New Bitcoin Development Spurs Unnecessary Fear Of Centralization

William J. Luther

September 8, 2015

Unless you are actively involved in the bitcoin community, you probably haven't heard that developers Gavin Andresen and Mike Hearn launched a new version of the digital currency's software called Bitcoin XT—nor would you know why this would leave the "bitcoin community in disarray." In the event that you attend cocktail parties or water-cooler confabs where such topics are the norm, let's get you caught up to speed.

Bitcoin is a digital money, or cryptocurrency, that enables users to transfer funds securely over the Internet. Unlike traditional electronic payments, where funds must pass through a trusted third party, bitcoin can be sent directly from one user to another. Proponents argue that processing payments over a distributed system, as opposed to relying on a bank or clearinghouse, lowers the cost of transacting.

Since its launch in 2009, demand for bitcoin has soared. It is accepted by major online retailers and small businesses engaged in face-to-face transactions. Its current market capitalization puts it on par with national currencies like the Guatemalan quetzal and Costa Rican colon. Indeed, the relative success of bitcoin has inspired a host of alternatives. But it still has a long way to go towards widespread adoption.

The current debate centers on a perceived tradeoff between the ability to process a growing number of transactions, on the one hand, and maintaining a highly decentralized mechanism for processing transactions on the other.

The bitcoin system can currently handle around 300,000 transactions per day

Let's get technical: When one spends bitcoin, the transaction is bundled with others into a block. The new block of transactions is confirmed and added to the blockchain (think: public ledger) at bitcoin's core. At the moment, these blocks are limited in size to one megabyte and are processed roughly every 10 minutes. Hence, the bitcoin system as currently designed can handle around

300,000 transactions per day. For comparison, Visa averages around 150 million transactions per day and reports the ability to handle more than 24,000 transactions per second.

Andresen, Hearn and others want to increase the number of transactions bitcoin can support to make it even more competitive as a global payments mechanism. They cannot increase the speed at which blocks are added to the blockchain—as that would increase the rate at which new bitcoin is created—so they propose increasing the size of each block.

This isn't the first time bitcoin community members attempted to change the block size limit. Originally, there was no block size limit. The current limit was introduced early on to protect the system against "spam transactions." At the time, it wasn't a big deal since few people were using bitcoin. The one megabyte limit was like a 500 MPH speed limit. It was completely non-binding. But the system has grown a lot since then. Although it's not yet bumping up against the hard constraint—it averaged around 117,500 transactions per day over the last month—many believe the block size limit will become binding in the very near future.

Increasing the number of transactions could undermine the decentralized nature of the system

Why would anyone in the bitcoin community oppose increasing the number of transactions the system can support? Simply put, some worry that the proposed solution will undermine the decentralized nature of the system. If there is a long line of transactions to be processed, some users will be willing to pay high fees to skip the queue.

Fees are relatively unimportant at the moment since "miners" who successfully process a block of transactions are rewarded with newly created bitcoin. However, fees will become more important in the future because the amount of new bitcoin issued to a successful miner is cut in half roughly every four years. If increasing the block size lowers the transaction fees miners can expect to receive, one would expect fewer miners competing to process transactions as the block reward decreases over time. The bitcoin system would become more centralized as a result.

There's a related concern that bigger block sizes will require more bandwidth, which would preclude some smaller players from competing in the mining race. Opponents claim this, too, would result in a more centralized system.

The approach taken by Hearn and Andresen clearly indicates their commitment to a decentralized system

Fears over excessive centralization are warranted. After all, decentralization is a big part of bitcoin's value proposition. But the amount of centralization being considered at the moment still seems vastly more decentralized than traditional payment systems.

Indeed, the approach taken by Hearn and Andresen clearly indicates their commitment to a decentralized system. BitcoinXT will continue to enforce the existing blocksize limit until the protocol is so widely adopted that it is used to process at least 75% of all blocks added to the

blockchain. If (and only if) that occurs—but no earlier than January—BitcoinXT will increase the limit to eight megabytes and double that limit every two years thereafter.

The commitment to gradual change based on consensus observed with the issuance of BitcoinXT is incredible, but perhaps not surprising. It reflects the core values held by bitcoin supporters. And it is also a hallmark of well-functioning self-governing systems. It bodes well for bitcoin's future.

Mr. Luther is an adjunct scholar at the Cato Institute's Center for Monetary and Financial Alternatives and a fellow with the Atlas Network's Sound Money Project.