```
BIP: 339
Layer: Peer Services
Title: WTXID-based transaction relay
Author: Suhas Daftuar <sdaftuar@chaincode.com>
Comments-Summary: No comments yet.
Comments-URI: https://github.com/bitcoin/bips/wiki/Comments:BIP-0339
Status: Draft
Type: Standards Track
Created: 2020-02-03
License: BSD-2-Clause
```

Abstract

This BIP describes two changes to the p2p protocol to support transaction relay based on the BIP 141 wtxid of a transaction, rather than its txid.

Motivation

Historically, the inv messages sent on the Bitcoin peer-to-peer network to announce transactions refer to transactions by their txid, which is a hash of the transaction that does not include the witness (see BIP 141). This has been the case even since Segregated Witness (BIP 141/143/144) has been adopted by the network.

Not committing to the witness in transaction announcements creates inefficiencies: because a transaction's witness can be malleated without altering the txid, a node in receipt of a witness transaction that the node does not accept will generally still download that same transaction when announced by other peers. This is because the alternative -- of not downloading a given txid after rejecting a transaction with that txid -- would allow a third party to interfere with transaction relay by malleating a transaction's witness and announcing the resulting invalid transaction to nodes, preventing relay of the valid version of the transaction as well.

We can eliminate this concern by using the wtxid in place of the txid when announcing and fetching transactions.

Specification

1. A new wtxidrelay message is added, which is defined as an empty message where pchCommand == "wtxidrelay".
2. The protocol version of nodes implementing this BIP must be set to 70016 or higher.
3. The wtxidrelay message MUST be sent in response to a version message from a peer whose protocol version is >= 70016 and prior to sending a verack. A wtxidrelay message received after a verack message MUST be ignored or treated as invalid.

4. A new inv type MSG_WTX (0x00000005) is added, for use in both inv messages and getdata requests, indicating that the hash being referenced is a transaction's wtxid. In the case of getdata requests, MSG_WTX implies that the transaction being requested should be serialized with witness as well, as described in BIP 144.
5. After a node has received a wtxidrelay message from a peer, the node MUST use the MSG_WTX inv type when announcing transactions to that peer.
6. After a node has received a wtxidrelay message from a peer, the node SHOULD use a MSG_WTX getdata message to request any announced transactions. A node MAY still request transactions from that peer using MSG_TX getdata messages, such as for transactions not recently announced by that peer (like the parents of recently announced transactions).

Backward compatibility

As wtxid-based transaction relay is only enabled between peers that both support it, older clients remain fully compatible and interoperable after this change.

Implementation

https://github.com/bitcoin/bitcoin/pull/18044

Copyright