Weiss Cryptocurrency Ratings

Comments by Weiss Cryptocurrency Ratings, a division of Weiss Ratings, LLC, to the U.S. Commodity Futures Trading Commission in response to the request for input on crypto-asset mechanics and markets.

By Martin D. Weiss, PhD and Juan M. Villaverde, February 20, 2019

Introduction

We are very thankful for the opportunity to provide input to the Commission's Ethereum project, drawing from our independent cryptocurrency ratings and research.

Weiss Ratings, which began operations in 1971, grades 53,000 investments and financial institutions. More recently, in January 2018, Weiss Cryptocurrency Ratings were initiated and currently cover 120 distributed ledgers, based on an analysis of their technology, adoption investor risk and investor reward.[1]

We never accept any form of compensation from issuers, sponsors or other rated entities; our sole source of revenue is from end users. We firmly believe this conflict-free standard is essential in order to give the public objective and accurate assessments of both potential opportunities and possible dangers.

Today, we begin by expressing our overarching views regarding the viability of Ethereum derivatives in the current environment.

The Ethereum community — and the cryptocurrency industry as a whole — are anxious for the official recognition that regulated derivatives would afford, and so are we. It could help attract serious investors, enhance market liquidity, provide hedging opportunities, reduce market anomalies and ultimately bring a measure of much-needed stability to an oft-chaotic environment.

[1] The technology model evaluates each protocol's potential to achieve a variety of goals, including (a) high transaction speeds along with other scaling solutions, (b) decentralization, (c) energy efficiency, (d) sophistication of monetary policy, (e) governance capabilities, (f) flexibility to upgrade, and others. The adoption model evaluates real-world network security, network capacity, speed, scalability, market penetration, decentralization, developer participation, public acceptance, plus other key factors. The risk and reward models use past price history and volatility to estimate the potential for investor losses or gains.

What remains to be decided is, do we want it fast, or do we want it right? We can't have it both ways.

Among the many possible outcomes, we believe the worst would be a premature derivatives launch, followed by a series of unexpected backfires, which might deflate the collective appetite for a more sustainable launch in the future. There are four sources of concern:

First, debates in the industry are typically tainted by ideology, making it difficult to agree on facts.

Second, financial market expertise and deep cryptocurrency experience are rarely available from a single source, leading to misunderstandings on both sides. Crypto experts, for example, may be unfamiliar with hedging and its ability to help stabilize trading, while traditional financial experts may be baffled by the ins and outs of Distributed Ledger Technology (DLT).

Third, urgently needed upgrades in Ethereum network protocols may be difficult without hard forks, raising the mission-critical question, "what is the true Ether?" If no answer is readily forthcoming, the resulting community split, market confusion, and trading anomalies could be more difficult to manage than those historically experienced in some of the most volatile commodities and financials. Ethereum founders can provide needed leadership, but governance is mostly absent in the protocol. Since it borrows heavily from Bitcoin, there remains a legacy of immutability in an ecosystem that cries out for change and adaptability.

Fourth, auditing exchanges, where most of the trading occurs, could be very challenging until better standards are established for reserves and transparency.

We provide additional detail on these and other issues in our answers below.

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

Bitcoin pioneered the first-ever public, open, distributed ledger, applying DLT exclusively to peer-to peer-electronic payments. Its design was elegant in its simplicity but limited in its functionality. The latter aspect then opened the door for Ethereum to pioneer a more complex array of use-cases with the creation of Turing complete smart contracts.

The problem: Along with these smart contracts comes an additional layer of complexity that can be more difficult to monitor, standardize and regulate.

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

If it can be said that Bitcoin used DLT to create a decentralized payment network, then it follows that Ethereum used DLT to create a decentralized global computer. This helps usher in the era of Web 3.0, where all data is encrypted, stored on a distributed database, processed by validators and paid for with Ethereum's Ether token. In addition, Ether itself can also be a Bitcoin-like payment vehicle, but not as its primary, or intended, use-case.

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?

As the world's most popular smart-contract platform, Ethereum use-case examples abound.

- Cryptokitties allows users to create — and exclusively access — unique digital collectibles stored on the Ethereum blockchain.
- Augur is a prediction market designed to bet on elections, weather, financial markets, and an unlimited array of future events.
- Bancor is a protocol-based exchange, wherein the price discovery mechanism is driven by an algorithm rather than an order book.
- Plus, a wider range of other innovative applications, including many in the pipeline.

