CFTC Request for Input on Crypto-asset Mechanics and Markets

This response is written by John Quarnstrom, Founder of Inveth, a decentralized options marketplace which utilizes Ethereum smart contracts to conduct call and put options through the Ethereum blockchain, in which "Ether" is the underlying asset. Given the nature of our business, it is imperative that regulators within the United States fully understand the technology behind the platform, hence the comprehensive set of answers to each question contained within the RFI. Please contact [redacted] for any further questions or clarification.

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

Bitcoin enables transactions from one wallet to another. All "addresses" on the Bitcoin blockchain are simply wallets created by individuals and the only functionality they have is **send** and **receive**, which is extremely limiting.

In contrast to Bitcoin, the Ethereum blockchain supports two types of "accounts", externally owned accounts ("Wallets") which function like Bitcoin wallets, and contract accounts (the technical term for "Smart Contracts"). Here is a detailed explanation of the two, taken from one of my whitepapers:

Externally owned accounts ("Wallets"), have four important characteristics: (1) They are controlled by private keys, thus enabling multi-party access via sharing of private keys. (2) They have an ether balance, colloquially known as "Ethereum". (3) They can send and receive Ethereum through signed transactions to other Wallets or contract accounts. (4) They are responsible for the creation of contract accounts, but have no direct ownership or control thereafter *in most cases*.

Contract accounts (CA) are autonomous agents created by an EOA or other CA's and are colloquially referred to as "Smart Contracts" - they have no private keys and are simply blocks of codes which operate in pre-defined ways. Due to the immutability of transactions, there exists a permanent record indicating the Ethereum address responsible for initializing a Smart Contract - furthermore, activities conducted on a Smart Contract pursuant to its creation are not controllable due to its inherent public accessibility (thus bringing into question the liability of who creates a smart contract, and who interacts with it thereafter).

Furthermore, Smart Contracts generally lack any direct ownership or control mechanisms through which a Wallet (i.e. average person) can interface with, without a protocol which directly supports ownership and control of the smart contract. Hence, this document outlines the ERC50 protocol which implements the functionality for facilitating call options between EOA's and CA's, in addition to the ownership and control mechanisms needed to distribute digital assets based on traditional call options through a CA.

Understanding the "autonomous" and "pre-deterministic" nature of smart contracts is vital to identifying the necessary evolution and introduction of the Ethereum network. Smart contracts allow one or more parties to engage in financial transactions in predefined ways. Furthermore, smart contracts can "escrow" assets and hold within them Ethereum, ERC20 tokens, or even ERC721 tokens. From a financial infrastructure perspective, this clearly removes the need for clearinghouses within derivatives markets.

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

Smart contracts have the following added functionality:

1. Escrow of digital assets.
2. Predefined logic and outcomes from within those contracts (*e.g. 5,000 Ethereum investment will release 250 Ethereum each month to a specified wallet*).
3. Endless possibilities for smart contract protocols, and given that the network is a decentralized and autonomous system (*meaning no third party can prohibit the initiation and execution of any financial transaction*) there exists the possibility for entirely distributed exchanges and marketplaces, or private agreements that are executed via a smart contract, or prediction markets such as Augur.
4. Creation of "ERC20" tokens which function similarly to stocks or equities, however they also support stablecoin infrastructures (DAI, USDC) which could lead to "ERC20 stocks" which distribute stablecoins as dividends.

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

MakerDAO utilizes smart contracts to conduct collateralized debt positions via protocols which enables one person to initialize a smart contract, deposit Ethereum, and withdraw "DAI" against the Ethereum collateral at ~66% ratio ($1,000 ETH → 666 DAI).

TrustToken currently utilize smart contracts to enable minting of their stablecoin TrueUSD, in addition to "burning" their stablecoins, in which they send TrueUSD tokens to the burn address and receive a wire deposit to their bank account shortly after.

