

How To Create Time-locked Transactions with Bitcoin (Free Bitcoins Inside!) ⁽¹⁾

In this guide I will be explaining how to easily create a time-locked transaction on the Bitcoin blockchain. Time-locked transactions could be seen as a form of primitive smart contracts that allow you to create transactions that cannot be spent before a certain date or block height.

We will be using a local copy of the website [Coinb.in](https://github.com/coinb.in), which you can download through Github. I strongly recommend you to make sure your computer is free from malware before you continue.



Before We Start

It's recommended that you create a new Bitcoin address, we will be using the public and private keys of this address to create and unlock our time-locked transaction.

I've used [Election](#) to generate a new address, I assume that this process is easy enough that it doesn't require any further explanation.

You can see that I've funded this newly generated address with 0.0015 BTC. You can claim this amount after the timelock expires (minus fees). This way I also don't have to worry about showing you the private keys and it gives you hands on experience with claiming a time-locked Bitcoin transaction.

Newly Created Bitcoin Address:

Electrum 3.0.4 - Timelock-steemit [standard]





File Wallet View Tools Help

History Send Receive Addresses

Filter: Receiving All

Address	Label	Balance	EUR Balance	Tx
1ACfbLSv9afVrCG6Kd498owMRGdMLa57vy		0.0015	13.41	1
17CHHLG8YiJhE1TviPZMnw8mUVruyKLeJN		0.	0.00	0
13WY5Jigaxy9aVag93B7MKPdMoz7rBiUtw		0.	0.00	0
12Jb2EhbH8LskYLHD3DeUx88ziPDn7973h		0.	0.00	0
1AyViNRnbcbwEeeb2xpU8HcbZYeVmJ1Yg		0.	0.00	0
1EoP1mtsc9GLZAGYnjuWnu5DJcvwTSJ21r		0.	0.00	0
1A2z73f8iyrdczCn67whQygfukT3sLsSw		0.	0.00	0
17dYepggxjc4KYYhC5uks5UgpE22APV5s		0.	0.00	0
1PP3rh8GcRKHK7y5HJi3q58ft5CJeZ66Nj		0.	0.00	0
1E978gNjB9JTYdHsxiE2stKG2vwiMDTei		0.	0.00	0
15r4u2wSYMKtGjbFf3aJ4ctqVtgFpTpt68		0.	0.00	0
1LmzbfgC5hR3XMG9Rbxg5SV1fBqgKSSfD		0.	0.00	0
18R7rCYMqYcsT62YPJweu3p5HQf66pCqw2		0.	0.00	0
1FHj5xh4GB1jAwLZoy9ZKuhnr5uthqJVgM		0.	0.00	0
1KNBH7oap4hNdLUP8tNbnFpDPW11coo5J8		0.	0.00	0
1BJnDAjtSQnGzhX8XSV4kWNzasDQt3io4E		0.	0.00	0
19vJwAibtFVWpYGR7auc7MaXSk7BuN11MJ		0.	0.00	0
1F5ujJYUKRBdf6XhFwdJSqgS8iy5zRbaZG		0.	0.00	0
15LEnfduLLujNXhZQVUznndvwVQKgaCgVA		0.	0.00	0
1A8fo9794mzyReLhtqoNhJ7DPLzRgoShCu		0.	0.00	0
1Ho1xwuiNHVWazYvq6q2tYBg3pzCDhMjot		0.	0.00	0

Balance: 0.0015 BTC (13.48 EUR) 1 BTC~8,985.45 EUR

Creating Vanity Address inside ADDRESSKY.com.

Vanity addresses, or vanity addresses, are cryptocurrency addresses personalized and created respecting a series of parameters given by the users of said addresses. This with the aim of making them more personal and easily identifiable, but without giving up the security they provide.

En Bitcoin you can find different types of addresses, including custom addresses, also known as Vanity Address. The vanity addresses or Bitcoin vanity addresses they are normal addresses, with the same functionality as any other, they only contain a custom alphanumeric character string, a message or a special word for its owner.

The standard addresses that are generated in the wallets are composed of randomly ordered alphanumeric characters, without any special order or meaning. However, today, there is the ability to personalize these same addresses, and add a special touch, either through a name, a brand, a special word or a slightly more complete message.

EXAMPLE Vanity Address from www.ADDRESSKY.com



HISTORY

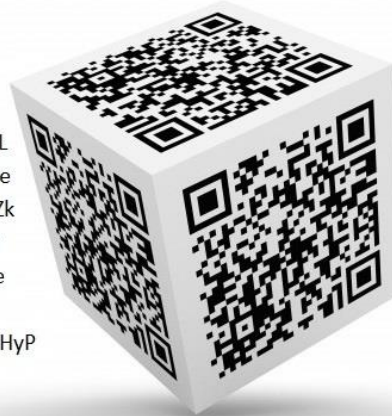
EXAMPLE ADDRESSES BITCOIN.

