BIP 0112 - CHECKSEQUENCEVERIFY (soft fork)

return to the Bitcoin Improvement Proposals

Table 1: Data sheet for CHECKSEQUENCEVERIFY

Title	CHECKSEQUENCEVERIFY
Layer	Consensus (soft fork)
Author	BtcDrak, Mark Friedenbach, Eric Lombrozo
Comments-Summary	No comments yet.
Comments-URI	https://github.com/bitcoin/bips/wiki/Comments:BIP-0112
Status	Final
Type	Standards Track
Created	2015-08-10
Post History	
Description	https://github.com/bitcoin/bips/blob/master/bip-0112.mediawiki
License	PD

> **Note**: The following is an excerpt from the official Bitcoin site. It is provided here as a convenience and is not authoritative. Refer to the original document(s) as the authoritative reference.

Abstract

This BIP describes a new opcode (CHECKSEQUENCEVERIFY) for the Bitcoin scripting system that in combination with BIP 68 allows execution pathways of a script to be restricted based on the age of the output being spent.

Summary

CHECKSEQUENCEVERIFY redefines the existing NOP3 opcode. When executed, if any of the following conditions are true, the script interpreter will terminate with an error:

- *the stack is empty; or*
- *the top item on the stack is less than 0; or*
- *the top item on the stack has the disable flag (1 « 31) unset; and*
  a. the transaction version is less than 2; or
  b. the transaction input sequence number disable flag (1 « 31) is set; or
  c. the relative lock-time type is not the same; or
  d. the top stack item is greater than the transaction input sequence (when masked according to the BIP68);

Otherwise, script execution will continue as if a NOP had been executed.

BIP68 prevents a non-final transaction from being selected for inclusion in a block until the corresponding

input has reached the specified age, as measured in block-height or block-time. By comparing the argument to CHECKSEQUENCEVERIFY against the nSequence field, we indirectly verify a desired minimum age of the the output being spent; until that relative age has been reached any script execution pathway including the CHECKSEQUENCEVERIFY will fail to validate, causing the transaction not to be selected for inclusion in a block.

Motivation

BIP68 repurposes the transaction nSequence field meaning by giving sequence numbers new consensus-enforced semantics as a relative lock-time. However, there is no way to build Bitcoin scripts to make decisions based on this field. By making the nSequence field accessible to script, it becomes possible to construct code pathways that only become accessible some minimum time after proof-of-publication. This enables a wide variety of applications in phased protocols such as escrow, payment channels, or bidirectional pegs.