The resolution of the Bitcoin experiment

I've spent more than 5 years being a Bitcoin developer. The software I've written has been used by millions of users, hundreds of developers, and the talks I've given have led directly to the creation of several startups. I've talked about Bitcoin on Sky TV and BBC News. I have been repeatedly cited by the Economist as a Bitcoin expert and prominent developer. I have explained Bitcoin to the SEC, to bankers and to ordinary people I met at cafes.

From the start, I've always said the same thing: Bitcoin is an experiment and like all experiments, it can fail. So don't invest what you can't afford to lose. I've said this in interviews, on stage at conferences, and over email. So have other well known developers like Gavin Andresen and Jeff Garzik.

But despite knowing that Bitcoin could fail all along, the now inescapable conclusion that it *has* failed still saddens me greatly. The fundamentals are broken and whatever happens to the price in the short term, the long term trend should probably be downwards. I will no longer be taking part in Bitcoin development and have sold all my coins.

Why has Bitcoin failed? It has failed because the community has failed. What was meant to be a new, decentralised form of money that lacked "systemically important institutions" and "too big to fail" has become something even worse: a system completely controlled by just a handful of people. Worse still, the network is on the brink of technical collapse. The mechanisms that should have prevented this outcome have broken down, and as a result there's no longer much reason to think Bitcoin can actually be better than the existing financial system.

Think about it. If you had never heard about Bitcoin before, would you care about a payments network that:

- Couldn't move your existing money
- Had wildly unpredictable fees that were high and rising fast

- Allowed buyers to take back payments they'd made after walking out of shops, by simply pressing a button *(if you aren't aware of this "feature" that's because Bitcoin was only just changed to allow it)*
- Is suffering large backlogs and flaky payments
- … which is controlled by China
- … and in which the companies and people building it were in open civil war?

I'm going to hazard a guess that the answer is no.

