Bitcoin: Bitcoin Improvement Proposals (BIPs)

return to Bitcoin page

Bitcoin Improvement Proposal (BIP) is a design document for introducing features or information to Bitcoin. ... This is the standard way of communicating ideas since Bitcoin has no formal structure. The first BIP (BIP 0001) was submitted by Amir Taaki on 2011-08-19 and described what a BIP is. Bitcoin Improvement Proposal (BIP) Source: Bitcoin list of BIPs

Final BIPs

The following non-forking BIPs have been finalized.

- BIP 0011 - M-of-N Standard Transactions
- BIP 0013 - Address Format for pay-to-script-hash
- BIP 0014 - Protocol Version and User Agent
- BIP 0021 - URI Scheme
- BIP 0022 - getblocktemplate - Fundamentals
- BIP 0023 - getblocktemplate - Pooled Mining
- BIP 0031 - Pong message
- BIP 0035 - mempool message
- BIP 0037 - Connection Bloom filtering
- BIP 0061 - Reject P2P message
- BIP 0070 - Payment Protocol
- BIP 0071 - Payment Protocol MIME types
- BIP 0072 - bitcoin: uri extensions for Payment Protocol
- BIP 0073 - Use "Accept" header for response type negotiation with Payment Request URLs
- BIP 0137 - Signatures of Messages using Private Keys
- BIP 0144 - Segregated Witness (Peer Services)
- BIP 0145 - getblocktemplate Updates for Segregated Witness

Forking BIPs

There are three kinds of forks: Temporary [1)], Soft [2)], and Hard[3)]. The following forking BIPs have been finalized.

- BIP 0016 - Pay to Script Hash (soft fork)
- BIP 0030 - Duplicate transactions (soft fork)
- BIP 0034 - Block v2, Height in Coinbase (soft fork)
- BIP 0042 - A finite monetary supply for Bitcoin (soft fork)
- BIP 0065 - OP_CHECKLOCKTIMEVERIFY (soft fork)
- BIP 0068 - Relative lock-time using consensus-enforced sequence numbers (soft fork)
- BIP 0091 - Reduced threshold Segwit MASF (soft fork)
- BIP 0112 - CHECKSEQUENCEVERIFY (soft fork)

- BIP 0113 - Median time-past as endpoint for lock-time calculations (soft fork)
- BIP 0141 - Segregated Witness (Consensus layer) (soft fork)
- BIP 0143 - Transaction Signature Verification for Version 0 Witness Program (soft fork)
- BIP 0147 - Dealing with dummy stack element malleability (soft fork)
- BIP 0148 - Mandatory activation of segwit deployment (soft fork)

1)

Temporary forks are forks that occur when miners, on cryptocurrency systems, discover a block at the same time. This results in two split competing blockchains. Temporary forks are resolved in proof-of-work systems such as Bitcoin when miners select which chain to form subsequent blocks upon. The longest blockchain is viewed as being the 'true' blockchain, and will win out, whilst the shorter chain will be abandoned.

2)

A **soft fork** is a backward compatible method of upgrading a blockchain. In other words, a soft fork is a software upgrade that is backward compatible with previous versions of the software. Soft forks do not require nodes on the network to upgrade to maintain consensus, because all blocks on the soft-forked blockchain follow the old set of consensus rules as well as the new ones.
[[dido:public:ra:xapend.glossary:b:blkchn Soft Fork & Hard Fork Explained]]

3)

A **hard fork** is a permanent divergence from the previous version of a blockchain; a new set of consensus rules are introduced into the network that is not compatible with the older network. In other words, a hard fork can be thought of as a software upgrade that is not compatible with previous versions of the software. All network participants are required to upgrade to the latest version of the software in order to continue verifying and validating new blocks of transactions.