EtherDelta is a prime example of a decentralized and autonomous system, operated fully by a single smart contract that handles the clearing and settlement of all Ethereum and ERC20 token trading activities. The EtherDelta exchange is powered by a single smart contract:

https://etherscan.io/address/0x8d12a197cb00d4747a1fe03395095ce2a5cc6819

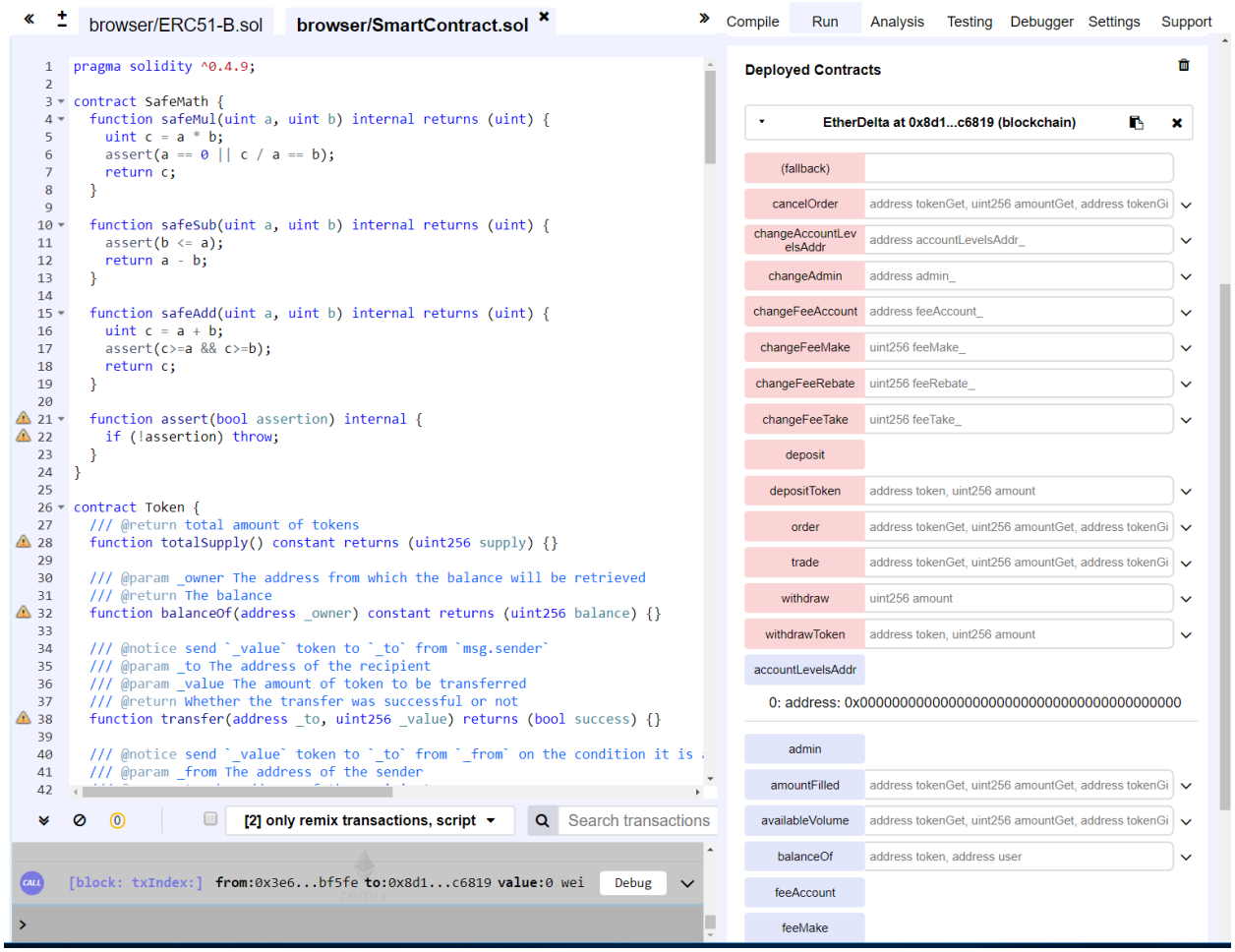
You will notice there are transactions occurring every day through this smart contract, executed by various outside parties. By navigating to the "Code" tab on the link above, one can see the exact source code which dictates various outcomes and predefined logic for the entire EtherDelta marketplace (*fascinating to think about, given that the total balance of all tokens held within that smart contract once exceeded $1.3 billion*).

