FIA Principal Traders Group
2001 Pennsylvania Avenue NW
Suite 600 | Washington, DC 20006

T 202 466 5460
F 202 296 3184

ptg.fia.org

February 15, 2019

Mr. Christopher J. Kirkpatrick
Secretary
Commodity Futures Trading Commission
1155 21st Street NW
Washington DC 20581

Re: Request for Input on Crypto-Asset Mechanics and Markets

Dear Mr. Kirkpatrick:

The FIA Principal Traders Group ("FIA PTG") appreciates the opportunity to comment on the Commodity Futures Trading Commission's ("CFTC" or "Commission") Request for Input on Crypto-Asset Mechanics and Markets (the "RFI"). FIA PTG is an association of firms that trade their own capital primarily in the exchange-traded and cleared derivatives markets. FIA PTG members engage in manual, automated and hybrid methods of trading, and are active in a wide variety of asset classes, including equities, fixed income, foreign exchange and commodities. FIA PTG members are a critical source of liquidity in the markets in which we trade, enabling those who use these markets, including commercial end-users, to manage their business risks and to enter and exit the markets efficiently. In recent years, many of our members have begun trading crypto-assets and are now active traders and liquidity providers in both the spot market, and, in futures on Bitcoin listed on the CME and Cboe. In connection with their trading activities, many of our members have invested significant time researching these crypto-asset products, technologies and related ecosystems and, accordingly, are qualified to respond to the RFI.

FIA PTG understands that it is helpful for the CFTC to know as much as possible about Ethereum, as it is among the most actively traded crypto-assets and the CFTC plays an important role in enforcing rules against fraud and manipulation in the spot markets. Moreover, we believe that the time is right for launching additional crypto-asset derivative contracts and that Ethereum is mature enough to support futures contracts. Launching futures based on Ethereum, and hopefully other crypto-assets to follow, on futures platforms under CFTC oversight will bring many benefits to the marketplace. In particular, it will allow market participants to gain exposure to these products for both hedging and investment purposes on familiar, transparent, professional and well-regulated markets.

While we welcome this RFI process, we do not believe this template is likely to be necessary for future listing of derivatives on crypto-assets. We find the level of due diligence on the underlying, in this instance Ethereum, unusual or even unique based on our understanding of the Commission’s history of contract reviews, and would hope this would not set the precedent for the launch of additional crypto-asset derivatives. While it is important for the CFTC to understand certain features of the underlying market for crypto-assets, we believe that after gaining experience with Bitcoin and Ethereum derivatives, the requirements can be streamlined and, going forward, more of the focus can be on the proposed derivative contract rather than the underlying.

Attached as Appendix A please find our detailed responses to the questions posed in the RFI. Some of our members are quite active providing liquidity in the crypto-asset space and were happy to share their expertise and experience with Ethereum. We trust you will find our responses helpful.

If you have any questions about these comments, our responses to the RFI, or if we can provide further information, please do not hesitate to contact Joanna Mallers (jmallers@fia.org).

Respectfully,

FIA Principal Traders Group

Joanna Mallers

Joanna Mallers
Secretary

Appendix A: CFTC Request for Input on Crypto-Asset Mechanics and Markets

Purpose and Functionality

1. What was the impetus for developing Ether and the Ethereum network, especially relative to Bitcoin?
    - Ethereum was born out of the idea that Bitcoin was too limited in its ambitions. Instead of simply verifying transactional data, Ethereum developers conceived that a layer 1 blockchain could also function as a "super computer" that could execute smart contracts, and any other applications that a regular computer might be able to handle. Thus, the underlying architecture to Ethereum's blockchain is more complex than Bitcoin's.
    - Bitcoin is built on a simpler "unspent transaction outputs" model (UTXO model), which means its underlying blockchain can only handle verifying transactions data – i.e. "Sally had 8 BTC in her balance. Sally sent Bobby 5 BTC, and now her wallet balance reads 3 BTC." Bitcoin supports simple scripting language to execute signature checks, hashlocks, and timelocks. Executing more complex smart contracts and communicating with other blockchains, are abstracted onto layer 2 solutions such as Rootstock.
    - In addition, Ethereum was motivated by general concerns for facilitating transactions between "consenting individuals who would otherwise have no means to trust one another"; see section 1.1 "Driving Factors" in Ethereum's white paper for a summary (https://ethereum.github.io/yellowpaper/paper.pdf.)
    - Relevant links: https://medium.com/@ConsenSys/thoughts-on-utxo-by-vitalik-buterin-2bb782c67e53