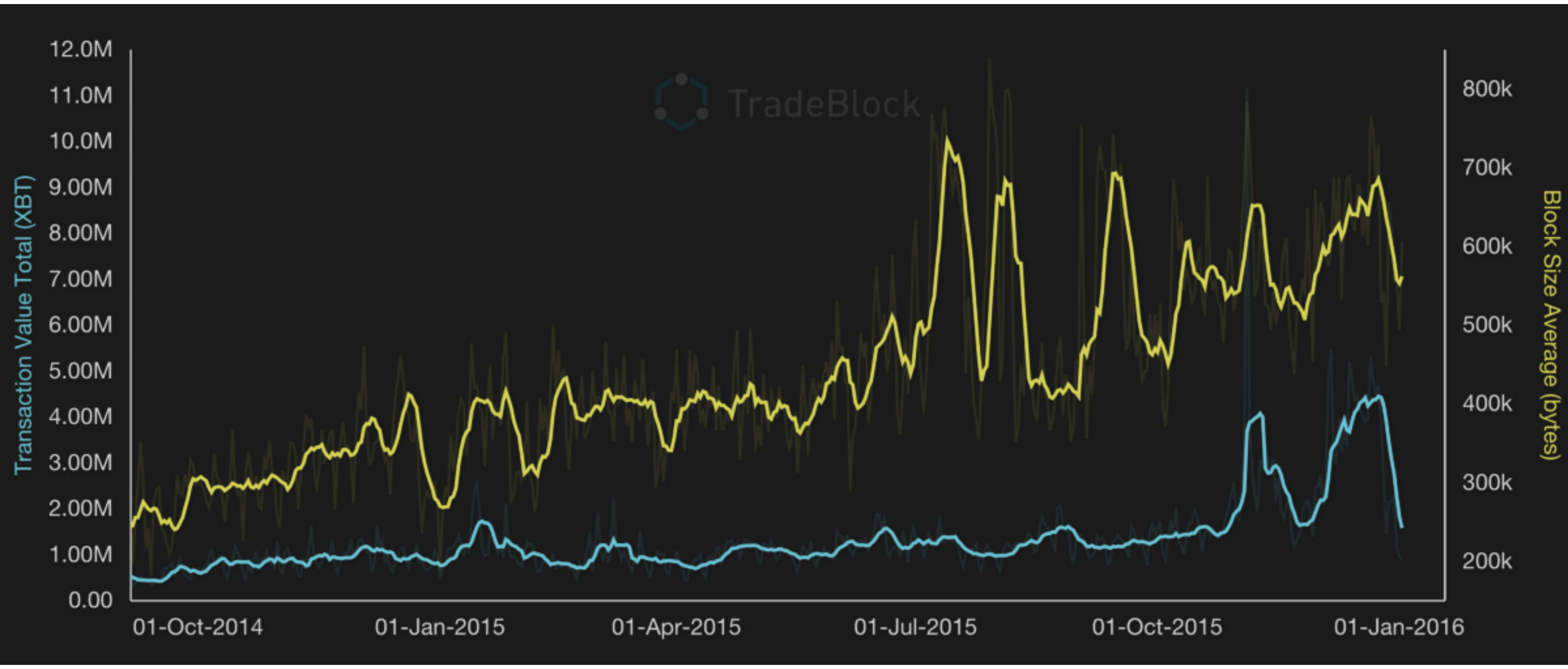
· · ·

Deadlock on the blocks

In case you haven't been keeping up with Bitcoin, here is how the network looks as of January 2016.

The block chain is full. You may wonder how it is possible for what is essentially a series of files to be "full". The answer is that an entirely artificial capacity cap of one megabyte per block, put in place as a temporary kludge a long time ago, has not been removed and as a result the network's capacity is now almost completely exhausted.

Here's a graph of block sizes.



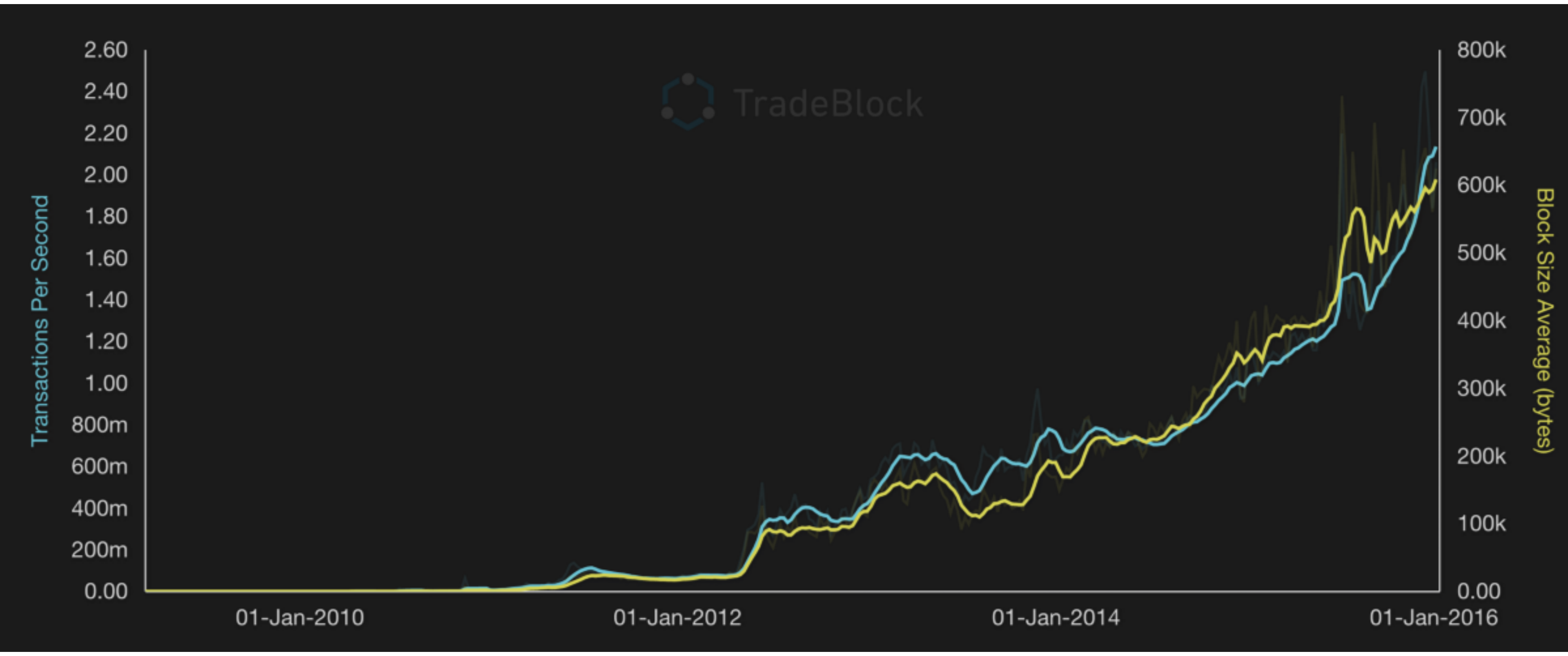
The peak level in July was reached during a denial-of-service attack in which someone flooded the network with transactions in an attempt to break things, calling it a "stress test". So that level, about 700 kilobytes of transactions (or less than 3 payments per second), is probably about the limit of what Bitcoin can actually achieve in practice

