ADAMANT
RESEARCH

SIZING UP THE BLOCK SIZE DEBATE

June 2015

INTRODUCTION

In the virtual streets of Bitcoin City, a fiery debate is taking place about whether or not to change financial policy.

One group of developers think that if the protocol is not changed over the coming months, the effects will be devastating for the future of Bitcoin. Meanwhile, another group of developers think that the pain ahead may be a necessary catalyst to bring the cryptocurrency to the next level.

Whatever decision is made by the community, it will have an important effect on the Bitcoin price, and so is worthy of careful consideration.

> "Scheduling an increase to the maximum block size now is a short-term, 'kick the can down the road' fix. It is ugly, but necessary."
>
> GAVIN ANDRESEN
> CORE DEVELOPER
> MAY 5, 2015

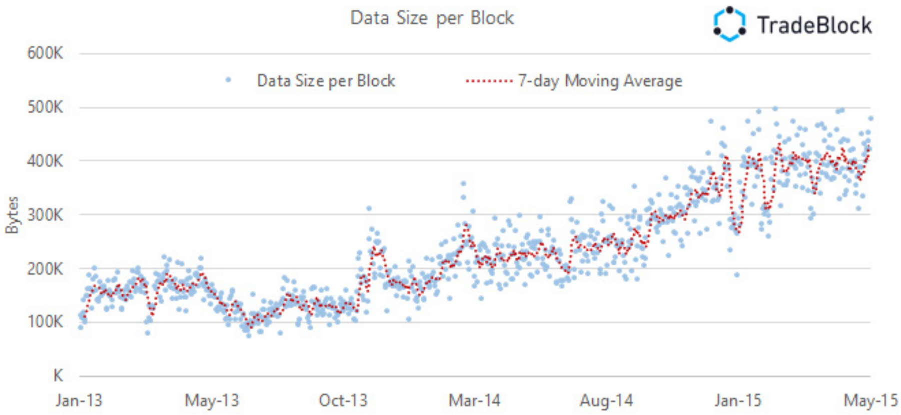
> "...by increasing the blocksize the incentives to actually make Bitcoin scale go away. Even if amazing technologies get built, no one will have any reason to use them."
>
> MATT CORALLO
> BLOCKSTREAM CO-FOUNDER
> MAY 29, 2015

ONE
THE ISSUE OF THE BLOCK SIZE LIMIT

Blocks in the blockchain are like trains for transporting transactions, and a new one arrives every ten minutes. In the early days of Bitcoin, there was plenty of space on the trains. Each block could contain 32 MB of transactions. In 2010, some miners used this feature of the software to broadcast arbitrarily large blocks of meaningless transactions, or *dust spam*. This raised concerns in the community about the possibility of *denial of service* (DOS) attacks that could destabilize the network. Later that year the Bitcoin network was limited to issuing only 1 MB of new transactions every 10 minutes, which amounts to a maximum of 3 to 7 transactions per second.[1]

Now that the average transaction block size has gone up from 0.2 MB in 2014 to 0.5 MB in 2015, it looks like we'll probably hit the limit in the next 6 months already. So what should be done going forward? The two most discussed options are either to leave the 1 MB limit intact or to increase the limit to something like 20 MB.

This discussion is important for investors because if the network approaches the 1 MB limit before the Bitcoin economy is ready for the transition to fee-based transactions, then—as core developer Mike Hearn argues—Bitcoin software could freeze due to huge confirmation times, rejected transactions, and a ballooning transaction backlog.



In early 2013, Bitcoin block sizes never exceeded 0.2 MB. This grew steadily, and by early 2015 the block size regularly started hitting levels of 0.5 MB. (source: tradeblock.com)

"I'm curious as to what discussions people have seen; e.g., are people even here aware of these concerns? Are you aware of things like the hashcash mediated dynamic blocksize limiting? About proposals like lightning network? Do people think a future where everyone depends on a small number of "Google scale" node operations for the system is actually okay? (...) I think not"

GREGORY MAXWELL
CORE DEV, MAY 7, 2015

"How do you think ordinary Bitcoin users would react on hearing of crashing nodes, a swelling transaction backlog, a sudden spike in double spending, skyrocketing fees? They would conclude that the Bitcoin developer community was incompetent. [...] the overload would eventually go away .... because the users would go away. The backlog would clear. Fees would fall to the minimum again. So life would go on. Bitcoin would survive. But it would have lost critical momentum. It would have become the MySpace of digital currencies."