2. What are the current functionalities and capabilities of Ether and the Ethereum network as compared to functionalities and capabilities of Bitcoin?
    - As stated above, Ethereum is built on the concept that a blockchain can be "richly stateful" – a term coined by Vitalik Buterin to refer to how Ethereum accounts store contract code and data beyond simple transactional balances. This allows developers to write code to any complexity they wish using information as provided by an "oracle"; the Ethereum Virtual Machine (referred to as the 'EVM') is responsible for executing every line of code.
    - Much of the code that runs on Ethereum executes so-called "smart contracts." The CFTC has published a useful primer on smart contracts including a number of examples (https://www.cftc.gov/sites/default/files/2018-11/LabCFTC_PrimerSmartContracts112718.pdf)
    - Similar to how every full node running the Bitcoin blockchain must store and update the transactional backlog, every Ethereum full node runs the EVM and executes the same instructions in parallel. While running these smart contracts in parallel is a massive computational task, this feature allows data to be unchangeable and censorship-resistant; hence, Ethereum maintains decentralized consensus across all participants.

- ➢ As a result of Ethereum's smart contract capability, developers have primarily used the Ethereum network to launch other decentralized token projects; these projects mostly utilize what is called the ERC-20 token standard. Some projects intend to port over to their own native blockchain, or mainnet, and use the ERC-20 standard as a stopgap; these include/ have included top market-cap tokens such as Tron, EOS, and Zilliqa. Other projects intend to remain on the Ethereum network and issue their own utility token separately from Ethereum.

3. How is the developer community currently utilizing the Ethereum network? What are prominent use cases or examples that demonstrate the functionalities and capabilities of the Ethereum network?
   - ➢ Fundraising for other decentralized applications; potential investors post Ethereum to their wallets and easily receive the new ERC-20 token in return.
   - ➢ The most prominent use cases so far, indicated by applications utilizing the largest contract storage on the Ethereum network, are decentralized finance applications (USD stablecoins, Maker DAO, decentralized exchanges), and gaming (Cryptokitties, Decentraland).

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?
   - ➢ Most progress on the Ethereum network has been made by the network's developers. The Ethereum Enterprise Alliance is an association dedicated to building customized Ethereum applications for industry players. The Alliance partners help develop use cases within different industries such as post trade settlement and supply chain tracking. Enterprise specific applications will often be permissioned ledgers and not require the ETH token itself to power the transaction.
   - ➢ For accounting purposes, International Financial Reporting Standards ("IFRS") guided in 2016 that digital currencies should not be considered as cash or cash equivalents, but instead as intangible assets. There is not yet a clear set of accounting rules issued by the Financial Accounting Standards Board ("FASB") or IFRS.

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?
   - ➢ While there are commercial tools such as Alchemy Insights and Coinfi, crypto market participants still generally rely on numerous open-source tools to determine key Ether metrics. Several of the most popular open-source tools used are listed below:

    i. For determining market size/ liquidity: CoinMarketCap, Etherscan (also includes comprehensive information on every single transaction made on Ethereum and affiliated ERC-20 token networks), BitInfo, CoinMetrics and more. Most exchanges also release their trading statistics for free, such as Coinbase, Kraken, and Poloniex.
    ii. For determining ownership concentration: the list of top holders associated with a cryptocurrency is colloquially called a “rich list”. The Ethereum rich list is readily available on Etherscan here: https://etherscan.io/accounts.
    iii. For determining the types of traders: Most analyses track large wallet movements and extrapolate based on the transactional footprint what kind of addresses appear to be most active. For example, the wallet addresses associated with the major exchanges are public and known.

- More advanced users will directly generate data on their own utilizing APIs offered by these open-source tools. Some will also parse data directly from the Ethereum network using their node client (Geth, Parity, etc.), or an Ethereum network explorer.

