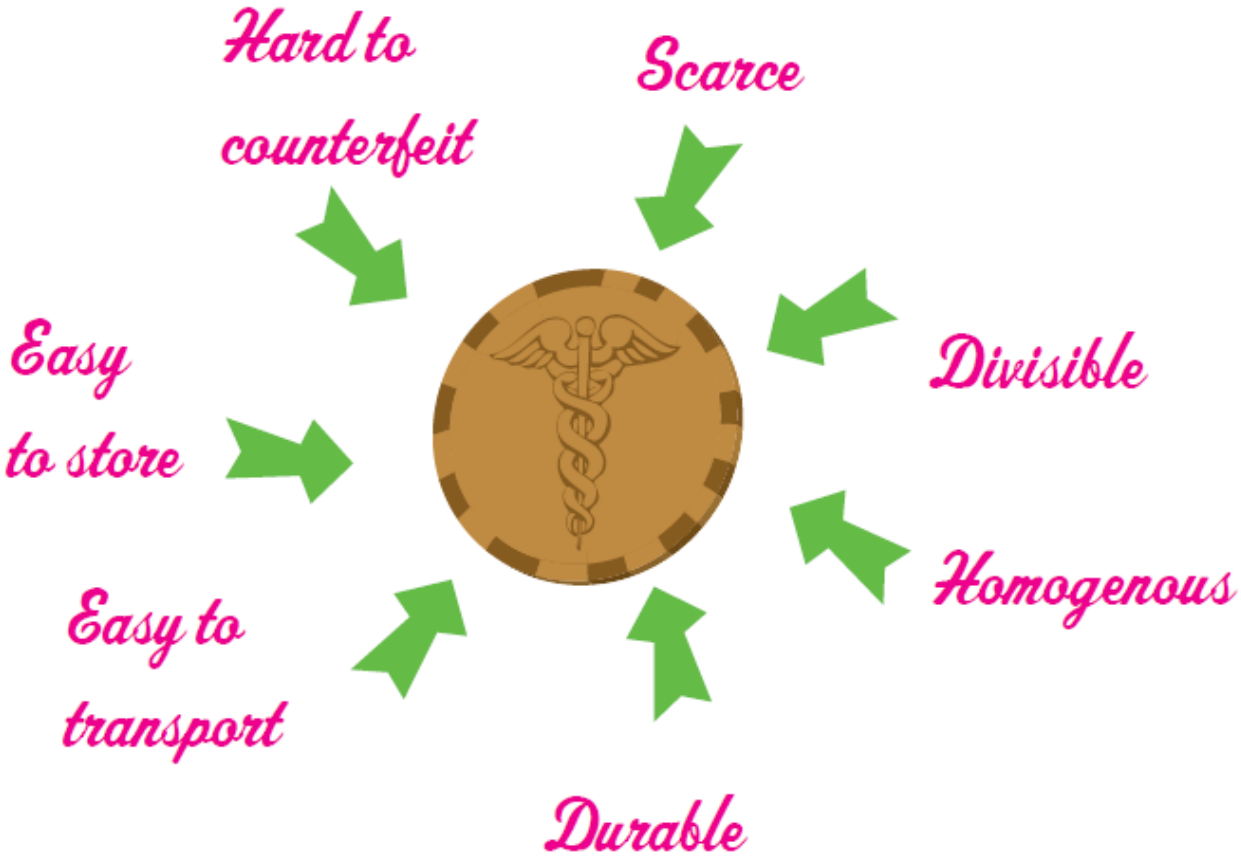
What is Bitcoin?

Bitcoin: A Peer-to-Peer Electronic Cash System

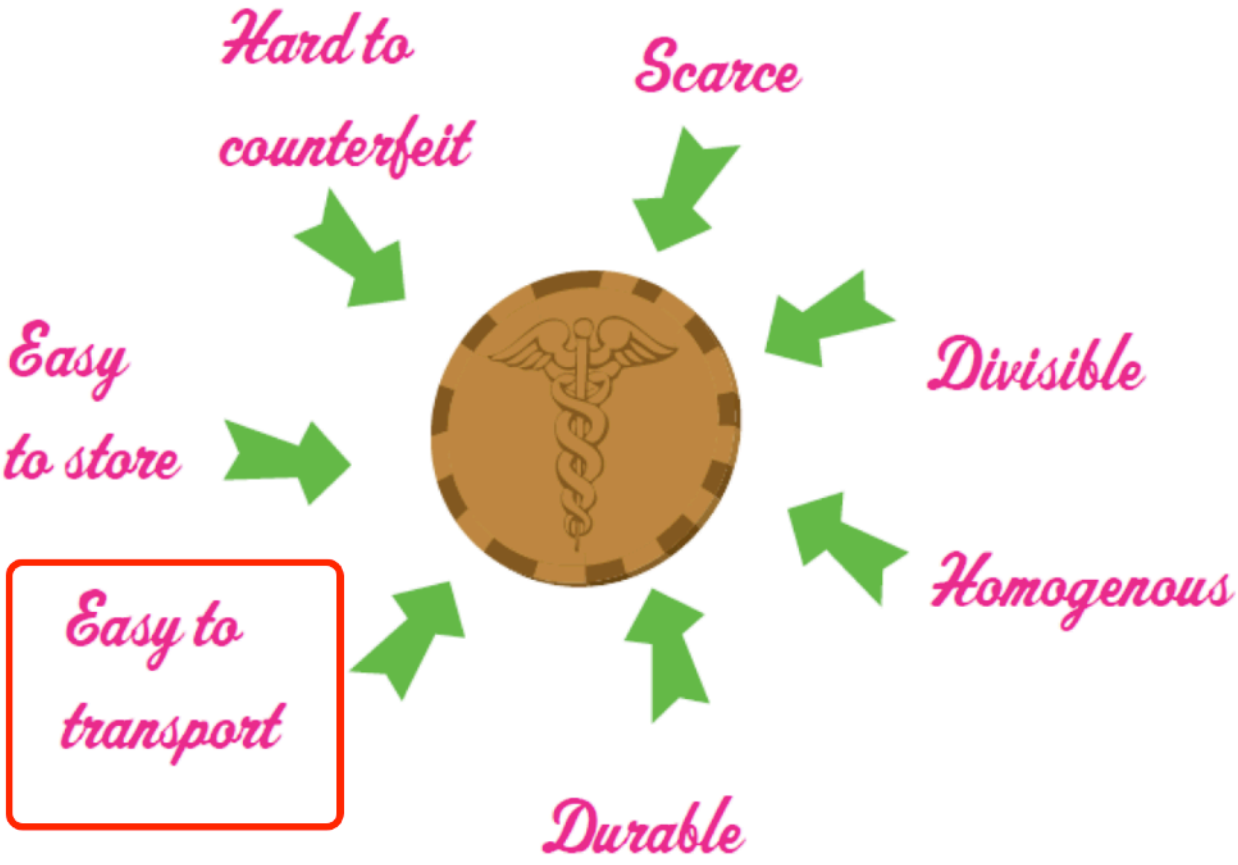
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