MIKE HEARN
CORE DEV, MAY 7, 2015

[1] *7 is the popularly cited number, but because of the growing number of larger transactions, it is probably closer to 3 transactions per second. Armory's Alan Reiner mentions tests that show certain types of transactions run into trouble already when the network propagates only 400-600 KB worth of transactions.*

WHY IS THIS DEBATE SO FIERCE?

Increasing the block size limit comes at a two-fold price. The first cost is that it makes running the Bitcoin software require more memory (i.e. it would be more expensive), which would result in less nodes in the network and a relatively less decentralized and less secure Bitcoin network. The second cost of a limit increase is that it removes scarcity of capacity on the Bitcoin blockchain. This means that Bitcoin miners would barely be able to generate income in the form of transaction fees and so would have to rely solely on block rewards of new bitcoins. Over time, this puts pressure on mining revenues and on the hashrate of the entire network, thus weakening the network's security compared to how it would be with a smaller block size. **In sum, every time the block size limit is increased, it makes the Bitcoin network less robust and less decentralized.**

Some proponents of a block size increase think it should be increased indefinitely. However, most acknowledge the validity of the aforementioned concerns and side with core developer Gavin Andresen, who says, "Scheduling an increase to the maximum block size now is a short-term, 'kick the can down the road' fix. It is ugly, but necessary."

There are also developers who are against an increase of the block size limit; they see the Bitcoin blockchain as a value anchor which should offer the highest security possible with a network of sidechains offering various security and functionality trade-offs layered on top (for more on this, see our forthcoming report *Sidechains: Bitcoin's Batman?*).

OPINIONS MIXED ON WHETHER LIMIT WILL BE RAISED

On May 16, I organized a poll in my network and received responses from CEOs and managers of Bitcoin companies (their companies have raised a combined total of $150M in VC investments), industrial Bitcoin mining operations (together representing about 12% of the network), and core developers with a combined 1,400 commits to the Bitcoin protocol.[2]

The **entrepreneurs** I contacted, as well as the VCs, were unanimous: they think the block size limit will be increased, and their average estimate of when that will happen is December 2015, with 90% of responses falling between July 2015 and March 2016.

The **core developers** were more nuanced in their responses, with a 'yes, but' as the dominant answer. Here's an email excerpt, with bolded emphasis added:

> *I have my doubts whether it will be possible to get the necessary consensus in the community. [...] Changing a fully decentralized consensus system means that *everyone* that participates by running a node needs to agree. This will be* ***more than a year away, at least****. Once everyone agrees that changing the block size is the way to go, a block number will be planned at which the transition is to happen. Before that block everyone*

"There are lower risk approaches to increasing blocksize to get breathing room for better scalability. [...] A miner enforced modest blocksize increase is maybe a lesser evil than the risk of a non-consensus hard-fork that risks a splitting the network, if it really is the case that people don't understand the danger."

ADAM BACK
INVENTOR OF BITCOIN MINING
MAY 31, 2015

"I'm very uncomfortable with this block size limit rule. This is a 'protocol-rule' (not a 'client-rule'), what makes it almost impossible to change once you have enough different softwares running the protocol. Take SMTP as an example... it's unchangeable."

'CAVEDEN'
ON BITCOINTALK.ORG
NOV 10, 2010

"My prediction is that the block size limit will probably never be abolished, but will be constantly pushed up by a factor of two as amount of transactions approaches the limit. Maybe after a couple of updates, people would decide that it's safe to abolish the limit completely if it is cheaper to account for it, than to have uncertainty of a hard fork."

OLEG ANDREEV
SOFTWARE DESIGNER
FEB 22, 2015

[2] *Mining stats based on these estimates: http://organofcorti.blogspot.dk/2015/05/may-24th-2015-block-maker-statistics.html.*

> *has to upgrade their software, so this cannot be short-term.*

A Bitcoin mining analyst was more optimistic (bolding added):

> *I'm going to guess **May 2016** - that should be enough time to: a) Implement methods to handle utxo space increases. b) Have a clear block size increase implementation plan available. c) Get general agreement to follow the block size increase fork.*

Upping the block size limit requires a hard fork of the Bitcoin protocol, which means that for the network to upgrade, a consensus among the Bitcoin miners is required—if half of them upgrade, and the others don't, there will be two separate blockchains operating independently which creates economic and security concerns.