> ***NB**: You may have read that the limit is 7 payments per second. That's an old figure from 2011 and Bitcoin transactions got a lot more complex since then, so the true figure is a lot lower.*

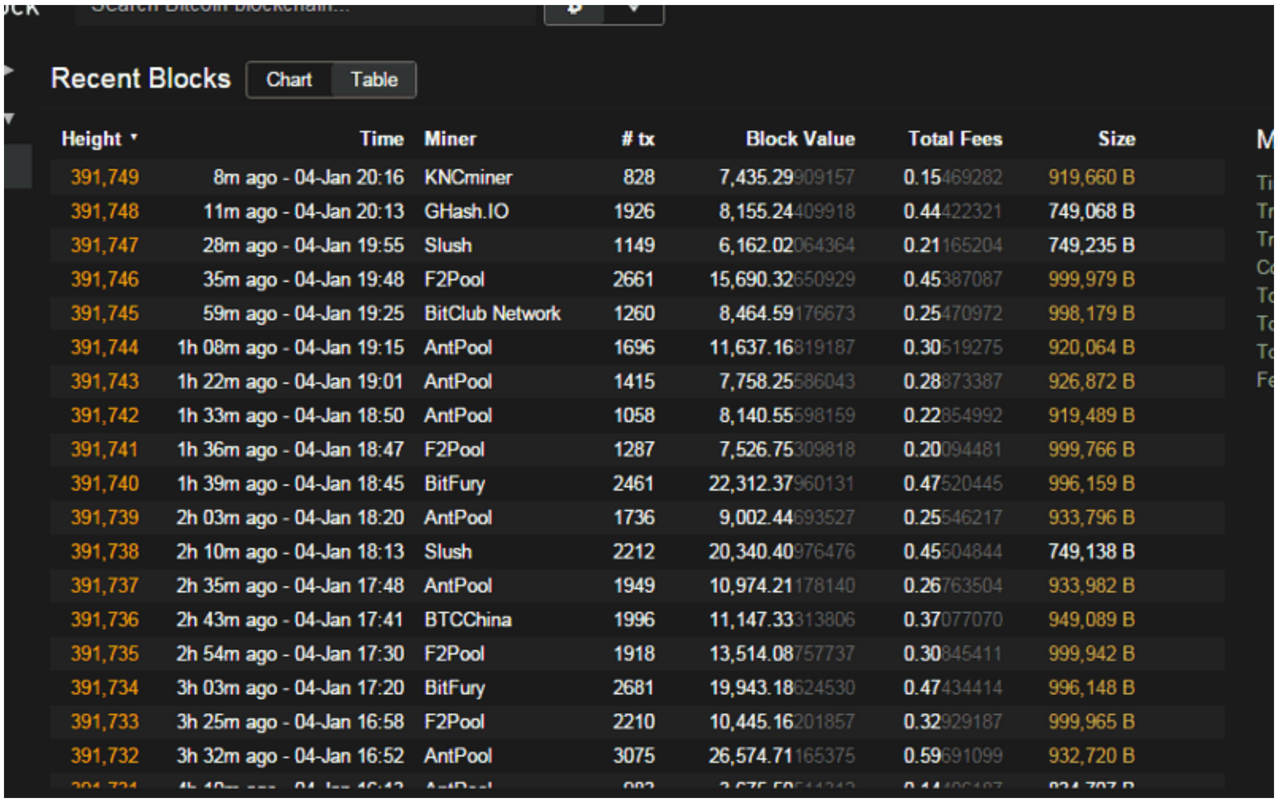
The reason the true limit seems to be 700 kilobytes instead of the theoretical 1000 is that sometimes miners produce blocks smaller than allowed and even empty blocks, despite that there are lots of transactions waiting to confirm— this seems to be most frequently caused by interference from the Chinese "Great Firewall" censorship system. More on that in a second.

