Bitcoin   Blockchain   FinTech   ETH   Learn

Free   PR   Widget

Next →

Indian Ministers Suggest Tax on Cash Withdrawals Abov...

Explore   Menu

Bitcoin Slows to a Crawl as Transactions Backlog Reaches a Quarter of a Billion Dollars
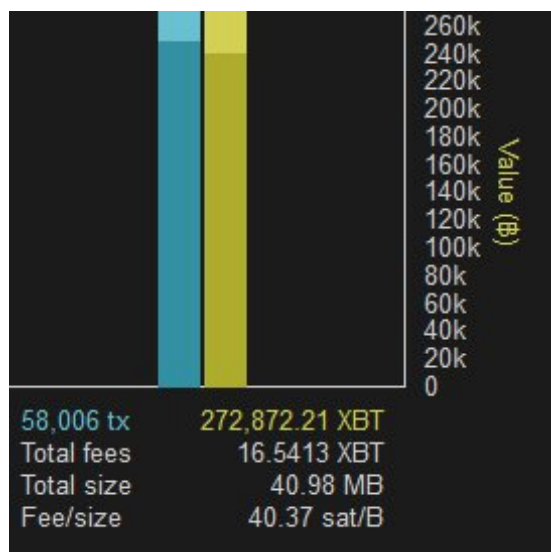
Andrew Quentson on 25/01/2017

214
SHARES

F ollowing the re-adjustment of bitcoin's network difficulty after a sudden increase, a massive transaction backlog began developing yesterday, leading to a torrent of complaints.

An incredible sum of 278,872.21 bitcoins, worth around a quarter of a billion dollars, is currently in limbo, stuck in the ether, unable to move.

58,006 tx   272,872.21 XBT
Total fees   16.5413 XBT
Total size   40.98 MB
Fee/size   40.37 sat/B

*$250 Million Are Currently Stuck in Limbo
– Image from TradeBlock*

In response, angry users have littered public spaces to vent their frustration at the situation. One of them is a representative from Vaultoro, a bitcoin and gold exchange, who publicly stated:

"[W]e paid 0.0005 fee (45 cents) to get a client their withdrawal and it took 17 hours to clear and actually

Recent Posts

BitGo Enhances Its Security With Ledger's Hardware Based Key Storage

The US Postal Inspection Service is Seeking Bitcoin 'Intelligence Gathering Specialists'

Bitfinex's Hacked Bitcoins Are on the Move; 5% Recovery Bounty Offered

Italian Politician Links Bitcoin to Mafia Controlled Gambling Industry

Bitcoin Core Dev Recommends a 70% Reduction in Transaction Capacity after $250 Million Backlog

only cleared because I put it into the Viabtc transaction accelerator."

As a bitcoin only (maximalists if you will) business, we are starting to find it very hard. Clients get pissed off when we charge more for withdrawals, they get pissed off when it takes ages to deposit and the company gets the blame. If we raise fees, we get complaints and it totally cuts out the developing world because some people live on 5 bucks a day so a 50 cent fee is too much for them to bother."
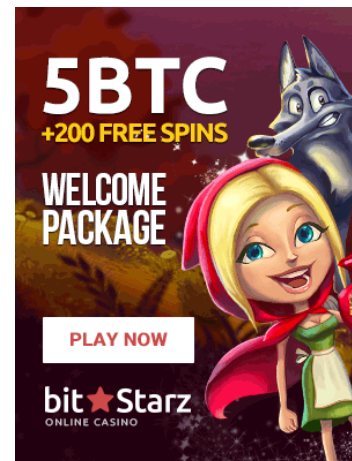
Another user could not contain himself. After stating he mistakenly entered a lower fee, the lack of any remedy made him feel the bitcoin network had told him to **** off:

"Obviously this is my fault. I should have set a higher fee… But I didn't. I made a newbie mistake. And now I'm *****ed. My money is there but I can't touch it until some random undetermined future date when the tx drops out of the mem pool. Bitcoin just told me to go **** myself, essentially."

The New Normal?

One highly important mechanism of bitcoin's system design is network difficulty, a sort of calculator who measures the total network hashpower and increases

Search

Search here...

or decreases the difficulty of finding a block reward of 12.5 btc based on whether the hashpower increased or decreased. Accordingly, it adjusts every two weeks.

