Countdown to SegWit: These Are the Dates to Keep an Eye On

Aaron van Wirdum

10:50 AM
JULY, 03 2017

Bitcoin's very public scaling debate is entering a crucial phase. Two of the most popular scaling proposals available today — **BIP148** and **SegWit2x** — both intend to trigger **Segregated Witness** ("SegWit") activation within a month, which means that the protocol upgrade could be live within two.

At the same time, there is a very real risk that Bitcoin "splits." Both BIP148 and SegWit2x could diverge from the current Bitcoin protocol, which could in turn lead to even more splits.

Here is a list of dates for July, August and beyond to keep an eye on.

Recap: Segregated Witness Activation

First, a brief recap on **Segregated Witness**, and its potential activation methods.

SegWit is a backwards compatible protocol upgrade originally proposed by the **Bitcoin Core** development team. It has been a centrepiece of the scaling **roadmap** supported by Bitcoin Core since the protocol upgrade was first proposed in December 2015, and it is implemented on many active Bitcoin nodes on the network today. SegWit is now also part of the "**New York Agreement**": an alternative scaling roadmap forged between a significant number of Bitcoin companies, including many miners. And **Bitcoin Improvement Proposal 148**, or BIP148, a **user activated soft fork** (UASF) scheduled for August 1st, also intends to activate SegWit.

The difference lies in how the activation should happen.

The first and original option was proposed by the Bitcoin Core development team. Their SegWit code, defined by **BIP141**, activates if 95 percent of hash power within a single difficulty period of about two weeks signals readiness, before November 15th. Assuming that the miners who signal readiness are actually ready to support the upgrade, risks of a split in Bitcoin's blockchain and currency are minimal.

However, currently only some 40 to 45 percent of hash power is signaling readiness for BIP141. This is why a segment of Bitcoin users plans to activate SegWit with the BIP148 UASF. Starting on August 1st, their nodes will reject all blocks that do not signal readiness for BIP141. If this proposal is supported by any majority of miners (by hash power), these miners should always claim the longest valid chain, which should activate SegWit on all SegWit-ready Bitcoin clients and avoid a split. But if this proposal is only supported by a minority of miners, a "BIP148 chain" could split off from the current protocol.

The New York Agreement, also referred to as the "Silbert Accord" or "SegWit2x," plans to activate SegWit through **BIP91**. Like BIP148, all BIP91 nodes would reject any blocks that do not signal readiness for BIP141. But unlike BIP148, BIP91 nodes would only do this once 80 percent of hash power signals that they support BIP91, within a period about two days. This should also minimize the chance of a split.

However, the second step of the New York Agreement is a hard fork to double Bitcoin's "base block size." This change, as opposed to Segregated Witness itself, is not backwards compatible, and could therefore lead to a

"split" as well.

There is also such a thing as miners signaling intent to support the New York Agreement, but this is effectively **meaningless** and will be ignored for the purpose of this article.

