

Blocksize

This issue comes up repeatedly, sparking many heated discussions. Some people think issues surrounding the blocksize will be the ultimate downfall of bitcoin; others think the theoretical problems are largely overstated and/or completely resolvable. Count me in that latter camp.

What is it?

The number of transactions per second that bitcoin can handle on-blockchain is directly tied to the data size of each block. Since bitcoin's inception, the size of a block has been fixed in the bitcoin code to a maximum of 1MB. Since one new block is generated on the bitcoin network every 10 minutes on average, this works out to a theoretical maximum of 7 transactions per second. Compared to the thousands of transactions per second that the Visa and Mastercard networks handle, this is not a lot.

Why is the blocksize limited?

As with many things in life, there's a tradeoff. Larger blocks would require more processing and bandwidth resources from bitcoin nodes (the global network of "volunteer" computers running the bitcoin software), which would eventually cause fewer people to be willing to run nodes. On the flipside, the network's transaction processing capacity is clearly limited by the blocksize. To be a global currency handling everything from inter-bank settlement payments to online tipping and micro-transactions, clearly 7 transactions per second is far few. The current 1MB size was chosen by bitcoin's creator, Satoshi Nakamoto, in the original codebase as a reasonable balance during bitcoin's birth and initial growth stage.

What can be done about it?

Simple - change the code to raise the blocksize limit. While this is a one-line change to the code itself, it would require most nodes to incorporate the change at about the same time. Ever prescient, Satoshi even suggested how this can be done eventually, [stating on the bitcointalk forum](#) in 2010:

It can be phased in, like:

if (blocknumber > 115000)

&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;maxblocksize = largerlimit

It can start being in versions way ahead, so by the time it reaches that block number and goes into effect, the older versions that don't have it are already obsolete.

*What ***should*** be done about it?*

This is where people differ. Some are adamant that the 1MB limit stay in place forever, in order to keep it cheap for small-time operators (individuals with laptops) to run full bitcoin nodes. Others, myself included, prefer a more market-driven/organic approach. Acknowledging that [Moore's Law](#)

continually reduces the cost of computing power and bandwidth, I think a steady or market-defined increase in the blocksize is reasonable. It could even be eliminated entirely. In theory, bitcoin miners would be incented to strike a balance between including lots of transactions to gather fees, and the costs of processing and transmitting larger blocks. Like many dynamics in bitcoin, this seems like one where a natural market-driven optimum can efficiently emerge.