Daxia Selected Responses to CFTC Request for Input 6351-01-P

Dear Mr. Kirkpatrick:

Daxia applauds the CFTC for releasing this Request for Input (RFI). Asking for assistance and further clarification on a new technology is a noteworthy endeavor and we hope that our responses, along with those of the Ethereum communities can lead to the Commission making informed and principled decisions.

To summarize our answers to selected questions from the RFI, the regulations set forth by the CFTC should be technology and underlying agnostic. Daxia recognizes the limited resources of the CFTC, however more work will be needed before the US derivatives regulatory regime is in a state to properly handle this and further innovations.

As a self-declared member of the Ethereum community, we are glad that you are trying to learn about our technology. We recognize that the Commission must have a basic understand a commodity that underlies a derivative contract, however if the goal is proper disclosure and limited systemic risk, an in-depth understanding of underlying technologies and commodities is not needed. The Commission is not worried about the sustainability of agricultural production, the physical properties of the metals underlying contracts, or even the business models of companies which underlie futures contracts. When rules are written to address specific types of derivatives or commodities, they tend to be overly prescriptive and limiting to future circumstances.

Daxia accepts the invitation to partner with the CFTC to create a better regulatory environment that fosters innovation, customer safety, and market integrity.

Note only some questions are answered by Daxia and we have left the Commission's numbering intact for reference to the RFI.

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?

Bitcoin, Ethereum, and many other chains do not have 'finality' or an irrevocable settlement process similar to the traditional financial sector. As several CFTC employees have made clear, you can take guesses and at certain times be 99% sure, but the possibility of 100 percent certainty is a feature of these systems. The CFTC's previous 'Proposed Interpretation on Virtual Currency "Actual Delivery" in Retail Transactions' afforded the Commission responses in this regard and the Commission is rightfully undetermined on how to handle such assets. Recent PoW attacks have shown that deep chain reordering is possible and is always a threat, so the CFTC might focus on further defining delivery in the terms of being an intangible and especially a revertible one. It is our opinion that current regulatory definitions, timetables for, and incentives built around actual delivery do not work for the cryptocurrency space and should be amended as to be broad enough to handle new technologies.

Technology

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?

A hands-off approach is best. Similar to traditional computing spaces, developers and users find intertemporal equilibriums where the true use cases and the current technology match.

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?

The validity or security of one underlying consensus mechanism versus another is likely not to be easily determined by a regulatory agency. There are new consensus mechanisms and versions of proof-of-stake (PoS), proof-of-work (PoW) and many others coming out on a frequent basis. Some have been battle-tested in the wild but few have had large derivatives contracts available to test their robustness.

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.

Failure in the consensus mechanism is not 'manipulation' per se. It's a destruction of the asset itself which might be a component of a larger manipulation scheme. If PoS or PoW proves to fail on one of the larger coins, then it is likely that the coin that is attacked will have its value drop to in value relatively quickly. Unfortunately, off chain derivatives on the asset create a greater potential for attacks. Relative to PoW, PoS it may be easier to quickly destroy value as it does not require the purchase and set up of physical hardware. As a practical matter, they are similar to PoW and in an abstracted version of PoS through the purchase of computing power (staking wealth vs buying specialized machinery still leads to certain parties having more control).

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?

Yes. As Bitcoin proved with the block-size debate of 2017, large disagreements within a community can exist and lead to fragmented chains. This is a feature and not a bug of these networks. The ability to branch off and experiment with new code or maintain an ideological focal point for the community is a feature to be envied by closed systems. The Commission is likely worried as to how market participants and institutions will handle a fork, however this is stipulated by contract. Some derivatives contracts may specify delivery on every chain (and/or sum of the prices on each chain), whereas other contracts may seek to only follow a mainchain. Both are useful and fair if properly disclosed.

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

The development of core protocols is not required to further the use of a network. Unlike products owned by a single entity, the Ethereum network is maintained by open source developers and will continue to be so as long as demand for its chain exists. More use on a network increases the cost to utilize the network and only applications that can afford the increased cost will continue to use the main chain. Developments for off-chain networks such as Plasma, state-channels, and side-chains see the main Ethereum network being utilized as a settlement layer while applications will be hosted on other chains. Should these research efforts prove fruitful, the current mainchain could theoretically be sufficient to handle any number of applications built upon secondary layers.

