BIP 0137 - Signatures of Messages using Private Keys

return to the Bitcoin Improvement Proposals

Table 1: Data sheet for Signatures of Messages using Private Keys

Title	Signatures of Messages using Private Keys
Layer	Applications
Author	Christopher Gilliard
Comments-Summary	No comments yet.
Comments-URI	https://github.com/bitcoin/bips/wiki/Comments:BIP-0137
Status	Final
Type	Standards Track
Created	2019-02-16
Post History	
Description	https://github.com/bitcoin/bips/blob/master/bip-0137.mediawiki
License	BSD-2-Clause

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 describes a signature format for signing messages with Bitcoin private keys.

The specification is intended to describe the standard for signatures of messages that can be signed and verified between different clients that exist in the field today. Note: that a new signature format has been defined which has a number of advantages over this BIP, but to be backwards compatible with existing implementations this BIP will be useful. See BIP 322 [1] for full details on the new signature scheme.

One of the key problems in this area is that there are several different types of Bitcoin addresses and without introducing specific standards it is unclear which type of address format is being used. See [2]. This BIP will attempt to address these issues and define a clear and concise format for Bitcoin signatures.

Copyright

Motivation

Since Bitcoin private keys can not only be used to sign Bitcoin transactions, but also any other message, it has become customary to use them to sign various messages for differing purposes. Some applications of signing messages with a Bitcoin private key are as follows: proof of funds for collateral, credit worthiness, enterence to events, airdrops, audits as well as other applications. While there was no BIP written for how to digitally sign messages with Bitcoin private keys with P2PKH addresses it is a fairly well understood process, however with the introduction of Segwit (both in the form of P2SH and bech32) addresses, it is unclear how to distinguish a P2PKH, P2SH, or bech32 address from one another. This BIP proposes a standard signature format that will allow clients to distinguish between the different address formats.

1)

https://github.com/bitcoin/bips/blob/master/bip-0322.mediawiki

2)

https://github.com/bitcoin/bitcoin/issues/10542