BIP 0013 - Address Format for pay-to-script-hash

return to the Bitcoin Improvement Proposals

Table 1: Data sheet for Address Format for pay-to-script-hash

Title	Address Format for pay-to-script-hash
Layer	Applications
Author	Gavin Andresen
Comments-Summary	No comments yet.
Comments-URI	https://github.com/bitcoin/bips/wiki/Comments:BIP-0013
Status	Final
Type	Standards Track
Created	2011-10-18
Post History	
Description	https://github.com/bitcoin/bips/blob/master/bip-0013.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 describes a new type of Bitcoin address to support arbitrarily complex transactions. Complexity in this context is defined as what information is needed by the recipient to respend the received coins, in contrast to needing a single ECDSA private key as in current implementations of Bitcoin.

In essence, an address encoded under this proposal represents the encoded hash of a script, rather than the encoded hash of an ECDSA public key.

Motivation

Enable “end-to-end” secure wallets and payments to fund escrow transactions or other complex transactions. Enable third-party wallet security services.