It Isn't 'Consensus': Toward Cooler Protocol Debates

Jim Harper

September 10, 2016

If Ayn Rand were involved in the bitcoin or crypto world, she might well identify "consensus" as an "anti-concept".

The **anti-concept,** she said, is a "rationally unusable term". It conveys an approximate sense of meaning, but lacks the precision needed to fully communicate an idea. "In the realm of cognition," Rand said, "nothing is as bad as the approximate."

"Consensus" mischaracterizes the decision-making processes that exist around bitcoin. Adoption or non-adoption of network software says nothing about the broader expectations, wants or needs of users and potential users. Talk about "consensus" will tend to sting users whose preferences conflict with the majority-run protocol and software.

That does not mean that credit isn't due to an author going by **@MAbtc** for the thoughtful contribution of his recent article: "**Hard forks and Consensus Networks: Meta Questions and Limitations.**" It is a helpful exploration of important ideas, and it won **high praise** from **Bitcoin Core** developer Adam Back. In particular, it offers valid thoughts on the **ethereum hard fork**, a development that is ripe for examination. (Another excellent after-action report is Josh Stark's "**Building the Foundations for a Scalable Ethereum Community**").

@MAbtc's article draws an intuitive distinction between the "consensus mechanism" for validating transactions described in Satoshi Nakamoto's **Bitcoin white paper** and the "consensus rules" on which the broader bitcoin network operates. In his view, one set is amenable to change and the other is not. His aim is to clear up "widespread misunderstanding of the limitations of consensus networks".

Alas, the word "consensus" doesn't sit well in the piece, and in many other places it's often used to describe the nature of bitcoin development and governance. Using it with reference to networks, @MAbtc must mean to distinguish another category: "non-consensus networks." But non-consensus networks don't exist. One has to imagine that absurdity, in which participants select or amend protocols without regard to interoperability. Such "networks" wouldn't work.

As there is no such thing as a non-consensus network, the word "consensus" does no lifting in the phrase "consensus networks."

A network is simply a community that uses the same protocol. It is tempting to say that the protocol is "agreed upon" or "consented to" or some other phrase, but a participant's use of a network says nothing about their opinions or states of mind when adopting or continuing to use it.

All we can know is that they use it.

Defining consent

"Consent" has strong connotations of agreement knowingly and freely given. In some contexts, it is fair to say that use is a form of consent.

Given all the options, a person who picks a particular cereal on the cereal aisle is expressing an opinion about the better cereal. But imputing an opinion to the user of a network (or any product with strong network effects) is trickier, because the range of reasonable options is smaller.

US bitcoin users might rightly bridle at being told they're part of consensus around use of the dollar. Use of a network can coexist with any opinion from wholehearted endorsement to angry dissent.

Acute watchers of bitcoin protocol and software development may have a hard time believing it, but many bitcoin users probably adopted the protocol without knowledge of its finer functional details. Judging by various efforts at opinion-gathering in bitcoin and elsewhere, many miners, significant investors and business people are indifferent to protocol and software issues.

Against that background of indifference, some bitcoin users strongly back continuity, and some are deeply dissatisfied, acceding to use bitcoin's current protocols only grudgingly because others do.

Telling the latter group that their use of the network is based on "consent" or "consensus" might be thought of as the open-source world's version of the **click-wrap license**. It foists something onto the dissatisfied user.
In this case, the offense is not onerous copyright or licensing terms, but the insinuation that "You think this is a good idea."

@MAbtc surely doesn't mean to pique the audience that is most important for him to persuade, but he is strongly committed to using "consensus" as a foundational principle. "By definition," he says, "a hard fork violates the user consent that serves as the basis for a consensus network like bitcoin."

It is right and just for people to get what they want and expect from a network, as from any product or service.

Bitcoin use, however, is only bitcoin use.

Imperfect markets

With no way to aggregate bitcoin user opinion, concepts from articulated group decision-making such as "consensus" are not much help.

Bitcoin governance is better thought of as a **market-based process** of spontaneous ordering. What is commonly called bitcoin's "consensus mechanism" is a **market for transaction-inclusion services.** What @MAbtc calls bitcoin’s "consensus rules" are a non-price market for software.

Passion of some participants aside, those markets coldly produce whatever those markets produce. There are arguments for or against change, but there is no meta-rule around them that prohibits certain types of change.

The ethereum hard fork has taught valuable lessons. Along with experience with the **replay attack** gained in many quarters, we now know that there is room for a main chain and a minority chain to co-exist. Each chain serves the interests (and disinterests) of its users in ways only those users truly might know.
Ideally, each user would decide for himself or herself what dimensions of bitcoin are "of the essence" and vigorously protect those dimensions as a consumer and user of transaction-inclusion services and software.

But it's more realistic to recognize that proposed modifications have salience to some and non-salience to others.

There are going to be strong and weak arguments for and against any proposal. The early assumption that participants in the bitcoin network would converge upon a best use-case for the protocol and keenly adjust their actions to maximize bitcoin's utility and value has yet to bear out.

Here, as everywhere, there aren't perfect markets.

For the greater good

In the blocksize schism, there is a **divergence of values.**
Convergence on values and how to advance them must await the growth of more social capital: cool-headed, basic discussion of the purposes bitcoin and cryptocurrency can best serve; more mature technology and business leaders; greater knowledge of the economics and security factors around bitcoin and crypto; and much more.

At Cato's 32nd Annual Monetary Conference in **late 2014**, I moderated a bitcoin panel in which traditional monetary experts opined in ways that seemed to misunderstand the nature of open-source software development. (Among the presentations was a paper called "**Bitcoin Will Bite the Dust,**" which is sometimes mistakenly treated as a Cato position). At the end of the presentations, I explained as best I could how open source allows the bitcoin protocol and software to change in order to address flaws that the panelists mistakenly perceived as permanent.
My defense of bitcoin was inconsistent with @MAbtc's argument that a hard fork "violates the user consent that serves as a basis for a consensus network like bitcoin". Open source allows hard forks, and an open-source network allows for adoption of hard-forked software should the majority of users decide to adopt it.

The argument that existing users should be able to rely on certain elements of the status quo is a good one — the 21m BTC limit on bitcoin production is "of the essence," in my opinion — but it is not well-argued as based in consent or consensus.

At the scale of the bitcoin network, "consensus" can’t actually exist and doesn't. There is only use. Talk of consensus will needlessly offend dissenters from the current majority protocol and software.

Ayn Rand's notion of the "anti-concept" may be so malleable that it is an anti-concept itself. But "consensus" probably should not be used in place of arguments on the true merits: that a given protocol and software design should fulfill the highest and best use cases for bitcoin.

A reader of @MAbtc’s article will have little doubt that he can make good arguments on those merits.

Jim Harper is a senior fellow at the Cato Institute, and former global policy counsel at the Bitcoin Foundation.