1**Mozart**oG9Dz88sZp5vvDMhcr89Pf4PJnn
 1**945**FH5a7TeEh6fDf4jRjYa2KcYdG5sQip
 1**Newton**Z4KCX9pa7UMfWjjUXWeUfj8XhVw
 1**Gandhia**VgesAFY6z3n92avLNrfJouNwEb
 1**Lenind**ZDauttvqnBc1ySD82jmYCPcr84a
 1**Mahoma**X37gJSkuDGzfDtgQ5aeKKFC5Xzy
 1**HitLer**ExnSDkX6voUMnZddhCoBEr2Brvr

TECHNOLOGY

EXAMPLE ADDRESSES BITCOIN.

1**GoogLe**d9Uj5P3RzzLxwXvKjQGe5XSpjgL
 1**Amazon**2fFxh9JmkqVVucyASRYgaPtir7e
 1**Huawei**ETqZrUy3AebJ4px27yrZQXzbRZk
 1**DELL**fLuYXJLAQaecEAZIVTZDXh6vx8DP
 1**inteLo**JMATv2aao7FfYyuK1LMi8Mdqoe
 1**Yahoo**HHV4zAsDSxJsnkVs5f58mjL8cHP
 1**SAP**xQRW6NdGG8RHxzj3ux5DbAqBw1HyP



FEELINGS

EXAMPLE ADDRESSES BITCOIN.

1**SmiLe**CALwLKsijbyjWqwaYP1jrvfBrTa
 1**Cry**5khFozgkqkzKHVhoPLMf8XAv4HeJcN
 1**Love**394jyAgtEgHyzmCk16T9ZUYmJZyBe
 1**Hate**zY6izYPZUk9ZHPVDrJqBjUCSR6YiU
 1**Sad**pw5pyy6mRpEiQTBTXvBaYMvVZQbPm
 1**Happy**srZWYWGB7vZ9MQoFHra8UwtfjpxR





You can make your request to the email inside www.ADDRESSKY.com

Check service prices at www.ADDRESSKY.com

We received your request, in this order you must include the following information.

Send Email:

- 1.- Name of the user or owner.
- 2.- Bitcoin reference deposit (Deposit address for tracking).
- 3.- Name of the address you have chosen.

To: order@addressky.com

Check service prices.

www.ADDRESSKY.com

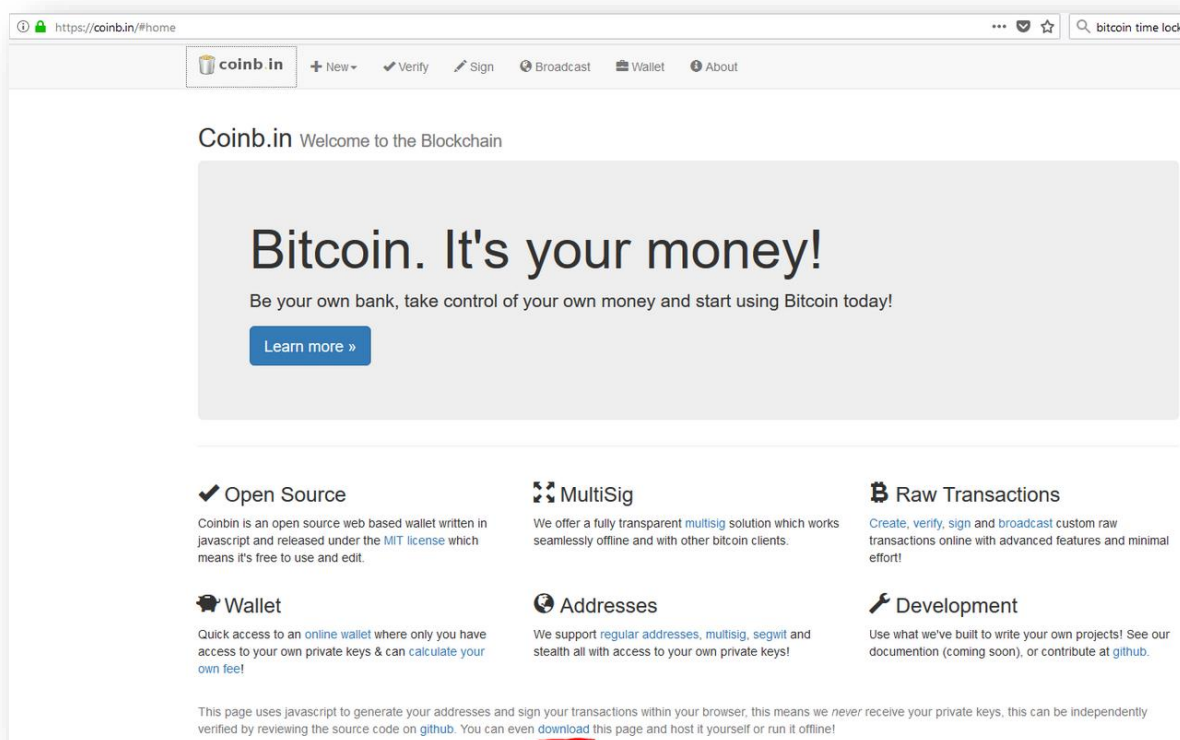
1. Creating time-locked address & sending your coins

[Download a local copy of Coinbin](#)