Nearly all share some common themes:

- Since no single entity owns or controls the data, the applications are viewed as more user-centric, more equitable and more democratic than their centralized counterparts;
- a new level of trust emerges, whereby users can know with certainty that digital items are scarce, unique, and can never be reproduced by any third party; plus
- self-monitoring, self-regulating financial exchanges and platforms are possible, whereby buyers meet sellers directly, while the protocol enforces the rules.

The use-cases are constrained only by the imagination of thought leaders and the future desires of users. Some will replace traditional internet applications with greater security, efficiency and fairness. Others will break new ground. And many could create a virtuous cycle of new applications, new human behaviors, new needs, followed by still *newer* applications to service them.

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?

All of the projects cited above — plus many others that create Distributed Applications (DApps) on the Ethereum network — are examples of commercial enterprises using Ether. Resulting transactions are recorded in the immutable Ethereum blockchain, which is open to the public and all-inclusive, making data readily available for most accounting functions.

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?

Because cryptocurrencies are so new, a large part of what drives the price — and indirectly, market capitalization — is speculation. Consequently, during boom-bust cycles, the volume of transactions processed by public ledgers grows dramatically and unpredictably, only to collapse in the same fashion.

Thus, to evaluate usage and adoption, we distinguish clearly between

(a) trading on exchanges, indirectly reflected in our risk/reward models and

(b) on-chain transactions, a factor in our adoption model.

The adoption model is aggregated from several sub-models,[2] among which the following two are among the best suited to address the question.

1. *Network security, based on hash rate, efficiency of mining hardware and other factors.* We find that, from February 2018 to February 2019, Ethereum's network security declined 42.1%, largely driven by a similar decline in its hash rate. In contrast, Bitcoin's network security rose 20.5%, and the industry overall enjoyed a 115% improvement in network security during the same period.

2. *Network capacity, reflecting on-chain transaction volume, fees and other variables.* On the Ethereum blockchain, although the volume of transactions fell, the decline was more than offset by cheaper fees, resulting in an overall improvement of 47.9% in the last 12 months. Meanwhile, Bitcoin's network capacity, which was severely compromised in February 2018, has enjoyed a sharp recovery; and industry-wide, we've witnessed a 175% improvement.[3]

Researchers seeking publicly available data related to the Ethereum blockchain can refer to sources such as

- https://etherscan.io/ — a block explorer to access the data recorded on the ledger
- https://www.blockchain.com/es/explorer?currency=ETH I — good for analytics on the size of the mining community and other fundamental data, as well as
- https://bitinfocharts.com/ethereum/ — a source of aggregated data on the hash rates, transaction volumes, active addresses, and many other key factors.

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?

Ethereum's block times are significantly faster than Bitcoin's, but this has one downside: The more quickly the blocks are created, the greater the risk of a chain split and an invalid block.

[2] These include sub-models designed to evaluate network security, network capacity, developer participation, history, concentration and social media, as described in our 2018 white paper on Bitcoin.

[3] The dramatic industry-wide improvement in network capacity over the last year is due to multiple factors, including (a) Bitcoin's unusually poor metrics in February 2018, (b) its recovery since that time, and (c) rapid growth in on-chain transaction volumes among distributed ledgers such as EOS, WAX, Bitshares, Tron, XRP, and others.

Thus, erring on the side of caution, at least 30 block confirmations are recommended in order to consistently achieve a level of certainty that a particular transaction has been recorded on the correct blockchain. Most exchanges also use 30 confirmations, while payment processors are less demanding, waiting for as few as six. These parameters assume normal market conditions. During periods of extreme stress, such as the threat of a malicious actor attempting to fork the chain, it may be necessary to wait for 1,000 confirmations or more. Therefore, any standards must be considered approximate and remain flexible.

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

Both Ethereum and Bitcoin are open blockchains based on Proof of Work, sharing the same basic algorithm for adding blocks and determining who's authorized to do so.

However, in nearly every other aspect, they diverge greatly — Ethereum designed to process more diverse and complex operations; Bitcoin, to strictly process payments. Moreover, in the future, if Ethereum can successfully incorporate new solutions, the technologies will diverge even further.

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?