If you look closely, you can see that traffic has been growing since the end of the 2015 summer months. This is expected. I wrote about Bitcoin's seasonal growth patterns back in March.

Here's weekly average block sizes:



So the average is nearly at the peak of what can be done. Not surprisingly then, there are frequent periods in which Bitcoin can't keep up with the transaction load being placed upon it and almost all blocks are the maximum size, even when there is a long queue of transactions waiting. You can see this in the size column (the 750kb blocks come from miners that haven't properly adjusted their software):



Recent Blocks

Height ▾	Time	Miner	# tx	Block Value	Total Fees	Size
391,749	8m ago - 04-Jan 20:16	KNCminer	828	7,435.29909157	0.15469282	919,660 B
391,748	11m ago - 04-Jan 20:13	GHash.IO	1926	8,155.24409918	0.44422321	749,068 B
391,747	28m ago - 04-Jan 19:55	Slush	1149	6,162.02064364	0.21165204	749,235 B
391,746	35m ago - 04-Jan 19:48	F2Pool	2661	15,690.32650929	0.45387087	999,979 B
391,745	59m ago - 04-Jan 19:25	BitClub Network	1260	8,464.59176673	0.25470972	998,179 B
391,744	1h 08m ago - 04-Jan 19:15	AntPool	1696	11,637.16819187	0.30519275	920,064 B
391,743	1h 22m ago - 04-Jan 19:01	AntPool	1415	7,758.25586043	0.28873387	926,872 B
391,742	1h 33m ago - 04-Jan 18:50	AntPool	1058	8,140.55598159	0.22854992	919,489 B
391,741	1h 36m ago - 04-Jan 18:47	F2Pool	1287	7,526.75309818	0.20094481	999,766 B
391,740	1h 39m ago - 04-Jan 18:45	BitFury	2461	22,312.37960131	0.47520445	996,159 B
391,739	2h 03m ago - 04-Jan 18:20	AntPool	1736	9,002.44693527	0.25546217	933,796 B
391,738	2h 10m ago - 04-Jan 18:13	Slush	2212	20,340.40976476	0.45504844	749,138 B
391,737	2h 35m ago - 04-Jan 17:48	AntPool	1949	10,974.21178140	0.26763504	933,982 B
391,736	2h 43m ago - 04-Jan 17:41	BTCChina	1996	11,147.33313806	0.37077070	949,089 B
391,735	2h 54m ago - 04-Jan 17:30	F2Pool	1918	13,514.08757737	0.30845411	999,942 B
391,734	3h 03m ago - 04-Jan 17:20	BitFury	2681	19,943.18624530	0.47434414	996,148 B
391,733	3h 25m ago - 04-Jan 16:58	F2Pool	2210	10,445.16201857	0.32929187	999,965 B
391,732	3h 32m ago - 04-Jan 16:52	AntPool	3075	26,574.71165375	0.59691099	932,720 B

When networks run out of capacity, they get really unreliable. That's why so many online attacks are based around simply flooding a target computer with traffic. Sure enough, just before Christmas payments started to become unreliable and at peak times backlogs are now becoming common.

Quoting a news post by ProHashing, a Bitcoin-using business:

> *Some customers contacted Chris earlier today asking why our bitcoin payouts didn't execute …*

> *The issue is that* ***it's now officially impossible to depend upon the bitcoin network anymore to know when or if your payment will be transacted, because the congestion is so bad that even minor spikes in volume create dramatic changes in network conditions****. To whom is it acceptable that one could wait either 60 minutes or 14 hours, chosen at random?*

> *It's ludicrous that people are actually writing posts on reddit claiming that there is no crisis. People were criticizing my post yesterday on the grounds that I somehow overstated the seriousness of the situation. Do these people actually use the bitcoin network to send money everyday?*

ProHashing encountered another near-miss between Christmas and New Year, this time because a payment from an exchange to their wallet was delayed.