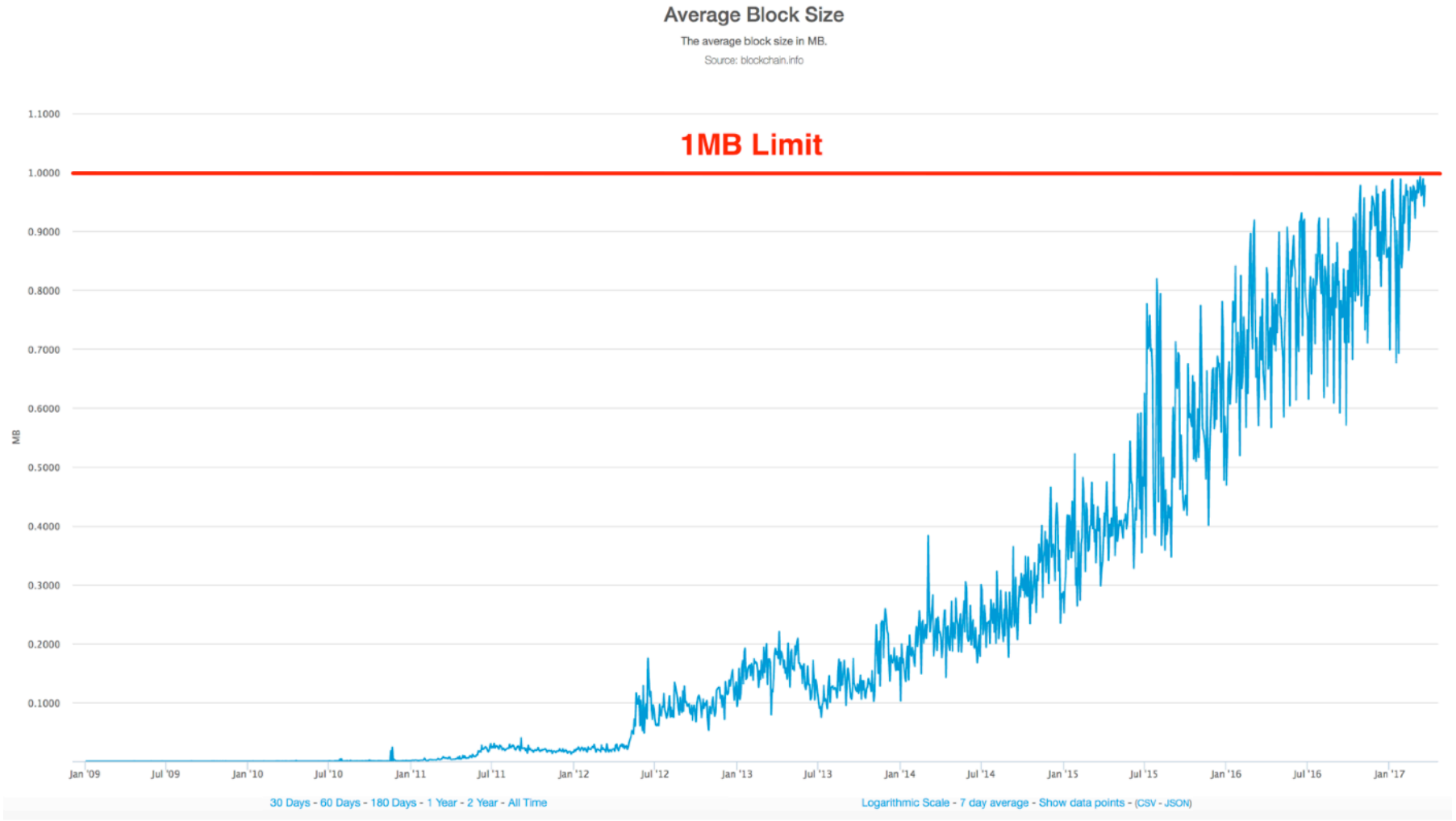
Good Money

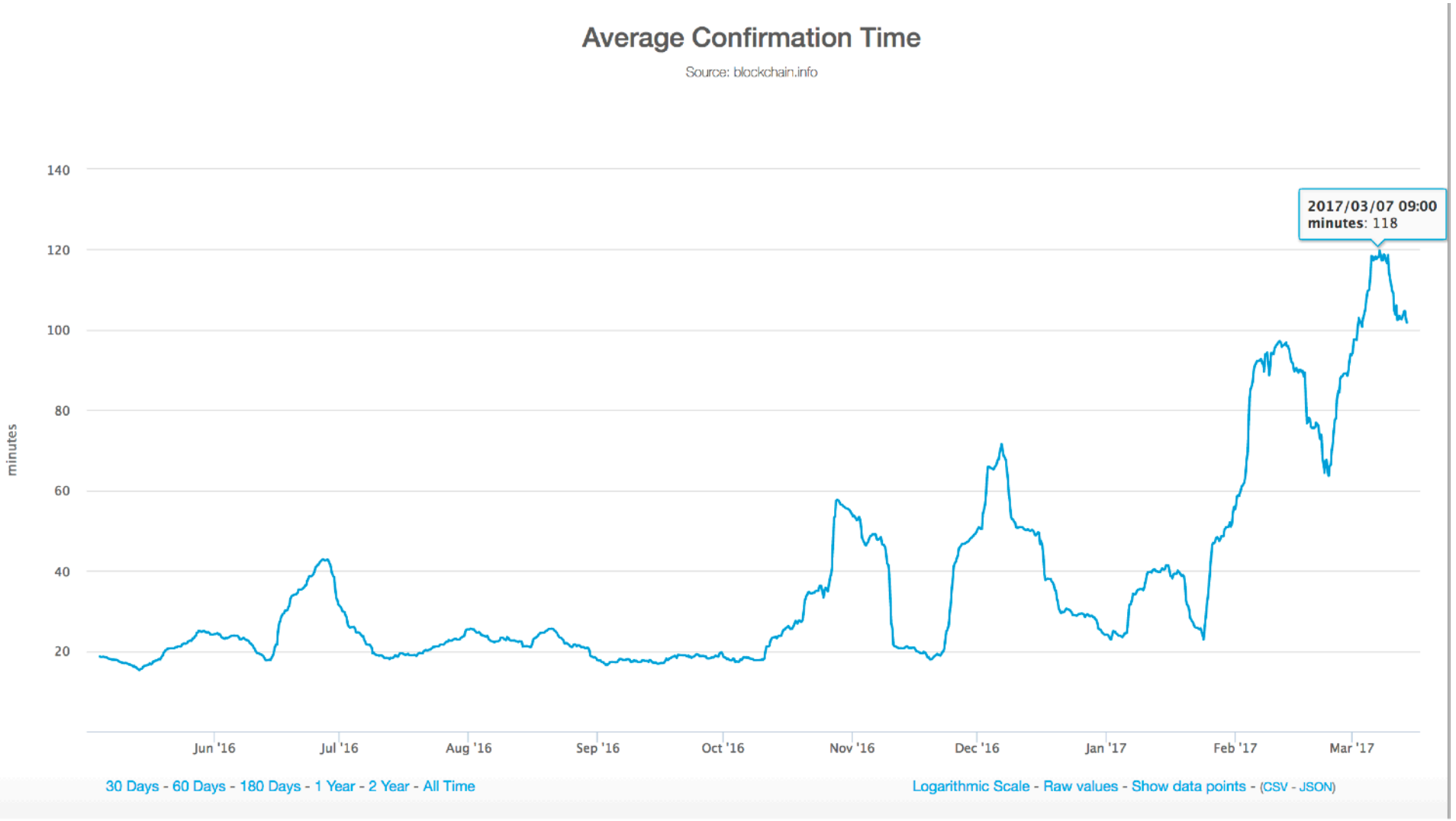

Hard to counterfeit
Scarce
Easy to store
Divisible
Homogenous
Easy to transport
Durable

Good Money



This is being damaged by Core

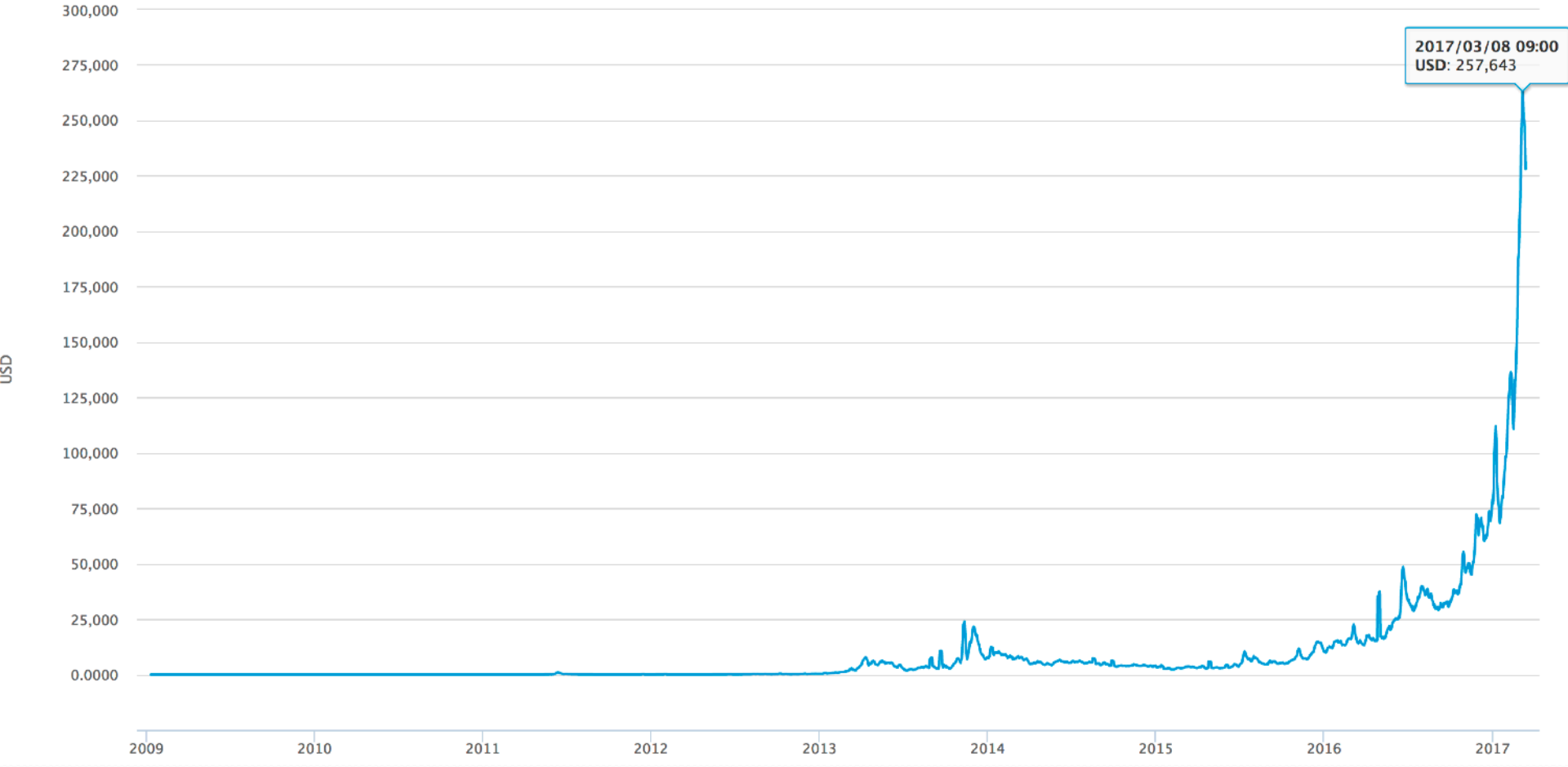

Average Block Size
The average block size in MB.
Source: blockchain.info
1MB Limit
MB
1.1000
1.0000
0.9000
0.8000
0.7000
0.6000
0.5000
0.4000
0.3000
0.2000
0.1000
Jan '09
Jul '09
Jan '10
Jul '10
Jan '11
Jul '11
Jan '12
Jul '12
Jan '13
Jul '13
Jan '14
Jul '14
Jan '15
Jul '15
Jan '16
Jul '16
Jan '17
30 Days - 60 Days - 180 Days - 1 Year - 2 Year - All Time
Logarithmic Scale - 7 day average - Show data points - (CSV - JSON)


Average Confirmation Time
Source: blockchain.info
minutes
140
120
100
80
60
40
20
2017/03/07 09:00
minutes: 118
Jun '16
Jul '16
Aug '16
Sep '16
Oct '16
Nov '16
Dec '16
Jan '17
Feb '17
Mar '17
30 Days - 60 Days - 180 Days - 1 Year - 2 Year - All Time
Logarithmic Scale - Raw values - Show data points - (CSV - JSON)

Total Transaction Fees in USD

The total value of all transaction fees paid to miners (not including the coinbase value of block rewards).