The feedback received from **Bitcoin miners** was mostly in favor of an increase in the block size limit. One miner wrote:

> *I think it will need to be increased after the block halving next year, I see that as a major shakeup of the mining industry, after that has happened the miners will be doing all they can to get more fees into a block.*

A mining pool operator commented:

> *I think there won't be any problem with the fork. The majority will simply follow the consensus of core devs because the topic itself is actually pretty uncontroversial. [...] As the fees are not main income, it's not an issue yet. Actually I think miners will welcome raising the maximal current *limit* of 1 MB, because it just adds a *opportunity*, not a *requirement* to create larger blocks. The actual size can be configured by miners (pools).*

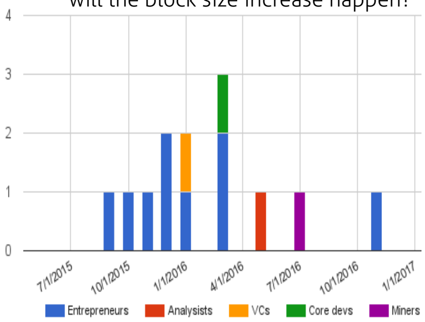
A dissenting voice came from an entrepreneur running an industrial mining operation (emphasis is mine):

> ***I'm not convinced that we should starting acting like a central bank here and start mucking around with the system**. [...] Arbitrarily deciding to hard fork in order to raise the block size limit would be such a move. Right now, the Bitcoin mining community generally takes the recommendation of the core devs on face value - if they want to implement a BIP [Bitcoin Improvement Proposal], we will generally take it. If we wait until block size limitations are clearly causing a problem, whoever is impacted most by that problem will promote the uptake of a particular change. **Large industrial miners and large pools make up the consensus, so ultimately we have that decision power**.*

This skepticism was echoed in an interview by BTCChina's director of engineering Mikael Wang (BTCChina's mining pool represents 10% of the network):

> *"A very large block size would be problematic for miners because the network bandwidth between China, where the majority of mining is done, and rest of the world is heavily restricted. Important proposals like these*

"In what month and year
will the block size increase happen?"



Source: Adamant Research network poll, May 17, 2015

"I'd prefer a more gradual increase, but overall I'm in favor. It's just a temporary hack, but 1MB is too low, and this will give us some breathing room while working on more permanent solutions."

MENI ROSENFELD

BITCOIN DEVELOPER
MAY 12, 2015

"I'm unconvinced that hitting the limit soon will be a tragedy: maybe a more healthy fee market develops, maybe people finally implement and deploy some form of payment channels."

JORGE TIMÓN

CORE DEVELOPER
MAY 19, 2015

> *need to factor in all of the nuances of the global landscape."*

Chun Wang, associated with the mining pool Disqus Fish (21% of the network), made his opinion clear in a recent comment:

> *I oppose 20MB because I estimate it may increase the overall orphan rate to an unacceptable level. 5MB, 8MB or probably 10MB should be ok.*

RECENT DEVELOPMENTS

On May 29, Gavin Andresen announced that he plans to move forward by helping Mike Hearn's Bitcoin-Xt client software simulate and implement "a big [block size] increase now that grows over time." He continued:

> *I'll then ask for help lobbying the merchant services and exchanges and hosted wallet companies and other bitcoin-using-infrastructure companies (and anybody who agrees with me that we need bigger blocks sooner rather than later) to run Bitcoin-Xt instead of Bitcoin Core, and state that they are running it. We'll be able to see uptake on the network by monitoring client versions.*

Once there are indications of success, Andresen plans to approach Bitcoin miners to convince them to implement the upgrade "to (hopefully) get a majority and then a super-majority willing to produce bigger blocks."

The request to upgrade to Bitcoin-Xt has so far been refused by BTCChina's mining pool, the position of other miners is still unclear to me.

