for markets. If the Ethereum network forked to support different use cases, then the opportunity for community members to focus development on specific use cases for both forks would likely present itself. Over time, specialization between networks would promote better price discovery and hedging, as the values of those networks could be more accurately charted.

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?

The primary impediment preventing market participants or potential bad actors from disrupting the Ethereum network is cost, as is the case with other robust blockchains like Bitcoin. Be it through proof-of-work or proof-of-stake, the cost associated with disrupting the network through a majority attack such as a Sybil attack[16] are in order of millions for ETH and BTC. A bad actor would need to either source the hashing power through other mining rental services, or make arrangements with other miners in order to accumulate the mining power necessary to successfully attack.

The act of buying up the requisite hashing power would attract attention from other miners and the Ethereum community at large, which would likely trigger attempts to counteract the attempted attack by turning on additional hardware and increasing hashing power (thus increasing the amount of miners and hashing power necessary to complete the attack). Since any majority attack attempt that does not succeed is entirely a sunk cost, this acts as a deterrent to not spend millions of dollars attempting to seize the network.

Another impediment to disruption is that it is likely to be uneconomic. Specifically, to justify spending millions of dollars attempting to disrupt the network, one would need to enter and exit a sizeable position while seizing control of the network (by depositing Ethereum to perform a double-spend attack[17], and trading out of the Ethereum). Exchanges that are liquid enough to have multi-million dollar orders filled generally conduct KYC and have a vested interest in not accepting double-spent funds. Conducting a trade large enough to justify the cost of the attack would alert exchange operators to the

[16] Sybil attacks occur when a single faulty entity can present multiple identities, and attackers use these multiple identities to control a substantial fraction of the system. *See* https://www.microsoft.com/en-us/research/wp-content/uploads/2002/01/IPTPS2002.pdf.

[17] A "double-spend attack" is a problem seen in blockchains due to their decentralization. With centralized ledgers/mints, one only has to trust one version of a list of transactions. With blockchains, the network needs to ensure a bad actor cannot send the same tokens to two different destinations, which would imply the supply has been increased arbitrarily, and allow a bad actor to defraud one of the recipients.

potential benefactors of the attack, and freeze their accounts before the benefactors are able to lock in the ill-gotten profits. Currently, decentralized/non-custodial exchanges (i.e., ones without robust KYC) do not have enough liquidity to allow for orders worth multiple millions in USD to be filled, so while benefactors of a 51% attack would be able to hide their identities on those platforms, the network's participants would act to block any profit-taking from that attack.

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?

There are not many impediments or risks associated with converting Ether to and from legal tender. Ethereum is one of the most liquid crypto assets available on spot trading platforms, and there are numerous trading platforms that also contain fiat on-ramps, including Coinbase, Gemini, Kraken, Bitstamp, itBit, HBUS (Huobi), and others.

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?

The introduction of derivative contracts on Ether would arguably be orthogonal to the incentive structures underlying a PoS consensus model. When we view the function of futures contracts for ETH on one overseas futures/derivatives trading venue, it is notable that while the ETH derivatives markets are liquid, they are settled in BTC.

If there were ETH derivatives markets settled in physical ETH, the parties holding the contract at its expiry wouldn't receive any additional ETH, as the trading venue holding the ETH may not necessarily deposit the ETH into a staking node.[18] If the trading venue staked the ETH, they could still choose not to distribute the additional tokens that resulted from staking. One potential benefit would be that if an exchange is both a staking node and offered derivative contracts for Ether, the exchange could potentially give stakers a means of hedging, which would allow for more liquid markets and better price discovery.

[18] *See* ETH Staking, https://ethstaking.io/what-is-ethereum-staking/.

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?

We believe that one would employ the same risk management procedures used in spot markets for any digital asset: paying attention to issues that would affect the price of the underlying asset. Examples of issues that could affect the spot price of a digital asset include majority or Sybil attacks, drastic changes in the consensus protocol underlying an asset's network, hacks or bugs in the underlying network, and other factors.

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.

Generally, we believe the listing and trading of derivative contracts would be orthogonal to the functionality of the Ethereum Network, as networks are designed to be used independent of the existence of trading markets for their respective tokens. We also note that there may be second-order effects (as stated above), wherein the existence of derivatives allow for better price discovery over time.