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?
    - Technically, only one confirmation is needed to validate and confirm a transaction. However, major exchange or wallet service providers require more than one confirmation. Answers from user forums and Ethereum developers vary on just how many are needed to ensure against potential chain re-organizations or exploits, and each exchange will have their own best practices.
    - Major exchanges wait for between 12 and 30 confirmations before crediting an Ethereum deposit to a user.
        I. Binance: 30 confirmations
        II. Gemini: 12 confirmations
        III. Huobi: 15 confirmations
    - In an official blog post from Vitalik Buterin (https://blog.ethereum.org/2015/09/14/on-slow-and-fast-block-times/), he states that, “the 17-second blockchain will likely require ten confirmations (~3 minutes)”.

Technology

7. How is the technology underlying Ethereum similar to and different from the technology underlying Bitcoin?
    - Mining: Bitcoin uses a different hash algorithm to encrypt inputs than Ethereum. Bitcoin utilizes the SHA-256 algorithm, while Ethereum utilizes the Ethhash algorithm. The crucial difference between these two algorithms is that SHA-256 is easier to design high-efficiency ASIC mining chips for. Larger, better capitalized mining operations tend to have access to ASICs while more home-grown, smaller

operations utilize GPU mining cards. Therefore, Ethereum is mined more on GPUs than ASICs. Bitcoin mining is more centralized across a small number of large firms relative to Ethereum mining.

- Consensus mechanism: While Ethereum is currently similar to Bitcoin in that it utilizes proof-of-work to mine blocks and validate transactions, the Ethereum network is currently transitioning to a proof-of-stake model that will enable validators to lock up a certain amount of Ether (currently proposed to be 32) in exchange for validating blocks. Full transition to proof-of-stake is predicted to come in early 2020 in the form of an update called Serenity, also known as Ethereum 2.0. Once Serenity/ Ethereum 2.0 is implemented - the old proof-of-work mainnet will temporarily co-exist with the newly implemented proof-of-stake beacon chain. The intention is to phase out the proof-of-work mainnet slowly.
- Contract data storage: As mentioned in answers 1 and 2, the blockchain architectures underlying Bitcoin and Ethereum are inherently different. Bitcoin's blockchain "state" is intentionally very simple, comprised of a collection of UTXOs ("unspent transaction outputs") that can only be generated and spent; once spent, these coins are subtracted from the user's wallet. In contrast, the Ethereum blockchain "state" is designed to accommodate all data associated with each account – this includes wallet balances, keys, and historical actions.
- Contract execution: The Ethereum Virtual Machine (EVM) is responsible for executing all operations for each smart contract. Each operation has a fee associated with performing it, which is denominated in 'gas'.

8. Does the Ethereum network face scalability challenges? If so, please describe such challenges and any potential solutions.
   - While scalability challenges are inherent to all blockchain platforms, Ethereum is more exposed to scaling woes due to how its architecture embraces complexity on layer 1. Other smart-contract capable blockchains opt to only host transactional data on layer 1, and then abstract computational abilities to layer 2 or even layer 3.
   - The key scalability issues facing Ethereum are:
     i. Blockchain size rapidly growing to an unsustainable rate, also referred to as bloat. Core developers generally agree that a solution to bound, or limit, the state of the blockchain is necessary. Calculations show that if the current mainnet gets a 10x capacity bump, and assuming gas limits are unchanged from 8MB, each node will have to store 5-6 terabytes (TB). At that size, the only stakeholders able to accommodate those storage needs would be limited to a select few – EF, archive.org, and Consensys – and hurt the network's decentralization. Total node count has declined from 30,000 to around 9,500 today, which core Ethereum developer Lane Rettig has publicly attributed in part to how cost-prohibitive it is for network participants to maintain a full node. If no changes are made to how state

rent is managed today, we believe the Ethereum network can only handle growth for three more years at best.

ii. Handling more transactions per second. Currently, the network can only handle approximately 15 transactions per second compared to the 45,000 handled by Visa. There are discussions of implementing sharding (splitting the blockchain into groups that run transactions in parallel), and also raising the gas limit (how the amount of transactions per block is currently capped).