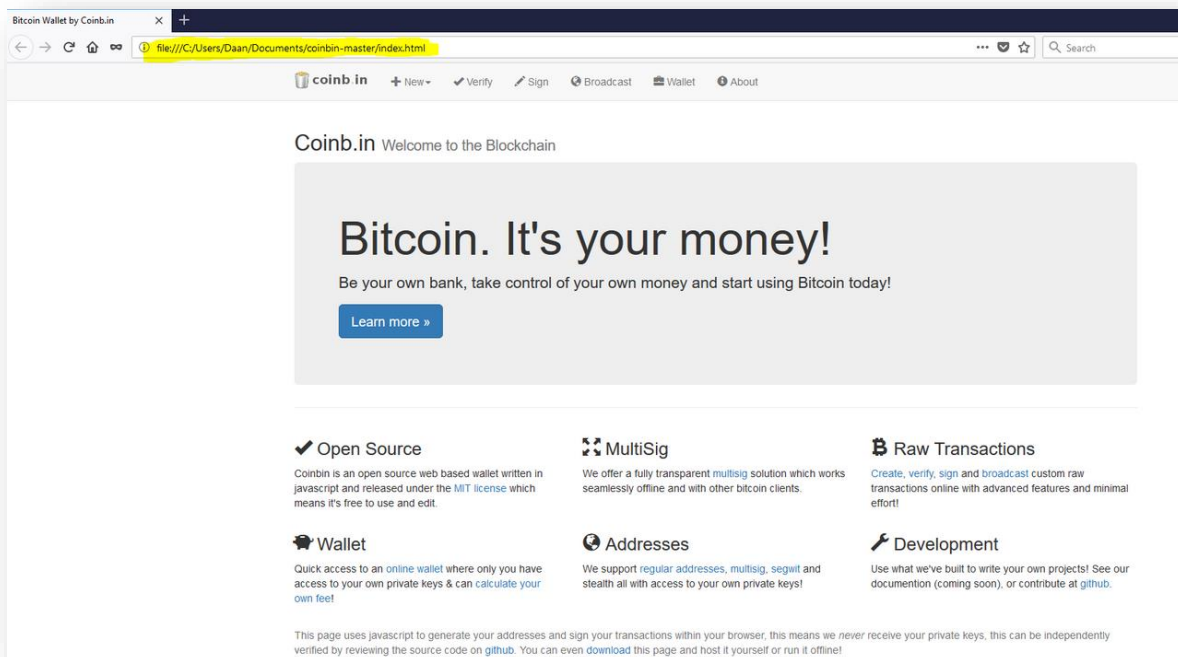
Go to Coinb.in and download the master branch of their website through Github. I'm not going to link the actual download here, because it's very important that you know you're downloading from a trusted source.

Extract the archive and open the index.html file in your browser of choice. You're now running a local copy of the coinb.in website.

[Download Coinbin Master Branch:](#)



Extract the archive and open Index.html:



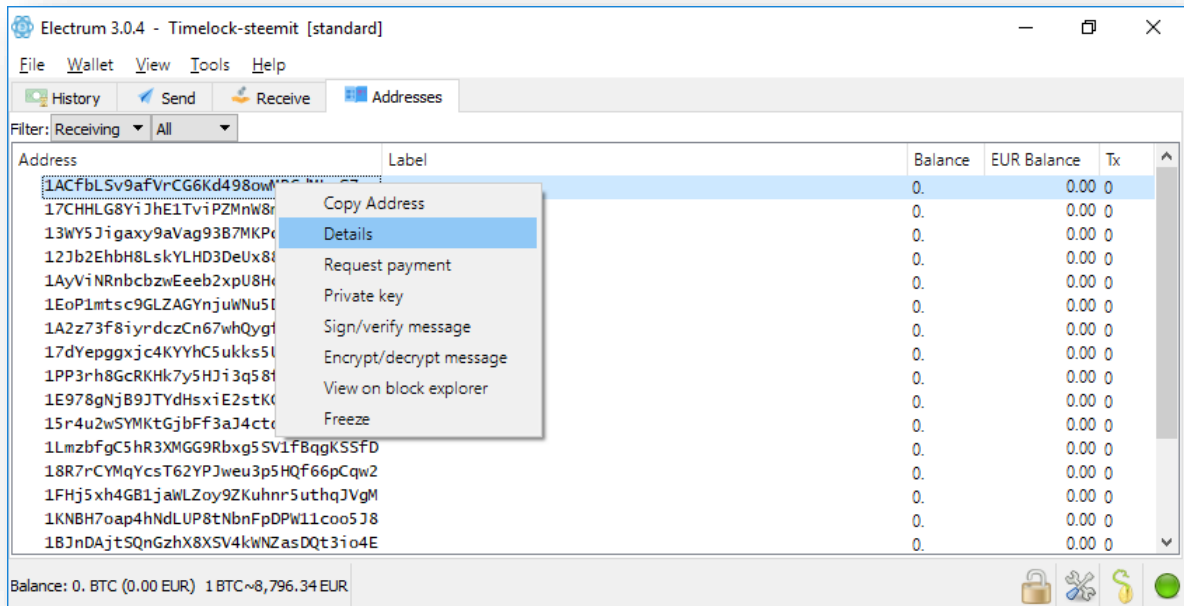
Now we're working with a local copy of the Coinb.in website, check the address bar to be sure.

