Chatham Financial ("Chatham") thanks the Commodity Futures Trading Commission ("the Commission") for the opportunity to comment on this "Request for Input on Crypto-asset Mechanics and Markets."

Chatham is the largest advisor and technology provider to derivatives end users, serving over 2,000 clients worldwide. Chatham serves both financial end users, including regional and community banks, and non-financial end users, touching virtually every segment of the economy.

As a service provider in the derivatives field, Chatham is particularly intrigued with the opportunities presented by blockchain, especially smart contracts and crypto-derivatives. Among other initiatives, Chatham has been involved in the International Swap and Derivatives Association's Common Domain Model (ISDA CDM) initiatives. Chatham seeks to be prepared to advise and support our clients as these technological developments move from the realm of the most technologically advanced to more mundane, everyday uses.

Chatham has answered the questions posed by the Commission as our expertise allows.

**Purpose and Functionality**

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

The development of blockchain and distributed ledger technology (DLT) that undergirds Ethereum and Bitcoin reflect a desire to reshape some of the norms, such as centralization and data ownership, that had been unquestionably accepted by most internet users.

Users have only recently started questioning the efficacy of a system that grants ownership of data pertaining to them to third parties. Centralization of the internet, in particular as it pertains to where users' digital information is held, used, and monetized by companies who have shown themselves to be poor stewards of the data they have amassed with little oversight or control given to the users themselves, have made it such that a few large companies hold the data of many.

Blockchain was created counter to those norms. It is decentralized, with data replicated across several unrelated nodes with users maintaining control over their data through encryption keys.

Smart contracts reflect a similar desire to reshape legal processes by establishing a process that removed any question of whether the parties will perform. The self-executing smart contracts seek to create a system that makes trust irrelevant.

As stated by Dr. Gavin Woods in "Ethereum: A Secure Decentralised Generalised Transaction Ledger", one of the key goals of the development of Ethereum was to "facilitate transactions between consenting individuals who would otherwise have no means to trust one another. This may be due to geographical separation, interfacing difficulty, or perhaps the incompatibility, incompetence, unwillingness, expense, uncertainty, inconvenience, or corruption of existing legal systems."

The technology seeks to create one truth—one that cannot be corrupted or changed by bad actors, a system that cannot be manipulated or controlled by any outsized presence. While Bitcoin functions as a store of value, Ethereum is a technology that leverages many of the core features of DLT (fully

transparent, anonymous, time-stamped, unanimous, immutable, secure, and programmable) and pairs it with smart contracts to allow for parties to enter into legal agreements with full confidence they can anticipate the possible outcomes regardless of their counterparties and the systems in which they exist.

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

Ethereum is a decentralized network of computers that is a (1) blockchain that can record transactions and (2) a virtual machine that can execute smart contracts. Because Ethereum leverages smart contract functionality on the blockchain, it has a very different abilities as compared to Bitcoin.

Ethereum is a platform that is built specifically for the creation of smart contracts. It is a blockchain with a built-in Turing-complete programming language, which can be used to create decentralized applications (Dapps) and whole decentralized autonomous companies (DAOs). Smart contracts are self-executing, immutable, self-verifying, auto-enforcing, cost-saving, and removes third parties or escrow agents. Bitcoin, on the other hand is a much more limited example of a smart contract, one that can only transfer value from one person to another. Smart contracts built on Ethereum can be written to perform a far wider range of activities such as managing agreements between parties; providing utility between other contracts; supply chain management; financial derivatives; and tokens.