- ➢ Core developers are actively working on two major scaling improvement proposals for implementation in late 2019/2020. "Eth 1.x" focuses on improving the layer 1 mainnet, while "Serenity" focuses on implementing the proof-of-stake enabled beacon chain. Below, a summary of the proposals in each that pertain to improving scalability.
  - i. Eth 1.x: Incubated in November 2018 during Ethereum's annual developer's conference, Eth 1.x proposes charging smart contracts some kind of storage fee for taking up space on the blockchain. If the rent is not paid, the account is completely removed from the blockchain state. According to initial calculations, this would eliminate around 28M inactive "dust" accounts, roughly equivalent to 15% of the blockchain state. https://medium.com/@lrettig/how-open-is-too-open-bfc412cf0d24. For active accounts, charging developers rent proportional to how much disk space their dAPPs are consuming may force them to make more efficient programming decisions.
  - ii. Serenity: Also known as Ethereum 2.0, Serenity will implement the first spec of the new proof-of-stake beacon chain. The beacon chain will initially co-exist with the proof-of-work mainnet. By locking up 32 ether, every participant will have a chance to become a validator and get paid interest in return for validating transactions / securing the network. The maximum number of validators allowed is 113,664, allowing an upper bound of 3,637,428 Ether to be staked at any time.
- ➢ Analyses/ data sources to assess scalability concerns:
  - i. Discussion forums: https://ethereum-magicians.org/

9. Has a proof-of-stake consensus mechanism been tested or validated at scale?

- ➢ It is important to note the difference between DPOS (Delegated Proof-of-Stake) and POS (Proof-of-Stake). DPOS consensus is based on an 'elected' group of delegates who validate blocks and determine protocol changes whereas in POS consensus, block validation and protocol changes are determined by validators who lock-up an asset in the network. Ethereum developers are working on implementing POS. Ethereum has multiple testnets where protocol upgrades are deployed and tested in preparation to changes or upgrades.

- There are various top market-cap tokens reliant on proof-of-stake being traded right now. So far, we believe all of them are in the 'testing' phase, and none of them can be deemed "validated at scale".
- Multiple issues with implementing proof-of-stake have been exposed this year among those in the testing phase. For example, top block producers for EOS (delegated proof-of-stake token at #5 market-cap at time of writing), were revealed to have possibly conducted quid-pro-quo agreements with each other for votes. (https://www.trustnodes.com/2018/09/29/rampant-collusion-in-eos-exposed-by-huobi-leak).

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? (consider that the chance of validating a block may be proportional to staked wealth)
    - Proof-of-stake has thus far not been implemented in the scale that proof-of-work has.
    - In general, all proof-of-stake methods run some risk of becoming more centralized entities where a few participants conduct the lion's share of verifying transactions. These risks afflict delegated proof-of-stake, as opposed to pure proof-of-stake, protocols the most. Most protocols have built-in features to mitigate this effect, such as imposing time limits on when a staker can verify blocks again and rewarding those who have not been chosen for a while.
    - Regarding Ethereum specifically, there is a risk that a participant could open up multiple validator accounts. If a malicious group of validators attempted to prevent others from joining or executed a 51% attack, the community would simply coordinate a hard fork and slash the offending validators' deposits. See Vitalik's proof-of-stake design philosophy, where he addressed this issue, here: https://medium.com/@VitalikButerin/a-proof-of-stake-design-philosophy-506585978d51

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?
    - While there may have been disagreements when the transition to proof-of-stake was first introduced years ago, we are not currently aware of any active disagreements within the community. The vast majority of core developers, community supporters, and investors agree that it is a necessary step towards Ethereum's ultimate ambition to support millions of users at scale one day.
    - We believe the group that may exhibit opposition are the current Ethereum miners who generate a sizeable return mining blocks for the block reward and transaction fees. Upon Ethereum's transition, these miners will be forced to support other cryptocurrencies or switch to becoming validators themselves,

which based on proposed current economics would not be as profitable as mining. However, without support from at least one developer group, the probability of these miners actively collaborating and forking the Ethereum coin are low.

