



Own a piece of Bitcoin history.
Buy a collector's edition Bitcoin Magazine.

Blocktrail CTO and BitcoinJS Co-Maintainer Ruben De Vries: Segregated Witness Not Very Complicated



3:28 PM CST

January 25th, 2016

by Aaron van Wirdum

- Aa +



SHARE



TWEET



UPVOTE



SHARE



EMAIL





The long-lasting block-size dispute has catapulted into the center of attention again. One of the most talked about developments right now is Segregated Witness, of which a public testnet iteration was launched last week. The innovation as recently proposed by Blockstream co-founder and Bitcoin Core developer Dr. Pieter Wuille is a centerpiece of a scalability “roadmap” set out by Bitcoin Core.

But relying on Segregated Witness as the next step of Bitcoin’s scalability process is contended by recently launched Bitcoin Core fork Bitcoin Classic. Rather than a Segregated Witness soft fork, Bitcoin Classic prefers to deploy a “cleaner” hard fork in order to increase the block-size limit to 2 megabytes.

To find out where the development community stands on this issue, Bitcoin Magazine reached out to library and wallet developers, those who will need to do the heavy lifting needed to utilize Segregated Witness once rolled out.

In part 1: Blocktrail CTO and BitcoinJS co-maintainer Ruben de Vries.

Segregated Witness

Wuille’s Segregated Witness proposal offers several improvements to the Bitcoin network. The

Bitcoin's Segregated Witness proposal offers several improvements to the Bitcoin network. The benefit that probably received most attention is its potential to effectively increase the block size to some 1.75 megabytes to 2 megabytes. Interestingly, however, many developers are more excited about the other improvements Segregated Witness has to offer, which they believe makes it well worth the effort.

De Vries, too, emphasized that Segregated Witness offers more than just added block space:

““Even if we wouldn't use the deployment of Segregated Witness to increase the block size in a nifty way, it fixes various issues that would benefit Bitcoin tremendously, and should be deployed as soon as possible, regardless. Being able to increase the block size as a side effect presents us with a chance we should clearly embrace, especially considering that it can be done on almost the same timeline as alternative block-size increase proposals.”

One of the main arguments against Segregated Witness, is that it presents an “ugly” workaround of existing code. This would lay an added burden on library and wallet developers, as they would need to re-write their code to utilize the innovation.

De Vries believes this effort is manageable, however. Most of the work needs to be done by library maintainers, a group of developers who essentially provide a standard for all wallets using a specific programming language. All other wallet developers using that programming language merely need to add some minor details.

“It's not very complicated if you already know the ins and outs of the Bitcoin protocol, which a library maintainer will,” De Vries said. “To grasp the concept when you don't is a bit harder. But then again, if you don't know the ins and outs of the Bitcoin protocol, there's no real reason for you to know the details of Segregated Witness in the first place.”

De Vries himself has been developing for the Segregated Witness testnet for several weeks now.

and the cross-platform Blocktrail wallet will support Segregated Witness transactions as soon as it is rolled out on the Bitcoin network.

“I started experimenting with the Segregated Witness testnet even before it entered the public phase, in order to start working on support for a bunch of libraries I contribute to a lot,” De Vries said. “Getting as many libraries to support Segregated Witness as soon as possible will help a lot with adoption, and, as a result, will make it so that we can get the increased block-size effect of Segregated Witness as soon as possible.”

On Soft Forks and Hard Forks

Perhaps the most notable difference between Bitcoin Core and Bitcoin Classic is that the former prefers a soft fork increase through Segregated Witness. This can be employed through miner-support only, and is, therefore, considered a safer solution by Bitcoin Core developers. The Bitcoin Classic team, however, believes these risks are overblown, and considers a hard fork more desirable.

For De Vries, the solution is clear-cut, however. He believes a soft fork through Segregated Witness is the best way forward for now.

“Considering how much the Bitcoin Core development team has done for us in the past year, I feel that pushing them aside by forking is an insult to their expertise: They consider a hard fork too dangerous right now,” De Vries said. “Moreover, it could result in them losing their motivation or even quitting. It’s simple, really. Segregated Witness fixes various issues that should have been in Bitcoin from the start, and, as a side effect, we can avoid a hard fork for now, which is great.”

For more information on Segregated Witness, see Bitcoin Magazine’s [three-part series](#) on the subject.

Read More: [bitcoin](#) [core](#) [developers](#) [megabytes](#) [more...](#)

 COMMENT

 SHARE

 TWEET

 UPVOTE

 SHARE

 EMAIL

PayPal: Unprecedented Disruption in Payments and Financial Services



[SHARE](#)[TWEET](#)[UPVOTE](#)[SHARE](#)[EMAIL](#)

“In a telling move about the future of money, PayPal has added a Bitcoin entrepreneur to its board of directors,” *CNN Money* [reports](#). Fintech entrepreneur Wences Casares joined the board on Tuesday, [PayPal announced](#) Wednesday. The move has been interpreted as the beginning of a new phase in PayPal’s timid love story with Bitcoin, which could conceivably culminate in open adoption.

