MAGICAL CRYPTO
CONFERENCE
2019

MCC

Briefly, Why Block Sizes Shouldn't Be Too Big

Luke Dashjr

PGP Key Fingerprint:

E463 A93F 5F31 17EE DE6C
7316 BD02 9424 21F4 889F

How does Bitcoin work? What keeps it secure?

Miners collect transactions into blocks. Users verify the blocks.

What if a miner includes an invalid transaction? Users reject the block.

51% attacks are limited to reorgs. Miners can't create inflation; steal bitcoins; etc. They can if users don't verify the blocks!

Why would a miner make an invalid block? No reason if it just gets rejected; but plenty of reason if they can get away with it - verification is needed to maintain incentives too!

How many full nodes are needed?

If only miners run a full node, they have free reign to make, remove, and violate almost all protocol rules at will.

What happens if you don't run a full node, but others do? You see one thing; they see another. Not good for business if your currency isn't what others use.

What if most people don't run a full node? Everyone is buying and selling in the miner-issued currency! Miners don't necessarily care about the minority; by the time the minority can complain, the majority won't want to lose money.

Global markets: if nodes are in the USA, what happens when the USA sleeps?

How difficult is it to run a full node?

Strawmen; "Everyone can download 2 MB in 10 minutes"; "We have multi-TB hard drives now" - these aren't a problem, admittedly!

How difficult is it to run a full node?

Problem 1: Initial Blockchain Download/sync - the time it takes new users to really begin using Bitcoin themselves.

Not "can it be done", but "how long will people tolerate?"

Technology improves only about 18%/year. 2 MB blocks are 105 GB/year, or around 50% increase in blockchain size. Technology can't keep up!

People want to reduce computer usage to phones. That counter-acts improvements. Battery life and heat become concerns. (It <u>used</u> to be easy!)

Some day we may find we can't improve further.

How difficult is it to run a full node?

Block size	300k	1 MB	2 MB	8 MB
Peak sync time vs 2019 / 2013	1x / 6x	1.11x / 6x	1.65x / 9x	5.3x / 30x
Peak in year	2019	2022	2024	2025
Return to 2019 sync time in year	n/a	2025	2033	2045
Return to 2013 sync time in year	2035	2043	2048	2059
Blockchain size in 2039	500 GB	1.24 TB	2.3 TB	8.6 TB

Other problems with large blocks

- Fee market
- Low bandwidth links (satellite, radio relays, etc)
- De-anonymised mining (which currently needs centralised peering)
- Bandwidth quotas (per month limits)
- Etc

Answering objections

Won't smaller blocks result in higher fees?

- Spam demand is infinite and sets the fee floor.
- If fees rise, unimportant* transactions will stop rather than bid up fees higher. (Important ones will optimise.)
- Not all transactions need on-chain security. Many can drop to L2.
- We don't know the "correct" fee point: it costs what it costs.
- Fees should probably be higher than node costs anyway.

Answering objections

Eventually, we *will* need a block size increase.

- Uncertain. Future improvements may be sufficient for future needs.
- Bitcoin needs to provide a compelling use case to get to that point.
- We don't need to fix future problems today. Reducing the block size now might actually make it more practical to then increase it sooner and larger.
- *Eventually*, technology will catch up, and *then* increasing it is safer.
- Any reductions made, can be explicitly made temporary (not *just* in intent).

Answering objections

We can just use pre-synced nodes / sync snapshots to make the IBD problem go away?

- Changes Bitcoin's security model: we end up trusting the snapshot-issuer.
- Verification of snapshots can be done only with IBD.

Answering objections

Isn't it already too late? We can't *reduce* the blockchain size.

- Avoid making the problem worse.
- Technology can catch up faster, sooner.
- Future block size increases become safer.

Possible solutions

- Ignore the problem (ie, give up on mobile nodes and hope for the best)
- Miners can always make smaller blocks (no change needed!)
- Artificial transaction weight (not currently supported, but only a p2p change)
- Temporary softforks that automatically expire (needs community support)
- Permanent softfork (risky and a bad idea in the long term)

MAGICAL CRYPTO
CONFERENCE
2019

MCC

Briefly, Why Block Sizes Shouldn't Be Too Big

Luke Dashjr

PGP Key Fingerprint:

E463 A93F 5F31 17EE DE6C
7316 BD02 9424 21F4 889F