

Bitcoin version 0.5.3 is now available for download at: <http://sourceforge.net/projects/bitcoin/files/Bitcoin/bitcoin-0.5.3/>

This is a bugfix-only release based on 0.5.1. It also includes a few protocol updates.

Please report bugs using the issue tracker at github: <https://github.com/bitcoin/bitcoin/issues>

Stable source code is hosted at Gitorious: <http://gitorious.org/bitcoin/bitcoind-stable/archive-tarball/v0.5.3#.tar.gz>

PROTOCOL UPDATES

BIP 30: Introduce a new network rule: "a block is not valid if it contains a transaction whose hash already exists in the block chain, unless all that transaction's outputs were already spent before said block" beginning on March 15, 2012, 00:00 UTC. On testnet, allow mining of min-difficulty blocks if 20 minutes have gone by without mining a regular-difficulty block. This is to make testing Bitcoin easier, and will not affect normal mode.

BUG FIXES

Limit the number of orphan transactions stored in memory, to prevent a potential denial-of-service attack by flooding orphan transactions. Also never store invalid transactions at all. Fix possible buffer overflow on systems with very long application data paths. This is not exploitable. Resolved multiple bugs preventing long-term unlocking of encrypted wallets (issue #922). Only send local IP in "version" messages if it is globally routable (ie, not private), and try to get such an IP from UPnP if applicable. Reannounce UPnP port forwards every 20 minutes, to workaround routers expiring old entries, and allow the -upnp option to override any stored setting. Skip splash screen when -min is used, and fix Minimize to Tray function. Do not blank "label" in Bitcoin-Qt "Send" tab, if the user has already entered something. Correct various labels and messages. Various memory leaks and potential null pointer dereferences have been fixed. Handle invalid Bitcoin URIs using "bitcoin://" instead of "bitcoin:". Several shutdown issues have been fixed. Revert to "global progress indication", as starting from zero every time was considered too confusing for many users. Check that keys stored in the wallet are valid at startup, and if not, report corruption. Enable accessible widgets on Windows, so that people with screen readers such as NVDA can make sense of it. Various build fixes. If no password is specified to bitcoind, recommend a secure password. Automatically focus and scroll to new "Send coins" entries in Bitcoin-Qt. Show a message box for --help on Windows, for Bitcoin-Qt. Add missing "About Qt" menu option to show built-in Qt About dialog. Don't show "-daemon" as an option for Bitcoin-Qt, since it isn't available. Update hard-coded fallback seed nodes, choosing recent ones with long uptime and versions at least 0.4.0. Add checkpoint at block 168,000.