Scaling is, indeed, Ethereum's greatest current challenge. According to available data, the network currently runs at full capacity 24/7, with approximately of 40,000-50,000 transactions unable to make it through traffic jams each day.[4] This is a constant reminder of surplus demand that the network is unable to satisfy. Meanwhile, anecdotal evidence suggests that these bottlenecks may be driving traffic from Ethereum to EOS, Tron and other distributed ledgers that can more readily handle the larger transaction volumes.

This issue is both practical and endemic. But the proposed solutions are still theoretical and academic. None are close to completion. Even the most widely-supported solutions — Proof of Stake and sharding — are experimental, with no certainty as to when they can be implemented, if at all.

The natural and immediate consequence has been a tidal shift in transactions to competing networks: Despite a vastly superior brand and popularity, Ethereum is currently processing

[4] At the moment of this writing, blockchain.info reports 41,201 unconfirmed transactions on the Ethereum network over the last 24 hours.

fewer than half a million transactions per day. In contrast, its closest competitor, EOS is doing approximately 5.5 million, or at least 11 times more.

We measure maximum capacity two ways:

- Our technology model evaluates the potential speed of each distributed ledger.
- Our adoption model looks at the real-world throughput and any bottlenecks that may appear. When the network is running near or at full capacity, it tends to drive up fees and drives down the output of our network capacity sub-model. The high fees, in turn, can compound the problem by discouraging economic activity on the ledger, further reducing the volume of transactions.

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?

In its submission to the Commission, the Ethereum Foundation concedes that Proof of Stake has never been tested in the manner that Ethereum plans to implement it. But this issue is not unique to Ethereum. In the industry as a whole, Proof of stake has never been tested on a scale that's comparable to Bitcoin's Proof-of-Work ledger. Thus, Ethereum's would be the first attempt to do so, helping to explain why Ethereum developers favor a slow-and-steady approach for rolling out this solution.

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.

With Proof of Work, it's easy for any new, well-funded participant to enter the competition to mine new blocks. In contrast, Proof-of-Stake systems we've studied have a tendency to "make the rich richer." The higher an agent's stake, the greater the portion of the network they can control; and the more they control, the higher their stake becomes.

This can also be true with Proof of Work, but to a lesser degree. Validation of transactions by an external mechanism (energy) helps make it more open and decentralized than Proof-of-Stake alternatives. Thus, to maintain a dominant position on a Proof-of-Work ledger requires advantageous deals with power suppliers and continual investment in cutting-edge computer hardware. In contrast, owning a stake in a Proof-of-Stake ledger comes with no cost beyond the initial investment itself. Then, the advantage can be maintained by simply re-staking the newly minted tokens that this stake produces.[5]

[5] There may be some costs incurred to maintain the status of a successful validator in a Proof-of-Stake ledger. But such costs are minimal compared to those of their Proof-of-Work counterparts and can be easily subsidized by other activities.

The resulting concentration of tokens can be large. Typically, any concentration that rises above a Gini coefficient of 60 could be considered problematic. However, on EOS, currently the largest Proof-of-Stake network, the Gini coefficient of token distribution is 97, implying a high degree of concentration, at least at this early stage in its evolution.

This is a common and hotly debated issue in the industry — not only for Proof of Stake but also for Proof of Work. Token distribution is almost always more concentrated than the raw hash rate, a measure used to assess a miner's dominance in Proof of Work. This problem is further exacerbated by the presence of exchanges, where a large number of users store their cryptocurrencies. Exchanges own the keys to the tokens they hold on their customers' behalf, and therefore could potentially use them in order to acquire controlling stakes on a Proof-of-Stake ledger.[6]

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, indeed. There are likely to be disagreements in how Proof of Stake is implemented. Because Ethereum doesn't have an adequate mechanism to form consensus on this issue, any major changes could trigger network splits.

The saving grace is that, in the past, whenever such splits have occurred, an overwhelming majority in the Ethereum community — including miners, users, and developers — have tended to gravitate to a single alternative. This same majority will likely adhere to the proposed roadmap to transition to Proof of Stake, while only a minority is expected to branch off and pursue its own goals. With time, it *should* not be very difficult to determine which is "the real" chain. But it would also be unwise to count on a transition without disruption.

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

The answer revolves around the issue of scalability, which reflects not only the ledger's processing speeds but also the cost of transactions. The faster and cheaper Ethereum becomes, the more it will be able to process applications for mainstream users.

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

[6] We have already seen this trend with EOS, where many of the top "Block Producers" (the validators on EOS) are controlled by exchanges or their proxies. The Ethereum community promises their results will be different. But so far, we have not seen concrete evidence of that outcome.

