```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

bitaddress.org
Open Source JavaScript Client-Side Bitcoin Wallet Generator

The bitaddress.org file contains all the JavaScript/Css/Images embedded
in the HTML document. Included in the file name is the file's version
number and hash.

The bitaddress.org software is available Open Source under the MIT License.
Visit the GitHub Repository for the full copyright and license information:
https://github.com/pointbiz/bitaddress.org

Bitcoin Forum thread:
https://bitcointalk.org/index.php?topic=43496.0

Donation Address: 1NiNja1bUmhSoTXozBRBEtR8LeF9TGbZBN

END USER NOTES:
 1) To print QRCode in IE8 you must enable the "Print Background Colors and
    Images" checkbox on the "Page Setup" screen.
 2) For Bulk Wallet I recommended using Google Chrome, it's the fastest.
 3) Requires IE8+, Firefox, Chrome or sufficient JavaScript support.
 4) Mobile Safari only works with iPhone4 or newer devices.
    Older devices timeout while executing JavaScript.
 5) DO NOT use Opera Mini it renders JavaScript output server side, therefore
    they might record the private key you generated.
 6) Art Wallet does not work properly in IE8 due to CSS limitations.
 7) BIP38 most likely will not work on mobile devices due to hardware limitations.

Here is a signed list of file names and version history.

2016-11-27: status ACTIVE
bitaddress.org-v3.2.3-SHA256-c9a0bb3ed50aa75a5ae9c606d81e3fd41a4ff686ad38ad5379e2402f481e79a4.html
 - wallet details: show error when checksum validation fails
 - wallet details: show error when private key outside of curve range

2016-08-21: status ACTIVE
bitaddress.org-v3.2.2-SHA256-f4d047c264a2b71946de319482a9365e56d8d7289dd85a352da3b1448b7647df.html
 - version bump for unix line endings
```

2016-07-31: status ACTIVE

bitaddress.org-v3.2.1-SHA256-42c3bcb643c451689e5bd1499ed4b516be2da06d2fe3886b0dd15b8fc2525ecd.html

- BigInteger modInverse should be positive
- throw if modInverse 0
- improve BigInteger constructor so that it works if caller forgets 'new'
- add unit tests for BigInteger
- thanks to dooglus, jprichardson, dcousens

2016-02-19: status ACTIVE

bitaddress.org-v3.2.0-SHA256-ad4fd171c647772aa76d0ce828731b01ca586596275d43a94008766b758e8736.html

- switch languages without full page load
- add BIP38 encryption to Bulk Wallet
- use compressed addresses on Single/Paper/Bulk Wallet
- add compressed address option on Brain Wallet

2016-01-17: status ACTIVE

bitaddress.org-v3.1.1-SHA256-8277de0a0c77761caa8f546c9885c36a3134a94823b14e24d364b86abb3a9ab3.html

- refactor translations into separate files per culture.

2015-11-22: status ACTIVE

bitaddress.org-v3.1.0-SHA256-c3d4d8da8fc6980435a520dff562b7f831b2f6037ec2d4dd6bf76c5321873303.html

- add BIP38 encryption on Wallet Details tab.

2015-10-25: status ACTIVE

bitaddress.org-v3.0.1-SHA256-24d2d7f047a9aa217bf69f3ef344c972c151b1e3f6a8aa86ceb9a3be62884bc0.html

- fix for session log not keeping track of keys from "Wallet Details" tab before entropy is collected.

2015-10-25: status ACTIVE

bitaddress.org-v3.0.0-SHA256-4781574ca09c07f65d1966619f37a762aac6decd8732cacc85b2f2f972f82751.html

- add session log icon that shows all the key pairs generated during the current session.

2015-08-16: status ACTIVE

bitaddress.org-v2.9.11-SHA256-40376eddc790a63d9afcfb72c0a45002827da965f3bfe6ba8c330e697bf188b2.html

- add status icons for checking the URI protocol used, support for

window.crypto.getRandomValues
and run the synchronous unit tests after entropy collection.

2015-07-18: status ACTIVE
bitaddress.org-v2.9.10-SHA256-445e44cfd04c8f1ea8f732c3ae7277b0166fdb3e2109251c54e4b367983fe04d.html
- add Portuguese. Thanks rhcastilhos.
- minor french updates.

2015-07-05: status ACTIVE
bitaddress.org-v2.9.9-SHA256-90ddaf250f6302acb53945128e38225208af5a2fa7cfdf51519213e8b144a76d.html
- improve tab usability. You can now get to the Brain Wallet and Wallet Details tabs before completing the entropy collection.

2015-01-08: status ACTIVE
bitaddress.org-v2.9.8-SHA256-2c5d16dbcde600147162172090d940fd9646981b7d751d9bddfc5ef383f89308.html
- fix French translations. Escape quotes.