Address Time-Lock

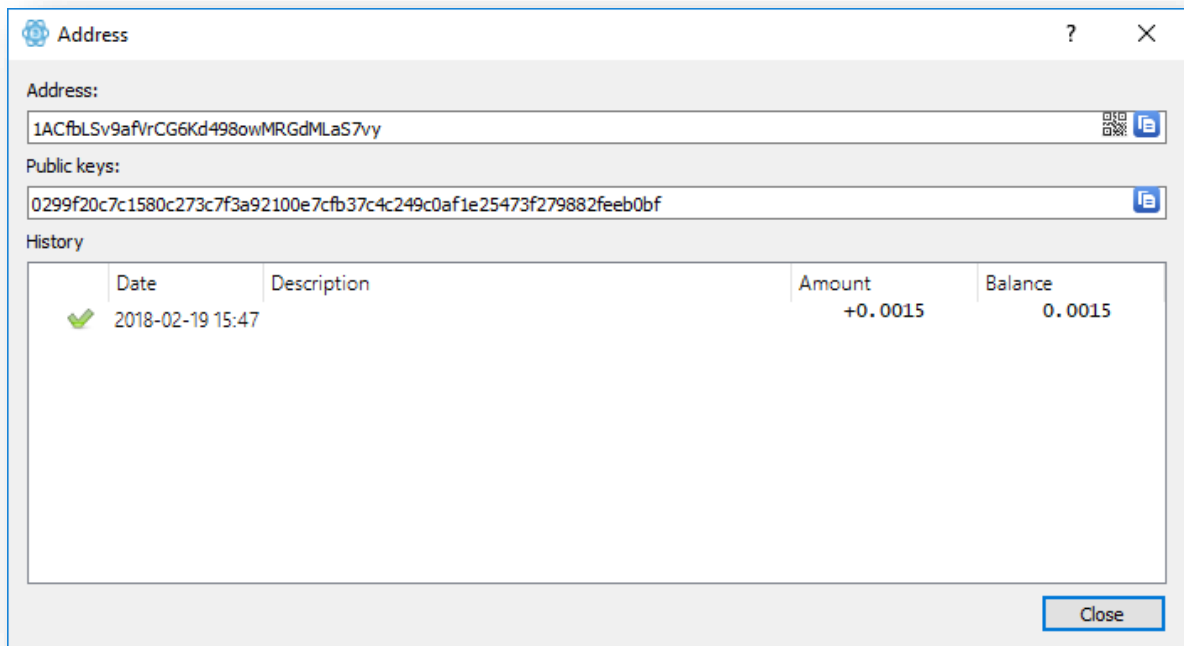
Make sure that you're using a local copy of the Coinbin website (as shown above) and create your time-locked address. Click on: 'New' >> 'Time Locked Address' in the top menu.

Fill in the public key of the address you've created with Electrum and enter either a date or block height by which the transaction should be unlocked.

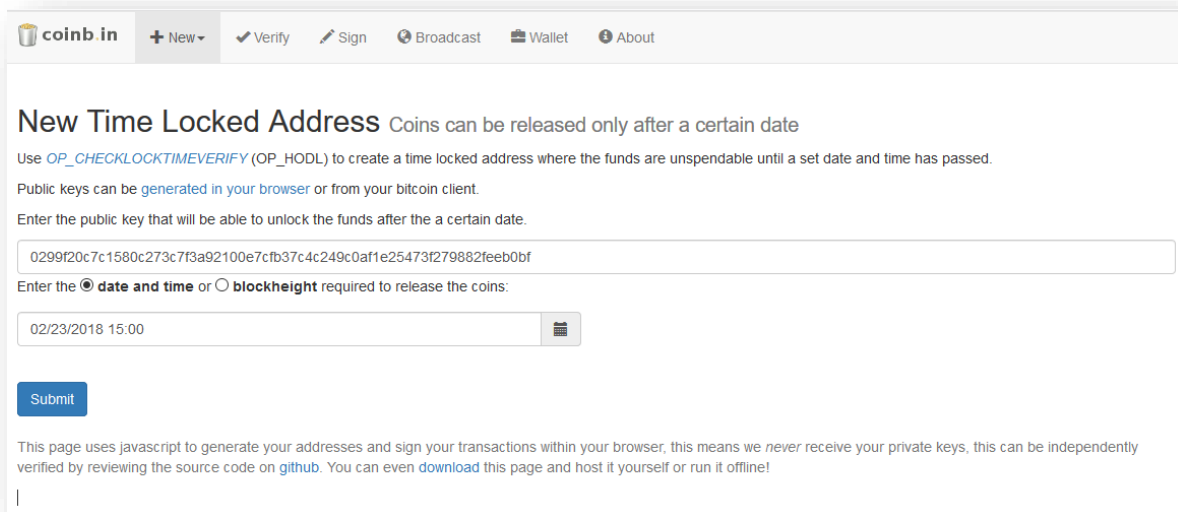
Where to find your public key:



Public key:



Enter your public key and set date or block height on Coinbin:



These coins can't be spend before 02/23/2018 15:00

Submit

Make sure you've filled everything in correctly and press the 'Submit' button.