ERC-20 and ERC-721 are crypto-assets, like Bitcoin, but are tokens rather than cryptocurrency. ERC-20 and ERC-721 are designed and used on Ethereum. They follow a list of standards so that they can be shared, exchanged for other tokens, or transferred to a crypto-wallet. Smart contracts are used to create the tokens, as well as facilitate transactions of tokens, and record balances of tokens in an account. The tokens, however, do not have value. The difference between ERC-20 and ERC-721 is that ERC-721 tokens are non-fungible, which gives ERC-721 a specific type of utility that reflects its nonfungible nature.[1]

**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?**

Chatham has been actively involved in ISDA's market initiative to create a CDM to serve as a standard, digital blueprint for how derivatives are traded and managed across their lifecycle. As demonstrated at the Barclay's DerivHack in September 2018, Chatham feels Ethereum is a prime platform on which to deploy the ISDA CDM. In Chatham's proposed solution, which won Best Solution Architecture in the US, the ISDA CDM use cases (setting up counterparty data, a new trade event, lifecycle events, etc.) were deployed on Ethereum. Chatham's team selected this approach because Ethereum is a public platform, which would allow market participants equal access to the model and its benefits. Chatham sees the ISDA CDM as a prime use case for capital markets to benefit from the functionalities and capabilities of the Ethereum Network.

**Question 4 is intentionally excluded.**

[1] Probably the most prominent DAO is CryptoKitties. Released over a year ago and relying upon the non-fungible nature of ERC-721 tokens, CryptoKitties is a blockchain-based video game that allows users to buy, sell, and breed their CryptoKitties. Ownership of specific CryptoKitties, as well as its phenotype and genotype are all stored on the blockchain.

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

There is a myriad of sources to rely upon, many of which are easily accessible online. A good place to start is on the Ethereum Stats page. It is also important to point out that in following with the core DLT feature of transparency, anything directly related to Ethereum is on the blockchain. Individuals interested in getting much of the above information can directly query the blockchain. However, with the different exchanges added to the system there is some opacity because the exchanges don't report back to the blockchain.

Additionally, the code of Ethereum is open source. Anyone interested in understanding its architecture can review the code at their leisure. Further, the Ethereum developer meetings are also all publicly available and can be found on YouTube.

**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?**

There is no official number, but Binance requires 30.

**Technology**

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

Both Bitcoin and Ethereum are public distributed blockchain technologies that currently use a Proof of Work (PoW) model. The application of the blockchain to Bitcoin is specific to tracking and transferring the ownership of Bitcoins anonymously between users. The Ethereum blockchain is a Turing-complete language capable of executing smart contracts which are subject to fees paid in Ether (ETH), Ethereum's cryptocurrency.

**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?**

In the Ethereum Network, each node, or block, stores the entire state of the previous block and processes all transactions. While structuring the protocol in this way provides security, it limits scalability. The Ethereum Network can only process 7-15 transactions per second.[2] Bitcoin and other distributed blockchains face a similar problem of processing only a limited number of transactions per second.

There is an identified trilemma that bounds all blockchain systems: decentralization, scalability, and security. Decentralization refers to the limitation of computation, bandwidth, and storage of each

[2] For More Information: https://github.com/ethereum/wiki/wiki/Sharding-FAQs

participant in the network. Scalability refers to increasing the number of transactions the decentralized system can process. Security refers to the system's ability to be protected from attacks, like 51% attacks and others. Blockchain systems can only possess two of the three identified properties. Ethereum, and other existing blockchains, are built on the properties of decentralization and security, forsaking scalability.

During high volume transaction periods, transaction fees (known as the gas price) increase, and confirmation times become noticeably longer.

A partial solution to improving scalability is to implement sharding into the Ethereum Network. Sharding alleviates the restraints of each network node needing to store the entire state of the blockchain. Instead, nodes are grouped into shards, and each shard processes a specific transaction, thus allowing multiple transactions to be processed at the same time.

