BRACEWELL

INSIGHTS

The Crypto Paradox: Code is Law and Consensus Rules

April 12, 2019

*By: **Michael W. Brooks** and **Joshua Robichaud***

As the world contemplates the future of cryptocurrencies and smart contracts – including whether and how to invest in them, to transact using them, and to regulate them – it will be important to recognize the significant implications of two core principles of most cryptocurrencies:

1. *Code is Law.* Every digital asset is governed by code. The security, usefulness, availability, transferability, and general malleability of any digital asset are all determined through the code by which it is created and stored. In this way, code is law, and the rule of law controls the asset.

2. *Consensus Rules.* At the same time, in the case of cryptocurrencies built using a consensus-based blockchain model, agreement among participants can change the code. That is, in something akin to majority rule, code can be updated to change the protocols governing the cryptocurrency and thereby change the characteristics of the digital asset.

Together, code and consensus create both opportunities and challenges. Code can provide stability and predictability but inevitably suffers from the limitations of human foresight. Meanwhile, modification by consensus allows for growth and adaption to correct design flaws and address changing circumstances, but the same flexibility increases uncertainty and undermines the stability sought from code. Although code may itself contain protocols for consensus-based modifications, the two are in constant tension. Of course, this is not unique to cryptocurrency; the same fundamental tension exists in any regime that attempts to balance rule of law and majority rule. However, the interplay between rule of law and majority rule is a special quality that is not as prominent in most commodity markets. Recognizing these dueling traits is helpful for considering the types of issues cryptocurrency markets are likely to face.

In many ways the interplay between these two concepts causes cryptocurrency to share common attributes to electricity traded in organized power markets in the United States. To begin, like U.S. power markets, cryptocurrencies (and the smart contracts that can interact with them) are complex, artificial constructs that are likely to suffer from design flaws that can be arbitraged or otherwise used by participants in a manner inconsistent with the interests of other parties. U.S. power markets provide one model for addressing this "gaming" risk.

Also similar to U.S. power markets, there is a risk that changes in market rules might impact the value of an asset and that these changes can be driven by competing factions within the

markets. With cryptocurrency, there is an added risk that such change can be retroactive and potentially unlimited. This risk has drawn the attention of would-be investors and regulators alike.

Gaming – lessons from U.S. power markets.

As artificial constructs implemented through complex rules, U.S. power markets have a history of both overt and latent market defects. In some cases, these design flaws present opportunities for market participants to profit from activities that are in accord with the letter of the rules but that may be inconsistent with the objectives underpinning the rules.

FERC, as the agency primarily responsible for regulating power markets, has found that taking advantage of these types of gaming opportunities violates its anti-manipulation rule. Specifically, FERC interprets the fraud prohibited by its rule "to include any action, transaction, or conspiracy for the purpose of impairing, obstructing or defeating a well-functioning market." ***[1]*** Moreover, FERC has concluded that fraud does not require a violation of any explicit rule but instead is determined subjectively based upon facts and circumstances.***[2]*** The CFTC proposed a similarly broad reading for its anti-manipulation rule but stopped short of expressly endorsing or rejecting this specific interpretation of fraud in its final rule. ***[3]***

FERC's prohibition against "gaming" has forced market participants in U.S. power markets to attempt to identify the purpose of specific features of the market and to interpret the intent underpinning the market rules. This can be challenging in power markets where rules are implemented by consensus and often involve negotiations between stakeholders regarding the allocation of risks, costs, and benefits. This will be an even greater challenge in cryptocurrency markets where the purpose of any given rule might never be expressed and the intent of individual participants in the network is even more opaque.

In an effort to self-regulate, cryptocurrencies can institute rules prohibiting conduct designed to impair the market or exploit market design flaws, but these types of prohibitions are inherently subjective and not easily susceptible to codification in machine code. To the extent that a regulator attempts to superimpose an anti-gaming concept to cryptocurrency markets, the lack of evidence of the purpose and intent of specific protocols may make both compliance and enforcement a challenge. To the extent that developers desire greater regulatory protections and certainty, documenting the purpose of certain market features may facilitate compliance and enforcement.