That said, because conventional futures settle on predictable timelines, one could attempt to temporarily impact the network in a way that benefits a certain position around the time of settlement. While this potential attack could affect markets, the impact could be mitigated with additional CFTC guidance on digital asset futures market conduct. Particularly, it would benefit the industry if there was more clarity on how futures/derivatives markets for digital assets should function (like the agency's proposed interpretation on "Virtual Currency 'Actual Delivery' in Retail Transactions"), along with guidance on how to potentially offer contracts that may not need conventional settlement dates (since "actual delivery" for digital assets can and should happen on-chain within minutes). Apart from guidance, industry participants employing solid controls and best practices would serve as further mitigation tools. Therefore, attempts to attack the network in order to manipulate the price near the time a contract settles would have their impacts softened.

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?

There are overseas markets offering ETH futures contracts with increased leverage (for example, 50x), and some believe that markets like these are manipulable. However, no one trader can force another trader to enter or exit a position; we believe that markets are generally efficient over time, and that futures contracts allow parties to predict the future value of an asset based on current variables, promoting better price discovery. Given guidance from the CFTC on how venues may properly offer ETH futures contracts and monitor markets, trading venues will be able to allow for better price discovery and a more efficient market over time.

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?

One factor that may affect markets oversight is decentralized (or non-custodial) trading venues, though currently decentralized/non-custodial trading venues are illiquid for numerous reasons (poor user experience, regulatory uncertainty, on-chain order books).

We also believe that regulatory clarity on issues such as custody, actual delivery, and smart contract liability would help businesses better understand how to run these markets efficiently and compliantly, which may attract liquidity to these venues.

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

Best practices for monitoring the Ethereum network and other blockchains depend on the use of the network and chain. Blockchain forensics tools,[19] block explorers, blockchain analysis services like Google's BigQuery Public Data, transaction graphing sites, and application-specific tools could be helpful in monitoring.[20]

---

[19] *See, e.g.*, Chainalysis, https://www.chainalysis.com/ and Elliptic, https://www.elliptic.co/
[20] *See, e.g.,* NonFungible (https://nonfungible.com/) or CuriousGiraffe (https://www.curiousgiraffe.io/)

Cyber Security and Custody

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

There are not security issues peculiar to the Ethereum Network that currently need to be addressed. It is also worth noting that smart contracts running on Ethereum can be compared to programs or services running on the Internet: while the latter runs on the former, an exploit or issue with the latter does not indicate an exploit or issue with the former.

Smart contracts are still computer programs written by people, and should be properly audited by security teams ensuring that there are not defects that would jeopardize funds being lost. Additionally, smart contracts are separate from the larger functioning of the Ethereum Network; if a smart contract fails, that does not necessarily mean that the entire Ethereum network contains that same fault.

Over time, developers have learned how to reconcile the immutability of on-chain smart contracts, iterating on previous software development processes in order to make smart contracts capable of upgrading over time.

24. Are there any best practices for the construction and security of Ethereum wallets, including, but not limited to, the number of keys required to sign a transaction and how access to the keys should be segregated?

Best practices for construction and security of cryptocurrency wallets is different for online and offline wallets. The Ethereum Network only supports a single signature for transaction, which means that best practices cannot be implemented natively in Ethereum, but could in the future be implemented with technologies such as threshold signatures. Attempts to date to implement multi-signature externally have all been vulnerable to attack.

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

Auditing of cryptocurrencies like Ethereum focuses on proving control over claimed funds. Generally a sample of addresses is selected that are held by a company and the following takes place:

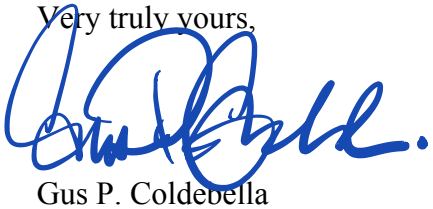
1. The balances of those addresses are confirmed on the blockchain at a point-in-time. This is generally done by an audit firm standing up their own independent Ethereum node.
2. The owner of the funds proves that they control the addresses in question using a signed message (standard functionality of an Ethereum wallet). The message to sign is independently defined by the auditor and is signed using the private keys associated with the addresses by the owner. The signed message is then confirmed using the public keys associated with those same addresses by the auditor.

□ □ □

Again, we appreciate the opportunity to respond to the Commission's RFI regarding Ether and its use on the Ethereum Network. Should you have any questions on our response or would like further information, please do not hesitate to contact me at gcoldebella@circle.com.

Thank you.

Very truly yours,



Gus P. Coldebella