Now for the dates...
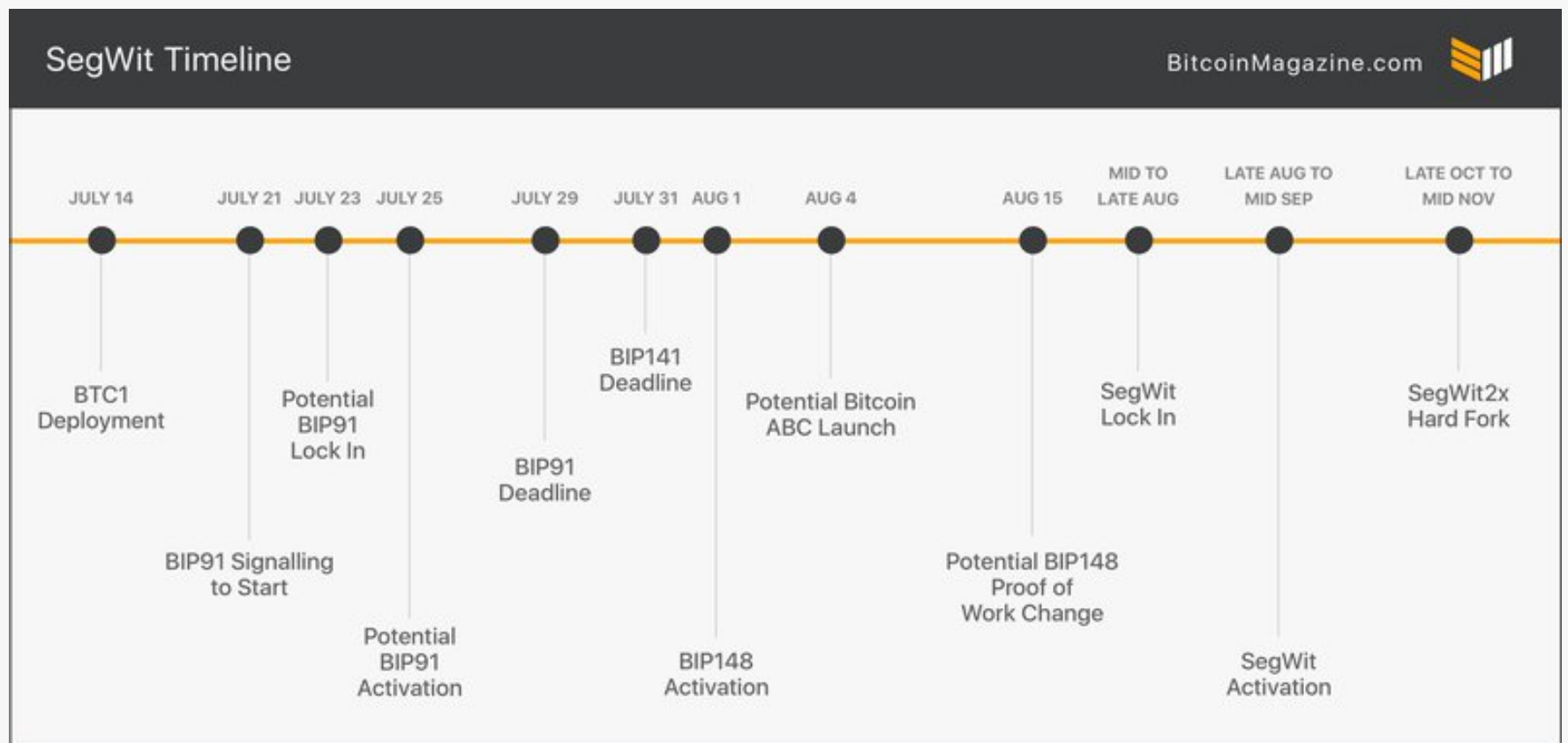
July 14: BTC1 Deployment

The software client that resulted from the New York Agreement is a fork of the Bitcoin Core codebase, called "BTC1." BTC1's beta software was **released** on June 30th. But according to the SegWit2x **roadmap**, July 14th is the day that signatories to the New York Agreement should actually install the BTC1 beta software and test it for themselves.

This shouldn't affect regular users or miners much, however.

July 21: BIP91 Signaling to Start

The SegWit2x development team aims for July 21st to be the day that BTC1 nodes are actually up and running, and, importantly, the day that miner signaling should commence.

This shouldn't really affect regular users either.

But if you are a miner, you may want to help activate SegWit by signalling readiness for BIP91. (This is done by mining "bit 4" blocks; for example, by mining with BTC1 or with Bitcoin software that includes a BIP91 patch.)

July 23 (at the earliest): BIP91 Lock In

The precise threshold for BIP91 activation requires that within a pre-defined series of 336 blocks, 269 blocks must signal readiness. That's some 80 percent of hash power, over about 2 1/3 days. So assuming the SegWit2x roadmap is followed, BIP91 could, at the very soonest, lock in on July 23rd.

Again, this shouldn't really affect regular users.

But if you are a miner, and BIP91 does activate, you now have another day or two to comply with the BIP91 soft fork. If you don't, you risk mining invalid blocks.

July 25 (at the earliest): BIP91 Activation

On July 25th, another 336 blocks after BIP91 "lock in", BIP91 could actually go into effect, at the soonest. Any blocks that do not signal readiness for Segregated Witness (per BIP141) will now be rejected.

This still shouldn't really affect regular users.

But if you are miner, you should now only mine blocks, and only mine on top of blocks, that signal readiness for SegWit (BIP141). Else you risk having your blocks rejected by a hash power majority.

