BIP 0011 - M-of-N Standard Transactions

return to the Bitcoin Improvement Proposals

Table 1: Data sheet for M-of-N Standard Transactions

Title	M-of-N Standard Transactions
Layer	Application
Author	Gavin Andresen
Comments-Summary	No comments yet.
Comments-URI	https://github.com/bitcoin/bips/wiki/Comments:BIP-0011
Status	Final
Type	Standards Track
Created	2011-10-18
Post History	2011-10-02
Description	https://github.com/bitcoin/bips/blob/master/bip-0011.mediawiki

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 proposes M-of-N-signatures required transactions as a new 'standard' transaction type.

Motivation

Enable secured wallets, escrow transactions, and other use cases where redeeming funds requires more than a single signature.

A couple of motivating use cases:

- *A wallet secured by a "wallet protection service" (WPS). 2-of-2 signatures required transactions will be used, with one signature coming from the (possibly compromised) computer with the wallet and the second signature coming from the WPS. When sending protected bitcoins, the user's bitcoin client will contact the WPS with the proposed transaction and it can then contact the user for confirmation that they initiated the transaction and that the transaction details are correct. Details for how clients and WPS's communicate are outside the scope of this BIP. Side note: customers should insist that their wallet protection service provide them with copies of the private key(s) used to secure their wallets that they can safely store off-line, so that their coins can be spent even if the WPS goes out of business.*
- *Three-party escrow (buyer, seller and trusted dispute agent). 2-of-3 signatures required transactions will be used. The buyer and seller and agent will each provide a public key, and the buyer will then send coins into a 2-of-3 CHECKMULTISIG transaction and send the seller and the agent the transaction id. The seller will fulfill their obligation and then ask the buyer to co-sign a*

transaction (already signed by seller) that sends the tied-up coins to him (seller).

If the buyer and seller cannot agree, then the agent can, with the cooperation of either buyer or seller, decide what happens to the tied-up coins. Details of how buyer, seller, and agent communicate to gather signatures or public keys are outside the scope of this BIP.

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

Permanent link:
https://omgwiki.org/dido/doku.php?id=dido:public:ra:xapend:xapend.b_stds:defact:bitcoin:bips:bip_0011

Last update: **2021/08/13 16:05**