2015-01-07: status OFFLINE
bitaddress.org-v2.9.7-SHA256-1b0f71dfc2e064426328c15c4dbd1f467cb26afe0e84841347ad11d8ca668f70.html
- fix translations

2015-01-05: status ACTIVE
bitaddress.org-v2.9.6-SHA256-34728a9cec417cf8060423c77e8793e4aa133cf3d66a6b8073b4290cf1f4695c.html
- Japanese translations for Split Wallet. Thanks dabura667.
- remove promise to show MINI key on details tab. MINI key
  will only be shown when it is provided since it cannot
  be derived from other key formats.
- fix README
- Russian translations. Thanks e5faf2.
- Simplified Chinese translations. Thanks kwl01skz.
- add direct link to zip on github
- add this CHANGELOG to repository and add detached sigs in repository.
  add link to sig of HTML.
- hash with SHA256 instead of SHA1. SHA1 hash still provided in package.json.

2014-04-23: status ACTIVE
bitaddress.org-v2.9.3-SHA1-7d47ab312789b7b3c1792e4abdb8f2d95b726d64.html
- increased the HTML height to allow for greater range of mouse

seed values on large monitors. Thanks danbartram.
- Japanese translations. Thanks dabura667.

2014-04-21: status ACTIVE
bitaddress.org-v2.9.1-SHA1-67b1facd70890aa9544597e97122c7a1d4fdc821.html
- Hungarian translation. Thanks bitcoin333.
- Auto detect culture and translate. Thanks onovy.

2014-04-15: status ACTIVE
bitaddress.org-v2.9.0-SHA1-6e9ae5c64d510b53fa39e36a3017d5342b838984.html
- Split Wallet: Shamir's Secret Sharing for a Bitcoin private key.
  Thanks to Jeff Weiss.

2014-01-19: status ACTIVE
bitaddress.org-v2.8.1-SHA1-a6e63f2712851710255a27fa0f22ef7833c2cd07.html
- Czech translation
- remove firstbits link
- fix mouse movement visualization for Firefox and IE

2014-01-18: status ACTIVE
bitaddress.org-v2.8.0-SHA1-87dcf19f02ee9fb9dd3a8c787bcf52eef944aa82.html
- more entropy from browser fingerprinting for PRNG seed
- user can add entropy through URL hash tag
- seed mouse movement as 16-bit number
- whole seed pool initially filled by window.crypto.getRandomValues
- added textbox as an alternative input source for entropy
- address will not generate without a minimum amount of human added entropy
  from mouse or keyboard
- discard mouse movements less than 40ms apart
- visualize points of entropy collection from the mouse

2013-12-23: status ACTIVE
bitaddress.org-v2.7.2-SHA1-364542f1ccc5777c79aebb1692a6265cf3e42e7e.html
- keys and addresses in monospace font.

2013-12-22: status ACTIVE
bitaddress.org-v2.7.1-SHA1-6dfa290d1a133fc444c5580e2a8f1f890d5edf17.html
- more entropy for the PRNG seed.
- use ?showseedpool=true to see the contents of the seed pool in hex.

2013-12-09: status ACTIVE
bitaddress.org-v2.6.6-SHA1-0d68accca48df174b6b4f48544498f333dc6e33a.html
- German translations thanks to gerEDH.

2013-12-01: status ACTIVE
bitaddress.org-v2.6.5-SHA1-fa763c2bbc97e1b37bc6d3945647aed869ec8c18.html
- dice FAQ on detail wallet tab.
- QR code spacing adjusted to 4x on single wallet and detail wallet tab.
- update to JSBN 1.4
- add passphrase required alert to paper wallet tab for bip38 keys.

2013-11-14: status ACTIVE
bitaddress.org-v2.6.2-SHA1-4d98755d7e78caa4361228a2b11b0faa0f65e6de.html
- Italian translations thanks to Coin-Escrow
- Add base6 support to Wallet Details tab

2013-11-03: status ACTIVE
bitaddress.org-v2.6.0-SHA1-4f1fea4620287f863473193b8d93a8f3877ba972.html
- Usability improvements to Single Wallet, Paper Wallet and Brain Wallet.

2013-10-24: status ACTIVE
bitaddress.org-v2.5.1-SHA1-b7bda19c2327cc44a81b68a44926a9f8057ed681.html
- BIP38 passphrase protected paper wallets. Thanks to casascius, scintill, Zeilap.
  Paper Wallet tab and Wallet Details tab support BIP38.
- Compressed address support on Bulk Wallet tab.
- Greek translations thanks to ifaist0s

2013-02-17: status ACTIVE
bitaddress.org-v2.4-SHA1-1d5951f6a04dd5a287ac925da4e626870ee58d60.html
- French translations thanks to blockgenesis.

