



WHEN SEGWIT?

An open letter to those who love bitcoin.

Dear bitcoin community:

We need to break bitcoin.

SegWit is an impressive upgrade that reduces transaction size and packs more transactions into the bitcoin network, which lowers fees and sets the foundation for future scaling prospects. Pretty much everybody who loves bitcoin agrees that the more we all use SegWit, the better off we'll be.

Yet, surprisingly, SegWit is only utilized by around 40% of bitcoin transactions today. This means the throughput of the bitcoin network is not fully optimized. Available space is being wasted, which results in higher fees for everyone. Right now fees are fairly affordable, but it won't be long until we see \$50 transaction fees again, just like we did last year. So why hasn't Segwit reached 100% adoption?

One reason could be a lack of sufficient incentives. The majority of current SegWit transactions are wrapped inside of an address format called P2SH, which is backwards-compatible with clients that don't support SegWit. This allows the receiver of a transaction to utilize Segwit even if the sender doesn't support it yet. This is a great way to let individual users do their own part to drive adoption forward, but it doesn't do much to encourage the sender of the transaction to upgrade.

Bech32 is a new address format created specifically for SegWit. It allows the direct use of SegWit without the wrapper, on top of other improvements, but is not backwards compatible with clients that don't support SegWit. The hope for SegWit, as shared by Andreas Antonopoulos ([@aantonop](#)), Peter Wuille ([@pwuille](#)), and many other industry insiders, is to transition fully to Bech32 and move away from wrapping SegWit transactions in P2SH.

The fact that Bech32 isn't backwards compatible can actually be used as a tool to speed up adoption. If we can rapidly establish Bech32 as the default address format, and discourage the use of P2SH addresses, we can create a temporary rift where senders are obliged to upgrade their software in order to serve receiving customers. The good news is that sending to a Bech32 address isn't a particularly challenging feature to implement, making the transition reasonably straightforward. Indeed, BRD has had this capability since early 2018.

One could argue SegWit isn't yet at 100% because there is little reason to move away from backwards-compatible address formats. Thus, we propose the need to "break" bitcoin by dropping support for these formats altogether, creating a compelling reason for both senders and receivers to upgrade their support of bitcoin and let it become the best it can be.

To do our part, the BRD crypto wallet will convert to 100% Bech32 receive addresses. Support will start with an opt-in period beginning in October 2018, allowing all forward-thinking pioneers to take the plunge into the new Bech32 world and turn their smartphones into a pure SegWit machine. Shortly thereafter, these changes will be rolled out to our entire user base as the default setting.

In preparation of this transition, it is important to get as many companies and services as possible to start supporting Bech32. We are proud to have already secured pledges from 5 of our valued partners—Changelly, Simplex, Kraken, Coinberry, and Coinify—to update their software and enable the ability to send to Bech32 to continue serving our customers.

But we won't stop there, and neither should you. As far as we are concerned, this is a community-driven campaign where all advocates are welcome. On this page we will collect a comprehensive list of companies and services that offer Bech32 functionality to illustrate progress made towards this goal. We will update this page regularly, and if you know of a logo that should be here but isn't, or if you are a service that needs a little help adding Bech32 support, please send an email to Aaron Lasher at lasher@brd.com.

To all the bitcoiners out there, we encourage you to join us: Share this page, start a discussion, be among the first to go full Bech32, and with your help, we'll get SegWit to 100% and take bitcoin to the moon.

Sincerely,

Aaron Lasher, Co-Founder and Chief Strategy Officer at BRD

James MacWhyte, Chief Product Officer at BRD

Aaron Voisine, Co-Founder and President at BRD

“ To all the bitcoiners out there, we encourage you to join us: share this page, start a discussion, be among the first to go full Bech32, and with your help, we'll get SegWit to 100% and take bitcoin to the moon.