July 29: BIP91 Deadline

If Bitcoin miners want to avoid a "split" in Bitcoin's blockchain and currency, July 29th is a first deadline day for them.

To ensure that BTC1's BIP91 is activated in time to be compatible with BIP148, it should be locked in on this day at the very latest, say, before 08:00 UTC. (That's 4 am on the U.S. east coast.) But sooner is better: The closer to the deadline BIP91 locks in, the bigger the risk it doesn't activate in time.

If BIP91 has not activated by this deadline, Bitcoin may well be heading for a chain-split.

If this happens, and if you are a regular user, and you haven't prepared for a potential BIP148 UASF chain-split yet, you now have two days left to do so. And you really should. **This article** explains how.

If BIP91 has not activated by July 29th and you are a miner, you now have two days to decide on which chain you will mine on August 1st: on the BIP148 chain or on the original ("Legacy") chain.

July 31: BIP141 Deadline

Technically, July 31st is the miners' second deadline day to avoid a split.

On this day (UTC), at the very latest, either BIP91 must activate, or BIP141 must lock in. In other words, if BIP91 did not lock in in time, there must now have been a two-week difficulty period in which 95 percent of hash power signals support for SegWit.

In reality, the chance is small that July 31st actually coincides with the closing day for a difficulty period. And even if it does, it's unlikely that it will take until this day before it's clear whether the 95 percent threshold will be met.

As such, both users and miners should have probably already prepared for a potential split, as explained for July 29th. But July 31st really is your last chance to get ready.

August 1: BIP148 Activation

This is the day BIP148 activates, which makes it the third and final deadline day for miners to avoid a split.

On August 1st, at 00:00 UTC (note that this is still July 31st in the U.S.), all BIP148 nodes will start rejecting any blocks that do not signal readiness for Segregated Witness (per BIP141). If Bitcoin Core's BIP141 or BTC1's BIP91 have locked in and/or activated in time, there should be no chain-split.

If neither has happened, a majority of miners (by hash power) now have one last chance to avoid a chain-split: by supporting BIP148 themselves. This would ensure they always (re-)claim the longest valid chain according to all current Bitcoin nodes, and will activate SegWit through BIP141.

If BIP141, BIP91 nor BIP148 have attracted sufficient hash power by August 1st, but BIP148 does gain some traction, the chain could split on this day. If that happens, there will be two types of "Bitcoin," which we'll refer to as "148 Bitcoin" or "148BTC" for the BIP148 side of the split, and "Legacy Bitcoin" or "LegacyBTC" for the other side. (This split could resolve over time if 148 Bitcoin ever reclaims the longest chain, but that's not the focus of this article.)

If you own bitcoin (that is: private keys) at the time of split you should automatically own both 148BTC and LegacyBTC. Though, to access both types, you probably need to download new software. That said, if you are a

regular user, it is probably best to initially halt any and all transactions, at least until the situation is more clear. Failing to do so may cost you money! For more information, see **this article**.

If a split happens and you are a miner, you should have by now decided on which chain you'll mine. (Of course, you can still switch at any time. You may simply want to mine the most profitable chain, for example.)

August 4: Potential Bitcoin ABC Launch

Although the exact date is not set in stone, August 4th may see the introduction of a new "Bitcoin": **Bitcoin ABC**.

Major Bitcoin mining hardware producer Bitmain **recently announced** that if BIP91 does not activate before August 1st and BIP148 is showing signs of life after August 1st, it will launch a "contingency plan." More recently, the implementation to embody this contingency plan — named "Bitcoin ABC" — was announced at the **Future of Bitcoin** conference.

Bitcoin ABC will share a common history with Bitcoin up until August 1st, but will, for the first couple of days after that, probably be privately mined by Bitmain. It will also include several new and incompatible protocol rules, perhaps most importantly an increased block size limit.

If you owned bitcoin at the time of split — August 1st, 00:00 UTC — you should automatically own "Bitcoin ABC" as well. But you may, in that case, need to download software to be able to send (and receive) the coins. More information will likely become available if this event occurs.

If you are a miner you should be able to mine Bitcoin ABC on August 4th. (And perhaps sooner.)

August 15: Potential BIP148 Proof-of-Work Change

While this date is not set in stone either, August 15th could see the introduction of yet another type of "Bitcoin," which we'll refer to as "NewPoW Bitcoin" or "NewPoWBTC."