Now you'll see a newly generated address to which you can send Bitcoin. Any coins you send to this address can only be redeemed after a certain date or block height has been reached.

You will also see a redeem script, you should save this or otherwise you won't be able to redeem your coins afterwards.

Redeem script:

04601e905ab175210299f20c7c1580c273c7f3a92100e7cfb37c4c249c0af1e25473f279882feb0bfac

Payment address & redeem script

 coinb.in
 + New
 Verify
 Sign
 Broadcast
 Wallet
 About

New Time Locked Address


Coins can be released only after a certain date

Use [OP_CHECKLOCKTIMEVERIFY](#) (OP_HODL) to create a time locked address where the funds are unspendable until a set date and time has passed.

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


Enter the public key that will be able to unlock the funds after the a certain date.

Enter the ☒ **date and time** or ☐ **blockheight** required to release the coins:



Address

Payment should be made to this address:



Redeem Script

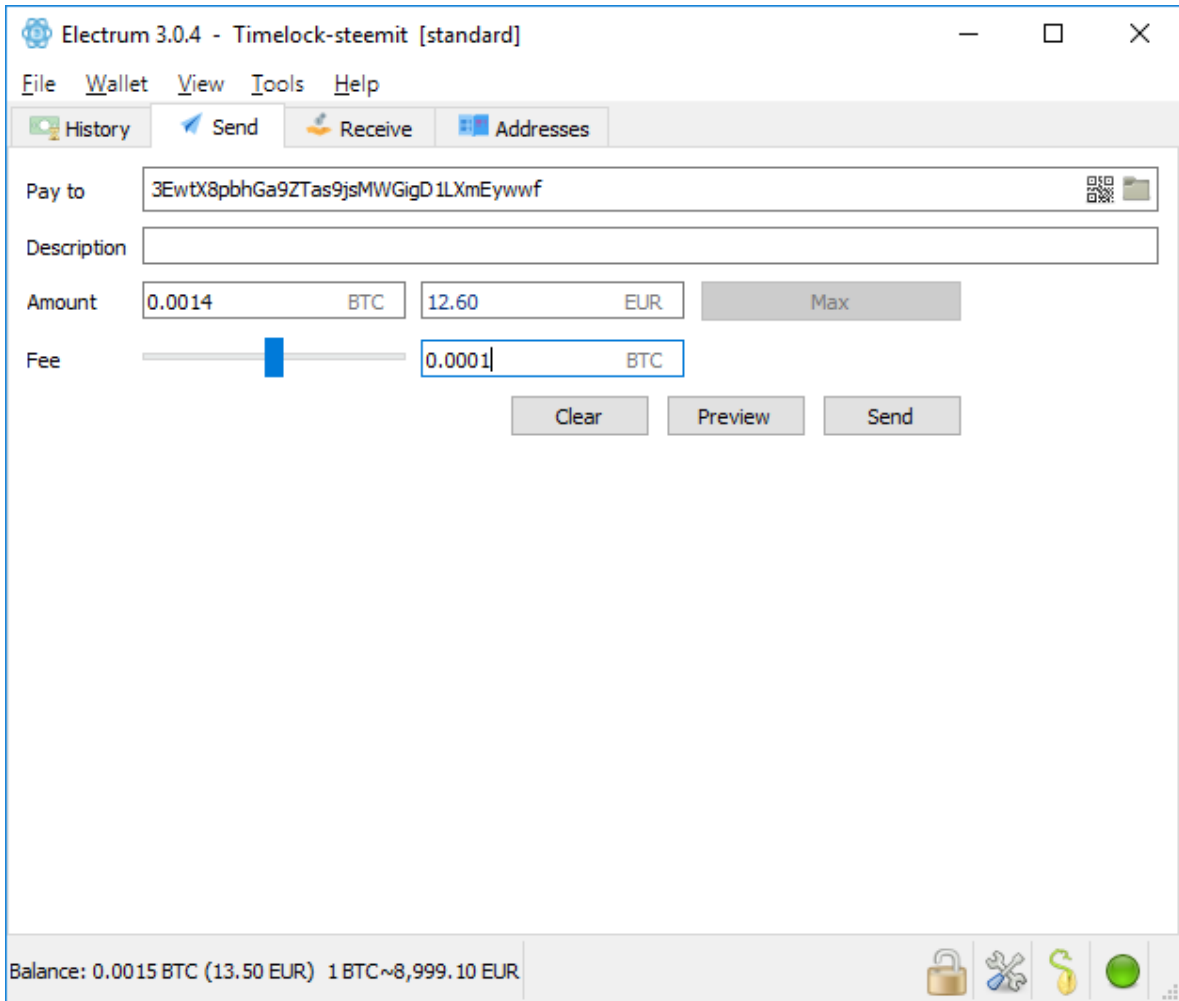
This script should be *saved and should be shared with all the participants before a payment is made*, so they may validate the authenticity of the address, it will also be used later to release the bitcoins.

