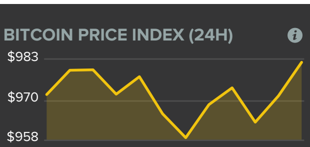
CoinDesk

TRENDING
CoinDesk Research Poll: Will Blockchain Disrupt Venture Capital?

BITCOIN PRICE INDEX (24H)



USD -0.68% ▾
$982.19
EUR €923.62

CNY 4.69% ▴
¥6,627.74
GBP £786.11

NEWS PRICE & DATA GUIDES EVENTS RESEARCH PRESS RELEASES Search

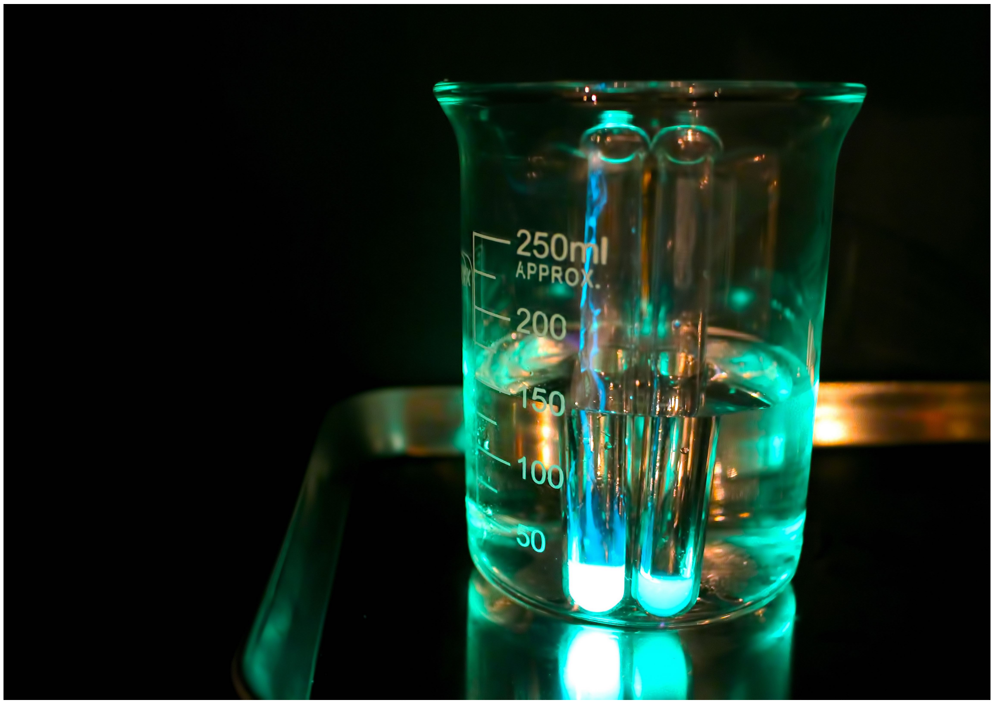
BITCOIN PROTOCOL • FEATURES • INTERVIEWS • TECHNOLOGY

A Bitcoin Hard Fork? The Science of Contentious Code is Advancing

Alyssa Hertig (@AlyssaHertig) | Published on February 10, 2017 at 14:35 GMT

FEATURE

162 3



Bitcoin developers are probing deeper into how best to execute a so-called hard fork, a contentious upgrading tool that's been at the heart of the nearly $16bn network's most divisive debate for years now.

The issue is that to be used cleanly and without unintentional consequences, a hard fork requires all the digital currency's miners to move to a new blockchain, or version of its transaction history. One case study of what can otherwise happen came last summer, when ethereum inadvertently split into two networks after executing a hard fork some users disagreed with.

That's not to say that all hard forks have the same outcome.

Interestingly, the following two ethereum hard forks went according to plan, as they were non-contentious changes to fix attacks on the network, perhaps demonstrating that they can go well if all participants agree.

Meanwhile, against this backdrop, some in the bitcoin community have long been calling for a hard fork to increase transaction capacity by raising the blocksize parameter to 2MB or more, with Bitcoin Unlimited being the latest software to take up the call for action.

One impediment is that, since increasing the block size is a contentious change, a similar ethereum-like split could occur in bitcoin if a hard fork were executed.

For that reason and others, the engineering consensus seems to be that more research needs to be done before giving it a try in bitcoin.