As a UASF, August 1st's BIP148 fork is initially effectuated by users — not miners. Users will start to reject any blocks that do not signal readiness for Segregated Witness (per BIP141). This should incentivize miners to follow the BIP148 chain (ideally to the point where it's the only chain left). But whether this will actually happen remains to be seen. So far, few miners have publicly indicated they will support the UASF.

If miner support on 148 Bitcoin remains low, (some of) its users may opt to implement a hard fork to change the proof-of-work algorithm. This would "fire" the existing group of miners by making their specialized ASIC

mining hardware obsolete on the BIP148 side of the split, and could open the door for new miners — possibly re-decentralising the mining landscape back to home users with CPUs or GPUs. (At least temporarily.)

An open BIP148 "working group" on a sub-channel of the "**Bitcoin Core Community**" Slack is currently working out the details to be proposed. But it seems that if by August 15th less than 15 percent of total hash power mines on 148 Bitcoin, this hard fork will be deployed. This will make the split with "Legacy Bitcoin" definite. It could technically also lead to another split on the 148 Bitcoin side, if some of its users decline to join the hard fork that changes the proof-of-work algorithm.

If you are a regular user and owned bitcoin at the time of the August 1st split, and you didn't spend any until August 15th, you should now also own NewPoWBTC. If you bought or earned 148BTC between August 1st and August 15th, you should now (also) own NewPoWBTC.

But if you did spend bitcoins on any side of the split, that's not as certain. Again, if you want to be on the safe side, don't transact at all until the situation becomes more clear. (For more information, see **this article**.)

If you are one of the few miners that was mining on 148 Bitcoin with ASIC hardware, you may now want to point your hardware elsewhere — or shut it down completely. (This depends, of course, on whether or not it's still profitable to mine 148BTC or anything else.)

And of course, anyone should by now be able to mine on NewPoWBTC without specialized ASIC hardware.

Mid- to late- August: SegWit Lock In

If miners avoided a chain-split through BIP141, BIP91 or BIP148, Segregated Witness should at the latest lock in between mid-August or late August. This should be a bit a non-event if it happens through BIP91 or BIP148, as it would at this point be expected, and wouldn't change much for anyone.

But what the lock-in means is that all SegWit ready clients will start enforcing the new rules in the next difficulty period: after another two weeks. So if you are a regular user and would like to use the new features or want to maintain top-notch security, you now have two weeks to upgrade to software that enforces SegWit.

If a chain-split is not avoided, the situation could become far more complex. By mid August, there could potentially be one, two, three or maybe even four "Bitcoins": "148 Bitcoin", "NewPoW Bitcoin", "Bitcoin ABC," as well as "Legacy Bitcoin".

At the time of writing this article, it's hard to say how best to deal with this situation. For a regular user, it's always best to hold onto your private keys, and it's probably best not to transact at all until the situation resolves in some way or another. (For more information, see **this article**.)

For a miner, it's probably best to just mine the most profitable chain.

Late August to Mid-September: SegWit Activation

If a chain-split is avoided, SegWit should activate around this time. If you're running a compatible client by now, you can begin to enjoy the new features while maintaining top-notch security.

If a chain-split was not avoided, the situation will probably still be too complex to predict.

Late October to Mid-November: SegWit2x Hard Fork

Toward the end of this year (though potentially even up to early 2018), the hard fork part of SegWit2x should take place. To be exact, this hard fork activates on BTC1 clients three months after SegWit locks in. This activation means that a "base block" bigger than 1 megabyte should be mined, which makes BTC1 clients incompatible with all Bitcoin clients that do not have the hard fork code implemented.

At this point in time, it seems almost certain that not everyone will change their software to support this hard fork. Bitcoin's development community in particular has almost unanumously **rejected** the proposal, while several companies have indicated their intentions not to support the change, and not all users seem on board either. As such, this could lead to

another chain-split. (Theoretically, this could lead to the fifth "Bitcoin," though it seems very unlikely there would still be four "Bitcoins" by then in the first place.)

How to deal with this situation as a regular users will be announced on Bitcoin Magazine closer to the actual date.

If you are a miner and you were only running the BTC1 client to help activate SegWit with no intention to support the hard fork, you should make sure to switch back to a non-BTC1 client by this point.

This article will be updated as the news develops.