Bitcoin and the Politics of Non-Political Money

Jim Harper

January 25, 2016

An early trope about Bitcoin was that it was 'non-political' money. That's a tantalizing notion, given the ugliness of politics. But a monetary system is a social system, technology is people, and open source software development requires intensive collaboration—particularly around a protocol with strong network effects. When the group is large enough and the subject matter important enough, human relations become politics. I think that is true even when it's not governmental (read: coercive) power at stake.

Bitcoin's politics burst into public consciousness last week with the "whiny ragequit" of developer Mike Hearn. In a Medium post published ahead of a *New York Times* article on his disillusionment and departure from the Bitcon scene, Mike said Bitcoin has "failed," and he discussed some of the reasons he thinks that.

As do most people responding to the news, I like Mike and I think he's right to be frustrated. But he's not right on the merits of Bitcoin, and his exit says more about one smart, impatient man than it does about this fascinating protocol.

But there is much to discover about how governance of a project like Bitcoin will proceed so that politics (in the derogatory sense) can be minimized. Stable governance will help Bitcoin compete with governmental monetary and record-keeping systems. Chaotic governance will retard it. We just need to figure out what "stable governance" is.

If you're just tuning in, usage of Bitcoin has been steadily rising, to over 150,000 transactions per day. That is arguably putting pressure on the capacity of the network to process transactions. (And it undercuts thin, opportunistic arguments that Bitcoin is dead.)

Anticipating that growth, last May developer Gavin Andresen began pushing for an expansion of the network's capacity through an increase in the size of "blocks," or pages on the Bitcoin global public ledger. The current limit, 1 MB about every 10 minutes, supports about three transactions per second.

Eleven months earlier, Gavin had stepped down as Bitcoin's lead developer to focus on broader issues. He handed the reins of "Bitcoin Core" to a group that—it later became clear—doesn't share his vision. And over the summer and fall last year, the arguments in the blocksize debate grew stronger and more intense.

In August, Gavin and Mike introduced a competing version of the Bitcoin software called Bitcoin XT, which, among other things, would increase the blocksize to 8 MB. Their fork of the software included a built-in 75 percent super-majority vote for adoption, which made it fun to discuss as "A Bitcoin Constitutional Amendment."

This move catalyzed discussion, to be sure, but also deepened animosity in some quarters. Notably, the controller(s) of various fora for discussing Bitcoin on the web began censoring discussion of XT on the premise that this alternative was no longer Bitcoin. Nodes running XT were DDOSed (that is, attacked by floods of data coming from compromised computers), assumedly by defenders of Core.

A pair of conferences entitled "Scaling Bitcoin" brought developers together to address the issues, and the conferences did a lot of good things, but they did not resolve the blocksize debate. The Bitcoin community is in full politics mode and the worst of politics are on display.

Well, actually, not the worst. Politics is at its worst when the winners can force all others to use their protocol or ban open discussion of competing ideas entirely.

Competing ideas. Competing software. To my mind, these seem to be the formative solution to Bitcoin's current governance challenge. The relatively small Bitcoin community had fallen into the habit of using a small number of web sites to interact. Those sites betrayed the open ethos of the community, which prompted competing alternatives to spring up.

The community has likewise fallen into the habit of relying on a small number of developers–of necessity, in part, because Bitcoin coding talent is so rare. Now, though set back by the censorship and DDOS attacks, Bitcoin XT is joined by Bitcoin Unlimited andBitcoin Classic as competitors to Bitcoin Core.

The developers of each version of the Bitcoin software must convince the community that their version is the best. That's hard to do. And it's supposed to be hard. Competition is great for everybody but the competitors.

The coin of the realm in these competitions–as in all debates–is credibility. Each software team must share the full sweep of their vision, and how their software advances the vision. They must convince the community of users that they have thought through the many technical threats to Bitcoin's success.

I'll confess that the Core team's vision remains relatively opaque to me. I gather that they weight mining centralization as a greater concern than others do and thus resist the centralizing influence of a larger block size. As a technical layman, the best articulation for Core I've found is a response to Mike Hearn from BitFury's Valery Vavilov. In it, one can at least see the reflection of the vision. Core's recent statement and a December discussion of capacity increases don't overcome the need for more sense of where they see Bitcoin going and why it's good. I'm certain that they intend the best, and I'm pretty sure they feel that they've already explained their plans until they're blue in the face. (Or, at least, blue in the hair…) But the community might benefit from more, and Peter R's presentation in Montreal–though needlessly peppery at the end–is the clearest and thus most plausible explanation of blocksize economics I've found. (Much in this paragraph may be evidence of my ignorance.)

The reason Mike Hearn could ragequit is because he no longer wants a place in the Bitcoin community. He set a match to all his political capital. Everyone else in the Bitcoin community, and especially the developers, must do everything they can to build their political capital. They must explain the merits of their ideas and–in the fairest possible terms–the demerits of others. They should back up their ideas with supportive evidence, which–happily–an open technical system allows. And they should turn away "allies" who censor dsicussion forums or sponsor DDOS attacks. They should avoid impugning the motives of others, and, when they lose, lose gracefully.

All these behaviors cultivate credibility and the ability to persuade over the long haul. They offer the prospect of long-term success in the Bitcoin world and success for the Bitcoin ecosystem. Good behavior is good "politics," which is something this non-political money needs.

Jim Harper is a senior fellow at the Cato Institute, working to adapt law and policy to the information age.