The interface procured on the EtherDelta website enables parties to interact with that smart contract - however, due to the smart contracts public accessibility, anyone could copy-paste the source code to https://remix.ethereum.org/ and generate an interface for interacting with the exact same smart contract. I have supplied a photo on the next page which showcases this (*it took me about 30 seconds to pull that interface up, in which the red buttons are contract functions and the blue buttons show static information*).

I am now able to access the entire EtherDelta infrastructure through a third-party website. This is a solution that showcases the public accessibility features of smart contracts, and also the longevity of smart contracts - once they are deployed, unless a specific "kill switch" is implemented, it is next to impossible to stop or prevent that smart contract from functioning altogether.

If you take a closer look at the image, you will notice that I am able to deposit a token via the "depositToken" function, and withdraw my tokens through the "withdrawToken" function. Furthermore, I can execute trades and orders through the corresponding "trade" and "order" functions - all without the help of EtherDelta's website or interface.

This begs the question - is remix.ethereum.org a national securities exchange? If mining facilities are responsible for confirming transactions such as these on the Ethereum network, are they considered unregistered "broker-dealers"? Is the Ethereum blockchain itself considered a national securities exchange, or a derivatives clearing organization, given that it already operates as both? All I would need to do is type in my order in one of those function lines, and remix.ethereum.org would have conducted an illegal securities exchange (*for what it's worth, I have not done so - this is merely a real-world example which highlights the public accessibility of smart contracts*).



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?

Our firm is developing the infrastructure for Ethereum options trading which is physically-delivered (*according to the definition provided by the CFTC on physical delivery*) and powered by stablecoin transactions such as DAI or USDC. We intend to work with a registered commodity pool operator for issuing the options contracts and business for purchasing the contracts ("producers/processors/commercial users/ merchants").

DAI is an ERC20 token which is issued via the collateralized debt positions mentioned previously, and USDC is an ERC20 token which is issued in conjunction with audits on Circle's bank accounts, to verify that for each USDC issued has 1 USD in reserve. Thus, both MakerDAO and Centre (Circle) are utilizing smart contracts for stablecoins.

As far as accounting methods are concerned, I am unfamiliar with internal documentation and reporting of Ethereum or ERC20 transactions. However, smart contracts have event logs which contain all transactions (*amount, to, and from*). You can view all of the transaction history for USDC and DAI through EtherScan:

USDC: https://etherscan.io/token/0xa0b86991c6218b36c1d19d4a2e9eb0ce3606eb48
DAI: https://etherscan.io/token/0x89d24a6b4ccb1b6faa2625fe562bdd9a23260359

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?

EtherScan is a commonly used Ethereum Block Explorer mentioned previously which tracks the current market cap of Ethereum, as well as the throughput of Ethereum, in addition to mining rewards (*2 Ethereum each block, which occurs every 30 seconds*).

Google recently released BigQuery, a public dataset for smart contract analytics. This provides additional insight into on-chain transactions through the Ethereum network:

https://cloud.google.com/blog/products/data-analytics/ethereum-bigquery-public-dataset-smart-contract-analytics

Understanding the activity on various dark pools or centralized exchanges ultimately depends on how much you trust the integrity of data relayed by their API, which streams data in real-time. There are multiple data providers which aggregate this data and provides the average price of various cryptocurrencies, or specific volume for a digital asset based on the exchange. One project in particular is ChainRider, which I became involved with to help develop a more reliable average price for Bitcoin and Ethereum. https://www.chainrider.io/docs/finance/

An extreme concern of mine is the current reference rate that the CME and CBOE use for settling their Bitcoin futures and options contracts (*provided by CryptoFacilities*). Given that they only aggregate data from 2 - 3 exchanges for Bitcoin, which only captures approximately 3.0% - 4.0% of total market activity, it is apparent that the current data for CME Group's commodity exchanges forces traders to skate on thin ice, given that the underlying spot exchanges from which the reference rate is derived from is highly susceptible to manipulation - especially right before settlement of contracts.

