

# BIP 0147 - Dealing with dummy stack element malleability (soft fork)

[return to the Bitcoin Standards](#)

Table 1: Data sheet for Dealing with dummy stack element malleability

|                  |                                                                                                                                             |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| Title            | Dealing with dummy stack element malleability                                                                                               |
| Layer            | Consensus (soft fork)                                                                                                                       |
| Author           | Johnson Lau                                                                                                                                 |
| Comments-Summary | No comments yet.                                                                                                                            |
| Comments-URI     | <a href="https://github.com/bitcoin/bips/wiki/Comments:BIP-0147">https://github.com/bitcoin/bips/wiki/Comments:BIP-0147</a>                 |
| Staus            | Final                                                                                                                                       |
| Type             | Standards Track                                                                                                                             |
| Created          | 2016-09-02                                                                                                                                  |
| Post History     |                                                                                                                                             |
| Description      | <a href="https://github.com/bitcoin/bips/blob/master/bip-0147.mediawiki">https://github.com/bitcoin/bips/blob/master/bip-0147.mediawiki</a> |
| :icense          | 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 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 ([bip\\_0141](#)) 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.*

From:  
<https://www.omgwiki.org/dido/> - **DIDO Wiki**

Permanent link:  
[https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:xapend:xapend.b\\_stds:default:bitcoin:bips:bip\\_0147&rev=1559074497](https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:xapend:xapend.b_stds:default:bitcoin:bips:bip_0147&rev=1559074497)

Last update: **2019/05/28 16:14**

