Posted by u/ChaosGrid 7 years ago

# Citation needed: Satoshi's reason for blocksize limit implementation.

**theymos** · 7 yr. ago

Satoshi never used IRC, and he rarely explained his motivations for anything. In this case, he kept the change secret and told people who discovered it to keep it quiet until it was over with so that controversy or attackers wouldn't cause havok with the ongoing rule change.

Luckily, it's really not that important what he thought. This was years ago, so he very well could have changed his mind by now, and he's one man who could be wrong in any case.

I think that he was just trying to solve an obvious denial-of-service attack vector. He wasn't thinking about the future of the network very much except to acknowledge that the limit could be raised if necessary. The network clearly couldn't support larger blocks at that time, and nowadays we know that the software wasn't even capable of handling *1 MB* blocks properly. Satoshi once told me, "I think most P2P networks, and websites for that matter, are vulnerable to an endless number of DoS attacks. The best we can realistically do is limit the worst cases." I think he viewed the 1 MB limit as just blocking yet another serious DoS attack.

Here's what I said a few months after Satoshi added the limit, which is probably more-or-less how Satoshi and most other experts viewed the future of the limit:

> Can you comment on "max block size" in the future? Is it likely to stay the same for all time? If not how will it be increased?

It's a backward-incompatible change. Everyone needs to change at once or we'll have network fragmentation.

Probably the increase will work like this: after it is determined with great certainty that the network actually can handle bigger blocks, Satoshi will set the larger size limit to take effect at some block number. If an overwhelming number of people accept this change, the generators [miners] will also

Also see this post of mine in 2010, which I think is pretty much exactly how Satoshi reasoned the future would play out, though I now believe it to be very wrong. The main misunderstandings which I and probably Satoshi had are:

- No one anticipated pool mining, so we considered all miners to be full nodes and almost all full nodes to be miners.
- I didn't anticipate ASICs, which cause too much mining centralization.
- SPV is weaker than I thought. In reality, without the vast majority of the economy running full nodes, miners have *every incentive* to collude to break the network's rules in their favor.
- The fee market doesn't actually work as I described and as Satoshi intended for economic reasons that take a few paragraphs to explain.

29 Share Report Save

w0dk4 · 7 yr. ago

Thanks, that's actually helpful - so it was really mostly an anti-DoS measure.

> But it has been determined by the majority of the Bitcoin Core developers (**and the majority of Bitcoin experts in general**) that the network cannot actually safely handle significantly larger blocks, so it won't be done right now. And the economy has the final say, of course, not the developers.

I'm interested. How do you actually arrive at these statements? Did you conduct a survey among all "bitcoin experts"? What constitutes a "bitcoin expert"?

13 Share •••

Continue this thread →