Shareable URL

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!

Sending the transaction:



Electrum 3.0.4 - Timelock-steemit [standard]

File Wallet View Tools Help

History Send Receive Addresses

Pay to 3EwtX8pbhGa9ZTas9jsMWGigD1LXmEywwf

Description

Amount 0.0014 BTC 12.60 EUR Max

Fee 0.0001 BTC

Clear Preview Send

Balance: 0.0015 BTC (13.50 EUR) 1 BTC~8,999.10 EUR

That's it! You've now successfully locked your Bitcoins, they can't be spend before 02/23/2018 - 15:00. If you want to claim the coins I've used in this example, be sure to read the next section.

2. Redeeming your coins

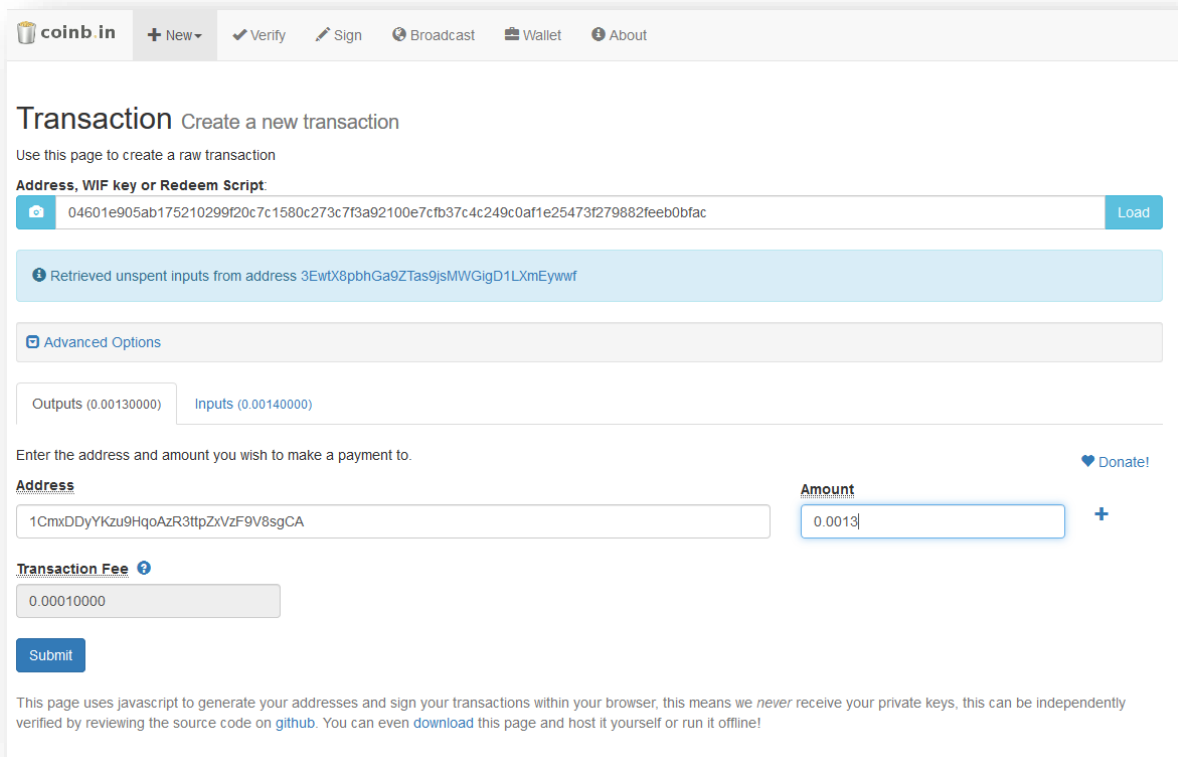
[Create a new transaction](#)

Again, only use your local Coinb.in copy.

Go to 'New' >> 'Transaction'

Paste your redeem script and click on 'Load'.

After pressing 'Load':



The screenshot shows the 'Transaction' page on the coinb.in website. The page has a navigation bar with links: '+ New', 'Verify', 'Sign', 'Broadcast', 'Wallet', and 'About'. The main heading is 'Transaction' with a subheading 'Create a new transaction'. Below this, it says 'Use this page to create a raw transaction'. There is a section for 'Address, WIF key or Redeem Script' with a text input field containing a long alphanumeric string and a 'Load' button. Below this, a blue box indicates 'Retrieved unspent inputs from address 3EwtX8pbhGa9ZTas9jsMWGigD1LXmEywwf'. There is an 'Advanced Options' section. Below that, there are tabs for 'Outputs (0.00130000)' and 'Inputs (0.00140000)'. The 'Address' field contains '1CmxDDyYKzu9HqoAzR3ttpZxVzF9V8sgCA'. The 'Amount' field contains '0.0013'. There is a 'Transaction Fee' field with a value of '0.00010000'. A 'Submit' button is at the bottom. A 'Donate!' link is also present. At the very bottom, there is a disclaimer: '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!'.