When hashpower does increase, as has often been the case, the bitcoin network is operating at speed and can handle more transactions as blocks are found faster than the usual average of 10 minutes. Once difficulty re-adjusts in two weeks, transaction processing returns to normal operations. With full blocks, that creates a sudden massive backlog as the temporary and somewhat artificial added transaction capacity instantly vanishes.
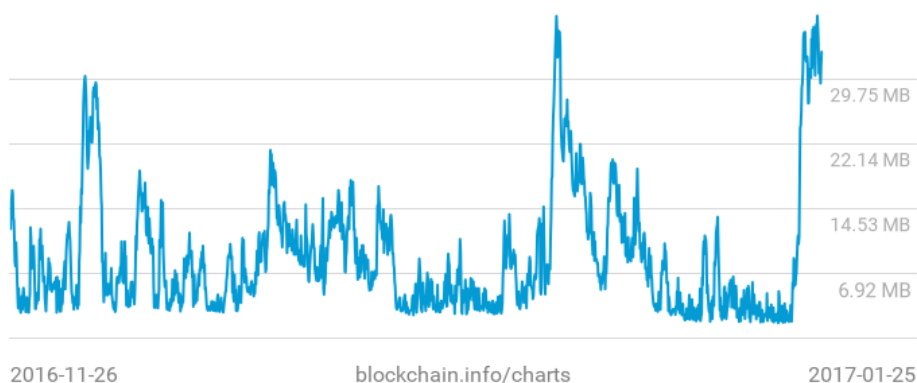
Bitcoin's Mempool Size From November 2016 to January 2017 – *Image from Blockchain.info*

In the past two months, there have been three serious backlogs and many smaller ones. If one transacts during this period, although you may have paid a

decent fee and perhaps even a higher than usual fee, you may still need to wait as transaction capacity is suddenly lowered.

If the sum is considerable or time sensitive, particularly as transacting in bitcoin is still a fairly new and unfamiliar experience, this denial of service can be extremely frustrating and somewhat scary with users wondering whether they will receive their bitcoin back. Usually, it leads to angry complaints that fill inboxes of bitcoin businesses as well as public discussion spaces. Price, too, tends to react by falling lower as has been the case since yesterday.

Bitcoin's Price Falls by $40 Following the Formation of a Transaction Backlog – *Image from BitcoinWisdom*

Is Bitcoin at Risk of

Being Replaced?

The experience might be excused once, perhaps twice, but as it repeats, the frustration and anger may turn to desperation with users eventually beginning to dread transacting in bitcoin and perhaps give up entirely, but there are two important aspects that keep bitcoin at the front. One is brand recognition, the other is investors' loyalty.

Bitcoin is, by all accounts, a brilliant name and a fairly widely recognized brand. It has now further developed to mean or symbolize many things, such as digital gold, internet money, freedom, the future of currency, a response to the banking crisis, part of the internet culture, etc, etc. That may help to delay the advancement of any competitor, but a new brand can build on it, take its symbolism, and further add "better" to its name recognition. On the other hand, persuading current investors to move may be more difficult, but their loyalty might quickly change if it appears the new brand has a real chance of overtaking the currency.

It is unlikely the process would be sudden, with investors probably at first diversifying a small amount, just in case, then more, until in effect they have moved, but would bitcoin respond if it became clear the currency is at serious risk of being replaced?

The Intractable Debate

We used to often argue that no other currency would overtake bitcoin as it would simply incorporate any new feature that appears desirable. That, however, has not actually happened. Although, for example, it has been proven (PDF) that Ethereum's confirmation times of as low as 17 seconds do work with zero problems and provide in 10 minutes (1 block confirmation on average for bitcoin) the same security as 6 block confirmations for bitcoin (which takes, on average, around one hour), there has been no serious discussion to lower confirmation times.

There are many other examples, such as Litecoin's 4MB blocks which allow the network to operate with no problem whatever. They are currently using on average only 1 or 2KB per block, with around 1,000x more space available, yet no one seems to care to create big blocks so as to gain some sort of advantage as has been suggested would happen if bitcoin's blocksize was increased. Ethereum operates on a dynamic blocksize, yet again no one has played the system to create bigger blocks as some have argued miners might.

This suggests that bitcoin might not currently be able to respond to the advances of a new currency in a constructive way by itself becoming more competitive, not least because the community is seemingly unable to act on solving the current transaction problem through a fairly simple upgrade, let alone reach any agreement on adding nicer things.

The Problem?

Open source development has one fundamental problem. It relies on unaccountable volunteers that go through no vetting process so randomly contributing and then gradually taking influential positions in a fairly subjective and arbitrary manner. They, so being just volunteers who are freely giving their work, have no requirements to perform at a satisfactory level nor any requirement to have the currency's best interest at heart. That means they may have their own agendas, whether political or economical, which may or may not align with what impartially could be said would be best for the network.