MOST LIKELY OUTCOME

Considering the polarization among developers and the concerns voiced by the Chinese Bitcoin mining community, it's likely the outcome will be a compromise.

I think Gavin Andresen's proposal to raise the block size limit to 20 MB will be softened (the dynamic block size limit may also be dropped), and the eventual BIP will settle on a lower limit, such as 8 MB. This compromise could help all parties feel like they've been heard. I anticipate that the block size limit increase will be implemented into the blockchain in spring 2016.

"I'm confident that there are no technical barriers to scaling up--I've shown [...] that our current code running on tomorrow's hardware would be able to handle the growth I'm proposing."

GAVIN ANDRESEN
CORE DEVELOPER
JAN 20, 2015

"A hard-fork that is not an obvious clear consensus is actually existentially dangerous for bitcoin, splitting the network in two with conflicting and rapidly diverging ledgers ends in disaster. Clearly no one wants that to happen."

ADAM BACK
INVENTOR BITCOIN MINING
MAY 31, 2015

"I have been talking to well known people and CEOs in the Bitcoin community for some time now. *All* of them support bigger blocks, this includes: 1) every wallet developer I have asked (other than Bitcoin Core) 2) So far, every payment processor and every exchange company."

MIKE HEARN
CORE DEVELOPER
MAY 29, 2015

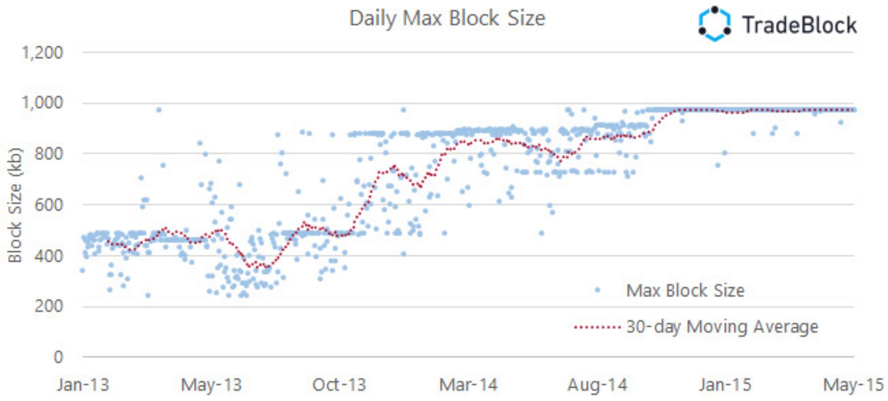
TWO
IMPACT ON THE BITCOIN PRICE & ECOSYSTEM

In this section, we take a look at Bitcoin's capacity limits, when they could be reached, and which players in the ecosystem could be most affected by a capacity crunch. We'll close with some thoughts about potential outcomes on Bitcoin and altcoin prices.

HOW SOON COULD THE BLOCK SIZE LIMIT BE REACHED?

The team at TradeBlock.com has come up with some useful observations with regards to current block sizes on the Bitcoin network:

> *The proportion of large blocks (defined as 725 KB or more) has been climbing steadily since last year, reaching an average of 20% of daily blocks, occasionally as high as 40%.*
>
> *While [the current 7 day moving average of] 425 KB is well below the 1 MB cap, that average figure doesn't quite offer the full picture. As shown in the chart below,* ***the maximum block size was reached an average of more than four times per day so far in 2015, meaning at least some otherwise-acceptable transactions are seeing delayed confirmations due to capacity issues on the network 3% of the time since the beginning of the year.***



Given that even today the Bitcoin network sometimes experiences delayed transactions as a result of the block size limit, it is likely that some businesses relying on fast transaction times are already affected by this, or will be soon.

"To say 'there is no time' is just FUD. We haven't even started to see a transaction fee market, or delays for transactions paying a low fee. I actively monitor this by sending all my bitcoin transactions without a fee - to date, every single one of them was mined in the very next block. [...] Blocks are maybe half full on average, and that is with miners neglecting spam filtering - if they start doing their job, we have even more breathing room."

LUKE DASHJR

FOUNDER ELIGIUS MINING POOL
MAY 8, 2015

"As we approach 100% full, the first thing that happens is that confirmation times start to become huge. According to Monte Carlo simulations by Dave Hudson, at 80% full half of all transactions take around 20 minutes to confirm. At 100% full half of all transactions should wait longer than 6 hours."