Bitcoin is supposed to respond to this situation with automatic fee rises to try and get rid of some users, and although the mechanisms behind it are barely functional that's still sort of happening: it is rapidly becoming more and more expensive to use the Bitcoin network. Once upon a time, Bitcoin had the killer advantage of low and even zero fees, but it's now common to be asked to pay more to miners than a credit card would charge.

Why has the capacity limit not been raised? Because the block chain is controlled by Chinese miners, just *two* of whom control more than 50% of the hash power. At a recent conference over 95% of hashing power was controlled by a handful of guys sitting on a single stage. The miners are not allowing the block chain to grow.

Why are they not allowing it to grow? Several reasons. One is that the developers of the "Bitcoin Core" software that they run have refused to implement the necessary changes. Another is that the miners refuse to switch to any competing product, as they perceive doing so as "disloyalty" —and they're terrified of doing anything that might make the news as a "split" and cause investor panic. They have chosen instead to ignore the problem and hope it goes away.

And the final reason is that the Chinese internet is so broken by their government's firewall that moving data across the border barely works at all, with speeds routinely worse than what mobile phones provide. Imagine an entire country connected to the rest of the world by cheap hotel wifi, and you've got the picture. Right now, the Chinese miners are able to—just about—maintain their connection to the global internet and claim the 25 BTC reward ($11,000) that each block they create gives them. But if the Bitcoin network got more popular, they fear taking part would get too difficult and they'd lose their income stream. This gives them a perverse financial incentive to actually *try and stop Bitcoin becoming popular.*

Many Bitcoin users and observers have been assuming up until very recently that somehow these problems would all sort themselves out, and *of course* the block chain size limit would be raised. After all, why would the Bitcoin community … the community that has championed the block chain as the future of finance … deliberately kill itself by strangling the chain in its crib? But that's exactly what is happening.

The resulting civil war has seen Coinbase—the largest and best known Bitcoin startup in the USA—be erased from the official Bitcoin website for picking the "wrong" side and banned from the community forums. When parts of the community are viciously turning on the people that have introduced millions of users to the currency, you know things have got really crazy.

· · ·

Nobody knows what's going on

If you haven't heard much about this, you aren't alone. One of the most disturbing things that took place over the course of 2015 is that the flow of information to investors and users has dried up.

In the span of only about eight months, Bitcoin has gone from being a transparent and open community to one that is dominated by rampant censorship and attacks on bitcoiners by other bitcoiners. This transformation is by far the most appalling thing I have ever seen, and the result is that I no longer feel comfortable being associated with the Bitcoin community.

Bitcoin is not intended to be an investment and has always been advertised pretty accurately: as an experimental currency which you shouldn't buy more of than you can afford to lose. It is complex, but that never worried me because all the information an investor might want was out there, and there's an entire cottage industry of books, conferences, videos and websites to help people make sense of it all.

That has now changed.

Most people who own Bitcoin learn about it through the mainstream media. Whenever a story goes mainstream the Bitcoin price goes crazy, then the media report on the price rises and a bubble happens.

Stories about Bitcoin reach newspapers and magazines through a simple process: the news starts in a community forum, then it's picked up by a more specialised community/tech news website, then journalists at general media outlets see the story on those sites and write their own versions. I've seen this happen over and over again, and frequently taken part in it by discussing stories with journalists.

In August 2015 it became clear that due to severe mismanagement, the "Bitcoin Core" project that maintains the program that runs the peer-to-peer network wasn't going to release a version that raised the block size limit. The reasons for this are complicated and discussed below. But obviously, the community needed the ability to keep adding new users. So some long-term developers (including me) got together and developed the necessary code to raise the limit. That code was called BIP 101 and we released it in a modified version of the software that we branded Bitcoin XT. By running XT, miners could cast a vote for changing the limit. Once 75% of blocks were voting for the change the rules would be adjusted and bigger blocks would be allowed.

