(https://servedbyadbutler.com/redirect.spark?MID=169476&plid=727177&setID=289765&channelID=0&CID=0&banID=519543343&PID=0&textadID=0&tc=1&mt=1521741565766317&hc=4271396bb6c8

By David Dinkins

SEP 19, 2017

Satoshi's Best Kept Secret: Why is There a 1 MB Limit to Bitcoin Block Size

43192 Total views **454** Total shares

Anybody familiar with Bitcoin is aware of the vexing problem caused by the 1 MB blocksize limit and the controversy that arose over how to scale the network. It's probably worthwhile to look back on how that limit came to exist, in hopes that future crises can be averted by a solid understanding of the past (https://cointelegraph.com/news/bitcoin-owes-success-to-three-different-waves-of-innovators).

A long time ago, in a land far away

In 2010, when the blocksize limit was introduced, Bitcoin was radically different than today. Theymos, administrator of both the Bitcointalk forum and /r/bitcoin subreddit, said, among other things

Hottest Bitcoin News Daily

For updates and exclusive offers, enter your e-mail below.

Email Address

SUBSCRIBE

(https://www.facebook.com/Cointelegraph)

(https://servedbyadbutler.com/redirect.spark?MID=169476&plid=732431&setID=255443&cha

(https://servedbyadbutler.com/redirect.spark?MID=169476&plid=736397&setID=255816&cha

(https://www.reddit.com/r/Bitcoin/comments/3giend/citation_needed_satoshis_reason_for_block size/ctygzmi/):

- "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."

It seems that late in 2010, Satoshi realized there had to be a maximum block size, otherwise some miners might produce bigger blocks than other miners were willing to accept, and the chain could split. Therefore, Satoshi inserted a 1 MB limit into the code.

And he kept it a secret.

Secret squirrels

Yes, Satoshi kept this change a secret until the patch was deployed, and apparently asked those who discovered the code on their own to keep quiet (https://www.reddit.com/r/Bitcoin/comments/3giend/citation_needed_satoshis_reason_for_block size/ctygzmi/). He likely kept things quiet to minimize the chances (https://www.reddit.com/r/Bitcoin/comments/449f57/the_circuit_breaker_and_satoshi_or_why_th e_one/) that an attacker would figure out how to use an unlimited blocksize to DOS the network.

Theymos puts it:

> *"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."*

It's also likely that Satoshi never expected the 1 MB blocksize to be a problem. At the time, the average blocksize was orders of magnitude smaller than 1 MB, and it looked like there would be time enough to devise a solution. Satoshi himself said, of the blocksize limit:

> *"We can phase in a change later if we get closer to needing it."*

And again:

> *"It can be phased in, like:*
>
> *if (blocknumber > 115000)*
>
> *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.*
>
> *When we're near the cutoff block number, I can put an alert to old versions to make sure they know they have to upgrade."*

It's apparent that Satoshi foresaw the removal of the blocksize limit as trivial and had no idea that such a minor code change would generate a firestorm.

Foreseeable problems

Bitcointalk user "kiba" presciently commented (https://bitcointalk.org/index.php?topic=1347.msg15590#msg15590), shortly after the cap was created:

> *"If we upgrade now, we don't have to convince as much people later if the bitcoin economy continues to grow."*

In response to Satoshi's comment that the limit could always be removed if necessary to support higher transaction capacity, Jeff Garzik pointed out:

> *"IMO it's a marketing thing. It's tough to get people to buy into a system, if the network is technically incapable of supporting high transaction rates."*

Clearly the warnings were present.

Why not bigger?

Many have asked why Satoshi didn't create a larger blocksize, like 8 MB. The answer is three-fold:

- It wasn't needed, as even 1 MB was far larger than the largest blocks that had ever been mined.
- It was technically easy to change, simply substituting one value in the code for another.
- Larger blocks create technical challenges.

Back in 2010, Internet technology was such that larger blocks would not have propagated properly. In 2015, Theymos recalled:

ı/sharer/sharer.php?
.com%2Fnews%2Fsatoshis-
-mb-limit-to-bitcoin-block-
t?text=Satoshi's Best Kept
imit to Bitcoin Block Size

> *"The easy-to-understand issue is that in order to be a constructive network node, you should quickly upload new blocks to many of your 8+ peers. So 8 MB blocks would require something very roughly like (8 MB * 8 bits * 7 peers) / 30 seconds = 15 Mbit/s upstream, which is an extraordinary upstream capacity. Since most people can't do this, the network (as it is currently designed) would fall apart from lack of upstream capacity: there wouldn't be enough total upload capacity for everyone to be able to download blocks in time, and the network would often go "out of sync" (causing stales and temporary splits in the global chain state)."*

Segregated Witness and Lightning Network

Today's Bitcoin uses a piece of code called Segregated Witness (SegWit) (https://cointelegraph.com/news/bitcoin-is-decentralized-but-not-distributed-and-that-fact-likely-contributed-to-bitcoins-civil-war) to separate signatures from transaction data, effectively allowing the network to "cheat" by creating larger blocks than 1 MB, yet still counting them as being below the cap. SegWit also fixes a vulnerability called transaction malleability, enabling the creation of something called the lightning network.

