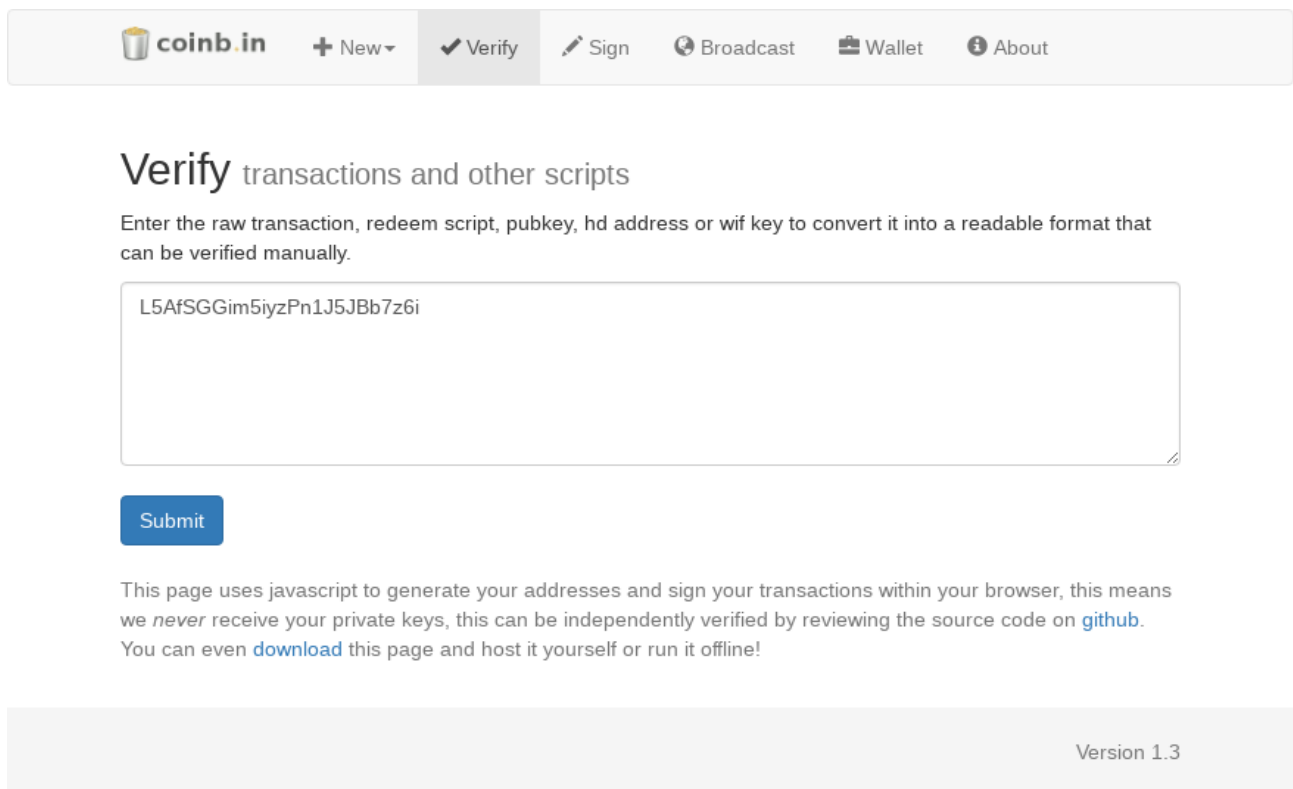


How to redeem

Suggested tool: coinb.in

1. Copy the string from the edge of the coin. It is the first half of a private key in the WIF format (**Priv1**).



The screenshot shows the coinb.in website interface. At the top, there is a navigation bar with the following items: a coin icon, the text 'coinb.in', a '+ New' dropdown menu, a 'Verify' button with a checkmark icon, a 'Sign' button with a pencil icon, a 'Broadcast' button with a circular arrow icon, a 'Wallet' button with a wallet icon, and an 'About' button with an information icon. Below the navigation bar, the main heading is 'Verify transactions and other scripts'. Underneath this heading is a paragraph: 'Enter the raw transaction, redeem script, pubkey, hd address or wif key to convert it into a readable format that can be verified manually.' Below this text is a large text input field containing the string 'L5AfSGGim5iyzPn1J5JBb7z6i'. Below the input field is a blue 'Submit' button. Below the button is a paragraph of text: 'This page uses javascript to generate your addresses and sign your transactions within your browser, this means we *never* receive your private keys, this can be independently verified by reviewing the source code on [github](#). You can even [download](#) this page and host it yourself or run it offline!'. At the bottom right of the page, there is a footer that says 'Version 1.3'.

