BIP 0037 - Connection Bloom filtering

return to the Bitcoin Improvement Proposals

Table 1: Data sheet for Connection Bloom filtering

Title	Connection Bloom filtering
Layer	Peer Services
Author	Mike Hearn, Matt Corallo
Comments-Summary	No comments yet.
Comments-URI	https://github.com/bitcoin/bips/wiki/Comments:BIP-0037
Status	Final
Type	Standards Track
Created	2012-10-24
Post History	
Description	https://github.com/bitcoin/bips/blob/master/bip-0037.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 adds new support to the peer-to-peer protocol that allows peers to reduce the amount of transaction data they are sent. Peers have the option of setting filters on each connection they make after the version handshake has completed. A filter is defined as a Bloom filter on data derived from transactions. A Bloom filter is a probabilistic data structure which allows for testing set membership - they can have false positives but not false negatives.

This document will not go into the details of how Bloom filters work and the reader is referred to Wikipedia for an introduction to the topic.

Motivation

As Bitcoin grows in usage the amount of bandwidth needed to download blocks and transaction broadcasts increases. Clients implementing simplified payment verification do not attempt to fully verify the block chain, instead just checking that block headers connect together correctly and trusting that the transactions in a chain of high difficulty are in fact valid. See the Bitcoin paper for more detail on this mode.

Today, SPV clients have to download the entire contents of blocks and all broadcast transactions, only to throw away the vast majority of the transactions that are not relevant to their wallets. This

slows down their synchronization process, wastes users bandwidth (which on phones is often metered) and increases memory usage. All three problems are triggering real user complaints for the Android "Bitcoin Wallet" app which implements Simple Payment Verification (SPV) mode. In order to make chain synchronization fast, cheap and able to run on older phones with limited memory we want to have remote peers throw away irrelevant transactions before sending them across the network.