Bitcoin is Doomed to Be Taken over by a Superior Cryptocurrency

by

Hiroshi Shibuya
Department of Economics, Otaru University of Commerce
shibuya@res.otaru-uc.ac.jp
July 17, 2014

There is a strange aspect about the Bitcoin mechanism design. It is related to the supply mechanism of Bitcoin. Economists generally agree that money supply should grow in line with economic growth, which is exponential. But Bitcoin is designed to grow more or less linearly (more precisely, in line with a logarithm function). In other words, the supply of Bitcoin is intentionally designed to grow at a far less rate than economic growth in such a way that its value will rise exponentially in the long run (assuming that the demand for Bitcoin grows with economic growth). This is, of course, good for the original Bitcoin holders because it will make them rich, but it also dooms Bitcoin to fail in the long run.

Bitcoin restricts its supply by reducing the reward for mining activities eventually to zero, and the miners only get transaction fees thereafter (see "6. Incentive" in Nakamoto (2008)). But this implies a serious potential problem. As the mining benefit goes down over time, it will eventually become more profitable for the miners to switch to another criptocurrency which offers a better mining reward. Or worse, it may become more profitable for the miners to attack Bitcoin and cash in. Such an outcome seems to be inevitable under the present Bitcoin design. In short, Bitcoin is doomed to disappear or to be taken over by a superior criptocurrency.

Mr. Satoshi Nakamoto (or the group under his name) either did not know much about economics (in particular, monetary theory) or actually knew all about its potential consequences. In the former case, he should make an attempt to improve the Bitcoin mechanism design. In the latter case, his intention was from the very beginning to make money (gain seigniorage) while Bitcoin lasts. Which is the truth, Mr. Nakamoto? Mr. Nakamoto is right in saying that Bitcoin does not depend on trust in the goodwill of a third party. But it does depend on trust in the mechanism design (ability) of Bitcoin. If Mr. Nakamoto wants Bitcoin to become a lasting currency, he

should fix any defect in the Bitcoin mechanism design.

Despite such a serious defect and some others, there is no question that the idea of Bitcoin is revolutionary in many ways. Indeed Bitcoin may be just a beginning for bigger social revolutions to come.

Reference

Nakamoto, Satoshi (2008), "Bitcoin: A Peer-to-Peer Electronic Cash System."
https://bitcoin.org/bitcoin.pdf