Source: blockchain.info



30 Days - 60 Days - 180 Days - 1 Year - 2 Year - All Time

Logarithmic Scale - Raw values - Show data points - (CSV - JSON)

Bitcoin Percentage of Total Market Capitalization
Zoom 1d 7d 1m 3m 1y YTD ALL
From Apr 28, 2013 To Mar 27, 2017
Percentage of Total Market Cap
90%
80%
70%
60%
Jul '13
Jan '14
Jul '14
Jan '15
Jul '15
Jan '16
Jul '16
Jan '17

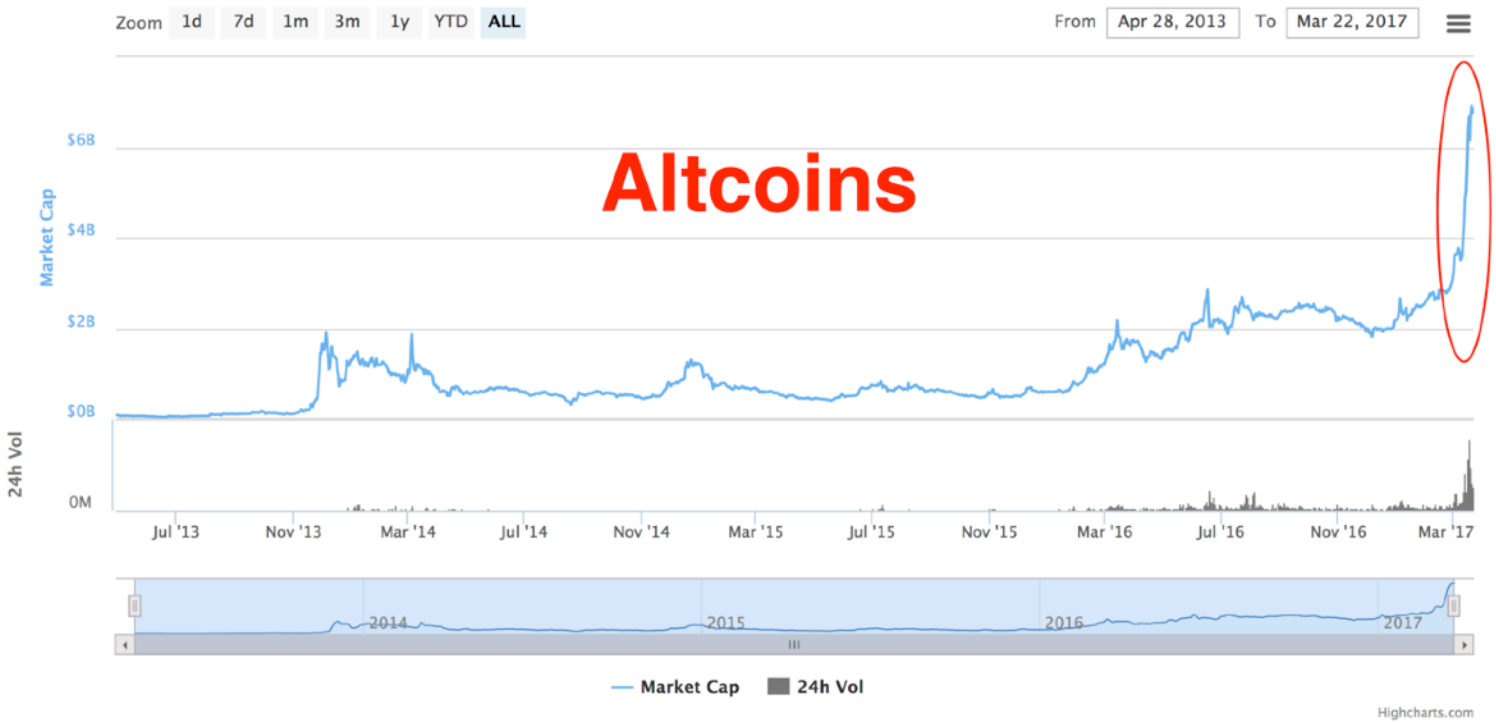
ECONOMICS HELP
HELPING TO SIMPLIFY ECONOMICS

Substitute Goods

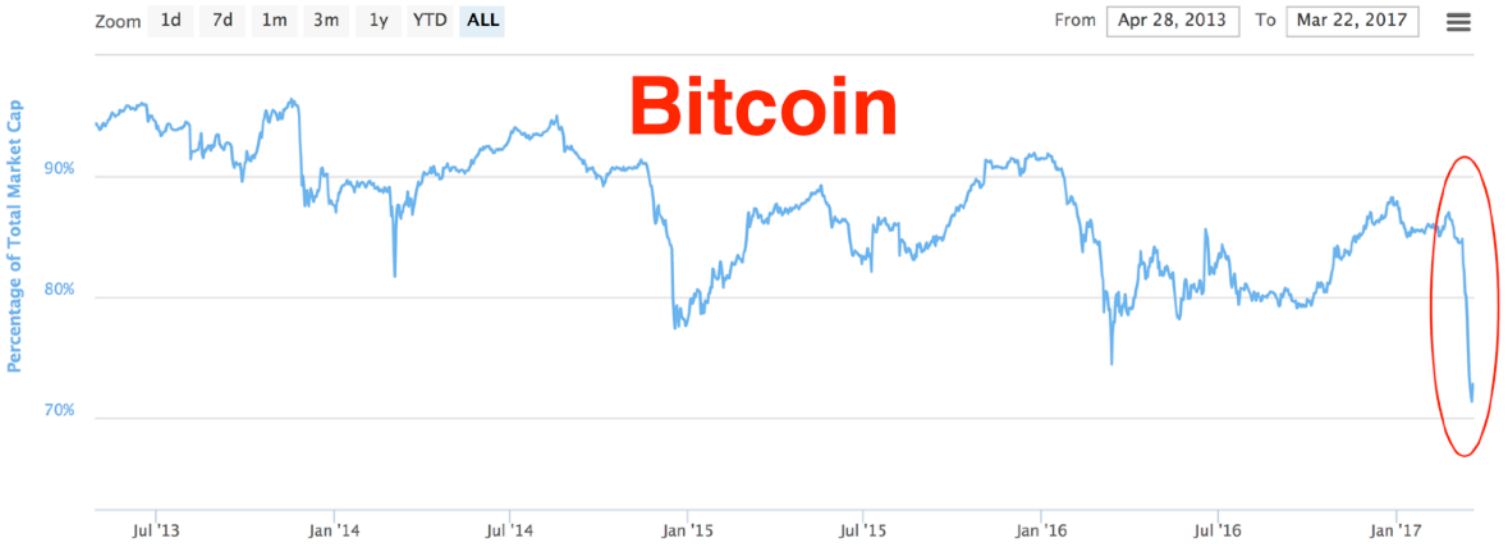
Definition of substitute goods.

- Substitute goods are two goods that could be used for the same purpose.
- If the price of one good increases, then demand for the substitute is likely to rise.

Combined Altcoin Market Capitalization



Bitcoin Percentage of Total Market Capitalization



Bitcoin Core and Blockstream

Advocate for 1MB Blocks
to intentionally create
High Fees
&
Full Blocks

Full Blocks lead to

High Fees

Long Waits

Horrible User Experience

This will result in

Fewer Users

Fewer Nodes

Lower Adoption

Lower Bitcoin market cap

ECONOMICS HELP
HELPING TO SIMPLIFY ECONOMICS

If you get the economics wrong

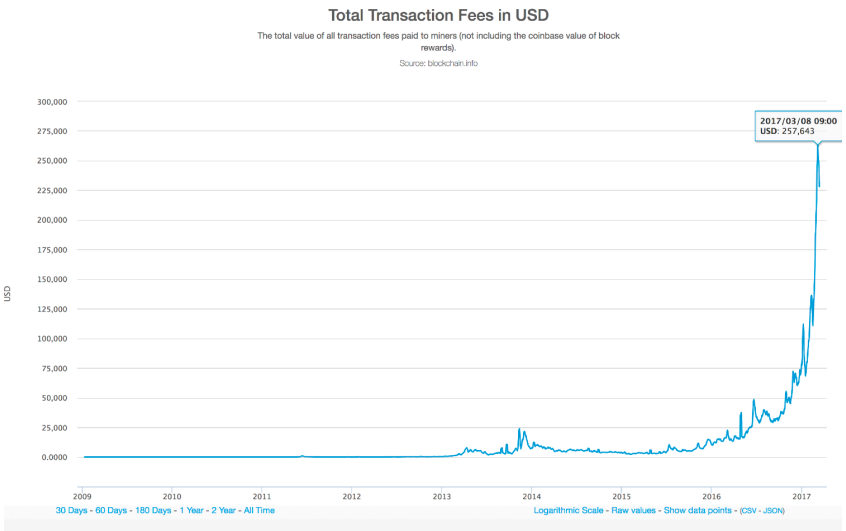
It doesn't matter how good of a programmer you are.

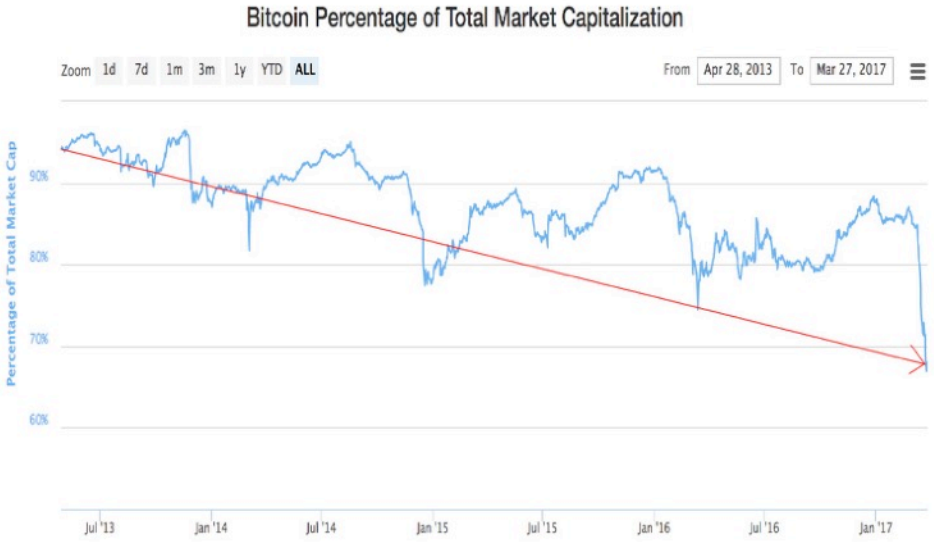
Bitcoin Core

Blockstream

Greg Maxwell, CTO

"I don't think that transaction fees mattering is a failing-- it's success!"