Usually, it's not a great problem because the project's founder – who naturally we should think must want the best for the network – takes a leadership role and sort of keeps everyone in check with Linus Torvalds a prominent example. Nakamoto, however, left. His chosen project leader, Gavin Andresen, who publicly

chosen project leader, Gavin Andresen, who publicly raised the capacity problem we are still facing more than two years ago, had his commits arbitrarily removed without any wide public discussion last year.

Business and miners now depend on the voluntary, non-paid, actions of developers with varied work quality and interests that just happened to contribute either purely altruistically or with the intention of steering the project for economical or intellectual reasons.

The Solution?

Businesses, early adopters and, in particular, miners, have failed to provide developers. They have further failed to create a structure where the priorities, speed and quality of work can have some sort of accountability, similar to the Linux Foundation.

Andresen tried to do so through the Bitcoin Foundation, but at a time when the ecosystem was still far too immature and courted much genuine and artificial controversy. It thus failed and in doing so created a vacuum which gave Blockstream the opportunity to hire many developers, gaining great influence in the direction of bitcoin. Unfortunately, Blockstream is a for profit company which owes a primary legal duty to their own shareholders and

investors, above bitcoin and the wider bitcoin
ecosystem.

Their interests may often align, but, at times, they
might not as Blockstream's primary business is to sell
private blockchains (sidechains) to banks and other
companies, with the core bitcoin protocol probably a
secondary consideration and likely only of relevance
as far as they retain influence and as far as they can
modify it in whatever way their business requires.

Specifically, whether a limited transaction capacity
directly benefits their business interest in the short
term or in the long run we do not know as their
presentations to investors have not been published
nor has any concrete business plan been released. We
are therefore left to read their actions.

In particular, Blockstream employees and companies
that do business with Blockstream tend to be the most
vocal in arguing for a limited transaction capacity.
Moreover, suggestions by some Blockstream
employees that they will quit bitcoin development if
the maxblocksize is increased does indicate that a
limited transaction capacity is of a fundamental
consideration, but it is not clear whether that is on a
personal or company level nor whether it is for
economical or intellectual reasons.

In any event, the way bitcoin currently operates, as far as development of the Bitcoin Core client is concerned, appears to very much depend on trusting Blockstream and its steering direction of Bitcoin Core as there is no longer any counterbalancing influence in Bitcoin Core development with Andresen, Garzik and Hearn seemingly pushed out.

That means that the interests of other businesses, miners and the wider ecosystem currently has no voice in Bitcoin Core development. That is primarily due to a failure by miners, businesses and the wider ecosystem to organize in such a way as to ensure the very important work of bitcoin development is undertaken in a way that impartially can be said benefits the entire ecosystem.

Until they do so, the increase or, the opposite, a lack of action on transaction capacity, might soon be replaced by some other steering action that may come at the expense of some other parts of the ecosystem. To address and solve this imbalance, development needs to be incentivized by all ecosystem participants in an accountable way both to ensure that actions, which impartially can be said are in the best interest of the ecosystem, are undertaken and to ensure the speed, quality and priority of development is accountable and incentivized.

As such, it may well be the case that the 1MB limit was placed there less for technical reasons and more to firstly see whether bitcoin can be hijacked and, if not, to incentivize ecosystem participants, especially miners, whom the system design trusts the most due to its design incentives, to contribute towards bitcoin development so as to ensure they operate in the best interest of the entire network.

What Should the Bitcoin Network Do?

Hardfork Through Bitcoin Unlimited

Softfork Through Segwit

Hardfork to 4MB Plus Segwit

Don't Know

Do Nothing

Hardfork to 2MB Plus Segwit

Vote   *Results*

Image from Shutterstock.

214
SHARES

Next

Indian Ministers Suggest …

25/01/2017

Previous

Blockchain Tech Used to …

25/01/2017

Tags

apple Australia bitcoin

bitcoin accepted here bitcoin asic miner bitcoin atm bitcoin exchange bitcoin foundation Bitcoin price bitcoin regulation bitfinex bitlicense bitpay bitstamp blockchain block chain Blockchain.info china coinbase cryptocurrency dogecoin Ethereum News fintech gavin andresen IBM india japan litecoin mark karpeles microsoft mtgox mt gox okcoin overstock paypal R3 reddit regulation ripple roger ver Ross Ulbricht russia satoshi nakamoto security silk road

Advertised sites are not endorsed by us. They may be unsafe, untrustworthy, or illegal in your jurisdiction.