Contrary to arguments that are often driven by ideology, there is qualitatively no difference between the governance of Ethereum and that of Bitcoin. Both protocols are severely handicapped when it comes to reaching consensus for needed changes to the ledger.

The primary difference between Ethereum and Bitcoin governance is the role of the founders. Bitcoin's founder has disappeared, leaving a leadership void. Ethereum's founders are still alive and well. The Ethereum Foundation, dedicated to education and promotion of the technology, also helps fill the void. Overall, this leadership makes it less difficult to propose and implement changes than it would be for Bitcoin. However, "less difficult" is still not easy. Moreover, in the future, unless its governance can be codified in the protocol, Ethereum could face some of the same governance deficiencies that are common with Bitcoin today.

In its submission of February 15, the Ethereum Foundation points out that, while Bitcoin typically upgrades via soft forks, Ethereum usually relies on hard forks, leaving the impression that the latter are less harmful and more beneficial. We find the opposite to be true: The reason Bitcoin implements upgrades via soft forks is to preserve the stability of the network, inasmuch as a soft fork does not risk a chain split. However, controversial hard forks can, and typically do, result in network splits tied to ideological differences between camps. They can be risky propositions that could ultimately rock the stability of the network, and it would be unrealistic to guarantee that Ethereum can consistently avoid severe growing pains as it moves its distributed ledger into uncharted territory.

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?

Yes, the lack of a proper governance protocol leads to the likelihood of splits in the future. Specifically, as cited earlier, attempts to implement Proof of Stake and/or sharding are likely to elicit strong disagreement by some portion of the community, prompting a fork from the main Ethereum chain.

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 price of Ether is driven by processes and events on centralized exchanges, some of which may be illicit or questionable. These hold large amounts of Ether and could, in theory, disrupt trading, causing harm to market participants. Fortunately, these don't directly impact the Ethereum network itself, which can usually continue to perform its function regardless of market price fluctuations.

A separate question is how to deal with bugs in the code. Again, because Ethereum lacks an adequate governance layer which might task specific actors with quality assurance responsibilities, bugs can potentially disrupt the Ethereum Network. At present, there is little the community could do other than halt the ledger and roll it back to a previous state before the

bug was exploited, risking confusion and chaos.[7] Bitcoin is arguably exposed as well, but thanks to its simplicity, tends to be far less vulnerable than Ethereum.

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?

Much as in commodity or financial futures, disciplined derivatives hedging could be an important stabilizing factor for cryptocurrencies. In addition to helping commercials better plan their business by locking in future costs or revenues, short-selling by speculators, although sometimes frowned upon by the general public, can also play a constructive role. They help offset the irrational exuberance of buyers at market tops. And they create a reserve of buying power that can spark much-needed recoveries from market bottoms.

Similarly, Bitcoin derivatives can make it easier for miners to hedge against volatility, and Ether derivatives could help stakers do the same. The big difference is that hedging with derivatives in the Bitcoin ecosystem is one-sided; in the Ether ecosystem, it's likely to be two-sided. Here's why:

- Bitcoin businesses that can derive significant benefits from derivatives are almost entirely on the sell side — large miners. With electricity costs relatively fixed, they have good reason to sell short futures contracts to hedge against price declines that would negatively impact their bottom line. However, on the buy side, we see little need for futures. BTC is not a significant cost factor in any business we're aware of. Thus, other than speculators, there is little need to hold long positions in BTC futures.

- On the Ethereum network it's a different story. Businesses that are partially or fully built on Ethereum smart contracts need to hold Ether in reserve in order to meet fee payment obligations. Depending on the size of the business and their reliance on the Ethereum network, the resulting costs can be significant, can vary greatly, and can be better managed with long positions in ETH derivatives.

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?

Cash markets are very atomized and disjointed with few or limited opportunities for effective arbitrage between them. As a result, price discrepancies between exchanges can be extreme.

- For example, when the Coinbase exchange listed Bitcoin Cash for the first time in December 2017, Coinbase BCH quotes shot up to US $9,500 per token, even while BCH traded near $4,000 on other exchanges. The exchange had to halt trading, and the only ensuing investigation was internal.

[7] We saw examples of this recently, when a proposed Ethereum upgrade for mid-January was delayed until February 28, as a bug was discovered that could have potentially harmed the network.