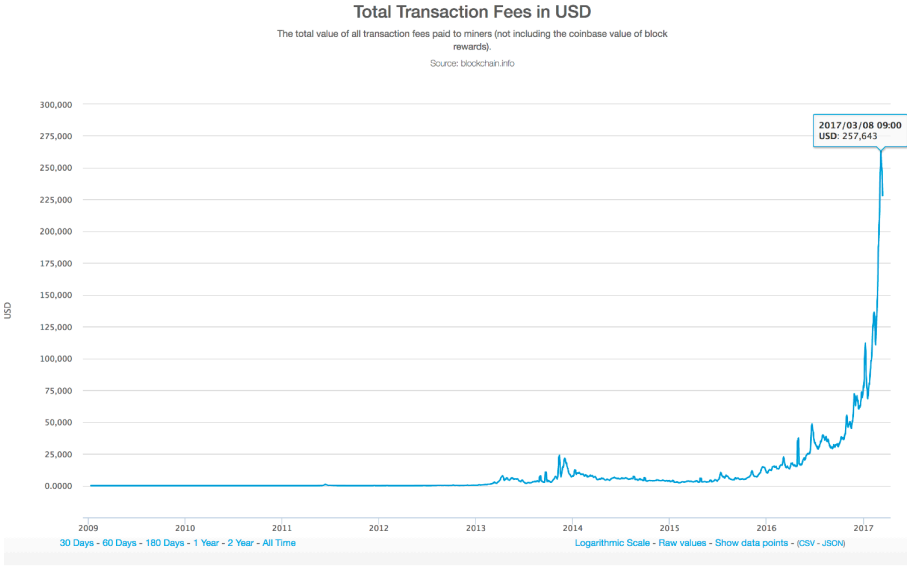
https://www.reddit.com/r/bitcoinxt/comments/3vxv92/peter_wuille_deer_caught_in_the_headlights/cxxfqsj/

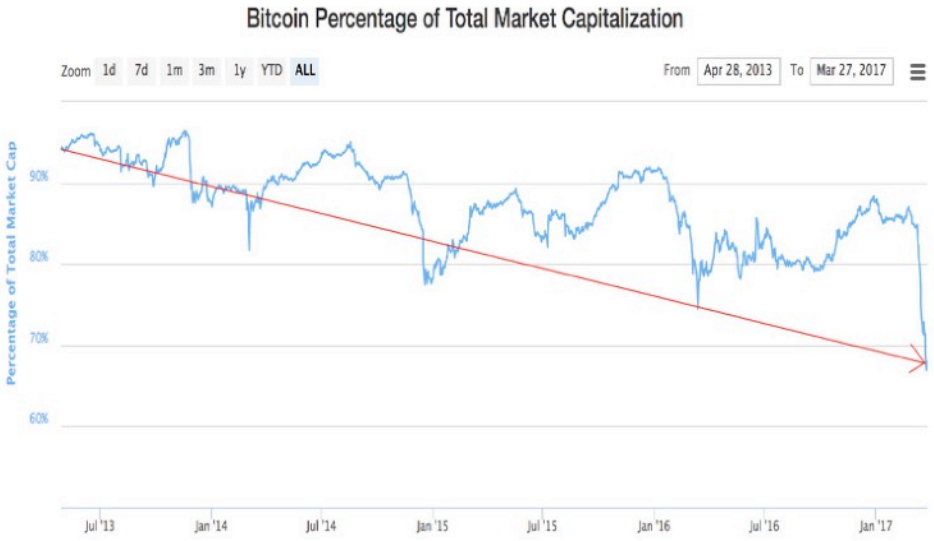
Bitcoin Core

Blockstream

Greg Maxwell, CTO

“fee pressure is an intentional part of the system design and to the best of the current understanding essential for the system’s long term survival. So, uh, yes. It’s good.”





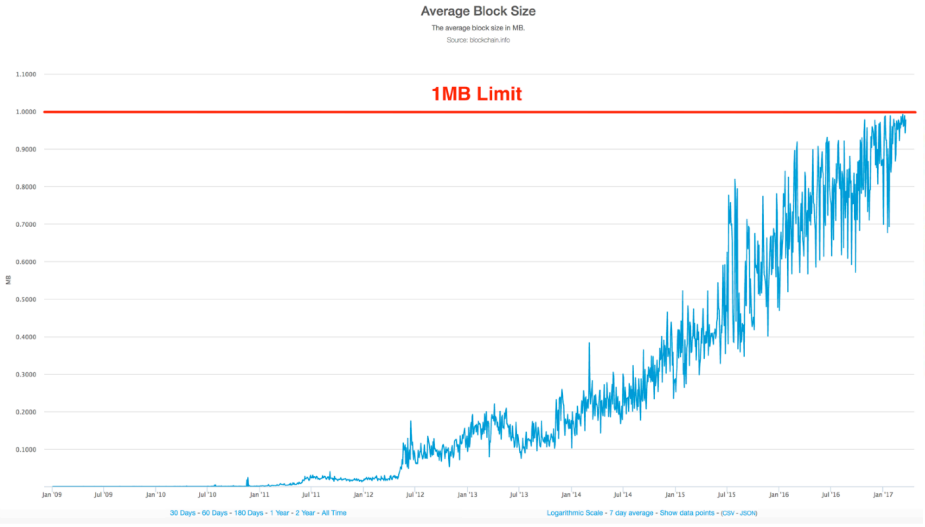
https://botbot.me/freenode/bitcoin-wizards/2016-01-17/?msg=58099943&page=1

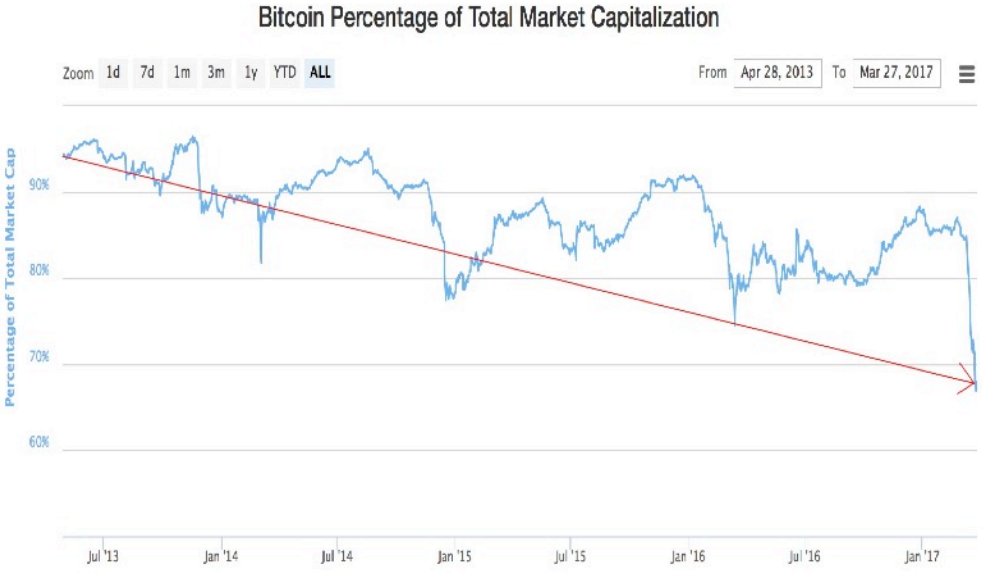
Bitcoin Core

Blockstream

Greg Maxwell, CTO

"There is nothing wrong with full blocks"





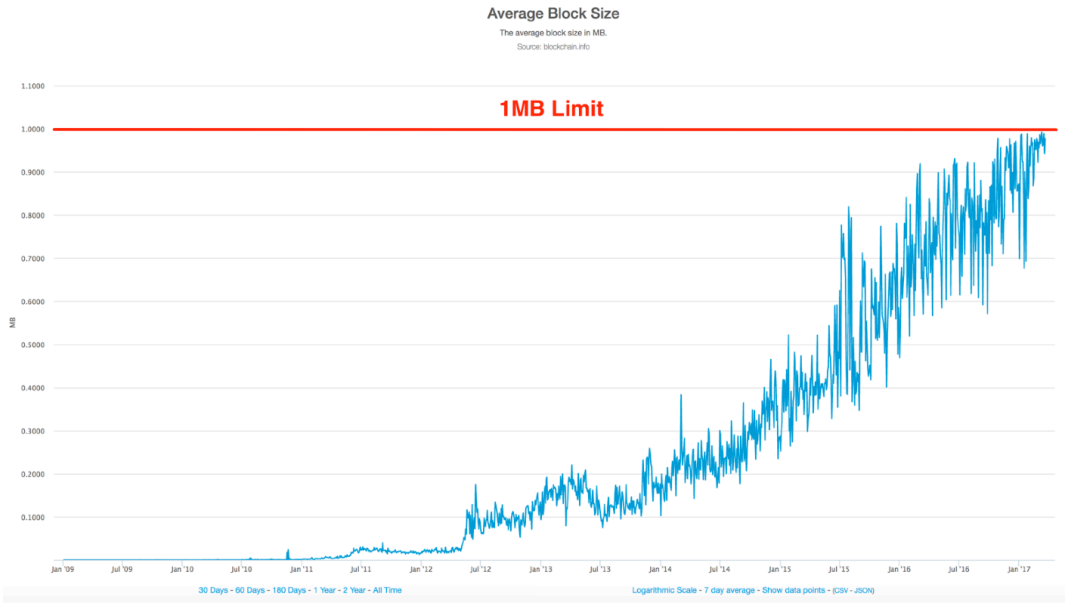
https://botbot.me/freenode/bitcoin-wizards/2016-01-17/?msg=58099943&page=1

Bitcoin Core

Blockstream

Greg Maxwell, CTO

“Full blocks is the natural state of the system”