Ultimately, even if a cryptocurrency is free from material defects, the gaming risk will remain with respect to smart contracts. This risk may not outweigh the potential benefits of smart contracts, but it warrants consideration and may weigh in favor of simplicity and/or the express provision for subjective (human) dispute resolution or other controls to mitigate the risk of gaming.

The Consensus Risk – accounting for change.

Like cryptocurrencies, the rules governing U.S. power markets are subject to change. The tariffs and associated manuals adopted by such markets establish the rules by which the commodity can be traded, but those rules can be modified through stakeholder processes based (in part) on consensus. In power markets, however, the influence of the majority is diluted by multiple layers of rules – first, the organized market has its own stakeholder processes that limit the

pace of change, then any change is subject to review by the Federal Energy Regulatory Commission (FERC), which is subject to statutory limits set by Congress, which is limited by the U.S. Constitution, which can be amended only by a super majority. On the other hand, cryptocurrency, absent external regulation, is subject only to the limits imposed by the code as amended by consensus.

Late in 2018 the CFTC sought details regarding the Ethereum Network and information about the similarities and distinctions between Ether and Bitcoin.***[4]*** Among the twenty-five questions posed to the public, the CFTC asked two directly related to the risk of consensus-based protocols:

Question 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?"***[5]***

Question 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?"

Many commenters elected to skip these questions or to summarily dismiss the concerns they raised. Others acknowledged the concerns but described mitigation measures and pointed to examples of the network's history of surviving nefarious efforts. The general sentiment among commenters was that change is a good and necessary component of an evolving market and that crypto communities will defend their networks from undesirable disruptions.

Nevertheless, even the most ardent proponent of cryptocurrency will acknowledge the risk (at least theoretical) of a 51% attack whereby a bad actor gains control of a majority of the network and uses the control to disrupt the network. The most repeated rebuttal to this concern is that the cost of seizing control of a robust network likely exceeds any potential payoff (at least when accounting for the probability of success).***[6]*** However, there may be a question regarding the reliability of economic disincentives in a world of state-sponsored cyberwarfare and terrorism. According to one commenter, "[t]he 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."***[7]***

Beyond cyberterrorists and state actors, the ability of cost to discourage manipulation also may be undermined by the existence of derivative markets that can provide leverage to offset the costs associated with disrupting underlying cryptocurrency markets. At their core, both the Bitcoin and Ethereum assume economically rational actors but only factor in the economics of the networks themselves.

Moreover, the risk of disruptions and distortions is not limited to overtly nefarious actors. Governance by consensus also empowers a majority of stakeholders to make changes to protocols (and even redistribute digital assets) over the objection of minority interests. This feature interjects uncertainty that is at least qualitatively different from the usual market risks associated with most commodities.

The DAO Fork – code vs consensus.

The best example of the tension between code and consensus may be the hard fork alluded to in Question 14 of the CFTC's Request for Input. The "DAO Fork," which created today's Ethereum Network, occurred in response to the hacking of The DAO (a Decentralized Autonomous Organization) smart contract. A hacker or hackers diverted more than 3.6 million Ether by exploiting a feature in The DAO that allowed participants to double-spend by splitting The DAO multiple times before the balance was updated.

The Ethereum community discussed several options to address the hack (which was of The DAO and *not* Ethereum). One option was to adopt a soft fork that would prevent the hacker from ever accessing the seized Ether. In response to this proposal, an author claiming to be "The Attacker" asserted that the code in smart contracts controls. The author argued:

"I have carefully examined the code of The DAO and decided to participate after finding the feature where splitting is rewarded with additional ether. I have made use of this feature and have rightfully claimed 3,641,694 ether, and would like to thank the DAO for this reward. It is my understanding that the DAO code contains this feature to promote decentralization and encourage the creation of 'child DAOs'."

"I am disappointed by those who are characterizing the use of this intentional feature as "theft". I am making use of this explicitly coded feature as per the smart contract terms and my law firm has advised me that my action is fully compliant with United States criminal and tort law."