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?

A statistician with the proper data on “uncle blocks” could provide a better answer. However, I would recommend 10 confirmations for general purposes and 25 confirmations for enterprise or commercial purposes.

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

Each blockchain utilizes “wallets” or “addresses” to store and receive the native asset. Each transaction requires a miner’s fee. The primary difference between the two blockchains is that Ethereum supports smart contracts, which are autonomous agents that contain protocols and “rules of engagement”.

I would recommend thinking about Ethereum as Bitcoin + Smart Contracts, and it’s also significant to note that Ethereum confirmation times are significantly less, ~30 seconds, compared to Bitcoin’s 10 minute confirmation times.

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?

The Ethereum Foundation is currently working to solve many of the scalability challenges Ethereum faces today. This will involve transitioning from a proof-of-work model to a proof-of-stake model. The data sources mentioned in Question #5 would help assess the throughput of the Ethereum blockchain, as well as the growth and adoption of additional smart contracts.

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?

I am not familiar with any proof-of-stake models that have been tested at scale, however the proposed solution from Vitalik in regards to economic incentives for a proof-of-stake model within the Ethereum ecosystem is fundamentally sound. They are currently testing the proposed solution on testnets as well, prior to launching on the mainnet.

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.

In traditional markets, individuals are awarded based upon the amount of capital they put at risk (*i.e. purchasing and holding 10,000 shares of a high yield income-fund as opposed to 1,000 will net more profits*). The idea of having more opportunity to validate a block, and consequently receive the reward, being dependent upon how much wealth is staked isn't a particularly foreign concept - and should be rewarded appropriately.

https://www.youtube.com/watch?v=VqOlOMAqCo8

In the explanation of Casper presented by Vitalik (*linked above*), he proposed 1500 ETH minimum for staking and operating a validator node. In a situation where your node makes "conflicting votes" against other nodes - this is where you maliciously operate by proposing transactions to the network which didn't occur, or conflict with a majority of other votes (*leading to a loss of your initial deposit in an amount between 1% - 100%*). Furthermore, in the event of hardware corruption leading to a node going offline, having a failure and recovery procedure in place to restore the node is vital. In fact, Vitalik proposed during that presentation at 23:30 the incentivization of having "maximally discorrelated" failure modes that differ from other system's failure modes. This ensures that multiple nodes supporting the Ethereum blockchain do not rely on the same recovery methods, which could lead to unilateral failure across an entire system.

In current mining pools, decentralization and trust issues occur - furthermore, you'll likely see the advent of "Staking Pools" once Ethereum finalizes the transition to PoS. In the situation where a staking pool is centralized, ensure that the firm or entity handling the Ethereum complies with the proper "commodity pool operator" procedures, given that this entity would likely qualify as a fund soliciting commodities for the purpose of "investing" in another commodity pool - given that staking returns % rewards based on amount staked over an annual time period.

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?

I'm unsure. It is possible the Ethereum mining community which has power to support one network over another would "split" into two communities - akin to the Ethereum and Ethereum Classic divergence, resulting in a forked blockchain. However, given that Vitalik Buterin supports the Proof-of-Stake model heavily, I truly believe this "upgrade" to the Ethereum blockchain will unfold without too many conflicts.

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

There are languages such as Solidity which act as "compilers" for Ethereum smart contracts. Solidity itself has numerous versions, and as a programming language, can be upgraded to higher versions as newer functionalities or stronger error handling features are introduced. Through this, the continued development of smart contracts can continue at the "compiler" level, which will facilitate more development at the "protocol" level (*the level at which programmers are implementing Solidity to develop new protocols for smart contracts - the "application" level, so to say*).