2013-01-27: status ACTIVE
bitaddress.org-v2.3-SHA1-1d067dc4f3103622ca9de332c3c86fc57d76ec83.html
- Vanity Wallet now supports compressed keys.
- Elliptic Curve and Bitcoin.ECKey libaries now support compressed keys.
- English Json used for translations is now output to a textarea when
  you run the unit tests.
- more unit tests, use ?unittests=true to run them.

2012-12-30: status ACTIVE
bitaddress.org-v2.2-SHA1-d414530eea984e9ebdd40dc27af9078cd73dc3b3.html
- critical bug fix to Vanity Wallet multiplication of a public key with a private key.
  Bug was due to incorrect construction of BigInteger object. Which results in the incorrect
  Bitcoin Address being displayed. Therefore, v2.1 has been taken offline.
- new translations code and initial spanish translation. Thanks to dserrano5 for translating.

```
2012-12-24: status OFFLINE
bitaddress.org-v2.1-SHA1-af431934553aeef3e042e796a31ee101cdabc496.html
 - Vanity Wallet now supports adding/multiplying of public/private keys.
   Compressed keys not supported.
 - refactored wallet HTML/JavaScript to make the code more modular.
   Now it's easier to add/remove a specific wallet.
 - reusable public and private key math has been extracted to
   ninja.privateKey and ninja.publicKey
 - created unit tests

2012-10-20: status ACTIVE
bitaddress.org-v2.0-SHA1-c0300a88d2de421106560185e4916f4eee6ed9df.html
 - Added Vanity Wallet merged from n1bor
 - Paper Wallet merged high resolution QR code from ironwolf

2012-10-11: status ACTIVE
bitaddress.org-v1.9-SHA1-a487b495d710d6f617d688e5f758e40c8b6c510e.html
 - fixed Testnet Edition WIF and Compressed WIF private keys. It now prepends
   the correct byte (0xEF) for testnet when activated.

2012-10-07: status ACTIVE
bitaddress.org-v1.8-SHA1-97d52a44eeb261e2398e98e1eed2bd56b99c845a.html
 - Paper Wallet Tab: Art wallet is now the default.
 - Paper Wallet Tab: The PNG has been resized to fit better into physical
   wallets when printed.
 - Paper Wallet Tab: The PNG has been rendered using the Ubuntu font.

2012-09-29: status ACTIVE
bitaddress.org-v1.7-SHA1-46215e8a2f026b784f29ea86c00c866e634a22fa.html
 - Paper Wallet Tab now has the option to print an artistic wallet.
   Current implementation uses an embedded PNG. This feature is not supported
   in IE8.
 - Brain Wallet Tab now has passphrase confirm and show passphrase options.

2012-07-29: status ACTIVE
bitaddress.org-v1.6-SHA1-162d1ff4fd1e09222cbaca6c282672ee6c195e1b.html
 - Added Brain Wallet Tab. Algorithm is SHA256(passphrase).
   Minimum passphrase length is 15 characters.

2012-03-22: status ACTIVE
bitaddress.org-v1.5-SHA1-f2e410251c8741ac65d29a1c6fb8ef6919b6ab8b.html
 - Wallet Details Tab:
   coretechs fixed a bug with the display of the base64 private key
```

coretechs added support for compressed keys

2012-01-09: status ACTIVE
bitaddress.org-v1.4-SHA1-5c120c0860032e88a8fd81b802d6f53a5fc082bf.html
- Wallet Details Tab: Allow for a deterministic wallet to be created by entering a passphrase on the wallet details tab. If you input text that is not a valid private key you will be prompted and asked if you want to use the entered text as a passphrase to create a private key. If you select OK then it will perform a SHA256 of the passphrase to generate your private key.
- Wallet Details Tab: Added QRCodes. Added Public Key.
- Bulk Wallet Tab: added FAQs.
- Version number now shown in footer.

2011-11-28: status ACTIVE
bitaddress.org-v1.3-SHA1-88d9a17e6d6286d7840043b6df9980e85f44b8c0.html
- Testnet Edition: if you add ?testnet=true to the end of the URL it will activate testnet edition.
- isMiniFormat function updated to accept mini key formats of length 22, 26 or 30 characters.
- bitaddress.org software is now open source available under the MIT License.

2011-10-12: status ACTIVE
bitaddress.org-v1.2-SHA1-1770e5e8993cca823a2ad956e2aab5c291151692.html
-Wallet Details Tab: Added extra check on validity of Wallet Import Format and Base64 Private Keys.

2011-10-11: status ACTIVE
bitaddress.org-v1.1-SHA1-969273be66ecf93d8bb3525edc1fa0cf3de228d2.html
-Removed 'Standard Format' from Wallet Details tab.