Bitmain's James Hilliard, who has tested code for Bitcoin Core, said that, though he's generally “conservative” on the issue of a hard fork (as are the most active contributors), though he said there might be a potential need for one in the future, especially since it's the only way to make certain types of changes.

Hilliard told CoinDesk:

> *"I think research is definitely helpful as it gets us closer to being able to do safe hard forks."*

Of late, there's been an uptake in research in this direction, with some bitcoin code contributors continuing long-standing studies into how a hard fork might be used.

Lengthy analysis has been posted to the bitcoin developer mailing list over the last couple of months, and there's now even an open-source website filled with links to notable public hard fork research.

Bitcoin developers appear to be approaching the option carefully, looking into a range of considerations, such as how to safely execute such a change.

Hard fork proposals

Along those lines, a batch of new hard fork proposals have been released in the last few months.

None have received much support in terms of near-term execution, but they have generated discussion and show an uptake in attention.

Perhaps most notably, Bitcoin Core contributor Johnson Lau, who has been perhaps the most prolific in terms of posting hard fork write-ups to the mailing list, just this week coded up a second experimental hard fork, called 'Spoonnet', with new features that bitcoin currently doesn't have.

He hinted that trying to activate it right now, without unanimous consensus, would not lead to positive results.

"Trying to activate it on testnet will get you banned. Trying to activate it on mainnet before consensus is reached will make you lose money," he wrote.

Despite the long write-up and code accompanying it, he mentioned that there are plenty of details to iron out before Spoonnet is ready to use, such as ensuring that wallets in the post-hard fork world would support transactions on the new network.

Lau’s other hard fork proposal, called Forcenet, codes up a type of hard fork known as a 'soft-hard fork', that makes old nodes follow the new rules, based on an earlier proposal by Bitcoin Core contributor Luke Dashjr.

It puts into practice a new block header format that adds room for more data, among other things.

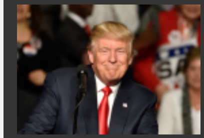
Then, there are some hard fork proposals that relate more specifically to the block size debate.

Dashjr posted two hard fork proposals last month, one of which proposes an initial optional decrease to the block size that would switch to a steady increase to 31 MB.

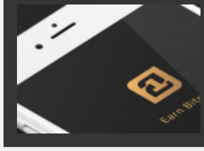
FEATURES

Charts: How an ETF Approval Could Impact Bitcoin's Price

Project Jasper: Lessons From Bank of Canada's First Blockchain Project



Bitcoin, Blockchain and Trump: Where Do We Go From Here?



LinkedIn Killer? Bitcoin Upstart 21 Takes on Social With Email Play

INDUSTRY PRESS RELEASES

Feb 6 | 13:21	**Press ReleaseThe Blockchain Academy London – A 2-day event on Bitcoin and Blockchain Technology**
Feb 6 | 13:16	**Press Release: The Bitcoin Users Group Welcomes Edward NG as Executive Director for Asia**
Jan 30 | 16:57	**Press Release: CoinDesk Acquires Lawnmower, Accelerating Growth in Research Offerings**
Jan 25 | 23:01	**Press Release: Bitcoin Faucets become the new entry points for Bitcoin in developing countries**

VIEW MORE **SUBMIT RELEASE**

Got a news tip or guest feature?

DON'T MISS A SINGLE STORY

Subscribe to our free newsletter and follow us

Hilliard pointed out that hard fork research pertaining to the block size in particular has been going on for a while. He drew up with his own hard fork proposal last February, though perhaps owing to the speed of R&D, he said he wouldn't vouch for it because it's "overly complicated".

Dangers considered

Notably, few of the newer proposals are related to making hard forks safer. For instance, addressing the issue that stakeholders could lose money (or see the value of their investment decline) if the blockchain splits.

One such proposal is for a 'hard fork warning system', with which wallets and miners can warn others in the case of a hard fork.

"With a hard fork warning system, users and merchants may stop trading when there is abnormality on the network until they are able to make an informed decision," Lau explained, mentioning that this might have been useful in former unintentional bitcoin splits, as well as that of ethereum.

Further, replay attacks featured heavily in the aftermath of ethereum's fork and resulting blockchain split. In a nutshell, because the transaction histories were the same on each resulting network, users could send transactions on both networks, which caused confusion – at least up until the issue was fixed.

Proposals from Dashjr and Lau grapple with this issue using different techniques.