2. The second half of **Priv1** is written on a paper certificate which came with the coin. Append it.

Verify transactions and other scripts

Enter the raw transaction, redeem script, pubkey, hd address or wif key to convert it into a readable format that can be verified manually.

```
L5AfSGGim5iyzPn1J5JBb7z6iu3rv1aMjW389eDUGqE5uxK6fVkJ
```

Submit

This page uses javascript to generate your addresses and sign your transactions within your browser, this means we *never* receive your private keys, this can be independently verified by reviewing the source code on [github](#). You can even [download](#) this page and host it yourself or run it offline!

3. Click Submit and note the generated public key (**Pub1**).



Verify transactions and other scripts

Enter the raw transaction, redeem script, pubkey, hd address or wif key to convert it into a readable format that can be verified manually.

```
L5AfSGGim5iyzPn1J5JBb7z6iu3rv1aMjW389eDUGqE5uxK6fVkJF
```

WIF key

The above wif key has been decoded

Address:

```
1MofjNtr7YRX8cuU6jdzMNVqiG4GBQUXhP
```

Public key:

```
02ac8eb28e22c1f2d40c84aa938e1fa3ff8061e8b9855f0d91519a4bd72bfaa011
```

Private key:

```
ed21a8edd53308eff3141c3a0ae3fef8c307dc8911a7c20e94b89bfde511e101
```

Is compressed: true

Submit

This page uses javascript to generate your addresses and sign your transactions within your browser, this means we *never* receive your private keys, this can be independently verified by reviewing the source code on [github](#). You can even [download](#) this page and host it yourself or run it offline!

4. Scan the QR code on the attached „BitNote“, it contains a second public key (**Pub2**). You can use any QR code scanner, e.g. Zxing ([Android](#), [iOS](#)).
5. Generate a redeem script using **Pub1** and **Pub2** in this order.

New Multisig Address Secure multisig address

Public keys can be [generated in your browser](#) or from your bitcoin client.

Enter the public keys of all the participants, to create a [multi signature address](#). Maximum of 15 allowed. Compressed and uncompressed public keys are accepted.

[Need a Mediator?](#)


02ac8eb28e22c1f2d40c84aa938e1fa3ff8061e8b9855f0d91519a4bd72bfaa011 +

027007ea9a90e9daab8f8a7378bc3d4bb6fcc33bb1cf5842c6c35a825eb3916db8 -

Enter the amount of signatures required to release the coins

Address

Payment should be made to this address:



Redeem Script

This script should be *saved and should be shared with all the participants before a payment is made*, so they may validate the authenticity of the address, it will also be used later to release the bitcoins.

Shareable URL

This page uses javascript to generate your addresses and sign your transactions within your browser, this means we *never* receive your private keys, this can be independently verified by reviewing the source code on [github](#). You can even [download](#) this page and host it yourself or run it offline!

- Construct a transaction using the redeem script from the previous step. Click the *Load* button and specify a destination address, where to redeem the coins. The amount should be 0.01 minus the recommended fee. Fee estimation can be done using [bitcoinfees.earn.com](#). Copy the transaction hexadecimal string.

Transaction Create a new transaction

Use this page to create a raw transaction

Address, WIF key or Redeem Script:

 Load

Retrieved unspent inputs from address 33isqqqmAK6PVVwtgqxyuQPpmGx6dKsoL

Advanced Options

Outputs (0.00990000) Inputs (0.01000000)

Enter the address and amount you wish to make a payment to.

♥ Donate!

| Address | Amount |
|---|-------------------------------------|
| <input type="text" value="1A9H7vexBaac8L4JTiZqYpcXbimDPgfP5A"/> | <input type="text" value="0.0099"/> |

Transaction Fee ?