The release of Bitcoin XT somehow pushed powerful emotional buttons in a small number of people. One of them was a guy who is the admin of the bitcoin.org website and top discussion forums. He had frequently allowed discussion of outright criminal activity on the forums he controlled, on the grounds of freedom of speech. But when XT launched, he made a surprising decision. XT, he claimed, did not represent the "developer consensus" and was therefore not really Bitcoin. Voting was an abomination, he said, because:

> *"One of the great things about Bitcoin is its lack of democracy"*

So he decided to do whatever it took to kill XT completely, starting with censorship of Bitcoin's primary communication channels: any post that mentioned the words "Bitcoin XT" was erased from the discussion forums he controlled, XT could not be mentioned or linked to from anywhere on the official bitcoin.org website and, of course, anyone attempting to point users to other uncensored forums was also banned. Massive numbers of users were expelled from the forums and prevented from expressing their views.

As you can imagine, this enraged people. Read the comments on the announcement to get a feel for it.

Eventually, some users found their way to a new uncensored forum. Reading it is a sad thing. Every day for months I have seen raging, angry posts railing against the censors, vowing that they will be defeated.

But the inability to get news about XT or the censorship itself through to users has some problematic effects.

For the first time, investors have no obvious way to get a clear picture of what's going on. Dissenting views are being systematically suppressed. Technical criticisms of what Bitcoin Core is doing are being banned, with misleading nonsense being peddled in its place. And it's clear that many people who casually bought into Bitcoin during one of its hype cycles have no idea that the system is about to hit an artificial limit.

This worries me a great deal. Over the years governments have passed a large number of laws around securities and investments. Bitcoin is not a security and I do not believe it falls under those laws, but their *spirit* is simple enough: make sure investors are informed. When misinformed investors lose money, government attention frequently follows.

. . .

Why is Bitcoin Core keeping the limit?

People problems.

When Satoshi left, he handed over the reins of the program we now call Bitcoin Core to Gavin Andresen, an early contributor. Gavin is a solid and experienced leader who can see the big picture. His reliable technical judgement is one of the reasons I had the confidence to quit Google (where I had spent nearly 8 years) and work on Bitcoin full time. Only one tiny problem: Satoshi never actually asked Gavin if he wanted the job, and in fact he didn't. So the first thing Gavin did was grant four other developers access to the code as well. These developers were chosen quickly in order to ensure the project could easily continue if anything happened to him. They were, essentially, whoever was around and making themselves useful at the time.

One of them, Gregory Maxwell, had an unusual set of views: he once claimed he had mathematically proven Bitcoin to be impossible. More problematically, he did not believe in Satoshi's original vision.

When the project was first announced, Satoshi was asked how a block chain could scale to a large number of payments. Surely the amount of data to download would become overwhelming if the idea took off? This was a popular criticism of Bitcoin in the early days and Satoshi fully expected to be asked about it. He said:

> *The bandwidth might not be as prohibitive as you think … if the network were to get [as big as VISA], it would take several years, and by then, sending [the equivalent of] 2 HD movies over the Internet would probably not seem like a big deal.*

It's a simple argument: look at what existing payment networks handle, look at what it'd take for Bitcoin to do the same, and then point out that growth doesn't happen overnight. The networks and computers of the future will be better than today. And indeed back-of-the-envelope calculations suggested that, as he said to me, "it never really hits a scale ceiling" even when looking at more factors than just bandwidth.

Maxwell did not agree with this line of thinking. From an interview in December 2014:

> *Problems with decentralization as bitcoin grows are not going to diminish either, according to Maxwell: "There's an inherent tradeoff between scale and decentralization when you talk about transactions on the network."*

> *The problem, he said, is that as bitcoin transaction volume increases, larger companies will likely be the only ones running bitcoin nodes because of the inherent cost.*

The idea that Bitcoin is inherently doomed because more users means less decentralisation is a pernicious one. It ignores the fact that despite all the hype, real usage is low, growing slowly and technology gets better over time. It is a belief Gavin and I have spent much time debunking. And it leads to an obvious but crazy conclusion: if decentralisation is what makes Bitcoin good, and growth threatens decentralisation, *then Bitcoin should not be allowed to grow*.