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

I'm not entirely sure how Ethereum and Bitcoin differ in governance mechanisms. From my understanding of the Ethereum and Ethereum Classic divergence, a small number of individuals were able to initiate the "Ethereum" fork, without the consent of miners. From this, I can only extrapolate that there are governance mechanisms which enable a small group of individuals to control the future of the Ethereum network, however I am clueless as to what those mechanisms are, how they are accessed, or who controls the rights to certain decisions.

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?

The word “vulnerable” in this question portrays hard forks or “splintering” as inherently bad outcomes, when the truth is that blockchain technology supports these outcomes. There is nothing inherently wrong with splitting a blockchain into two separate chains, each with their own unique governance and consensus mechanisms - and quite frankly, this functionality is important for precisely the reason Ethereum Classic originated.

Ethereum forked from the new “Ethereum Classic” because there were two groups:

1) Individuals against compensating those who lost Ethereum during the DAO hack.
2) Individuals for compensating those who lost Ethereum during the DAO hack.

Ultimately, there were enough miners who believed in compensating losses suffered during the DAO hack and forked into Ethereum - a blockchain which refunded the 3.6mm Ethereum lost by withdrawing a proportionate amount of Ethereum from every single wallet on the blockchain (*meaning if you held Ethereum in your wallet, you would have lost an equivalent amount, even if you weren’t responsible or involved with the DAO hack*). This Ethereum was then redistributed to those who lost their Ethereum, making everyone “whole”. Everyone who was against the idea of redistributing their wealth stayed in support of Ethereum “Classic”.

It is possible this situation will happen again, given that is has happened once before.

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 currently susceptible to congestion, wherein the network is overloaded with transactions, causing transaction fees to rise substantially. In a recent scheme, a cryptocurrency exchange FCoin supported voting for the next token listing by counting each individual deposit of a coin. This incentivized the community to make as many small deposits as possible for their coin, as each deposit was considered one vote.

This led to network congestion, an inflation of transaction fees, and some transactions which were placed with low gas fees were ignored by miners in lieu of other transactions with higher gas fees - thus causing an incredible backlog of 100k+ transactions waiting to be processed, some of which were likely “stuck” for 24 hours or more. However, moving to a proof-of-stake model would presumably end this potential attack vector.

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?

During a consultation job, I was paid in Ethereum and would cash out to my bank account via Coinbase. They continued to increase my daily and weekly limits, and there were no issues with receiving and withdrawing the money from my checking account. However, I have heard horror stories from numerous individuals in the space that were receiving quantities from Coinbase to their bank account in excess of $50k - $80k each week, which the banks were withholding.

Currently there is Wyre and Circle which have money transmitter solutions in place for converting digital assets into fiat currencies and depositing them into a bank account. Stablecoins are not considered legal tender, however a large portion of the community convert their digital assets into stablecoins for stability.

As mentioned in the first question, proving possession or control of Ether held as collateral is considerably difficult for “externally owned accounts” or “Wallets”, given that multiple parties could have access to the private keys and thus control of the digital assets. A “contract account”, also known as a Smart Contract, is not susceptible to this issue given that the source code is made publicly available and all parties can confirm that any Ethereum held in collateral will only be authorized for specific transactions or activities based on the “protocol” or “source code” of the smart contract.

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?

This is part of Inveth’s business plan - to offer options as a means of hedging Ethereum that is staked when operating a Casper validator node. This could sufficiently offset any risk, given the 4-month waiting period when withdrawing staked Ethereum. Offering derivatives contracts to companies that stake Ethereum will enable them to place larger amounts of capital into the network - furthermore, the transition to proof-of-stake will likely fuel more activities within derivatives markets precisely due to this new incentive mechanism which rewards staking, but requires hedging for risk management.

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?

Inveth is currently developing protocols which will support collateralization of a smart contract with both the DAI and USDC stablecoins. Thus, each stablecoin represents the potential underlying cash markets which enable options transactions. In regards to commercial risk management needs - there are two:

1) **Search and Destroy**
   In the event that a stablecoin is locked or stolen from a derivatives contract, the issuer of the stablecoin should enact a "search and destroy" mission which locates the account currently holding the stolen stablecoin and freeze their activity. From there, refund the stablecoins lost to the issuer of the options contract. Currently, Circle who issues USDC could probably support this. MakerDAO is unable to.