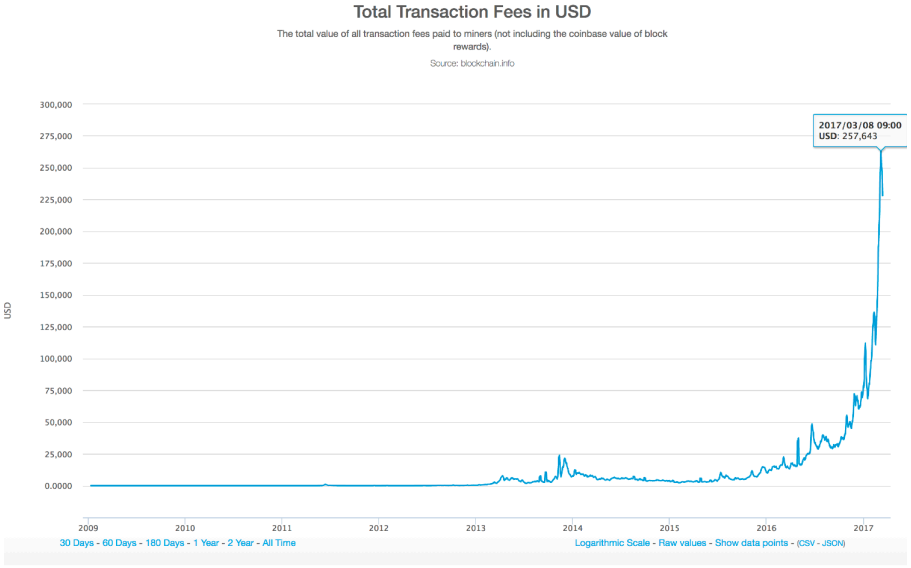
https://botbot.me/freenode/bitcoin-wizards/2016-01-17/?msg=58099943&page=1

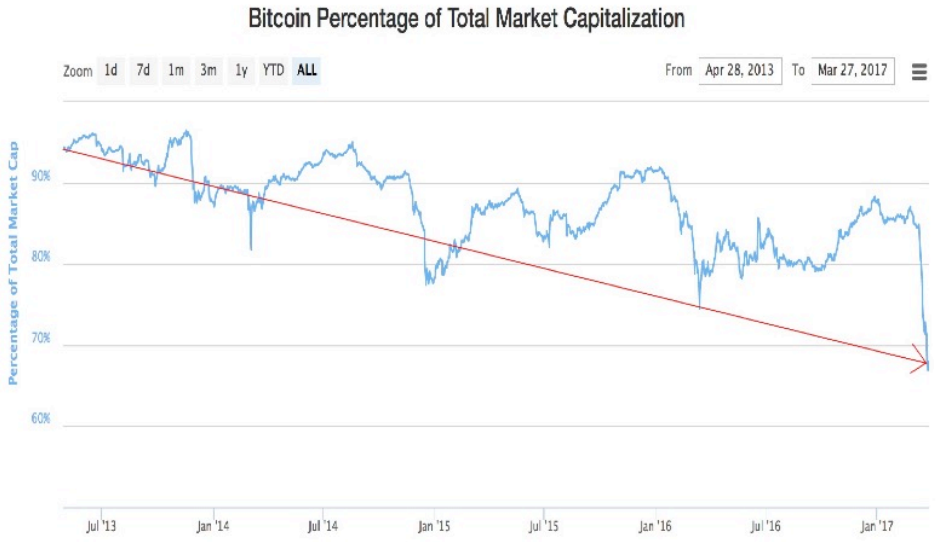
Bitcoin Core

Blockstream

Greg Maxwell, CTO

"There is a consistent fee backlog, which is the required criteria for stability."





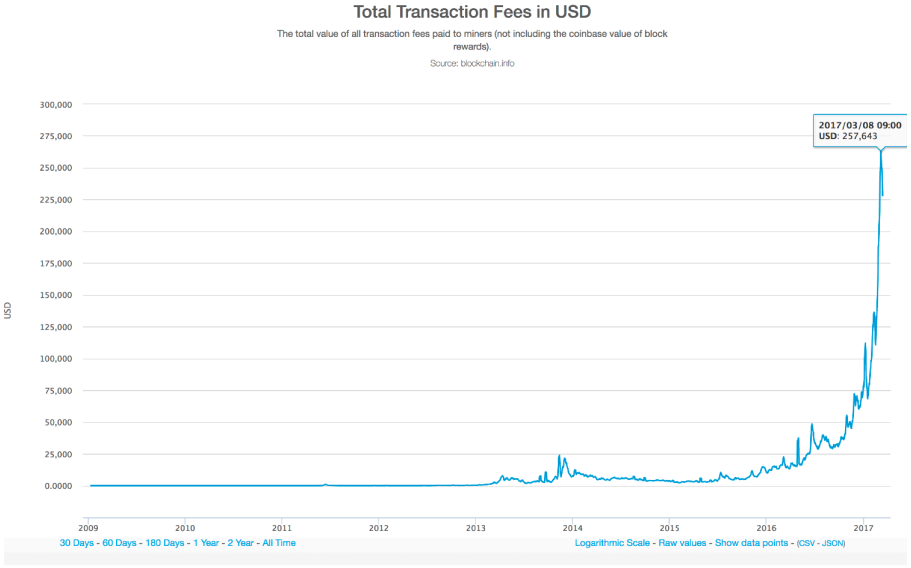
https://www.reddit.com/r/btc/comments/5tzq45/hey_do_you_realize_the_blocks_are_full_since_when/ddtb8dl/

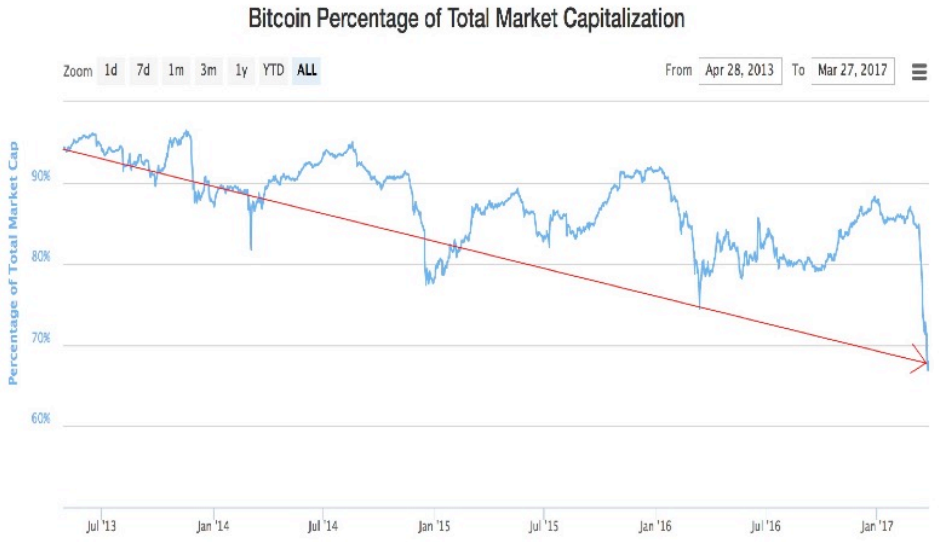
Bitcoin Core

Blockstream

Pieter Wuille

"we - as a community - should indeed let a fee market develop, and rather sooner than later"





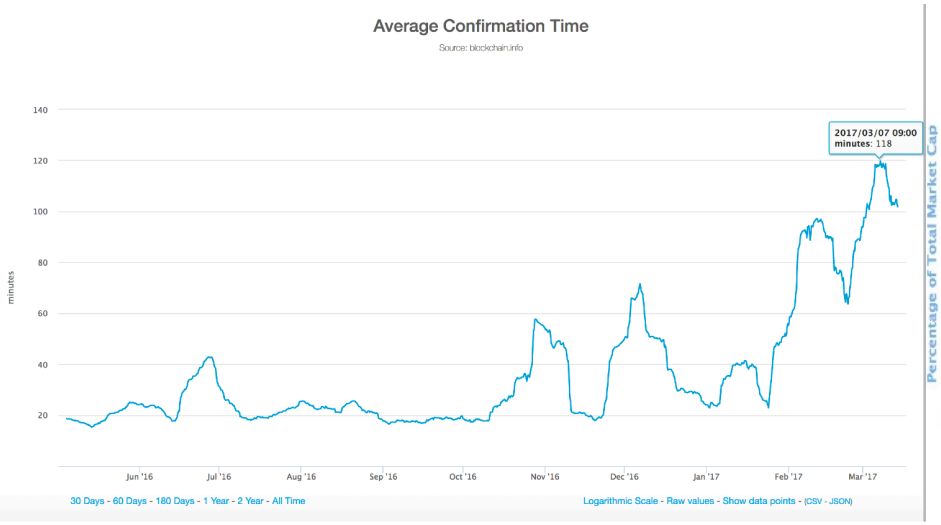
https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2015-July/009515.html

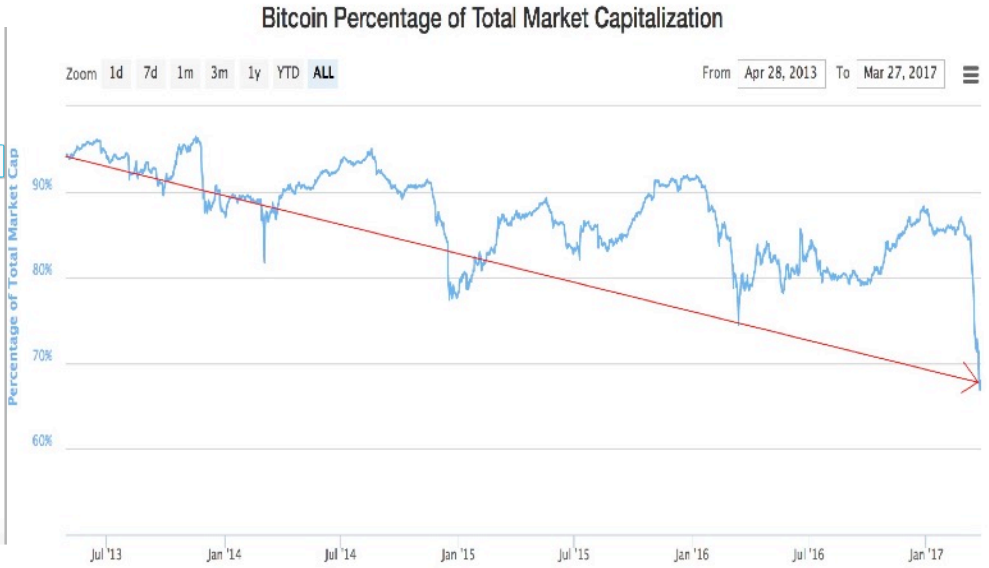
Bitcoin Core

Blockstream

Mark Friedenbach

“Slow confirmation, high fees will be the norm in any safe outcome.”