Instead, Maxwell concluded, Bitcoin should become a sort of settlement layer for some vaguely defined, as yet un-created non-blockchain based system.

The death spiral begins

In a company, someone who did not share the goals of the organisation would be dealt with in a simple way: by firing him.

But Bitcoin Core is an open source project, not a company. Once the 5 developers with commit access to the code had been chosen and Gavin had decided he did not want to be the leader, there was no procedure in place to ever remove one. And there was no interview or screening process to ensure they actually agreed with the project's goals.

As Bitcoin became more popular and traffic started approaching the 1mb limit, the topic of raising the block size limit was occasionally brought up between the developers. But it quickly became an emotionally charged subject. Accusations were thrown around that raising the limit was too risky, that it was against decentralisation, and so on. Like many small groups, people prefer to avoid conflict. The can was kicked down the road.

Complicating things further, Maxwell founded a company that then hired several other developers. Not surprisingly, their views then started to change to align with that of their new boss.

Co-ordinating software upgrades takes time, and so in May 2015 Gavin decided the subject must be tackled once and for all, whilst there was still about 8 months remaining. He began writing articles that worked through the arguments against raising the limit, one at a time.

But it quickly became apparent that the Bitcoin Core developers were hopelessly at loggerheads. Maxwell and the developers he had hired refused to contemplate any increase in the limit whatsoever. They were barely even willing to talk about the issue. They insisted that nothing be done without "consensus". And the developer who was responsible for making the releases was so afraid of conflict that he decided any controversial topic in which one side might "win" simply could not be touched at all, and refused to get involved.

Thus despite the fact that exchanges, users, wallet developers, and miners were all expecting a rise, and indeed, had been building entire businesses around the assumption that it would happen, 3 of the 5 developers refused to touch the limit.

Deadlock.

Meanwhile, the clock was ticking.

. . .

Massive DDoS attacks on XT users

Despite the news blockade, within a few days of launching Bitcoin XT around 15% of all network nodes were running it, and at least one mining pool had started offering BIP101 voting to miners.

That's when the denial of service attacks started. The attacks were so large that they disconnected entire regions from the internet:

> *"I was DDos'd. It was a massive DDoS that took down my entire (rural) ISP. Everyone in five towns lost their internet service for several hours last summer because of these criminals. It definitely discouraged me from hosting nodes."*

In other cases, entire datacenters were disconnected from the internet until the single XT node inside them was stopped. About a third of the nodes were attacked and removed from the internet in this way.

Worse, the mining pool that had been offering BIP101 was also attacked and forced to stop. The message was clear: anyone who supported bigger blocks, or even *allowed other people to vote for them*, would be assaulted.

The attackers are still out there. When Coinbase, months after the launch, announced they had finally lost patience with Core and would run XT, they too were forced offline for a while.

Bogus conferences

Despite the DoS attacks and censorship, XT was gaining momentum. That posed a threat to Core, so a few of its developers decided to organise a series of conferences named "Scaling Bitcoin": one in August and one in December. The goal, it was claimed, was to reach "consensus" on what should be done. Everyone likes a consensus of experts, don't they?

It was immediately clear to me that people who refused to even talk about raising the limit would not have a change of heart because they attended a conference, and moreover, with the start of the winter growth season there remained only a few months to get the network upgraded. Wasting those precious months waiting for conferences would put the stability of the entire network at risk. The fact that the first conference *actually banned discussion* of concrete proposals didn't help.

So I didn't go.

Unfortunately, this tactic was devastatingly effective. The community fell for it completely. When talking to miners and startups, "we are waiting for Core to raise the limit in December" was one of the most commonly cited reasons for refusing to run XT. They were terrified of any media stories about a community split that might hurt the Bitcoin price and thus, their earnings.

Now the last conference has come and gone with no plan to raise the limit, some companies (like Coinbase and BTCC) have woken up to the fact that they got played. But too late. Whilst the community was waiting, organic growth added another 250,000 transactions per day.

A non-roadmap

Jeff Garzik and Gavin Andresen, the two of five Bitcoin Core committers who support a block size increase (and the two who have been around the longest), both have a stellar reputation within the community. They recently wrote a joint article titled "**Bitcoin is Being Hot-Wired for Settlement**".

