BIP 0030 - Duplicate transactions (soft fork)

return to the Bitcoin Improvement Proposals

Table 1: Data sheet for Duplicate transactions

Title	Duplicate transactions
Layer	Consensus (soft fork)
Author	Pieter Wuille
Comments-Summary	No comments yet.
Comments-URI	https://github.com/bitcoin/bips/wiki/Comments:BIP-0030
Status	Final
Type	Standards Track
Created	2012-02-22
Post History	
Description	https://github.com/bitcoin/bips/blob/master/bip-0030.mediawiki
License	BSD-2-Clause

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 document gives a specification for dealing with duplicate transactions in the block chain, in an attempt to solve certain problems the reference implementation has with them.

Copyright

Motivation

So far, the Bitcoin reference implementation always assumed duplicate transactions (transactions with the same identifier) didn't exist. This is not true; in particular coinbases are easy to duplicate, and by building on duplicate coinbases, duplicate normal transactions are possible as well. Recently, an attack that exploits the reference implementation's dealing with duplicate transactions was described and demonstrated. It allows reverting fully-confirmed transactions to a single confirmation, making them vulnerable to become unspendable entirely. Another attack is possible that allows forking the block chain for a subset of the network.