2) **Liquidity**
   At any point in time, the firm issuing a stablecoin should have the capability of transferring the stablecoin for fiat currencies in a bank account. If at any point in time, a firm is unable to redeem their stablecoins for fiat currencies, then the underlying mechanism "stabilizing" the stablecoin has disappeared and the stablecoin is worthless. This could prove devastating if 1,000 different options contracts are collateralized with the DAI stablecoin and suddenly the DAI ecosystem collapses, rendering the stablecoin worthless. The derivatives contracts would then payout absolutely nothing, leaving many companies in financially distraught situations.

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.

Given the illiquid and thin market status of Ethereum, derivative contracts are highly susceptible to manipulation by nature of "whales" which could dump their Ethereum onto the open markets and profit considerably from short positions, while also exiting their physical position. If a traditional futures or options trader owns a considerable amount of Ethereum and wants to exit their position, they could likely open a short position the month before on the CME, crash the market, and profit in both trades.

20 // Are there any types of trader or intermediary conduct that has occured in the international Ether derivative markets that raise market risks or challenges and should be monitored closely by trading venues or regulators?

From my understanding, most derivative markets have moved to regions that legally support trading activities - furthermore, given that Ethereum markets are so illiquid and thin (*last week, exactly 800 ETH would have crashed the Coinbase Pro order book from $110 to $13*) there are much greater market risks and challenges within the spot markets as compared to the derivatives markets, from my perspective.

21 // What other factors could impact the Commission's ability to properly oversee or monitor trading in derivative contracts on Ether as well as the underlying Ether cash markets.

There is a zk-SNARKs implementation for the Ethereum blockchain which enables complete transaction privacy. The costs to enact a transaction via zk-SNARKS is currently too high for practical applications, however once Ethereum transitions to a proof-of-stake consensus model, zk-SNARKS implementations will be commonplace. This will prevent the Commission from viewing any transactional information, including the identity of any parties involved. Furthermore, transactions occurring on private blockchain networks (*such as Quorum from JP Morgan*) have the potential to facilitate dark pools for derivatives transactions. Settlement of these contracts could be conducted through an entirely abstracted means, possibly via the public Ethereum blockchain in conjunction with a zk-SNARKS implementation, creating an incredibly opaque and complex ecosystem of derivatives transactions and settlements.

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

Due to the complexity of monitoring blockchain transactions and extrapolating data, there are no "best practices" - especially without further context on the exact information or business requirements of the entity monitoring the Ethereum network. With that being said, I certainly have expertise in architecting solutions for monitoring various transactions, primarily through my involvement with ChainRider. If there is a particular solution the Commission is interested in, feel free to contact me regarding the development of monitoring and analysis tools - always interested in exploring RegTech.

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

In general, smart contracts work exactly as programmed. Developers often mistake the syntax or exact functionality intended within Solidity, leading to vulnerabilities and attack vectors. Numerous firms exist for auditing smart contracts to protect against this, however there is no guarantee that a smart contract is entirely secure. I am not aware of any security issues or flaws within the core Ethereum blockchain code.

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?

In the context of distributing access and private keys amongst multiple parties, I am not entirely aware of best practices.

For personal use, I highly recommend anyone that owns cryptocurrencies to purchase a hardware wallet and store their digital assets in "cold storage" on the hardware wallet. In addition, back-up the hardware wallet with a paper wallet (*which is simply a phrase of 24 words*) and store that paper wallet inside of a vault for emergency recovery.

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

If you are conducting an independent audit of an Ethereum deposit, you will first need to host your own full node on a computer (*requiring a download of the entire Ethereum blockchain*). From there, you can view transaction histories by working with the Geth console (Go-Ethereum) to interact with the APIs.

https://github.com/ethereum/wiki/wiki/JavaScript-API#web3ethgettransaction

This command in particular accepts the transactionHash as a parameter and returns the necessary information, including who sent the funds, who received the funds, at what block (*timestamp*) the transaction occurred, and the amount of Ethereum sent.