

Split on Forks? Blockchain Leaders Learn Tough Lessons from Bitcoin Scaling



Bailey Reutzel

Sep 18, 2017 at 10:00 UTC | Updated Sep 19, 2017 at 09:01 UTC

FEATURE

Cypherpunks attack ideas, not people – or so the saying goes.

If bitcoin's long-roiling [scaling debate](#) is any indication, though, that doesn't always work in practice. From suggestions that some were undermining the project's intent to outright personal attacks, things have gotten – and remain – heated.

But with at least the first chapter in bitcoin's scaling debate [in the books](#) (and maybe more to come), the lead developers of other blockchain protocols are taking note, hoping to draw lessons to create a smoother environment for upgrading the new form of software.

First and foremost for many, though, is determining whether bitcoin truly reached a "consensus" of stakeholders, and just how the network – by far the largest blockchain in terms of the number and diversity of users, startups, developers and miners – achieved the upgrade ([conclusions vary](#)).

All in all, the mix of competing proposals may have resulted in the feeling that open-source economics is becoming more of a republic than a direct democracy.

In fact, Riccardo Spagni, a monero core developer, went so far as to label the latter idea a fallacy, saying:

"When it comes to measuring consensus we have to view the opinion of people contributing a bunch of code worth more than the people on the sidelines just writing posts on reddit and tweeting a lot."

Actual consensus

That's not to say that any user should be left in the dark when a protocol is making changes, it's just that deciding who to listen to is easier said than done.

"We need to have discussions, not just as a group of developers, but actually discussing it with users, miners and economically-sensitive nodes like exchanges and merchants," Spagni told CoinDesk.

Still, efforts to advance a decentralized group can be compared to herding cats – for one, developers don't have a "magical relationship" with exchanges just by proxy of exchanges using the protocol developers work on, Spagni said.

"If I want to talk to Poloniex [for example], I have to go open a support ticket and pester them to push that up. I don't have anyone on speed dial," he said, pointing out that the process of determining consensus takes much more time and effort than people generally think.

Bitcoin Core developers [spoke about these same struggles](#) in interacting with a diverse and distributed community last year as members were looking to revamp the process of proposing code changes to allow more people to understand the consensus mechanism.

Yet, even with Core's willingness to bring others into the discussion, they were still looked at as the omnipotent dictators of bitcoin's future by some.

As it's advertised as a leaderless system, it remains unclear whether various user groups should advocate for changes – and how. For example, the Segwit2x agreement, a formalization of software changes put forth by businesses and miners, riled many for violating "community" processes largely followed by developers.

The difficult thing is that, given that these processes are often unspoken, they are hard to define.

In absence of any right or wrong, any group is capable of drawing its own lines, and just as equally, holding other groups accountable (sometimes angrily) to their violations.





There's also the matter of whether to look at bitcoin's recent scaling upgrade (and split) as a success or failure.

Ultimately, while the sudden creation of [bitcoin cash](#) hasn't been detrimental to bitcoin's price (arguably what many use to determine the cryptocurrency's standing), Spagni would argue that when any formerly united group of blockchain users goes in two different directions, it isn't ideal.

He told CoinDesk:

"The literal point when the blockchain changes, and those that aren't following the new rules get forked off the new chain, and if that leads to a split, you haven't done your job right."

And Spagni has some experience with this sort of thing since monero, with its \$1.8 billion market cap and more than \$55 million in daily volume, hard forks every six months.

These hard forks deliver new features to the protocol and keep the software on the network in sync, meaning nodes aren't running different software and behaving differently, making an unplanned fork more possible.

Instead of the vagueness that comes with voluntary upgrades, Spagni believes strongly there's merit in setting clear checkpoints for upgrades.

Monero uses a process called "flag-day activation," a term that denotes a point at which all nodes and miners switch to different code. This differs from bitcoin's "threshold activation," in which nodes and miners must signal support for a change for it to be locked in and activated.

The latter is what Bitcoin Core used to activate Segregated Witness.

"From our perspective, things like miners are an important part of the ecosystems, but typically and traditionally in bitcoin ... we've given them more importance than they probably should have," Spagni said.

For instance, while it's typically been fine to have miners in control on signaling soft fork support and activation, that wasn't the case with SegWit, according to Spagni.

"When trying to activate SegWit, which was not a particularly controversial or shouldn't have been a particularly controversial upgrade, [threshold activation] gave miners veto power," he said.