Transaction QR

The transaction below has been generated and encoded. It can be broadcasted once it has been signed.

```
0100000001849c179bc38c05716cb08fa0cefb0b164872b2a5b904024668fe85a018d58a5c01000000475
22102ac8eb28e22c1f2d40c84aa938e1fa3ff8061e8b9855f0d91519a4bd72bfaa01121027007ea9a90e9d
aab8f8a7378bc3d4bb6fcc33bb1cf5842c6c35a825eb3916db852aeffffff01301b0f000000000001976a914
6449ea6117751645bcb7249ecbe10b5a19d7d41188ac00000000
```

Size: 156 bytes

This page uses javascript to generate your addresses and sign your transactions within your browser, this means we *never* receive your private keys, this can be independently verified by reviewing the source code on [github](#). You can even [download](#) this page and host it yourself or run it offline!

7. Sign the transaction from previous step with **Priv1**.



Sign Transaction once a transaction has been verified

Once you have [verified](#) a transaction you can sign and then [broadcast](#) it into the network.

Private key

| | |
|-------|------|
| | Show |
|-------|------|

```
010000001849c179bc38c05716cb08fa0cefb0b164872b2a5b904024668fe85a018d58a5c010000004752210
2ac8eb28e22c1f2d40c84aa938e1fa3ff8061e8b9855f0d91519a4bd72bfaa01121027007ea9a90e9daab8f8a7
378bc3d4bb6fcc33bb1cf5842c6c35a825eb3916db852aeffffff01301b0f00000000001976a9146449ea611775
1645bcb7249ecbe10b5a19d7d41188ac00000000
```

Advanced Options

Signed transaction 

The above transaction has been signed:

```
010000001849c179bc38c05716cb08fa0cefb0b164872b2a5b904024668fe85a018d58a5c01000000920
0483045022100cf640d30ff76b4d1f5a2776ff8f6778d5c97abeac6623a9058480e5c50e5050302205e6fd7
118ffffbb16e4df0916055a50514db5ab579712193593c3546febbae0147522102ac8eb28e22c1f2d40c
84aa938e1fa3ff8061e8b9855f0d91519a4bd72bfaa01121027007ea9a90e9daab8f8a7378bc3d4bb6fcc3
3bb1cf5842c6c35a825eb3916db852aeffffff01301b0f00000000001976a9146449ea6117751645bcb724
9ecbe10b5a19d7d41188ac00000000
```

Size: 231 bytes

Submit

This page uses javascript to generate your addresses and sign your transactions within your browser, this means we *never* receive your private keys, this can be independently verified by reviewing the source code on [github](#). You can even [download](#) this page and host it yourself or run it offline!

- Now you need to scratch-off the holographic foil on the attached 'BitNote'. Do it with a coin as if it was a lottery ticket. Under the scratch-off field there is a second private key, Priv2. Scan it with QR code or copy down manually.
- Use the result from step 7 and sign it again, this time using Priv2.

Sign Transaction once a transaction has been verified

Once you have [verified](#) a transaction you can sign and then [broadcast](#) it into the network.

Private key

 Show

```
010000001849c179bc38c05716cb08fa0cefb0b164872b2a5b904024668fe85a018d58a5c010000092004
83045022100cf640d30ff76b4d1f5a2776ff8f6778d5c97abeac6623a9058480e5c50e5050302205e6fd7118fff
bbbb16e4df0916055a50514db5ab579712193593c3546febbbaee0147522102ac8eb28e22c1f2d40c84aa93
8e1fa3ff8061e8b9855f0d91519a4bd72bfaa01121027007ea9a90e9daab8f8a7378bc3d4bb6fcc33bb1cf584
2c6c35a825eb3916db852aeffffff01301b0f00000000001976a9146449ea6117751645bcb7249ecbe10b5a1
9d7d41188ac00000000
```

 [Advanced Options](#)