MIKE HEARN

CORE DEVELOPER
MAY 7, 2015

Still, for the network to suffer the extreme transaction delays as predicted by Mike Hearn and others, we'd probably need to see a large percentage of blocks per day reach the 1 MB limit. Based the historical 275% annual growth trend, TradeBlock predicts the maximum level of 2.8 transactions per second to be reached by December 2016.

It's important to keep in mind that volatility in block size growth has been high and so a 50% or 75% growth spurt over a period of one or two months is a scenario to take into consideration.

MAIN SOURCES OF BLOCKCHAIN BLOAT

It may come as a surprise to some that most of the block capacity on the blockchain is *not* used for investing or retail purchases. Most transactions come from faucets, spammers, Bitcoin casinos, and mixers.

Faucets are websites that feature a lot of click-based advertising and that pay out a few cents worth of Bitcoin to anyone who visits the site and gives them a Bitcoin address or sometimes an email address.

Bitcoin spammers are people who send even smaller transactions (like 0.00000001 BTC), dubbed *dust transactions*, to popular addresses in order to expose everyone looking at that address to an advertising message embedded in the transaction. It is rumored that this is a technique that is also used by agencies and corporations to try to decipher who owns which clusters of bitcoins.

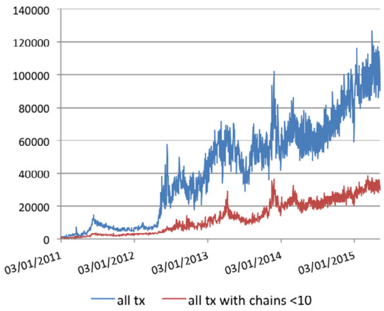
While faucets and spammers may contribute to the problem of blockchain bloat, I suspect they are not strong drivers of demand for Bitcoin. For example, with only 1 BTC I can send 100 million spam messages or hand out cents of Bitcoin to over 150,000 faucet visitors. I think the next two sectors of heavy blockchain users have a more significant impact on the Bitcoin price: casinos and mixers.

Players in Bitcoin casinos are attracted by ease of access, relative anonymity, quick cash payouts, and the increased probability of fairness (anyone can verify how much the house keeps of every bet). And they are popular: cryptocurrency news websites confirm that Bitcoin casinos are the companies with the largest advertising budgets. Review website www.thebitcoinstrip.com lists over 100 Bitcoin gambling sites, double that of a year ago, with a combined total daily volume of around $100 million—higher than the volumes of all major Bitcoin exchanges combined.[1] One of the more popular casinos, PrimeDice, reports over 9 million bets placed in 24 hours, and close to 2 million bitcoins distributed over that time. These are significant transaction volumes!

Bitcoin mixing services provide a method for people to protect their privacy, often to avoid getting caught buying illicit goods online. Heavy mixer users will buy bitcoins from an exchange, launder them using the mixing service, and then spend their anonymized bitcoins in the *darknet markets*

> "Bitcoin's best chance right now may well be to keep its block size limited and target the niche of digital gold. If that is what Bitcoin users want, then they should keep the limit, and perhaps even decrease it. But if Bitcoin users want to be a payment system, then up it must go."

VITALIK BUTERIN
FOUNDER ETHEREUM
JUN 1, 2015



Source: Adamant Research

In the spring of 2012, Bitcoin's first gambling game Satoshi Dice became popular, and that reflected in a massive growth of large sized transactions. Ever since, it's likely been the Bitcoin gambling sites who have been weighing the most on the size of the blocks.

> "Bitcoin as the ideal casino chip? Possibly. It provides a high level of user privacy, immediate access to funds and irreversibility — to the casino's and player's benefit. Online casino startups are embracing Bitcoin, primarily for its ease of crossing national borders, absence of multiple currency conversions and lack of restrictions that banks or credit card companies may place on users for online games of chance."

PwC
2014 REPORT "DIGITAL DISRUPTOR
"

[1] *See PWC's February 2014 report on Bitcoin, page 10: http://tinyurl.com/pwcBitreport. For volumes I used at tradeblock.com.*

(which are bazaars on the hidden Internet for the trade of illegal goods and services).

