

Verify Binaries

Preparation:

Make sure you obtain the proper release signing key and verify the fingerprint with several independent sources.

```
$ gpg --fingerprint "Bitcoin Core binary release signing key"
pub  4096R/36C2E964 2015-06-24 [expires: YYYY-MM-DD]
    Key fingerprint = 01EA 5486 DE18 A882 D4C2  6845 90C8 019E 36C2 E964
uid          Wladimir J. van der Laan (Bitcoin Core binary release signing
key) <laanwj@gmail.com>
```

Usage:

This script attempts to download the signature file `SHA256SUMS.asc` from <https://bitcoin.org>.

It first checks if the signature passes, and then downloads the files specified in the file, and checks if the hashes of these files match those that are specified in the signature file.

The script returns 0 if everything passes the checks. It returns 1 if either the signature check or the hash check doesn't pass. If an error occurs the return value is 2.

```
./verify.py bitcoin-core-0.11.2
./verify.py bitcoin-core-0.12.0
./verify.py bitcoin-core-0.13.0-rc3
```

If you only want to download the binaries of certain platform, add the corresponding suffix, e.g.:

```
./verify.py bitcoin-core-0.11.2-osx
./verify.py 0.12.0-linux
./verify.py bitcoin-core-0.13.0-rc3-win64
```

If you do not want to keep the downloaded binaries, specify anything as the second parameter.

```
./verify.py bitcoin-core-0.13.0 delete
```