Interestingly, even the details of this protective action were cause for disagreement, with Bitcoin Core contributor Matt Corallo arguing in response to Lau's bitcoin improvement proposal (BIP) that replay attack protection should be mandatory rather than opt-in.

Hilliard noted that another safety measure would be to have a "reasonably long" activation timeline of a year or so.

Scaling hurdle

As far as for what reason to carry out a hard fork, the block size debate continues to be the elephant in the room.

In Hilliard's opinion, the block size is not a good enough reason to hard fork, at least right now, where the split in opinion could manifest in two networks, and increasing the block size could increase the burden of running a volunteer node.

He added:

> *"The question is not, 'Should bitcoin scale?', the question is 'How can we scale bitcoin without breaking it?'"*

Still, figuring out a way to carry out hard forks safely might be beneficial, as there's no other way to make certain technical changes to bitcoin.

"Fixing tech issues would be a good reason, in my opinion," Hilliard said.

He pointed to a long list of bug fixes and other potential changes on the so-called 'hard-fork wish list', including header format changes that would "make it so that miners mining on pools can't withhold blocks".

One other such change could bundle in what Lau called a "secondary block header", which could store new data that, for one, could potentially boost the security of SPV nodes (which store less data than regular nodes).

"None of the core devs are really against hard forks, they are just conservative," Hilliard said.

Lau similarly indicated that it could happen as long as most one day agree with a change.

"When the vast majority of bitcoin users believe the system is too inefficient (in many aspects, not just transaction throughput) and they believe the benefits outweigh the risks, a hard fork will happen," he said.

Hilliard, though, doesn't seem to be in a hurry, noting that it might take a while to find a solution that everyone agrees with.

He concluded:

> *"I'm not entirely convinced we really need to do one in the near future."*

Research image via Shutterstock

Bitcoin Core Bitcoin Protocol Hard Forks

162 3

PREVIOUS ARTICLE

Ethereum Job Market Colony Enters Beta

NEXT ARTICLE

Illinois Legislator Calls for Blockchain Working Group

RELATED STORIES

Feb 10, 2017 at 13:00 | Carolyn Wilkins

Project Jasper: Lessons From Bank of Canada's First Blockchain Project

Canada's central bank discusses new takeaways from six months of distributed ledger experimentation.

Feb 8, 2017 at 10:44 | Alyssa Hertig

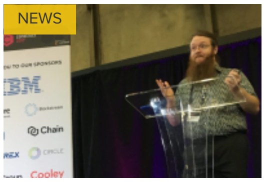
What Makes Bitcoin Great? One Scientist is On a Quest to Find Out

Academics still aren't sure why bitcoin is so robust, but one Cornell professor has made it her mission to find out.

Feb 7, 2017 at 14:00 | Alyssa Hertig

Inside MAST: The Little-Known Plan to Advance Bitcoin Smart Contracts

Bitcoin could soon be endowed with a range of new technical improvements including greater smart-contract functionality.



Jan 31, 2017 at 23:55 | Pete Rizzo

Greg Maxwell Breaks Down Blockchain: The 'Uncontrollable Noun'

Blockstream CTO Greg Maxwell addressed the growing blockchain hype in a nuanced talk at Construct 2017 today.

2 Comments CoinDesk 1 Login

Recommend Share Sort by Best

Join the discussion…

patrick cowan • 4 hours ago

Segwit.

1 • Reply • Share ›

Greg Greene ➦ patrick cowan • 3 hours ago

Warthog.

• Reply • Share ›

ALSO ON **COINDESK**

Two of China's Biggest Exchanges Stop Bitcoin Withdrawals

135 comments • a day ago•

disqusrocks — PBoC = incredible market manipulators

Blockchain Startup Hashed Health Raises $1.8 Million

2 comments • 3 days ago•

YouNeedAThneed — With a name like "Hashed Health" what could go wrong? "Titanic Shipping Co."

LinkedIn Killer? Bitcoin Upstart 21 Takes on Social Giant With Paid Email Play

6 comments • a day ago•

Andy Ofiesh — So far every business model that 21 has announced involves telling customers that they can make money, …

China Fears Spread Beyond Bitcoin As Crypto Markets Slide

9 comments • 21 hours ago•

sjs — If bitcoin was operating as a decentralised commodity/currency instead of being subject to margin trading/leveraged …

Subscribe Add Disqus to your site Add Disqus Add Privacy DISQUS