And so monero has kept voting out of its equation.

Do not feed the trolls

According to Spagni, no monero users have jumped ship because of its more aggressive hard-forking process.

While Spagni said two users complained about the increased size of a new transaction type in a recent update, he notes they were simply ignored due to overwhelming community support for the change. And overlooking people playing the opposition is something Spagni doesn't think is particularly insensitive.

Zooko Wilcox, founding member of another privacy-oriented cryptocurrency, zcash, agrees.

While he advocates for softer tactics, like setting a positive example and asking people to "play nice" first, there are times when people cross the line.

And Wilcox has no problem socially excluding people if they cross it.

"Individuals or groups who do more harm than they contribute, they can be excluded from the conversation. It's a good thing, not a bad thing, that you can exclude people from a seat at your table," Wilcox told CoinDesk.

Although, these protocols are riding a fine line of duplicity – and Spagni admits it:

"It's difficult as a community to encourage people to ask hard questions and continuously test each other, but on the other hand, unite when someone doesn't follow the groupthink and reject people and eject people who are causing division."

You've got an upgrade

Seemingly because of this notion blockchain participants should be given choice, Wilcox has adopted a softer fork method.

In his mind, splits should be easy and safe, but also predictable. In an effort to create this environment, Wilcox points to several features zcash offers.

The first is replay protection, where transactions on one chain are protected from being duplicated on the chain that hard forked. The process has been discussed in depth in bitcoin circles, since many [Core supporters contend](#) that Bitcoin Cash doesn't have adequate replay protection.

Secondly, Wilcox highlighted the reference client's auto-self-deprecation feature, which orders the client to turn itself off 18 weeks after an upgraded release.



ded to the newest software, they'll receive a message once the client is turned on again, saying the software "is too old to be the zcash blockchain, so you need to go upgrade to a newer version of me," said Wilcox.

This is nearly opposite of bitcoin. Actually, bitcoin's mechanisms for pushing people to upgrade are nearly non-existent, and Wilcox believes this has something to do with much of the community believing any small push from an individual or group of people is the beginning stages of coercion.

"There's almost a sense ... an implicit or unspoken thought [some in the community] might be having, that this is wrong, that it's necessary and morally imperative to support arbitrarily old versions of the software," said Wilcox.

While people can use old versions of the zcash software, but they won't get the zcash team's attention on diagnosing and fixing bugs and other performance upgrades.

Wilcox concluded:

"But we have opposite sense. We think it's necessary and morally imperative to communicate clearly to users which versions we support and which we don't."

Yet, controversy remains between which of these two ways – the methodical single arbitrator of the future versus an open, chaotic free for all – is the better one forward for securing consensus within cryptocurrency protocols. But maybe, a winner doesn't need to come out of this dyad, but an acceptance that both ways have their reasons for existing.

Disclosure: CoinDesk is a subsidiary of Digital Currency Group, which helped organize the Segwit2x agreement, and has an ownership stake in Zerocoin Electric Coin Company, developer of zcash.

Frustrated calculations image via Shutterstock

The leader in blockchain news, CoinDesk is a media outlet that strives for the highest journalistic standards and abides by a [strict set of editorial policies](#). CoinDesk is an independent operating subsidiary of Digital Currency Group, which invests in cryptocurrencies and blockchain startups.

Bitcoin

Scaling

zcash

Monero

Bitcoin Cash

Bitcoin

\$6,502.01

Ethereum

\$231.57

Bitcoin Cash

\$521.57

Litecoin

\$57.7

XRP

\$0.3033


coindesk | podcasts

Late Confirmation

Blood in the Water

Subscribe ▶

View all Podcasts →



Analyst

Circle: Manager, Talent Rewards

Circle: Manager, Talent Operations

Don't miss a single story

Sign up for Blockchain Bites and CoinDesk Weekly, sent Sunday-Friday. By signing up, you agree to our terms & conditions and privacy policy


Email Address

SUBSCRIBE


Have a breaking story?

Let us know here »


Most Read




Bitcoin's Double-Digit Drop Negates Long-Term Bull Market



Ether, ADA Crypto Prices Hit Lowest Levels In Over 1 Year



Bull Trap? Bitcoin Price Slides Below \$7K Despite Strong Indicators



About

Press

Events

Editorial policy

Comments policy

Terms & conditions

Privacy policy

Jobs

Advertising

Newsletter

English ▾