# BIP 0068 - Relative lock-time using consensus-enforced sequence numbers (soft fork)

return to the Bitcoin Improvement Proposals

Table 1: Data sheet for Relative lock-time using consensus-enforced sequence numbers

| | |
|---|---|
| Title | Relative lock-time using consensus-enforced sequence numbers |
| Layer | Consensus (soft fork) |
| Author | Mark Friedenbach, BtcDrak, Nicolas Dorier, kinoshitajona |
| Comments-Summary | No comments yet. |
| Comments-URI | https://github.com/bitcoin/bips/wiki/Comments:BIP-0068 |
| Status | Final |
| Type | Standards Track |
| Created | 2015-05-28 |
| Post History | |
| Description | https://github.com/bitcoin/bips/blob/master/bip-0068.mediawiki |

**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 introduces relative lock-time (RLT) consensus-enforced semantics of the sequence number field to enable a signed transaction input to remain invalid for a defined period of time after confirmation of its corresponding outpoint.*

## Motivation

*Bitcoin transactions have a sequence number field for each input. The original idea appears to have been that a transaction in the mempool would be replaced by using the same input with a higher sequence value. Although this was not properly implemented, it assumes miners would prefer higher sequence numbers even if the lower ones were more profitable to mine. However, a miner acting on profit motives alone would break that assumption completely. The change described by this BIP repurposes the sequence number for new use cases without breaking existing functionality. It also leaves room for future expansion and other use cases.*

*The transaction nLockTime is used to prevent the mining of a transaction until a certain date. nSequence will be repurposed to prevent mining of a transaction until a certain age of the spent output in blocks or timespan. This, among other uses, allows bi-directional payment channels as used in Hashed Timelock Contracts (HTLCs) and BIP112.*