12. What capability does the Ethereum Network have to support the continued development and increasing use of smart contracts?
    - Ethereum has one of the largest and most global developer communities of any cryptocurrency project. This includes the core developers building the protocol, and thousands of developers creating decentralized applications on the platform. All this provides a more decentralized, robust, and secure network.
    - Additionally, corporate working groups, such as the Ethereum Enterprise Alliance, help develop customized applications for companies who want to build blockchains using the Ethereum framework. Large financial services and technology companies are helping to create a more robust enterprise environment to help further the network.

<u>Governance</u>

13. How is the governance of the Ethereum Network similar to and different from the governance of the Bitcoin network?
    - Both networks use a public Github to track development through a proposal process in addition to a group of core developers who guide the changes to the network. Ethereum uses a more open and transparent consensus model to gauge the greater community feedback and acceptance of proposals through polling, survey and other sentiment analysis. Additionally, debates on various forums and calls are held between the developers on a regular basis to discuss Ethereum Improvement Proposals (EIPs). These processes guide the development and improvement of the network, but implementation is determined by users who run ETH nodes.

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?
    - Blockchains are inherently decentralized and therefore it is up to the users and node operators to determine the proposals that are implemented. If developers implement a certain proposal that is contentious and a minority group disagrees, that group can always fork off the main chain.
    - There is nothing inherent about Ethereum that makes the protocol more vulnerable than other protocols from hard forks other than the size of the network. A split in the ETH and ETC occurred due to the DAO exploit in 2016. As stated previously, decentralization allows one the freedom to choose the rules

that he/she supports and direct one's hash power or voting rights to the chain that best suits his/her values.

- Most of the time, the minority chain that forks does not gain enough traction due to the lack of exchange support. If a chain split from Ethereum gains large exchange support, it's likely that particular chain will survive.

<u>Markets, Oversight and Regulation</u>

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 Network is susceptible to several forms of attack that are common to all distributed ledgers: coordinated attacks on the performance of the network or 51% hacks. However, the more dispersed stakes in the network are, the more unlikely certain attacks generally become because they are harder to coordinate. The scale of the Ethereum Network makes these events less likely to affect Ether than other digital assets, but there is still a risk. Note that each consensus mechanism poses different benefits and drawbacks. Certain attacks require the coordination of a majority of computing power or stake in a network. The accumulation of such computing power or stake may cost inordinate amounts of capital and may, in certain circumstances, devalue the very thing that has been accumulated to conduct such an attack, thus disincentivizing the attack itself.

16. What impediments or risks exist to the reliable conversion of Ether to legal tender? How do these impediments or risks impact regulatory considerations for Commission registrants with respect to participating in any transactions in Ether, including the ability to obtain or demonstrate possession or control or otherwise hold Ether as collateral or on behalf of customers?

- Ether enjoys many points of access (so-called "on-ramps" and "off-ramps") to allow for fluid conversion from legal tender to Ether and back. These points of access are mechanisms through which an individual or entity may exchange legal tender for Ether. Examples include exchanges, dealers in the bilateral community, cryptocurrency ATMs, etc. Recent comments from SEC Director Hinman (https://www.sec.gov/news/speech/speech-hinman-061418) have given the market some indication that Ether will not be designated as a security, so it enjoys a broad listing and trading profile. Also, although the banking system is still developing for Ether, multiple banking options are available for exchange traded conversion to legal tender, as well as over-the-counter conversion. Ether's ability to be converted to legal tender is not dissimilar from certain FX pairs, which the CFTC has allowed derivatives to be listed upon.

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 derivatives contracts on Ether may allow a broader set of market participants to transact in the asset, and could promote a deeper and more robust form of price discovery. Because of the large number of participants that would have the ability to trade both the native asset and the derivatives contract, we would expect consistent price alignment between both markets to persist. It is our expectation that a global price available to a diverse set of participants would result in market-based incentives that are more like developed asset classes.

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?

