BIP 0070 - Payment Protocol

return to the Bitcoin Improvement Proposals

Table 1: Data sheet for Payment Protocol

Title	Payment Protocol
Layer	Applications
Author	Gavin Andresen, Mike Hearn
Comments-Summary	No comments yet.
Comments-URI	https://github.com/bitcoin/bips/wiki/Comments:BIP-0070
Status	Final
Type	Standards Track
Created	2013-07-29
Post History	
Description	https://github.com/bitcoin/bips/blob/master/bip-0070.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 protocol for communication between a merchant and their customer, enabling both a better customer experience and better security against man-in-the-middle attacks on the payment process.

Motivation

The current, minimal Bitcoin payment protocol operates as follows:

1. *Customer adds items to an online shopping basket, and decides to pay using Bitcoin.*
2. *Merchant generates a unique payment address, associates it with the customer's order, and asks the customer to pay.*
3. *Customer copies the Bitcoin address from the merchant's web page and pastes it into whatever wallet they are using OR follows a bitcoin: link and their wallet is launched with the amount to be paid.*
4. *Customer authorizes payment to the merchant's address and broadcasts the transaction through the Bitcoin p2p network.*
5. *Merchant's server detects payment and after sufficient transaction confirmations considers the transaction final.*

This BIP extends the above protocol to support several new features:

1. *Human-readable, secure payment destinations– customers will be asked to authorize payment to*

“example.com” instead of an inscrutable, 34-character bitcoin address.

2. *Secure proof of payment, which the customer can use in case of a dispute with the merchant.*
3. *Resistance from man-in-the-middle attacks that replace a merchant's bitcoin address with an attacker's address before a transaction is authorized with a hardware wallet.*
4. *Payment received messages, so the customer knows immediately that the merchant has received, and has processed (or is processing) their payment.*
5. *Refund addresses, automatically given to the merchant by the customer's wallet software, so merchants do not have to contact customers before refunding overpayments or orders that cannot be fulfilled for some reason.*