The letter continued:

"A soft or hard fork would amount to seizure of my legitimate and rightful ether, claimed legally through the terms of a smart contract. Such fork would permanently and irrevocably ruin all confidence in not only Ethereum but also the in the field of smart contracts and blockchain technology. Many large Ethereum holders will dump their ether, and developers, researchers, and companies will leave Ethereum. Make no mistake: any fork, soft or hard, will further damage Ethereum and destroy its reputation and appeal."

In essence, the author was arguing for playground rules in smart contracts – i.e., what might be unacceptable or even tortious in other environments is fair game when dealing in smart contracts. Ultimately, a majority of the Ethereum community rejected this view and opted instead for a hard fork to return the Ether to the original owners. In the days following the hack, and while a solution was being discussed, the price of Ether dropped from more than $20 to less than $13. A minority in the Ethereum community rejected the hard fork and continued with the original blockchain, which is now referred to as Ethereum Classic.

Although return of Ether to the original owners may have been fair and just in the case of The DAO, it unquestionably amounted to the forced redistribution of a digital asset. Notably, the initial diversion of the Ether was isolated to The DAO, yet it was the Ether community that controlled how to redistribute the wealth. The process worked if you believe the outcome was just, but what if it had not been just?

Conclusions

Although the uncertainty associated with cryptocurrency and smart contracts is qualitatively different from most commodities, all contracts involve uncertainty as to outside forces other

than supply and demand that might materially change the benefit of the bargain. As market participants and regulators continue to explore the possibilities of cryptocurrencies and smart contracts, it will be important to account for the risks of gaming and of consensus-based change, and U.S. power markets may hold answers to some of the challenges.

These risks might be mitigated by adopting subjective standards for evaluating conduct and providing for resolution of disputes outside of the code. Doing so would inject uncertainty into the code and is contrary to the ideology that is driving much of the developers of cryptocurrencies, but it also could serve as a safety net. Parties also could rely on other traditional contracting concepts such as addressing what happens if there is a change in law (or protocols) or the purpose of the contract is otherwise frustrated. With respect to forks, parties to a smart contract could agree as to how to handle a fork during the term of the agreement. Regardless of the fix, the first step is to recognize the risk.

---

[1] *Prohibition of Energy Market Manipulation*, Order No. 670, FERC Stats. & Regs. ¶ 31,202, reh'g denied, 114 FERC ¶ 61,300 (2006).

[2] *See, e.g.*, *In re Make-Whole Payments & Related Bidding Strategies*, 144 FERC ¶ 61,068 (2013) (characterizing as manipulative conduct consistent with the express terms of the applicable tariff).

[3] *See* Prohibition on the Employment, or Attempted Employment, of Manipulative and Deceptive Devices and Prohibition on Price Manipulation, 76 Fed. Reg. 41398, 41399 (July 14, 2011) (final rule); Prohibition of Market Manipulation, 75 FR 67657, 67659 (Nov. 3, 2010) (proposed rule, providing "the Commission proposes that subsection (c)(1) be given a broad, remedial reading, embracing the use or employment, or attempted use or employment, of any manipulative or deceptive contrivance for the purpose of impairing, obstructing, or defeating the integrity of the markets subject to the jurisdiction of the Commission").

[4] Request for Input on Crypto-Asset Mechanics and Markets, 83 Fed. Reg. 64,563 (Dec. 17, 2018).

[5] As background, changes to the protocols of a blockchain are referred to as "forks." A "soft" fork involves an update to the protocols that is compatible with older versions. A "hard" fork changes a protocol in a manner that renders prior versions of the blockchain incompatible with the new version. To the extent that a hard fork is not adopted by the entire network, the result will be two separate blockchains with some shared history prior to the fork but separate identities after the fork. Soft forks have occurred without much fanfare in an effort to address perceived flaws in the protocols of various cryptocurrencies. These are akin to software updates and typically are uneventful unless there is a bug in the update itself. Likewise, hard forks can be without controversy. However, hard forks can result in network splits and competing blocks. They also can result in a redistribution of the digital asset.

[6] *See, e.g.*, Circle Internet Financial Limited Comments at p. 11 (Feb. 15, 2019) (noting an "impediment to disruption is that it is likely to be uneconomic").

[7] Chatham Financial Comments at p. 6 (Feb. 15, 2019).