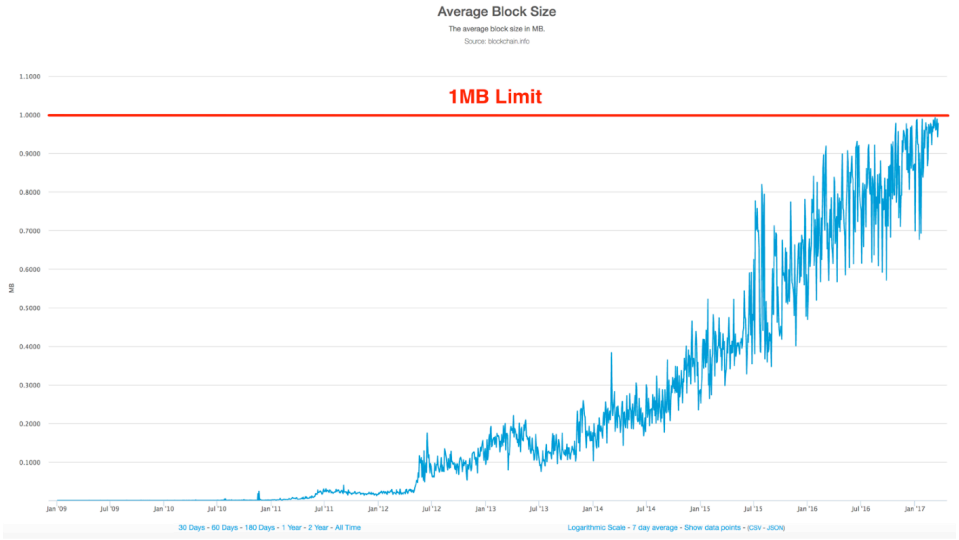
https://www.reddit.com/r/Bitcoin/comments/48zhos/what_happened_at_the_satoshi_roundtable/d0o5w13/

Bitcoin Core

Blockstream

Luke-jr

"Reasonable block sizes currently range from ~550k to 1 MB"



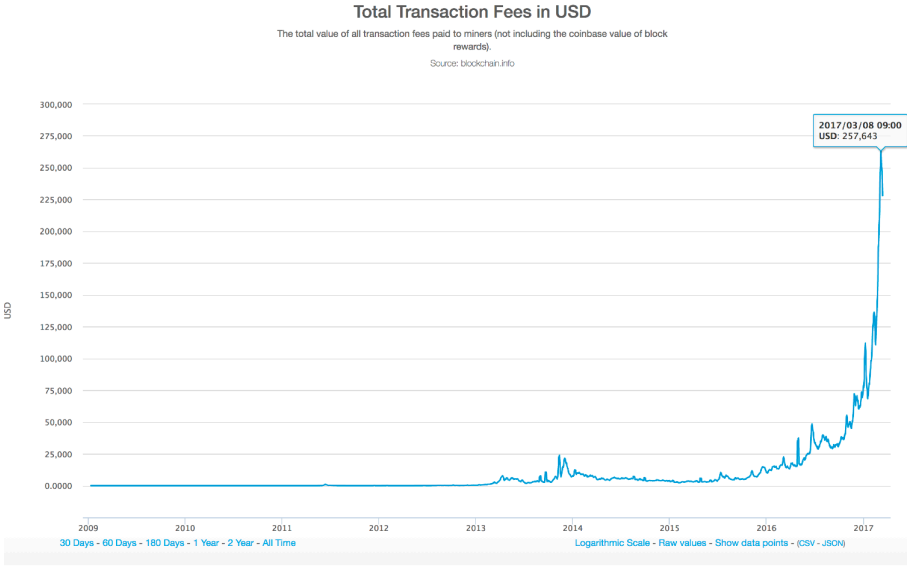
https://www.reddit.com/r/Bitcoin/comments/5fwq1k/the_case_for_compromise_in_the_block_size_debate/daoipml/

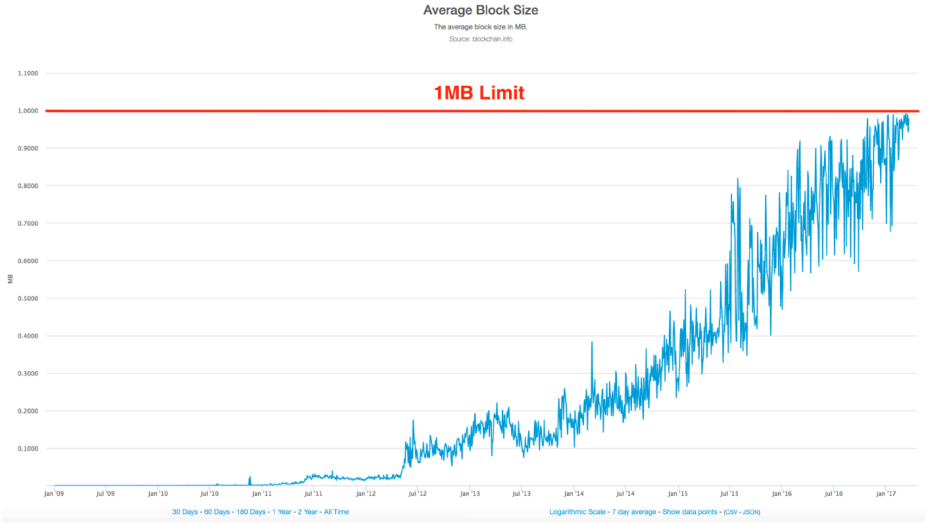
Bitcoin Core

Blockstream

Luke-jr

"It is no longer possible to keep fees low."





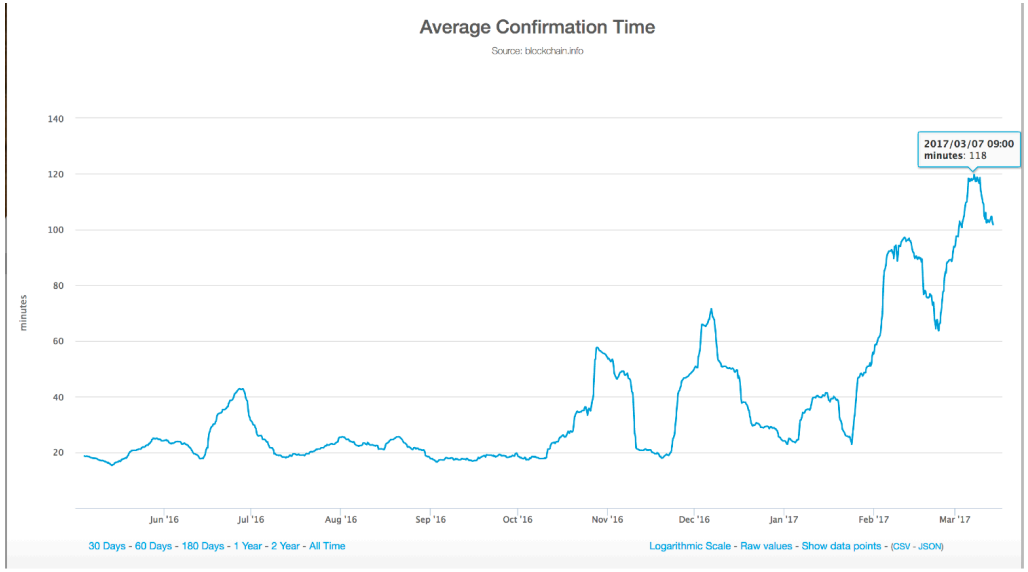
https://www.reddit.com/r/Bitcoin/comments/5fwq1k/the_case_for_compromise_in_the_block_size_debate/daoipml/

Bitcoin Core

Blockstream

Luke-jr

"Just pay a $5 fee and it'll go through every time unless you're doing something stupid."



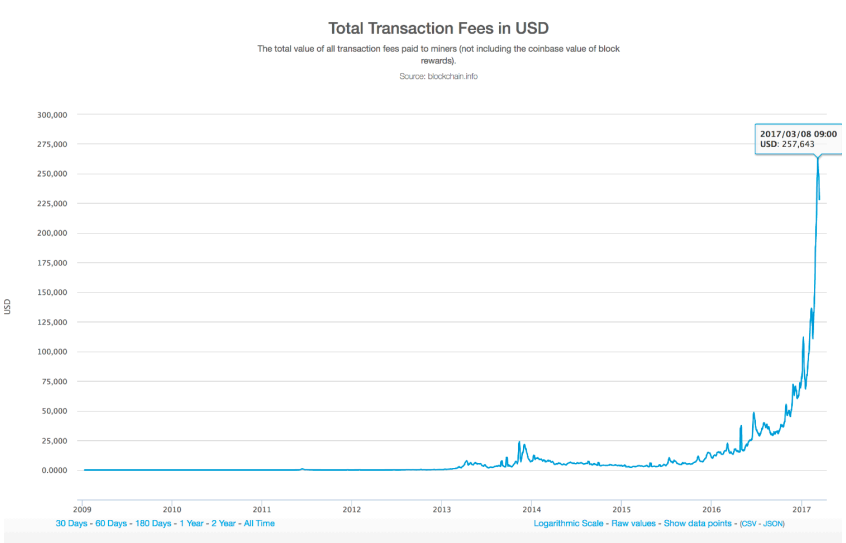
https://www.reddit.com/r/Bitcoin/comments/5rvtzx/75k_unconfirmed_tx_have_suggestion/ddaii2i/

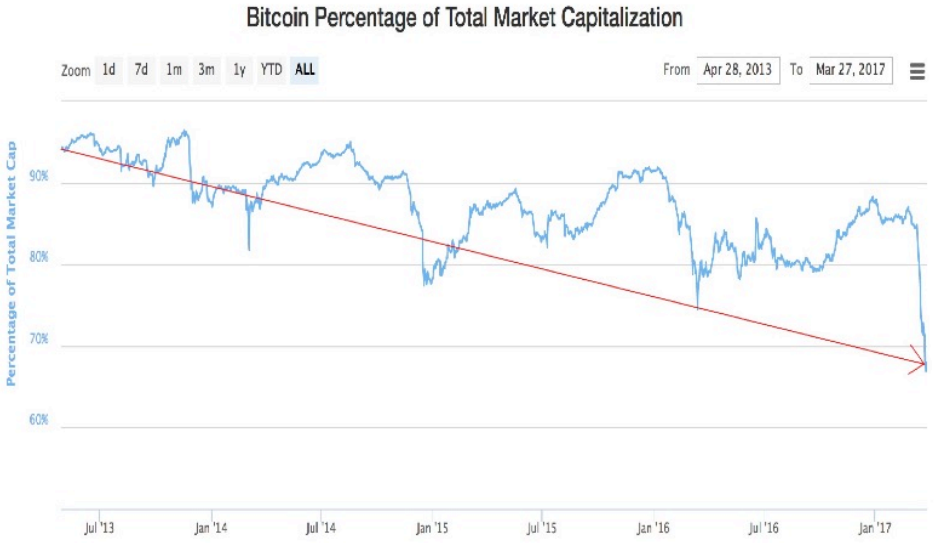
Bitcoin Core

Blockstream

Jorge Timon

"…higher fees may be just what is needed…"