“We’ve entered a period of unprecedented disruption in payments and financial services driven by the mass adoption of mobile technology and the digitization of cash,” said PayPal President and CEO Dan Schulman. “Wences’ long and successful track record as an international fintech entrepreneur with a focus on next-generation payment and cryptocurrency is a perfect fit for PayPal at this time. His unique line of sight into the future of commerce is ideally aligned with PayPal’s vision of transforming the management and movement of money for people around the globe.”

The fact that cryptocurrency and the transformation of money transfer are explicitly mentioned together in PayPal's official announcement is a telling sign. According to *CNN Money*, the appointment of Casares to the PayPal board of directors is yet another vote of confidence in Bitcoin's technology. PayPal, the leading company in Internet-based payments, had already shown interest in Bitcoin payments and the distributed blockchain technology that powers the Bitcoin network, and taken the first cautious steps toward integrating blockchain technology in its operations.

One of the clearest indications of PayPal's interest in Bitcoin is Paypal's subsidiary Braintree. The company, which was acquired by eBay (the former parent company of PayPal) for \$800 million in September 2013 and became part of PayPal after the split, permits merchants to accept Bitcoin payments seamlessly in partnership with Coinbase. The Braintree Bitcoin payment service is currently in public beta.

“No doubt a financial technology visionary, Casares has become best known for pioneering Bitcoin in recent times and that's exactly why PayPal has added him to its board,” notes TechCrunch. “It's exciting to see PayPal, the daddy of online payments and a true disruptor when it started out, open itself up to these new possibilities.” Casares is well positioned to help PayPal in identifying and acquiring promising Bitcoin companies and unlocking new blockchain-based opportunities for its business worldwide.

“I am honored to serve on the board of an iconic global company dedicated to driving the transformation of money on a global scale,” said Casares. “I look forward to working together with the PayPal board and leadership team to continue to deliver their compelling vision.”

Casares is the CEO of Xapo, a Swiss company that offers Bitcoin digital wallets and debit cards. Xapo, which has raised \$40 million to date, announced in May that it was relocating its corporate headquarters to Zurich, Switzerland, to take advantage of the country's strong privacy and banking secrecy. Xapo's primary deep cold storage vault is also located in Switzerland, with

additional secure sites deployed around the globe.

The company takes aggressive initiatives to promote Bitcoin payments worldwide. For example, in April Xapo partnered with social network Taringa!, the second-most-popular social network after Facebook and one of the main destinations in the Latin American Web, to compensate its content-providing members in bitcoins, offering a service that could boost Bitcoin adoption in the region.

Members of the Bitcoin community have wondered if this is just the first of ambitious and aggressive initiatives by PayPal. For example, PayPal could integrate Xapo in its own operations, to complement Braintree’s merchant-facing infrastructure with appropriate consumer-facing services. Another possibility is that Xapo could be acquired and become a PayPal company.

Photo Geoff Livingston / Flickr(CC)

Read More: [paypal](#) [bitcoin](#) [payments](#) [xapo](#) [more...](#)


 COMMENT

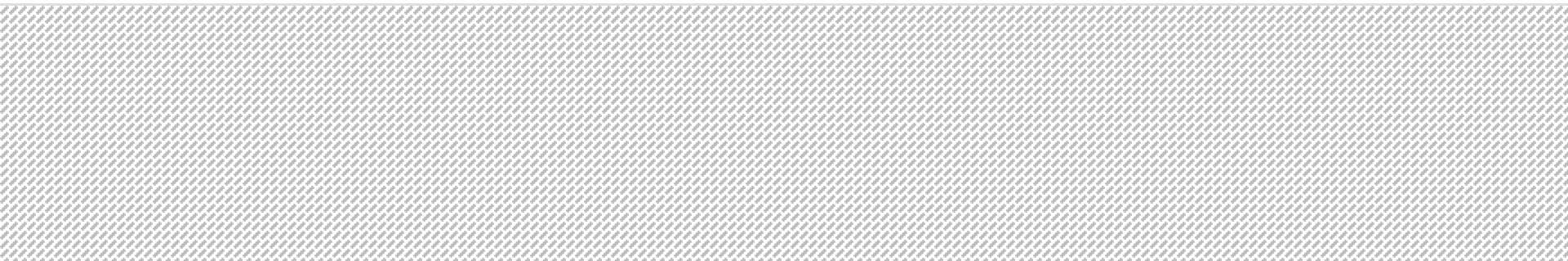
 SHARE

 TWEET

 UPVOTE

 SHARE

 EMAIL





[About](#) [Advertising](#) [Careers](#) [Contact](#) [Terms of Service](#) [yBitcoin](#) [Store](#) [Facebook](#) [Twitter](#) [Reddit](#)
[RSS](#)

© Copyright 2015 BTC Inc. All Rights Reserved.