The first and most infamous darknet market, The Silk Road, was raided by the FBI in November 2014 and shut down. Yet during its short existence it gave a strong signal to budding black market entrepreneurs. *The Hidden Wiki* now lists over 50 commercial services on the dark web, as well as over 30 websites that offer financial services. Traceable darknet markets drug listings have more than doubled since 2013.

To service these platforms with anonymous crypto-cash, there are at least seven popular Bitcoin mixing services available. This list includes www.sharedcoin.com, one of the more popular mixers. One study from September 2014 took a sample of 20,000 Bitcoin transactions and identified 2.6% of them as Shared Coin transactions.

"[Drug] vendors now have the opportunity to utilise banner adverts that are placed on Grams, a Dark Net search engine styled on Google. [...] with the creation of its news TorAds and Gramswords services it is set to gain advertising revenue that will help it to consolidate its place as the go-to search engine for darknet markets."

GLOBAL DRUG POLICY OBSERVATORY
JAN 2015

WHAT WILL HAPPEN IF BITCOIN BLOCKS ARE AT FULL CAPACITY?

If the blocks reach full capacity before there is a functioning transaction fee market in place, Bitcoin investors will likely see the price drop and may experience difficulty withdrawing their coins from an exchange. Elsewhere in the Bitcoin economy, problems could be much graver: casinos that literally stop functioning, coin mixers screeching to a halt, and coin faucets that run dry.

Faced with these difficulties, entrepreneurs running these services would likely set up working alternatives by moving away from the Bitcoin blockchain. This in turn would make the average block size drop significantly, thus **clearing up space for normal transaction confirmation times in the network**.

The process of gambling and laundering services moving away from the Bitcoin blockchain could cause **a series of rallies in the altcoins** (of which we may already be seeing the start). Shared Coin, for example, includes any fees within their transactions so that users can get quick access to their laundered coins. If the block size limit is reached, transaction times will be slower, and these users may switch from Bitcoin to altcoins.

It's likely that for gambling and mixing, the most liquid altcoins will be those highest in demand: Litecoin, actively traded in at least 17 markets, and Dogecoin, actively traded in at least 7 markets.[3] Privacy-oriented coins such as Dash and Monero could see significant rallies. The short history of altcoins suggests that when the most liquid coins rally, the rest are lifted with the tide, resulting in short-lived but strong rallies.

"The block size is also not just an economic policy. It is the compromise the _network_ chooses to make between utility and various forms of centralization pressure, and we should treat it as a compromise, and not as some limit that is inferior to scaling demands. I personally think the block size should increase, by the way, but only if we can do it under a policy of doing it after technological growth has been shown to be sufficient to support it without increased risk."

PIETER WUILLE
CORE DEVELOPER
MAY 28, 2015

[3] http://worldcoinindex.com/volume#altcoin — currency pairs with over 10 BTC in volume on May 26, 2015. Volumes in Litecoin may be overstated due to inacurate reporting from Chinese exchanges.

CONCLUSION

Over the next few months, based on concerns about the block size limit, the Bitcoin price is likely to be more subdued than it otherwise might have been (though this does not mean it cannot rally). As long as the hard fork in Bitcoin hasn't been decided, it is likely that limit worries would cause a rally in the most liquid altcoins.

As mentioned earlier, I anticipate that the block size limit increase will be implemented into the blockchain in spring 2016. If and when the final decision is made, a relief rally in Bitcoin could result—and it may be intensified by the general awareness that the supply of new coins will be cut in half in the summer of 2016.

There is also an alternative and more unlikely dark horse scenario for which few people are genuinely preparing. If Bitcoin reaches full capacity, the market is likely to go through a wave of fear and uncertainty which could push prices to the $100 support level (representing a fantastic buying opportunity). Meanwhile, a tug-of-war would ensue between two-way pegged sidechains and various Bitcoin 2.0 projects. In such a scenario, alternative cryptocurrency networks like altcoins and Ripple could rally strongly—although I expect that once the technical capacity issues are resolved, capital would fairly quickly return to be invested in Bitcoin again.

Tuur Demeester
Editor-in-Chief, Adamant Research

ADAMANT
RESEARCH