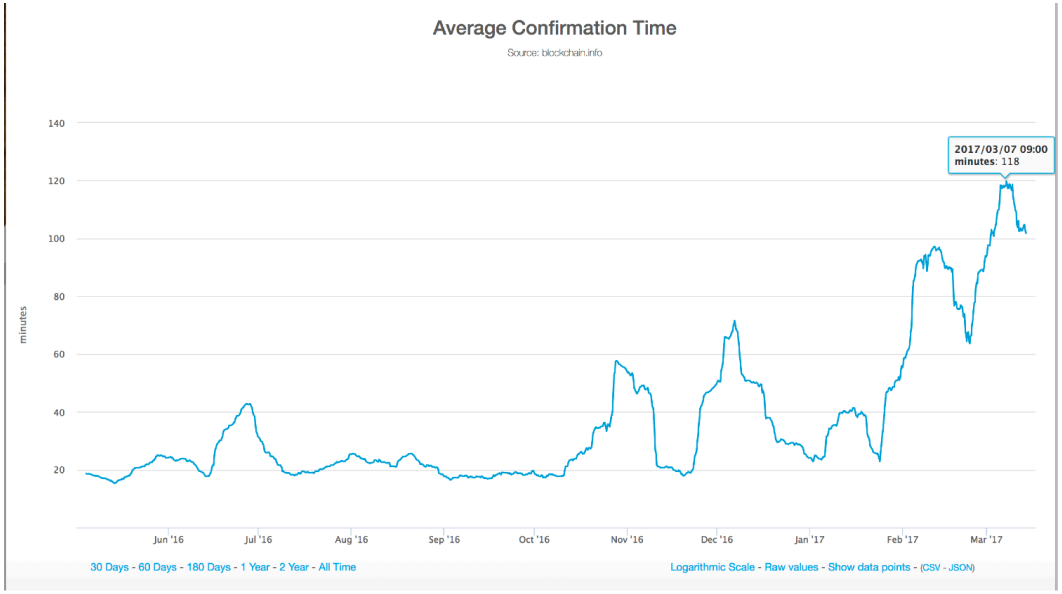
https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2015-July/009792.html

Bitcoin Core

Blockstream

Jorge Timon

"Confirmation times are fine for those who pay high fees."



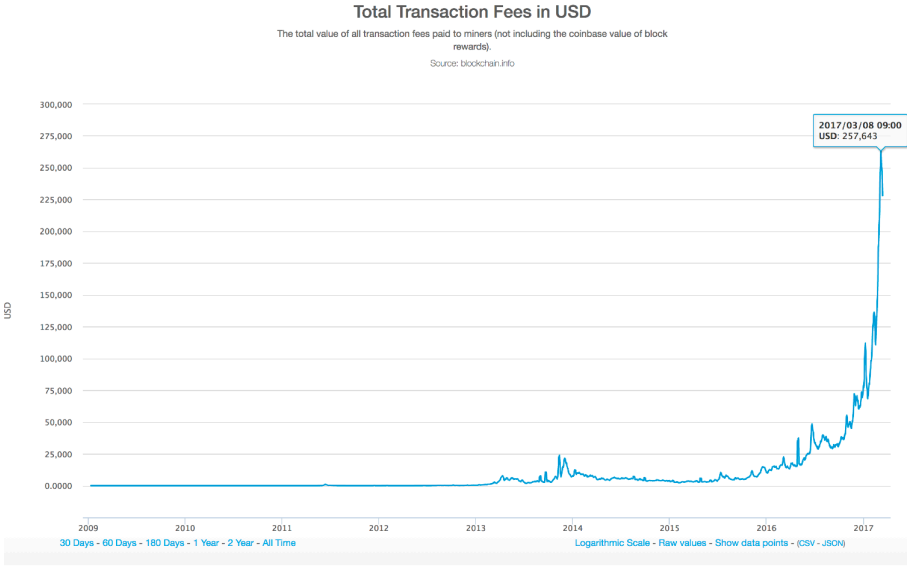
https://www.reddit.com/r/btc/comments/5jtzt6/there_is_a_correlation_coefficient_of_080018843/dbkqpxn/

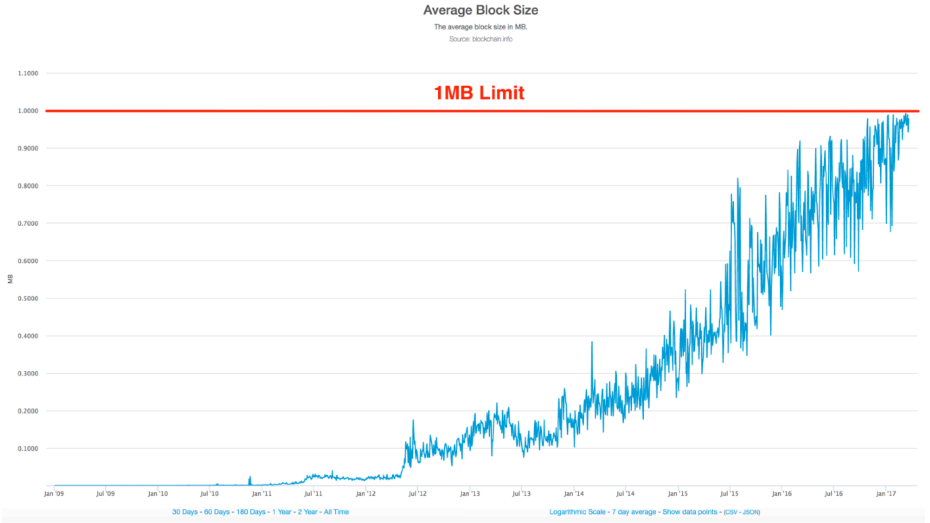
Bitcoin Core

Blockstream

Jorge Timon

“Bitcoin needs a competitive fee market in the long run to sustain pow once the subsidies are gone. I am very happy that we have it now….”





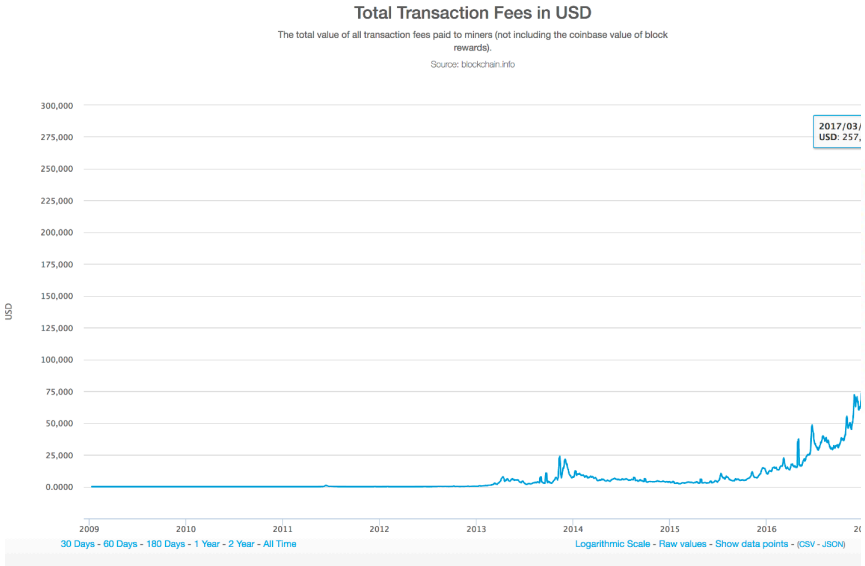
https://www.reddit.com/r/btc/comments/5jtzt6/there_is_a_correlation_coefficient_of_080018843/dbkqpxn/

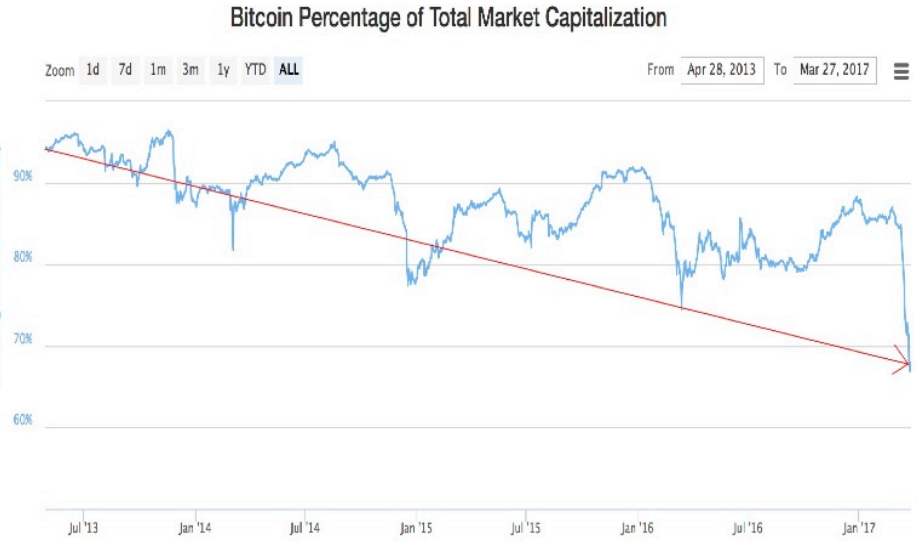
Bitcoin Core

Blockstream

Jorge Timon

"I think Adam and I agree that hitting the limit wouldn't be bad, but actually good for an young and immature market like bitcoin fees."