2011-10-10: status ACTIVE
bitaddress.org-v1.0-SHA1-8fc60a3ca4eb24c85c31b264e95a9298e41032c2.html
-Added Wallet Details tab.

2011-10-02: status ACTIVE
bitaddress.org-v0.9-SHA1-aa61ca480288e1bda00f1f042d60a057880a2321.html
-Added more entropy, all mouse movements in the window will add to the random seed pool.
-Added PaperWallet tab. You can now generate multiple QRCode pairs per page.

2011-09-22: status ACTIVE
bitaddress.org-v0.8-SHA1-47b989b8a33407df14d21dbd00fad653e0161d6c.html
-Css update to tabs
-Added double quotes around CSV bitcoin address and private key output

2011-09-22: status ACTIVE

bitaddress.org-v0.7-SHA1-34e344a0d229dc10c8f5c99ed6b6298e6fc5e39f.html

- Added Bulk Wallet tab. Now you can generate CSV lists of addresses!

2011-09-19: status ACTIVE
bitaddress.org-v0.6-SHA1-1cea2d8c437d49c550b9ec1cfc5d02ac85e8199e.html

- Removed QRCode donation address

2011-09-19: status ACTIVE
bitaddress.org-v0.5-SHA1-7ea8d0e32c3583d369dc4079443e0d6e215ac216.html

- DO NOT USE VERSION 0.1 TO 0.4! They infrequently could generate bad keys.
- Bug Fixed: v0.1 to v0.4 included a bug in the Elliptic Curve function:
  ec.PointFp.prototype.getEncoded
  The X and Y integers that were less than 32 bytes were not being zero padded.
  They are now zero padded which fixes the bug in generating public keys.
- Bug Fixed: v0.3 and v0.4 had a bug in the Wallet Import Format function:
  ECKey.prototype.getBitcoinWalletImportFormat
  Private keys there were less than 32 bytes were not being zero padded.
  They are now zero padded which fixes the bug in generating private keys.
- Requires IE8+, Firefox, Chrome or sufficient JavaScript support.
- Added function to build a CSV list of addresses and keys.
  Not supported in the GUI yet.
- Added a timeout to override the mouse move detection. Therefore, if the user
  has not moved his mouse before a certain random expiry the address and key
  will then be generated. This helps for mobile devices.

2011-09-18: status OFFLINE
bitaddress.org-v0.4-SHA1-9d3afda22f8cf526330c0387a77e4016fd050323.html

- Known bug: Bitcoin.Base58.encode is not working in IE7
- Removed Private Key Hex
- Added QRCode for Bitcoin Address
- Added QRCode for Private Key Wallet Import Format
- Added extra entrophy with mouse movement technique
- Footer now hides when printing
- QRCode shows with canvas, if canvas is not supported (IE8) then it shows
  with a table. Printing of the table is not supported by most browsers.

2011-09-13: status OFFLINE
bitaddress.org-v0.3-SHA1-bd94e796811d852f9db69e82adea9a9c48daf183.html

- Removed Private Key Base64
- Added Private Key Wallet Import Format

2011-09-12: status OFFLINE
bitaddress.org-v0.2-SHA1-71216f5b84ef8831a805dbf66e9d8b83ad1dc5fb.html

-Added doctype so IE9 renders in standards mode
-Added Array.prototype.map for IE7/8 compatibility
-Added New Address and Print buttons
-Added new logo
-Known bug: Bitcoin.Base58.encode is not working in IE7

2011-09-11: status OFFLINE
bitaddress.org-v0.1-SHA1-f40e706490f3eb2be56c31ddbf4c8646cd51ef40.html
-Initial release
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1

iQEcBAEBAgAGBQJYOz4QAAoJEIdJe5Fjl09ar74IAMiOx4/c/q7UaTEjlAQDmseh
CxSRHHQUwGaZG6z9pwt9ecdKht4t3Y2+CufcPmoV7A1Vq2EtoXFxEibwDwLuTzYL
pqcUZCV+fwd0PGGz69mL0iGrMJHy0lhBZb4Ib+2P6fXz4D35n1Dnq1jHGAOzcFEF
B2++ja2s8QJwd1S1xtOhBshVZDTHc8YYgv1JJSKDpJNeGSFHx9IapOv4ydETbhfT
L7kp9z6TKZ5khkRUCGR2qL4BzlTA/lSDj/cgVb6tRQmIgusRMjvJP076nEqiJ4TX
8YZrObi2yXM7bD8iBXIabc3W2r/R9olw+pCxI+ZuFEOU+UVndCRpP7XEMsTp4aw=
=/wYY
-----END PGP SIGNATURE-----