- Commercial flows in Ether are still in their infancy. The most notable use cases currently observed are the hedging of payments by ICO issuers for token sales paid for by Ether and the use of Ether in the operation of distributed applications running on the Ethereum platform. Although, it is likely that certain hedging needs abate substantially as the volume of new coin offerings slows, it is possible that the need to hedge an accumulation of Ether in anticipation of planned distributed application and smart contract development requires additional hedging. Large numbers of new use cases for Ether are expected to emerge as smart contracts and distributed applications begin to be used in the real economy and outside of the early adopters in digital assets. A well-functioning derivatives market available for hedging the price risk of such development would spur more innovation.
- In addition, when Ethereum transitions to proof-of-stake, stakers in the network must lock up their Ether for a certain amount of time in order to continue validating transactions on the network. Certain stakers may wish to hedge the price risk of locking up their Ether through derivatives.

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.

- Greater access, price stability, transparency, and an enhanced regulatory framework. All these factors are seen as pro-innovation and are likely to increase the entrepreneurial use of Ether as a medium of exchange.

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?

- Tools that allow token movement to be tracked and provenance to be known are still in the early stages of development for Ether. Blockchain analysis software such as Chainalysis and Elliptic would be a welcome addition to the regulatory arsenal to properly monitor any potentially illicit or illegal activity attempting to use Ether.

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?

- ➢ Delaying the introduction of a sound regulatory framework in the US is likely to force market development offshore. Many international jurisdictions are poised to move faster, and critical mass could develop in areas outside the reach of the CFTC and other US regulators.

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

- ➢ Blockchain information is public and multiple vendors, as noted above, are offering software for monitoring relevant blockchains and activity. As the industry and technology evolves, we should be wary of imposing an artificially defined "best practice" on what information should be monitored and how that information should be analyzed. This is a somewhat nascent area; artificially imposing standards can stifle ongoing innovation and may inhibit industry participants from monitoring the Ethereum Network and public blockchain in ways they deem to be most effective and compliant.

<u>Cyber Security and Custody</u>

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

- ➢ Ethereum is a turing complete smart contract protocol. "Turing complete" means that the contracts deployed on Ethereum have the theoretical ability to compute any problem given enough resources and time. As a result, Ethereum supported smart contracts are vulnerable to additional 'attack vectors' which Bitcoin and many other cryptocurrencies may not be susceptible to. There are numerous static and dynamic analysis tools available for smart contract developers to find and close these vulnerabilities. Additionally, many companies and developers will engage independent auditing firms to review their smart contracts for the sole purpose of identifying and patching potential security risks.

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

- ➢ There is often a trade-off between usability and security such that when you increase the security of a system, you reduce the usability of it and vice-versa. Most of the largest cryptocurrency exchanges implement two categories of wallets termed 'hot' and 'cold'. Cold wallets are used to transfer larger amounts of cryptocurrency and often require more participants signing off on valid transactions. Hot wallets on the other hand are used to 'buffer' funds into and out of the cold wallet and often require fewer participants to manage transactions. Cold wallets hold the majority of users' funds at any given time where hot wallets are used for customer deposits and withdrawals. Different organizations have alternate risk management strategies, responsibilities and use cases for managing cryptocurrency wallets. How an organization should construct the security of their keys is dependent on the use case.

25. Are there any best practices for conducting an independent audit of Ether deposits?
    - When auditing Ethereum deposits and withdrawals, there are a few elements to keep in mind. For example, as an exchange, one often needs to generate a unique Ethereum address per client to manage their deposits and withdrawals in and out of the exchange. When managing the transfer history for hundreds of thousands of clients exchanges often decide to operate their own Ethereum nodes to query these activities. When auditing this activity, it is advisable to also operate a separate node or group of nodes so that there is a separate data source to reconcile transfers against. Running a node has its own best practices for keeping data secure and software up-to-date.