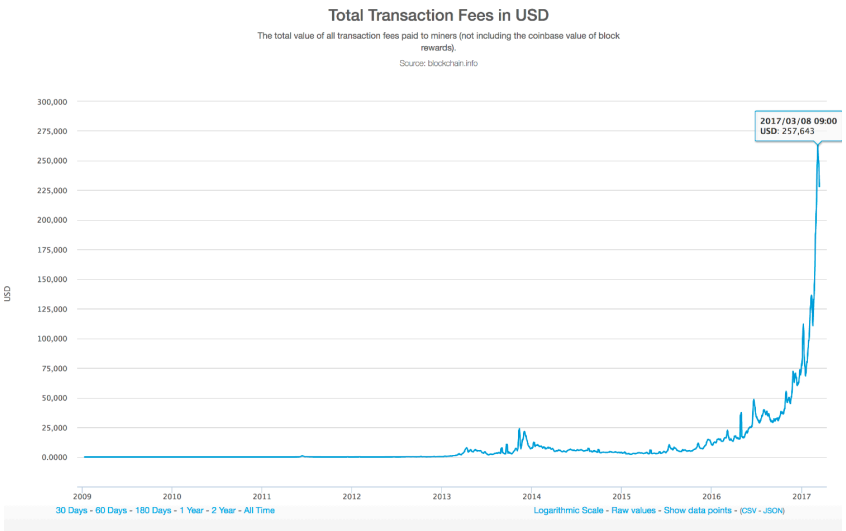


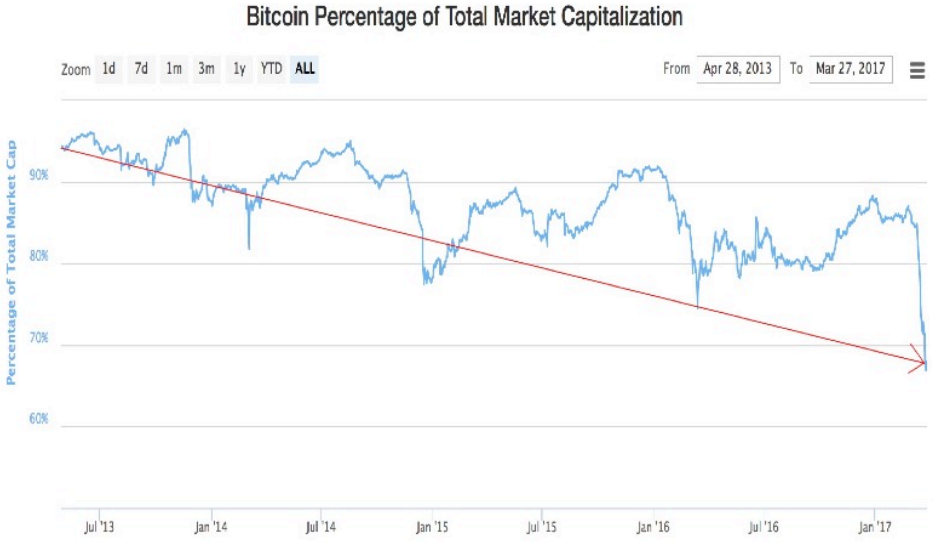
https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2015-July/009804.html

Bitcoin Core

Wladimir J. van der Laan

"A mounting fee pressure, resulting in a true fee market where transactions compete to get into blocks, results in urgency to develop decentralized off-chain solutions."



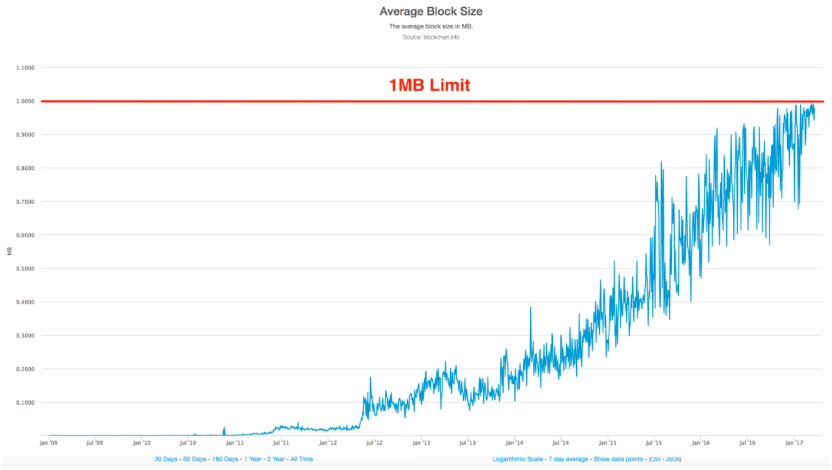


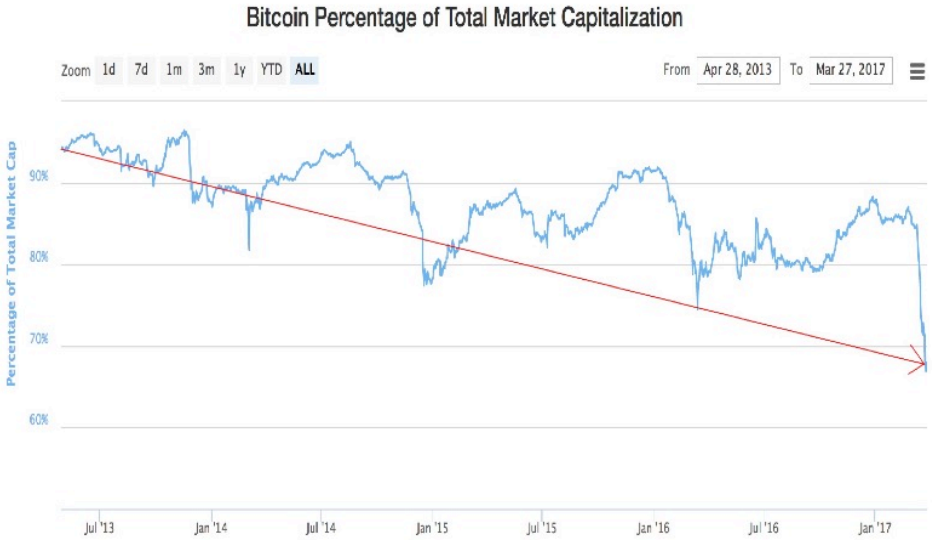
https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2015-May/007890.html

Bitcoin Core

Wladimir J. van der Laan

“ I'm afraid increasing the block size will kick this can down the road and let people (and the large Bitcoin companies) relax…”





https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2015-May/007890.html

What can we do about it?

Bigger Blocks

Lower Fees

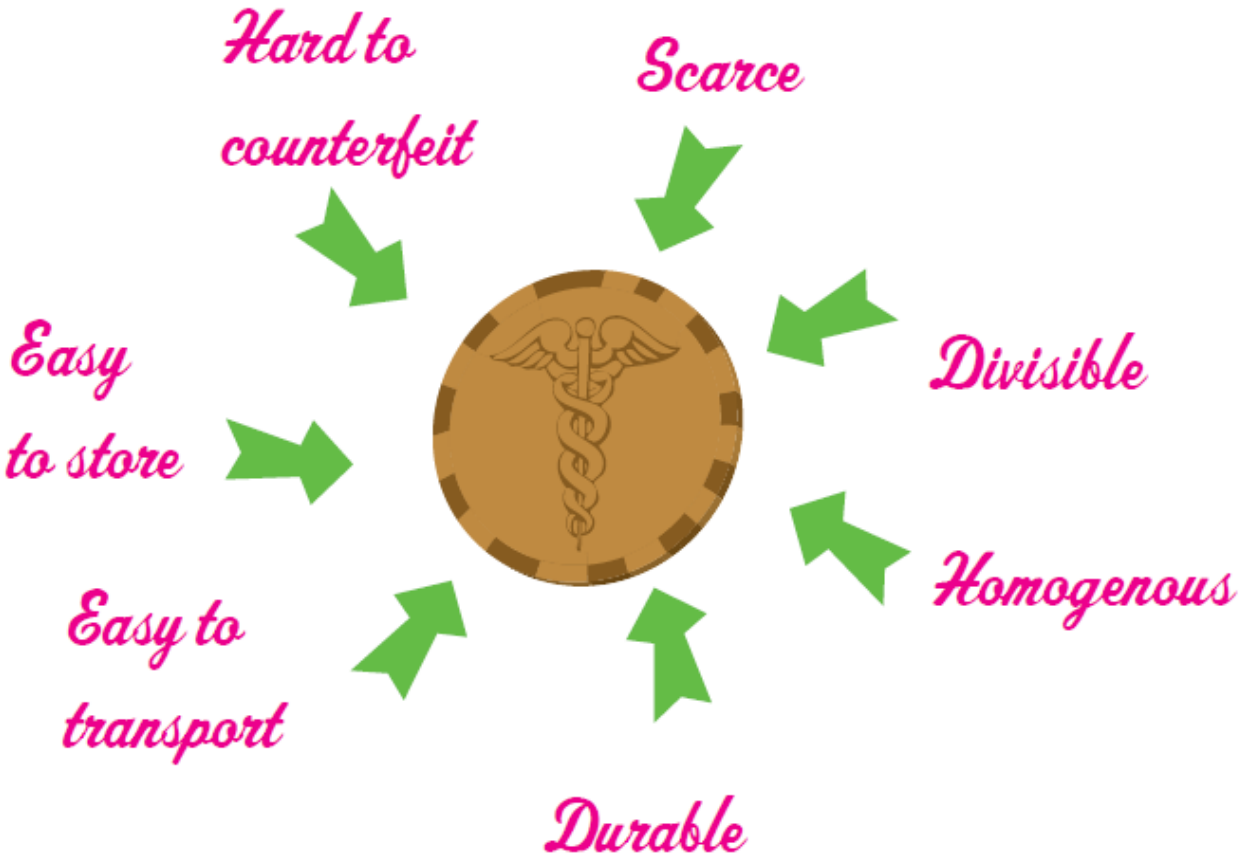
Faster Confirmations

+

Layer 2 Scaling

Bitcoin Unlimited's plan leads to…..

Better Money



Better Money Leads to:

More Users

More Nodes

More Adoption

More Censorship Resistance

Higher Market Cap

Higher price

Roger Ver

World's First Bitcoin Investor

Bitcoin.com

Q & A

@rogerkver

ripple BLOCKCHAIN bitpay

SHAPE SHIFT Purse kraken