```
BIP: 147
Layer: Consensus (soft fork)
Title: Dealing with dummy stack element malleability
Author: Johnson Lau <jl2012@xbt.hk>
Comments-Summary: No comments yet.
Comments-URI: https://github.com/bitcoin/bips/wiki/Comments:BIP-0147
Status: Final
Type: Standards Track
Created: 2016-09-02
License: PD
```

Abstract

This document specifies proposed changes to the Bitcoin transaction validity rules to fix a malleability vector in the extra stack element consumed by `OP_CHECKMULTISIG` and `OP_CHECKMULTISIGVERIFY`.

Motivation

Signature malleability refers to the ability of any relay node on the network to transform the signature in transactions, with no access to the relevant private keys required. For non-segregated witness transactions, signature malleability will change the `txid` and invalidate any unconfirmed child transactions. Although the `txid` of segregated witness (BIP141) transactions is not third party malleable, this malleability vector will change the `wtxid` and may reduce the efficiency of compact block relay (BIP152).

A design flaw in `OP_CHECKMULTISIG` and `OP_CHECKMULTISIGVERIFY` causes them to consume an extra stack element ("dummy element") after signature validation. The dummy element is not inspected in any manner, and could be replaced by any value without invalidating the script. This document specifies a new rule to fix this signature malleability.

Specification

To fix the dummy element malleability, a new consensus rule (`"NULLDUMMY"`) is deployed to require that the dummy element MUST be the empty byte array. Anything else makes the script evaluate to false immediately. The `NULLDUMMY` rule applies to `OP_CHECKMULTISIG` and `OP_CHECKMULTISIGVERIFY` in pre-segregated scripts, and also pay-to-witness-script-hash scripts described in BIP141.

Deployment

This BIP will be deployed by "version bits" BIP9 using the same parameters for BIP141 and BIP143, with the name "segwit" and using bit 1.

For Bitcoin mainnet, the BIP9 starttime is midnight 15 November 2016 UTC (Epoch timestamp 1479168000) and BIP9 timeout is midnight 15 November 2017 UTC (Epoch timestamp 1510704000).

For Bitcoin testnet, the BIP9 starttime is midnight 1 May 2016 UTC (Epoch timestamp 1462060800) and BIP9 timeout is midnight 1 May 2017 UTC (Epoch timestamp 1493596800).

Compatibility

The reference client has produced compatible signatures from the beginning, and the `NULLDUMMY` rule has been enforced as relay policy by the reference client since v0.10.0. There has been no transactions violating the requirement being added to the chain since at least August 2015.

For all scriptPubKey types in actual use, non-compliant signatures can trivially be converted into compliant ones, so there is no loss of functionality by this requirement. Users MUST pay extra attention to this new rule when designing exotic scripts.

Implementation

An implementation for the reference client is available at https://github.com/bitcoin/bitcoin/pull/8636

Acknowledgements

Peter Todd is the original author of NULLDUMMY. This document is extracted from the previous BIP62 proposal, which was composed by Pieter Wuille and had input from various people.

Copyright