Signed transaction

The above transaction has been signed:

```
010000001849c179bc38c05716cb08fa0cefb0b164872b2a5b904024668fe85a018d58a5c0100000d
a00483045022100cf640d30ff76b4d1f5a2776ff8f6778d5c97abeac6623a9058480e5c50e5050302205
e6fd7118ffbbbb16e4df0916055a50514db5ab579712193593c3546febbbaee01473044022072fd92020
78611286ce6603201fb2b19f051ea65b76d4156fdd24ba8986254370220648ea3a61bc81cb1c8413c9e
5e86e1b7e98fe356f11f64dc79295c6f54227f7e0147522102ac8eb28e22c1f2d40c84aa938e1fa3ff8061
e8b9855f0d91519a4bd72bfaa01121027007ea9a90e9daab8f8a7378bc3d4bb6fcc33bb1cf5842c6c35a
825eb3916db852aeffffff01301b0f00000000001976a9146449ea6117751645bcb7249ecbe10b5a19d
7d41188ac00000000
```

Size: 303 bytes

This page uses javascript to generate your addresses and sign your transactions within your browser, this means we *never* receive your private keys, this can be independently verified by reviewing the source code on [github](#). You can even [download](#) this page and host it yourself or run it offline!

- Now you can verify the transaction which you just constructed and signed. Double check the destination address.

Verify transactions and other scripts

Enter the raw transaction, redeem script, pubkey, hd address or wif key to convert it into a readable format that can be verified manually.

```
010000001849c179bc38c05716cb08fa0cefb0b164872b2a5b904024668fe85a018d58a5c01000000da00483
045022100cf640d30ff76b4d1f5a2776ff8f6778d5c97abeac6623a9058480e5c50e5050302205e6f7118ffbbbbb
16e4df0916055a50514db5ab579712193593c3546febbbaee01473044022072fd9202078611286ce6603201fb2
b19f051ea65b76d4156fdd24ba8986254370220648ea3a61bc81cb1c8413c9e5e86e1b7e98fe356f11f64dc792
95c6f54227f7e0147522102ac8eb28e22c1f2d40c84aa938e1fa3ff8061e8b9855f0d91519a4bd72bfaa0112102
7007ea9a90e9daab8f8a7378bc3d4bb6fcc33bb1cf5842c6c35a825eb3916db852aeffffffff01301b0f0000000000
01976a9146449ea6117751645bcb7249ecbe10b5a19d7d41188ac00000000
```

Transaction Script

The above script has been decoded



Version: 1

Transaction Size: 303 bytes

Lock time: 0

Inputs

| Txid | N | Script | Signed? | MultiSig? |
|--|---|------------|---------|-----------|
| 5c8ad518a085fe68460204b9a5b27248160bfbccea08ft | 1 | 0048304502 | ☑ 2 | 2 of 2 |

Outputs

| Address | Amount | Script |
|------------------------------------|------------|------------|
| 1A9H7vexBaac8L4JTizqYpcXbimDPgfP5A | 0.00990000 | 76a9146449 |

Submit

This page uses javascript to generate your addresses and sign your transactions within your browser, this means we *never* receive your private keys, this can be independently verified by reviewing the source code on [github](#). You can even [download](#) this page and host it yourself or run it offline!

11. If everything is fine you can broadcast the transaction to the bitcoin network.



Broadcast Transaction into the bitcoin network

Enter your hex encoded bitcoin transaction



```
0100000001849c179bc38c05716cb08fa0cefb0b164872b2a5b904024668fe85a018d58a5c01000000da004
83045022100cf640d30ff76b4d1f5a2776ff8f6778d5c97abeac6623a9058480e5c50e5050302205e6fd7118fff
bbbb16e4df0916055a50514db5ab579712193593c3546febbae01473044022072fd9202078611286ce660
3201fb2b19f051ea65b76d4156fdd24ba8986254370220648ea3a61bc81cb1c8413c9e5e86e1b7e98fe356f
11f64dc79295c6f54227f7e0147522102ac8eb28e22c1f2d40c84aa938e1fa3ff8061e8b9855f0d91519a4bd7
2bfaa01121027007ea9a90e9daab8f8a7378bc3d4bb6fcc33bb1cf5842c6c35a825eb3916db852aeffffffff013
```

txid: a316260c49f7335550f3f4372129063d2d091992d179d3789b5afcc0abb095a

Submit

This page uses javascript to generate your addresses and sign your transactions within your browser, this means we *never* receive your private keys, this can be independently verified by reviewing the source code on [github](#). You can even [download](#) this page and host it yourself or run it offline!

12. Congratulations! Now the coin is redeemed and the bitcoins are free again. But still, there is some silver left ;-)