Glossary

1. **layer 1 blockchain & layer 2 solutions:** In blockchain, there exists something called the 'scalability trilemma.' Coined by Vitalik Buterin, it covers the tradeoffs between building a system which is scalable, decentralized and secure. For example, Bitcoin and Ethereum's layer 1 blockchains are understandably more decentralized and secure than scalable. They cannot process enough transactions to be widely adopted, but the transactions they do process can be considered valid and highly censorship resistant. Layer 2 systems are built on top of layer 1 systems and attempt to create alternate tradeoffs regarding the scalability trilemma. A layer 2 system might sacrifice decentralization for scalability, with the option to at any time, fall back to layer 1 for higher decentralization. This allows a blockchain to support scalability, decentralization and security to varying degrees depending on an application's use case.
2. **signature checks:** More broadly, digital signatures are used for verifying the validity of a message. Within blockchain, one application of digital signatures ensure that only authentic transactions are validated on a network.
3. **hashlocks:** These locks are used within layer 2 scaling methods. A specific contract which takes advantage of these locks is called a Hash Time Locked Contract (HTLC).
4. **timelocks:** (see above)
5. **censorship-resistant:** needed to operate a trustless environment. Transactions are unalterable and the community within a censorship resistant environment operates under equal terms of service and is inclusive.
6. **decentralized consensus:** allows all participants of a decentralized ledger to agree on some content or action and eliminates the need to rely on a central authority to ensure trust.
7. **ERC-20 token standard:** the specifications that an Ethereum token contract has to implement.
8. **permissioned ledger:** is a private blockchain where access is limited, write permissions are kept centralized and read permissions may be public or restricted.
9. **mainnet:** Mainnet is the actual production blockchain where users are creating real contracts or transferring real digital value. Mainnet is synonymous with 'production environment'.
10. **beacon chain:** stores and manages the validator registry in the proof-of-stake consensus mechanism. The beacon chain upholds the rules of the proof-of-stake

protocol and monitors the behavior of the validators to ensure their adherence to the rules. The beacon chain assigns rewards and penalties when appropriate. It also tracks the validators ETH deposits and will eject validators under certain conditions.

11. **UTXOs ("unspent transaction outputs"):** the record-keeping model employed by Bitcoin that is a triple entry accounting system (double-entry plus cryptography). Each transaction that uses an UTXO model has an input, where the coin came from, and an output, where the coin is sent.

12. **denominated in 'gas':** a special unit of Ethereum that measures how much work is required to process an action, such as an Ethereum transaction, or the set of actions required to execute a smart contract. The amount of gas charged is proportional to the amount of work required.

13. **state rent:** a fee charged for contract data that is stored and maintained on the network. The fee provides an incentive to better manage data and avoid bloat.

14. **validator:** https://www.mangoresearch.co/blockchain-consensus-vs-validation. A Blockchain Validator is someone who is responsible for verifying transactions within a blockchain. In the Bitcoin Blockchain, any participant can be a blockchain validator by running a full-node. However, the primary incentive to run a full node is that it increases security. Unfortunately, since this is an intangible incentive, it is not enough to prompt someone to run a full node. As such, Blockchain Validators are comprised primarily of miners and mining pools that run full nodes.

15. **top block producers for EOS:** analogous to a proof-of-work miner, a block producer verifies transactions on a proof-of-stake blockchain and are voted in by the community who holds the digital asset. In this example, EOS. In addition to verifying transactions, block producers introduce software upgrades and vote on protocol changes.

16. **polling, survey and other sentiment analysis:** Consensus among network participants is an important aspect of a blockchain. Many blockchains build 'incentive' mechanisms into their underlying structure to encourage 'honest' participants who should validate transactions and operations without biases. When proposing an upgrade to a network, it can become critical to understand which network participants do or do not support a change. Some protocols support network signaling where parties such as miners can indicate their stance. Other blockchains might use tokens to vote for changes or public voting or sentiment systems outside of the network. https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/nodes

17. **ETH nodes:** A node is a device on a blockchain network, that is in essence the foundation of the technology, allowing it to function and survive. Each cryptocurrency has its own nodes, maintaining the transaction records of that

particular token. Nodes are the individual parts of the larger data structure that is a blockchain.

18. **node operators:** (implied above)
19. **hash rate**: https://www.buybitcoinworldwide.com/mining/hash-rate/ A hash is the output of a hash function and, as it relates to Bitcoin, the Hash Rate is the speed at which a compute is completing an operation in the Bitcoin code. A higher hash rate is better when mining as it increases your opportunity of finding the next block and receiving the reward.