The lightning network is envisioned as a way for Bitcoin users and/or merchants to open payment channels with one another in a secure and trustless fashion. Funds can be exchanged between these parties without the transactions being written to the Blockchain. This keeps the Blockchain small, capable of being served by reasonably powerful computers. The lightning network would periodically need to "anchor" to the main Bitcoin Blockchain, but would allow enormous increases in transaction capacity with very small increases in the size of the Blockchain.

So far there is no working implementation of lightning network on mainnet, although there are versions on test net. Lightning network will be entirely optional, and users can choose to send ordinary transactions instead, if they so choose.

Follow us on: Your Email Subscribe

#Bitcoin News (/tags/bitcoin) #Satoshi Nakamoto (/tags/satoshi-nakamoto)

#SegWit (/tags/segwit) #Bitcointalk (/tags/bitcointalk)

#Bitcoin Block Size (/tags/bitcoin-block-size) #Jeff Garzik (/tags/jeff-garzik)

#Bitcoin Mining (/tags/bitcoin-mining)

14 Comments

(https://servedbyadbutler.com/redirect.spark?MID=169476&plid=735144&setID=255444&channelID=0&CID=0&banID=519549093&PID=0&textadID=0&tc=1&mt=1521741772952915&hc=a476145e0d

By Molly Jane Zuckerman **7 HOURS AGO**

Nikkei Report: Japan To Issue Warning Against Crypto Exchange Binance, Twitter Cries FUD

18569 Total views **227** Total shares

Update: the CEO of Binance, Changpeng Zhao has made a post on Twitter (https://twitter.com/cz_binance/status/976783934074732544) denying that the exchange has "received any mandates" from the Financial Services Agency and describing Nikkei's report as "irresponsible journalism."

> *Nikkei showed irresponsible journalism. We are in constructive dialogs with Japan FSA, and have not received any mandates. It does not make sense for JFSA to tell a newspaper before telling us, while we have an active dialog going on with them.*
> *— CZ (not giving crypto away) (@cz_binance) March 22, 2018 (https://twitter.com/cz_binance/status/976783934074732544?ref_src=twsrc%5Etfw)*

Japan (https://cointelegraph.com/tags/japan) is set to issue a warning against crypto exchange Binance (https://cointelegraph.com/tags/binance), according to a report from the news outlet Nikkei (https://www.nikkei.com/article/DGXMZO28441290S8A320C1MM8000/), March 22.

Binance, the number one exchange by 24 hour volume according to CoinMarketCap (https://coinmarketcap.com/exchanges/volume/24-hour/), was affected by a hack (https://cointelegraph.com/news/possible-hack-of-third-party-tools-affects-binance-exchange-users) on March 7, impacting users that had issued API keys on their accounts.

Twitter crypto person @WhalePanda shared (https://twitter.com/WhalePanda/status/976753692258066433) @BTCVIC's tweet, wondering how Bitcoin's (https://cointelegraph.com/tags/bitcoin) (BTC) price will react to the alleged warning:

> *"Quite interesting how #Bitcoin (https://twitter.com/hashtag/Bitcoin?src=hash) reacts to this, even though Binance is just a s***coin exchange with no fiat on-ram"*

Several Twitter commentators on @WhalePanda's post saw the sharing of the future purported warning as just spreading FUD in the crypto sphere, while others seemed to confirm the legitimacy of the upcoming warning through personal private channels:

> *Let the FUD commence! pic.twitter.com/ZHZkJIIObk (https://t.co/ZHZkJIIObk)*
> *— Albit Coinstein (@AlbitCoinstein) March 22, 2018 (https://twitter.com/AlbitCoinstein/status/976754277111795712?ref_src=twsrc%5Etfw)*

> *Not fud. I spoke to people in the know and they've asked binance to take down the Japanese translation to discourage Japanese to use their platform*
> *— Henno van Rensburg (@hennokun) March 22, 2018 (https://twitter.com/hennokun/status/976756785435484160?ref_src=twsrc%5Etfw)*

Japan's Financial Services Agency (FSA) had begun inspecting crypto exchanges (https://cointelegraph.com/news/japans-financial-regulator-to-conduct-inspections-of-15-unregistered-crypto-exchanges) in the wake of the January hack (https://cointelegraph.com/news/japan-coincheck-exchange-freezes-all-withdrawals-as-up-to-723-mln-leaves-its-wallet) of over $500 mln NEM (https://cointelegraph.com/tags/nem) stored on a low security hot wallet (https://cointelegraph.com/news/coincheck-stolen-534-mln-nem-were-stored-on-low-security-hot-wallet) at exchange Coincheck. The FSA has issued seven "punishment notices" (https://cointelegraph.com/news/japanese-financial-regulator-issues-punishment-notices-for-7-crypto-exchanges) to as-of-yet unregistered Japanese exchanges, as well as temporarily halting operations at two more, for a lack of "the proper and required internal control systems."

Follow us on: ɔook. r.con annel am.r Your Email Subscribe

#Bitcoin News (/tags/bitcoin) #Japan (/tags/japan)

#Cryptocurrency Exchange (/tags/cryptocurrency-exchange) #Binance (/tags/binance)

#Twitter (/tags/twitter)

3 Comments