- Worse, in 2017, most crypto assets on South Korean exchanges traded at ridiculously high premiums of up to 40% relative to their US counterparts, largely driven by fears of war with North Korea. This abnormality, dubbed the "kimchi premium," was difficult to reduce due to capital controls that made it hard to buy US dollars and ship them to non-Korean exchanges.

These issues are to be expected in a young market with infrastructure still in development. But that doesn't mean they can't be managed or circumvented. To guard against cash price manipulation, Ether derivatives contracts can be based largely on an index that reflects price quotes from trusted market makers, such as those at select OTC trading desks. This could help provide a solid benchmark that enhances the opportunity for arbitrage between illiquid markets and publicly traded derivatives contracts.

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.

Ether serves as the digital fuel that powers the Ethereum Network. It can benefit from derivatives in much the same way as the oil and gas industry benefits from energy derivatives. Indeed, one of the thorniest issues preventing adoption of Ethereum-based businesses and dApps is the price volatility that affects all crypto assets.[8] Because of wild price gyrations, it's difficult to establish a business as a miner. The same applies to businesses that need Ether for smart contracts. Derivatives contracts can help address this issue.

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?

Heightened market risks are especially possible if there's a disagreement within a community that causes the network to split. When that happens, derivatives trading would need to be suspended, while exchanges and regulators closely monitor the feuding communities and make the difficult choice regarding which is the "real currency." Although such events can be known about in advance, a derivatives contract expiration that occurs while the network is splitting could still create confusion that's difficult to sidestep or overcome.

Regarding the role of short positions, we feel that the Ethereum Foundation is overstating the risk that they would create an incentive for bad actors to attack the network. Attacks on a distributed ledger like Ethereum involve a high cost that's virtually guaranteed, while delivering a benefit that's very uncertain. With these unfavorable risk/reward odds, we feel it's highly unlikely that any rational actor would place large bets on such a scheme.

[8] During hectic periods of 2017, a smart contract call to retrieve tokens from the EOS ICO on the Ethereum Network could range between just a few cents and as much as $50 at one time. That's just one example of how volatile the fees on these ledgers can be.

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 large number of exchanges scattered across the globe, plus the ease of setting up new ones, creates a potential labyrinth for regulators. Despite this challenge, however, data collection, aggregation and cleaning can be automated in a way that facilitates monitoring and regulation.

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

The technology is brand new, and the architecture of these networks can vary significantly. The the industry has yet to set viable standards.

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

Since Ethereum is more complex than Bitcoin, its "attack surface" is broader; relatively speaking, it's an easier target. If developers are not careful, there are a number of known exploits — with smart contracts and with the Ethereum Virtual Machine itself — that could allow hackers to duplicate or steal tokens from their legitimate owners. Fortunately, these issues do not affect Ethereum's native Ether token, or its functionality. Smart contract bugs rarely affect the Ethereum network as a whole.

Security issues are a delicate topic with public open distributed ledgers. They cannot be discussed publicly lest hackers exploit them before developers have a chance to address the problem. Thus, issues with Ethereum will not — and should not — be publicly disclosed until after they have been dealt with. Suffice it to be aware that, as with other public open distributed ledgers, the complexity of the system all but guarantees the existence of exploits that have yet to be fixed.

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

Any block explorer (such as etherscan.io) should be sufficient to conduct a full audit of an Ethereum address or smart contract. However, as we explained in a recent post, the primary concern is the auditing of exchanges, which is problematic due a convergence of the following issues:

1. Exchanges can become the largest holders of Ether or any other crypto-asset.
2. There is no simple way to verify how much an exchange has in deposit, as all addresses on the network are pseudonymous alpha-numeric accounts.
3. Exchanges do not operate in traditional regulatory frameworks; their accountability to customers and regulators is limited.
4. There is no industry standard for verification of deposits, and there have been several rumors of exchanges with insufficient deposits to meet customer obligations.

We are pleased to see that Bitcoin developer Blockstream has recently published commentary on the issue, calling for the standardization of "Proof of Reserves," but the debate has barely begun. Hopefully, the industry will set a standard for Bitcoin, and once it does, modified versions of the same standard can likely be applied to most other distributed ledgers.

To resolve this issue — as well as the others we cited at the outset — industry standards are sorely needed. They will help bolster transparency, data accuracy, and key metrics; foster a broader diversity of independent research organizations; reduce the burden on regulators to monitor each ecosystem; and create a more robust environment for crypto-derivatives.