Jeff and Gavin are generally softer in their approach than I am. I'm more of a tell-it-like-I-see-it kinda guy, or as Gavin has delicately put it, "honest to a fault". So the strong language in their joint letter is unusual. They don't pull any punches:

> *The proposed roadmap currently being discussed in the bitcoin community has some good points in that it does have a plan to accommodate more transactions, but* ***it fails to speak plainly to bitcoin users and acknowledge key downsides****.*

> *Core block size does not change;* ***there has been zero compromise*** *on that issue.*

> *In an optimal, transparent, open source environment, a BIP would be produced … this has not happened*

> *One of the explicit goals of the Scaling Bitcoin workshops was to funnel the chaotic core block size debate into an orderly decision making process. That did not occur.* ***In hindsight, Scaling Bitcoin stalled a block size decision*** *while transaction fee price and block space pressure continue to increase.*

Failing to speak plainly, as they put it, has become more and more common. As an example, the plan Gavin and Jeff refer to was announced at the "Scaling Bitcoin" conferences but doesn't involve making anything more efficient, and manages an anemic 60% capacity increase only through an accounting trick (not counting some of the bytes in each transaction). It requires making huge changes to nearly every piece of Bitcoin-related software. Instead of doing a simple thing and raising the limit, it chooses to do an incredibly complicated thing that might buy months at most, assuming a huge coordinated effort.

Replace by fee

One problem with using fees to control congestion is that the fee to get to the front of the queue might change after you made a payment. Bitcoin Core has a brilliant solution to this problem—allow people to mark their payments as changeable after they've been sent, up until they appear in the block chain. The stated intention is to let people adjust the fee paid, but in fact their change also allows people to change the payment to *point back to themselves*, thus reversing it.

At a stroke, this makes using Bitcoin useless for actually buying things, as you'd have to wait for a buyer's transaction to appear in the block chain … which from now on can take hours rather than minutes, due to the congestion.

Core's reasoning for why this is OK goes like this: it's no big loss because if you hadn't been waiting for a block before, there was a theoretical risk of payment fraud, which means you weren't using Bitcoin properly. Thus, making that risk a 100% certainty doesn't really change anything.

In other words, they don't recognise that risk management exists and so perceive this change as zero cost.

This protocol change will be released with the next version of Core (0.12), so will activate when the miners upgrade. It was massively condemned by the entire Bitcoin community but the remaining Bitcoin Core developers don't care what other people think, so the change will happen.

If that didn’t convince you Bitcoin has serious problems, nothing will. How many people would think bitcoins are worth hundreds of dollars each when you soon won’t be able to use them in actual shops?

Conclusions

Bitcoin has entered exceptionally dangerous waters. Previous crises, like the bankruptcy of Mt Gox, were all to do with the services and companies that sprung up around the ecosystem. But this one is different: it is a crisis of the core system, the block chain itself.

More fundamentally, it is a crisis that reflects deep philosophical differences in how people view the world: either as one that should be ruled by a “consensus of experts”, or through ordinary people picking whatever policies make sense to them.

Even if a new team was built to replace Bitcoin Core, the problem of mining power being concentrated behind the Great Firewall would remain. Bitcoin has no future whilst it’s controlled by fewer than 10 people. And there’s no solution in sight for this problem: nobody even has any suggestions. For a community that has always worried about the block chain being taken over by an oppressive government, it is a rich irony.

Still, all is not yet lost. Despite everything that has happened, in the past few weeks more members of the community have started picking things up from where I am putting them down. Where making an alternative to Core was once seen as renegade, there are now two more forks vying for attention (Bitcoin Classic and Bitcoin Unlimited). So far they’ve hit the same problems as XT but it’s possible a fresh set of faces could find a way to make progress.

There are many talented and energetic people working in the Bitcoin space, and in the past five years I’ve had the pleasure of getting to know many of them. Their entrepreneurial spirit and alternative perspectives on money, economics and politics were fascinating to experience, and despite how it’s all gone down I don’t regret my time with the project. I woke up this morning to find people wishing me well in the uncensored forum and asking me to stay, but I’m afraid I’ve moved on to other things. To those people I say: good luck, stay strong, and I wish you the best.