As Vitalik Buterin, creator of Ethereum, explains,

> *"Imagine that Ethereum has been split into thousands of islands. Each island can do its own thing. Each of the islands has its own unique features and everyone belonging on that island i.e., the accounts, can interact with each other AND they can freely indulge in all its features. If they want to contact other islands, they will have to use some sort of protocol."*[3]

Scalability concerns can also be addressed through state channels, like Plasma, that move payment interaction off the chain without requiring additional trust.[4]

**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 are several systems, such as Peercoin, BlackCoin, Lisk, and Nxt Coin, that implement a Proof of Stake (PoS) consensus algorithm. However, the methodology has not been tested at Visa's scale.[5]

**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.**

The PoS algorithm provides security to blockchain networks by relying on penalties instead of the rewards associated with PoW. Under PoS, "security comes from putting up economic value-at-loss."[6]

Mining under PoW requires computing power and electricity costs in order to run the calculations necessary to solve the next block on the chain. Benefits of PoS include lower electricity and hardware costs expanded to secure the blockchain which results in a lower barrier of entry for contributors to

[3] For More Information: https://www.bitrates.com/news/p/vitalik-buterin-scaling-is-ethereum-s-priority-and-casper-is-on-the-way-

[4] For More Information: https://www.jeffcoleman.ca/state-channels/

[5] Visa's scale is the gold standard of processing capacity exhibited by the electronic fund transfer company, Visa.

[6] For More Information: https://medium.com/@VitalikButerin/a-proof-of-stake-design-philosophy-506585978d51

participate in the consensus mechanism. This is achieved under PoS by creating proportionate returns on investment (whereas PoW encourages economies of scale for those who can afford mass-production equipment).[7]

Under PoS, the cost of a 51% is significantly higher because the attacker must obtain 51% of all staked coins rather than 51% of the mining power (which can be obtained through economies of scale under PoW). A 51% attack is also discouraged due to the withdrawal period. An attack executed for monetary gain would not be feasible as the staked funds could not be withdrawn from the network until four months after the attack, during which time, the attacker's identity could become known. Despite the challenges of executing a 51% attack for monetary gain, the attack could still be utilized as an economic weapon.

**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 adoption of any major protocol upgrades requires the use of the hard fork mechanism, under which users must upgrade to the newly created chain in order to remain on the hard-forked chain. In theory, after a hard fork, no new nodes are added to the original chain. Instead, nodes are only added to the hard-forked chain. In practice, this is rarely the case. Examples of a critical mass of users implementing a hard fork include Bitcoin/Bitcoin Cash and Ethereum/Ethereum Classic. There hard forks will make oversight and the enforcement of regulation difficult. As the Commission considers the future of derivative contracts on Ether, it must anticipate the governance of hard forks.

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

The Ethereum Foundation, supported by donations, is a Swiss nonprofit organization whose mission is to,

> *"Promote and support Ethereum platform and base layer research, development and education to bring decentralized protocols and tools to the world that empower developers to produce next generation decentralized applications and together build a more globally accessible, more free and more trustworthy Internet."*[8]

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

As an active participant in derivative markets, Chatham is especially interested in thinking through these questions, but struggled due to the feeling that some of the terms used in the below questions required agreed upon definitions. Chatham would be happy to return to these questions if the Commission could provide additional clarity.

[7] For More Information: https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQs

[8] For More Information: https://www.ethereum.org/foundation

**Derivatives contracts**
There are many ways to define derivative contracts on Ether. One useful way to think about derivative contracts is to break them into the following categories: futures, OTC swaps, or options on the USD/ETH exchange rate; futures or OTC derivatives stored on a blockchain using a system like ISDA CDM, but mechanically executed off-chain; futures or OTC derivatives stored on a blockchain using a system like the ISDA CDM and executed through a smart contract; futures or OTC derivatives stored on a blockchain using a system like the ISDA CDM and executed through a smart contract; and futures or OTC derivatives on the implied interest rate from PoS deposits.

As far as futures, OTC swaps or options on the USD/ETH exchange rate are concerned, within that category are deliverable and non-deliverable USD/ETH futures and OTC derivatives traded either on- or off-chain. For non-deliverable USD/ETH futures and OTC derivatives traded off-chain, Chatham believes that those crypto-derivatives could be treated like any other futures contract. There are several ways to approach deliverable USD/ETH futures and OTC derivatives traded off-chain. One such example is that the exchange could create a contract where the seller deposits the Ether and the buyer of the contract at delivery gains the right to withdraw the Ether. The Commission could audit this contract as well as monitor its usage. For deliverable USD/ETH futures and OTC derivatives traded on chain that are executed through a smart contract, there are a lot of potential issues to address including security, KYC, and the need for an oracle.[9]

**Ether cash market**
In terms of the Ether cash market, is this an exchange that supports ETH/USD only? Chatham believes that such a definition could also feasibly include the ETH token or ERC-20 tokens. Additionally, Chatham believes that bespoke insurance-like contracts on ERC-721 tokens could similarly fit within that definition.

