

BIP: 343  
Layer: Consensus (soft fork)  
Title: Mandatory activation of taproot deployment  
Author: Shinobius <quantumedusa@gmail.com>  
Michael Folkson <michaelfolkson@gmail.com>  
Comments-Summary: No comments yet.  
Comments-URI: <https://github.com/bitcoin/bips/wiki/Comments:BIP-0343>  
Status: Final  
Type: Standards Track  
Created: 2021-04-25  
License: BSD-3-Clause  
CC0-1.0

## Abstract

This document specifies a BIP8 (LOT=true) deployment to activate taproot.

## Motivation

The Taproot soft fork upgrade has been assessed to have overwhelming community consensus and hence should attempt to be activated. Lessons have been learned from the BIP148 and BIP91 deployments in 2017 with regards to giving many months of advance warning before the mandatory signaling is attempted. The mandatory signaling is only required if miners have failed to meet the signaling threshold during the BIP8 deployment. It is important that mandatory signaling is included as without it miners would effectively have the ability to indefinitely block the activation of a soft fork with overwhelming consensus.

## Specification

This BIP will begin an activation signaling period using bit 2 at blockheight 681408 with a minimum activation height of 709632 and an activation threshold of 90%. The signaling period will timeout at blockheight 760032 with a latest activation height of 762048. Lockinontimeout (LOT) is set to true so mandatory signaling will be enforced in the last signaling period before the timeout height. Blocks without the signaling bit 2 set run the risk of being rejected during this period if taproot is not locked in prior. This BIP will cease to be active when taproot is locked in.

## Reference implementation

- <https://github.com/BitcoinActivation/bitcoin>

## Backward Compatibility

As a soft fork, older software will continue to operate without modification. Non-upgraded nodes, however, will consider all SegWit version 1 witness programs as

anyone-can-spend scripts. They are strongly encouraged to upgrade in order to fully validate the new programs.

## Compatibility with later alternative activations

The activation mechanism “Speedy Trial” as proposed by Russell O’Connor and outlined in this bitcoin-dev mailing list post by David Harding was released in Bitcoin Core. It is effectively a BIP8 activation mechanism with one exception: start height and timeout height were defined using median time past (MTP) rather than block heights. It uses signaling bit 2, was deployed between midnight April 24th 2021 and midnight August 11th 2021, has a minimum activation height of 709632 and intends to activate BIPs 340, 341, and 342. The BIP8(LOT=true) deployment is compatible with the “Speedy Trial” deployment in Bitcoin Core as there was not a discrepancy between MTP and block height for the defined start heights.

The BIP8 (LOT=true) deployment has also been deliberately designed to be compatible with a future BIP8(LOT=false) or BIP8(LOT=true) deployment in Bitcoin Core assuming Bitcoin Core releases one of these activation mechanisms in the event of the Speedy Trial deployment failing to activate.

## Rationale

The deployment of BIP148 demonstrated that multiple implementations with different activation mechanisms can incentivize the necessary actors to act so that the different deployments activate in sync. A BIP8 LOT=true deployment can run in parallel with other BIP8 activation mechanisms that have eventual mandatory signaling or no mandatory signaling. Eventual mandatory signaling ensures that miners cannot prevent the activation of a desired feature with community consensus indefinitely.

## Acknowledgements

Thanks to Shaolin Fry and Luke Dashjr for their work on BIP148 and BIP8 which were important prerequisites for this proposal.

## References

- BIP8 Version bits with lock-in by height
- BIP148 Mandatory activation of segwit deployment
- BIP340 Schnorr Signatures for secp256k1
- BIP341 Taproot: SegWit version 1 spending rules
- BIP342 Validation of Taproot Scripts
- Taproot benefits

## **Copyright**

This document is dual licensed as BSD 3-clause, and Creative Commons CC0 1.0 Universal.