Governance

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

Although both have in the past used voting (whether by stake, hash power, or use of a full node), the ultimate power in these systems is really the vague consensus of the community. Disagreements have resulted in forks. Convincing the mass user base of these systems to adopt (or not adopt) a given change is accomplished using every tactic from technological presentations to smear campaigns to fear of a catastrophic failure if one solution is adopted. The two networks are similar in that they are both fragile to the user base which adopts them. To note the differences, the Bitcoin community has a more conservative leaning base (with regard to technology) and is reluctant to upgrade the system as many business models, ideologies, and reputations are tied to the "immutable" current state. The Ethereum community tends to be more technologically explorative, with goals to continue upgrading the system until it can fit their ultimate ideal of a secure and fully decentralized computing platform that all of the world's applications can in one way or another be secured by. The past has shown Bitcoin's reluctance to change resulting in numerous forks with viability; however, Ethereum seems to be more immune due to the community's general acceptance of proposals from the Ethereum Foundation and its founder Vitalik Buterin. This may change in the future though, as more business models are built upon the current system and upgrading may prove either too risky or run the risk of depleting potential revenue streams for these companies.

13. 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?

It most likely will split and there is no way to prevent an open system from splitting into multiple chains. With the massive amounts of upgrades coming to Ethereum, it is likely that the community will be divided on several paths forward. The solution needs to come from within the derivative contract itself by specifying the handling of forks.

Markets, Oversight and Regulation

14. 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 decentralized consensus mechanism that continues to run despite countless attacks. If someone took out a cash settled short position whose payout was larger than the cost to attack the network, a major disruption is likely. For this reason, I recommend physically settling and fully collateralizing all off-chain cryptocurrency derivatives.

16. How would the introduction of derivative contracts on Ether potentially change or modify the incentive structures that underlie a proof of stake consensus model?

It would depend on the specifics of the contract. Assuming a failure of the consensus mechanism, the value of Ether would be reduced. So, if the derivative contracts are paid in Ether, then the model should still hold. If, however the contracts are cash, or other crypto, settled then it becomes a security concern. The reality is that the security concerns are not much different than for a Proof-of-Work model. With PoS, the potential attacker can maliciously stake his Ether versus selling it for mining equipment.

17. 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?

As more applications are built on top of Ethereum, the need will become greater. The most established businesses will not invest in a currency or platform long term without the ability to hedge out price risk. Many dApps for instance are experimenting with ways to pay for user's gas fees. If this plays out, every dApp will have a direct reason to hedge Ether risk.

In addition to simply making products available, more clarification is needed with regard to end user exemptions for certain classes of derivatives and risk management practices. What constitutes an end-user with regard to cryptocurrency? Are they given the same exemptions as traditional commodity end-users?

18. Please list any potential impacts on Ether and the Ethereum Network that may arise from the listing or trading of derivative contracts on Ether.

As has been alluded to, off-chain derivatives that are cash settled create great risks for cryptocurrency networks in general as the incentive mechanisms built into their consensus protocols are not designed to handle large scale attacks that can be profitable regardless of the chains existence after said attack. Additionally, there is a real risk that the communities of many cryptocurrencies will not accept the incumbent financial institutions having a voice in their protocols. It may not be as much of a risk with the mild mannered Ethereum community, however I would not dismiss them as the ideological leanings of the community will ultimately decide the technology's fate. With known roadmaps toward privacy and increased decentralization, any corporatization of the network or attempt to harness the technology into something more regulatorily palpable may lead to a fork which slashes the balances of these institutions. Traditional assets do not have the problem of being confiscated en masse by anyone other than the government, however these systems afford a method to create a world where the assets on a custodian's balance sheet never existed.

19. 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?

As with most cash trades in Bitcoin, the vast majority of crypto volume occurs on over-the-counter markets or on international exchanges. Crypto instruments trade on similar volumes to some small commodities. Unfortunately, the open and anonymous exchanges overseas coupled with an ease of entrance into the space makes manipulation in digital currencies far easier than trading many physical goods. Ultimately, these systems may build up the trading volume necessary to support a heavily traded derivatives industry, but in systems where leverage is high, the temptation to move the price may prove too great for even traditional players.

20. 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?

Privacy features for Ethereum are being developed. For instance, there is a well-known partnership between the founders of Ethereum and Zcash. The ability to have an on-chain derivative contract that is completely secret to everyone but the participants is coming. The Commission will not be able to monitor or regulate these transactions except when they are eventually trading their gains for fiat currency. This risk however is not limited to Ether but to all relevant underlying mediums. For this reason, it is desirable that regulators provide safe alternatives to the coming dark markets and potential overseas bucket shops.

Cyber Security and Custody

23. 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?

Any CFTC statement on specific technology requirements of wallets, transaction signatures, or even custodial guidelines is likely to be too prescriptive. Yes, there are best practices. Yes, any custodian or exchange should know these quickly changing security measures. However, the space is too nascent and quickly developing to layout any specific standards. In the interim, Courts may be able to determine negligence on behalf of an intermediary.

Thank you for addressing these important issues. I look forward to any reply or further discussions.

Sincerely,

Nicholas A. Fett
CEO & Founder | DAXIA
www.daxia.us