**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?**

A properly decentralized network would prohibit most attempts to distort or disrupt the Ether market. Despite this, attacks have occurred.

Ethereum Classic's 51% attack occurred due to a reduced size in the pool of participants after the fork, making it easier for the attackers to gain 51% of the hashing power. While the attack was ongoing, the bad actors were able to claim valid transactions (despite their invalidity) and reap over $1 million rewards of the classic Ethereum coin (ETC).[10]

The largest concern relating to the disruption of the Ethereum Network is the disruption by state actors whose goal is to destabilize the economy rather than profit from it. The repercussions for these attackers are limited. In considering the possibility for these attacks, one must consider that most of the

[9] An oracle is a data feed used to provide the necessary external data to trigger smart contract executions when pre-defined conditions are met. For More Information: https://blockchainhub.net/blockchain-oracles/
[10] For More Information: https://cryptoslate.com/ethereum-classic-loses-1-million-51-attack/

hashing power for the Ethereum Network is currently owned by mining pools.[11] Many of these pools are domiciled in foreign countries.[12] There is a potential for state actors to commandeer the network.

**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 several risks to be considered. The Ethereum Network permits participants to remain anonymous complicating Know Your Customer preventative measures. As discussed elsewhere, the blockchain supports a limited number of simultaneous transactions and gas prices increase during high volume times. These limitations would create an unreliable exchange of Ether to legal tender which is already predicated on a volatile exchange rate. An additional complication exists when participants lose private keys and can no longer access their Ether. Private keys can also become compromised, allowing the Ether to be converted to legal tender by a participant other than the rightful owner.

**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?**

Introducing derivative contracts, such as futures, on Ether may lead to several interesting impacts on a PoS consensus model.

In general, PoS incentivizes market participants to hold long positions due to economic rewards. Due to the decrease in availability of tradeable Ether, the market experiences upward pressure on its price. However, the introduction of derivatives contracts typically adds downward pressure on price as there is now a way for market participants to short Ether. Under these market conditions, those who hold Ether must make a more complicated decision regarding how the value of Ether will be affected by derivatives and speculations.

As an example, these competing market forces are demonstrated through the interest rate parity effect that will occur during the initial phase of the upcoming Casper FFG protocol.[13] A participant in Casper will be an Ether stakeholder who locks their Ether to act as a validator. As compensation, the stakeholder gains an established rate of return during the duration of the deposit.

Alternatively, the Ether holder could exchange Ether to USD (or another currency) and deposit the USD into an interest-bearing instrument for the same time period as the previous example. Derivatives futures contracts on the ETH/USD exchange rate could be used to lock in a rate of return on the Ether.

[11] For More Information: https://www.blockchain.com/en/pools
[12] For More Information: https://www.ccn.com/bitmains-mining-pools-now-control-nearly-51-percent-of-the-bitcoin-hashrate
[13] The Ethereum Network is utilizing Casper to facilitate the transition from a PoW to a PoS consensus model.

In summary, participants would know:

