BIP 0113 - Median time-past as endpoint for lock-time calculations (soft fork)

return to the Bitcoin Improvement Proposals

Table 1: Data sheet for Median time-past as endpoint for lock-time calculations

Title	Median time-past as endpoint for lock-time calculations
Layer	Consensus (soft fork)
Author	Thomas Kerin, Mark Friedenbach
Comments-Summary	No comments yet.
Comments-URI	https://github.com/bitcoin/bips/wiki/Comments:BIP-0113
Status	Final
Type	Standards Track
Created	2015-08-10
Post History	
Description	https://github.com/bitcoin/bips/blob/master/bip-0113.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 is a proposal to redefine the semantics used in determining a time-locked transaction's eligibility for inclusion in a block. The median of the last 11 blocks is used instead of the block's timestamp, ensuring that it increases monotonically with each block.

Motivation

At present, transactions are excluded from inclusion in a block if the present time or block height is less than or equal to that specified in the locktime. Since the consensus rules do not mandate strict ordering of block timestamps, this has the unfortunate outcome of creating a perverse incentive for miners to lie about the time of their blocks in order to collect more fees by including transactions that by wall clock determination have not yet matured.

This BIP proposes comparing the locktime against the median of the past 11 block's timestamps, rather than the timestamp of the block including the transaction. Existing consensus rules guarantee this value to monotonically advance, thereby removing the capability for miners to claim more transaction fees by lying about the timestamps of their block.

This proposal seeks to ensure reliable behaviour in locktime calculations as required by BIP65 (CHECKLOCKTIMEVERIFY) and matching the behavior of BIP68 (sequence numbers) and BIP112

(CHECKSEQUENCEVERIFY).