S: spot exchange rate

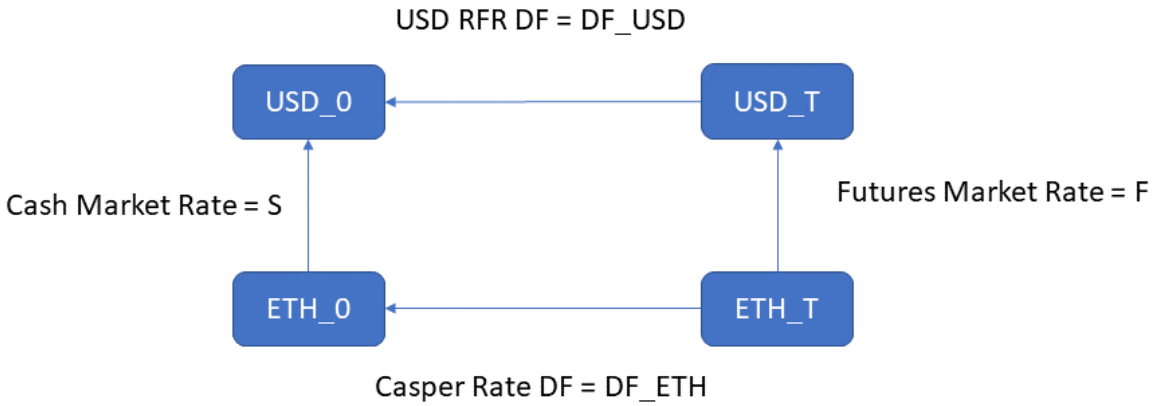
F: future exchange rate

DF_USD: USD discount factor (interest rate)

DF_ETH: ETH discount factor (interest rate).

If the USD interest rate is high enough, holders of Ether may prefer to lock in gains using USD interest and futures instead of participating in the PoS mechanism.

S = DF_USD/DF_ETH*F




If the situation is modified to assume liquid markets, interest rate parity would relate the four quantities. Deviations from interest rate parity could lead holders of Ether to not participate in PoS mechanisms.

**Question 18 is intentionally excluded.**

**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.**

Chatham requests clarity regarding the definition of Ether derivatives before addressing this question.

**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?**

Participants in the Ethereum Network are not necessarily financial professionals and lack the sophistication and expertise to appropriately engage in an Ether-based derivatives market. Participants that have historically been excluded from financial markets (terrorists, money launderers, etc.) are not excluded from the Ethereum Network and would therefore be able to participate in an Ether-based

derivatives market. The anonymity of the market makes Know Your Customer and Anti-Money Laundering standards problematic to enforce. The basis of blockchain supports on-chain contracts between any two or more parties without their need to know or trust each other.

In addition to the participation in an Ether-based derivatives market of undesirables, the market itself is highly manipulated. The tweets of prominent cryptocurrency personas, or accounts that impersonate them, have shared statements to manipulate the price of Ether in their favor or to promote Ponzi schemes. The occurrence has become so common that Twitter has proactively implemented signals to identify these fraudulent accounts and cryptocurrency scams.

Another interesting example of market manipulation can be seen in the creation, followed by the exchange, of the Useless Ethereum Token (UET). This token, which has no economic value, can now be bought, sold, and traded, like other cryptocurrencies, despite its absence of economic value. This case demonstrates the lack of financial sophistication by participants in the Ethereum Network.

**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?**

The Commission's ability to properly oversee Ether-based derivative contracts would be drastically limited for any deals executed off-chain as participants would be required to self-report their participation in such transactions. For this reason, it will be crucial for the Commission to define the types of Ether-based derivatives and provide refined regulations for each. As discussed in the previous question, the Ethereum exchange market is currently highly manipulated and would require the Commission to regulate often uncontrollable situations, like the tweets of a predominate market participant. Traditional oversight is not predicated on controlling these forces and will have to be reconsidered.

As an example of regulation deficiencies, despite providing guidance to market participants and classifying cryptocurrencies as property subject to capital-gain taxes under U.S. law, the IRS has experienced difficulty enforcing this regulation due to the networks' anonymity and a requirement of participants to self-report cryptocurrency gains. Traditional oversight has fallen short in this use case and the Commission should be wary of similar regulation limitations.

**Questions 22-25 are intentionally excluded.**

* * *

Chatham thanks the Commission for considering this matter. If the Commission would like to discuss these issues further, please contact Eric Juzenas, Global Chief Compliance Officer and Director of Regulatory Policy, at (484) 731-0061 or ejuzenas@chathamfinancial.com.