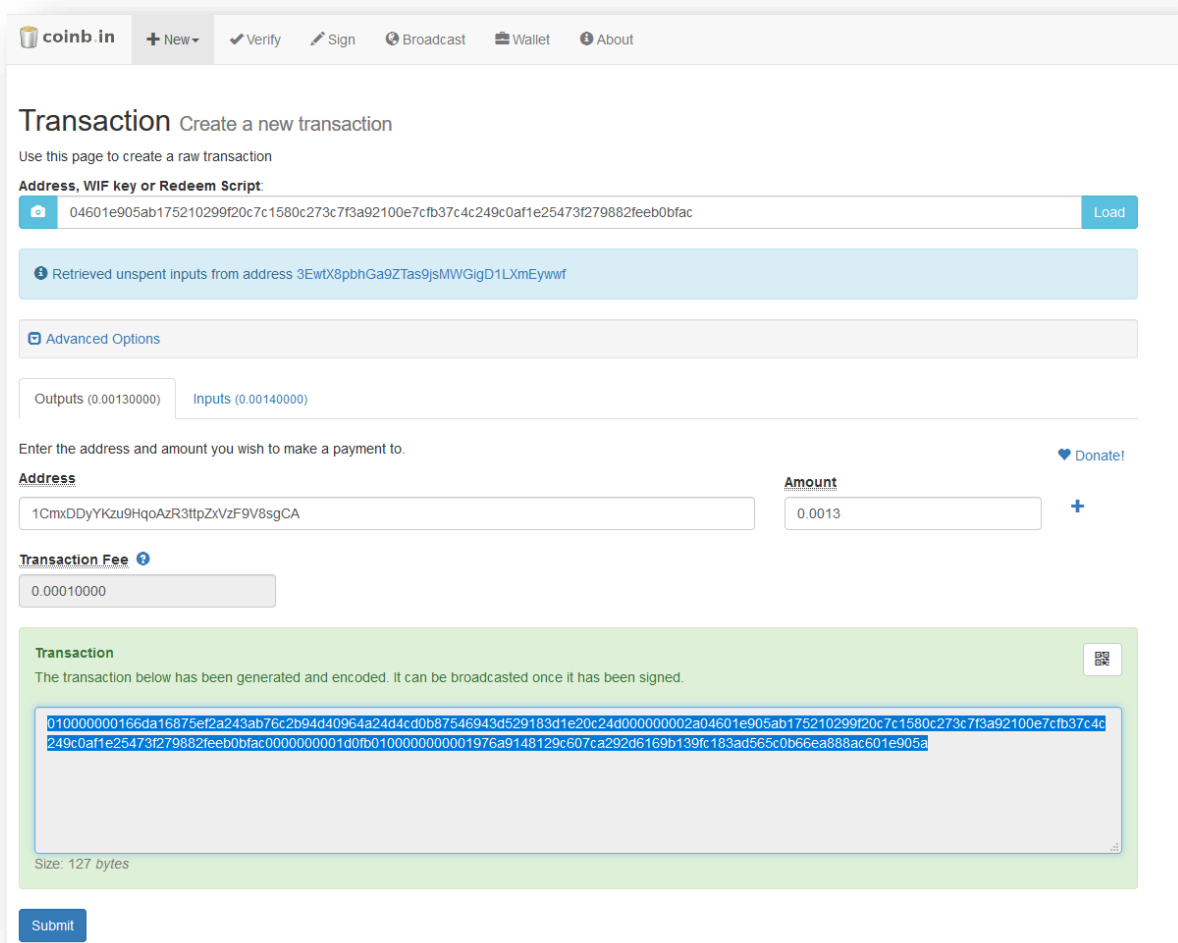
Enter the address you want the coins to be transferred to in the 'Address' field. Use another address than the one you've used to create this time-locked transaction.

Fill in the amount of Bitcoins you want to send. Use only part of the balance, the rest will be used for fees. In this case, you can fill in 0.0013 BTC, so 0.0001 BTC will be used as a fee.

Click 'Submit' after reviewing everything you've put in.

Now you should copy the raw transaction output as seen below.

Raw transaction output:

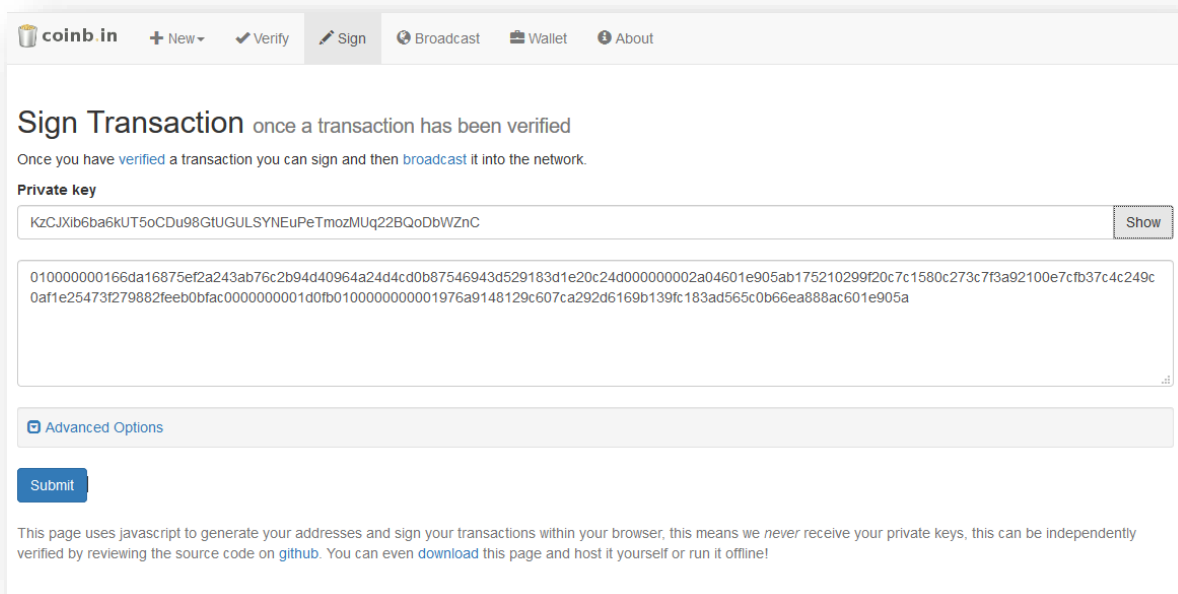


The screenshot shows the 'coinb.in' transaction creation page. It includes a navigation bar with links like '+ New', 'Verify', 'Sign', 'Broadcast', 'Wallet', and 'About'. The main heading is 'Transaction Create a new transaction'. Below this, there's a section for 'Address, WIF key or Redeem Script' with a text input field containing a long hexadecimal string and a 'Load' button. A blue box indicates 'Retrieved unspent inputs from address 3EwtX8pbhGa9ZTas9jsMWGigD1LXmEywwf'. There's an 'Advanced Options' section with tabs for 'Outputs (0.00130000)' and 'Inputs (0.00140000)'. Below this, there's a form to 'Enter the address and amount you wish to make a payment to.' with fields for 'Address' (1CmxDDyYKzu9HqoAzR3tPZxVzF9V8sgCA), 'Amount' (0.0013), and a 'Transaction Fee' (0.00010000). A 'Donate!' button is also present. The 'Transaction' section shows a green box with the message 'The transaction below has been generated and encoded. It can be broadcasted once it has been signed.' and a large text area containing the raw transaction output: 010000000166da16875ef2a243ab76c2b94d40964a24d4cd0b87546943d529183d1e20c24d00000002a04601e905ab175210299f20c7c1580c273c7f3a92100e7cfb37c4c249c0af1e25473f279882feeb0bfac0000000001d0fb0100000000001976a9148129c607ca292d6169b139fc183ad565c0b66ea888ac601e905a. The size is noted as 127 bytes. A 'Submit' button is at the bottom.

Output:

010000000166da16875ef2a243ab76c2b94d40964a24d4cd0b87546943d529183d1e20c24d00000002a04601e905ab175210299f20c7c1580c273c7f3a92100e7cfb37c4c249c0af1e25473f279882feeb0bfac0000000001d0fb0100000000001976a9148129c607ca292d6169b139fc183ad565c0b66ea888ac601e905a


After you've copied the raw transaction output, you should click on the 'Sign' tab and fill in the private key of the address used to create the time-locked transaction together with the raw transaction output. This is why we created a completely new address, you should never input your private keys unless you will not be using that address again.



The screenshot shows the 'Sign Transaction' page on the coinb.in website. The page has a navigation bar with links for '+ New', 'Verify', 'Sign', 'Broadcast', 'Wallet', and 'About'. The main heading is 'Sign Transaction' with a subtext 'once a transaction has been verified'. Below this, it says 'Once you have [verified](#) a transaction you can sign and then [broadcast](#) it into the network.' There is a section for the 'Private key' with a text input field containing 'KzCJXib6ba6kUT5oCDu98GtUGULSYNEuPeTmozMUq22BQoDbWZnC' and a 'Show' button. Below the private key is a large text area containing a long hexadecimal string representing the raw transaction output. At the bottom, there is an 'Advanced Options' section and a 'Submit' button. A footer note states: '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!'

Private key: KzCJXib6ba6kUT5oCDu98GtUGULSYNEuPeTmozMUq22BQoDbWZnC

Now you'll receive a signed transaction hash that you can broadcast to receive your time-locked Bitcoins.



[+ New](#)
[Verify](#)
[Sign](#)
[Broadcast](#)
[Wallet](#)
[About](#)

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

KzCjXib6ba6KUT5oCDu98GIUGULSYNEuPeTmozMUq22BQoDbWZnC

Show

010000000166da16875ef2a243ab76c2b94d40964a24d4cd0b87546943d529183d1e20c24d000000002a04601e905ab175210299f20c7c1580c273c7f3a92100e7cfb37c4c249c0af1e25473f279882feeb0bfac0000000001d0fb0100000000001976a9148129c607ca292d6169b139fc183ad565c0b66ea888ac601e905a

Advanced Options

Signed transaction

The above transaction has been signed:


010000000166da16875ef2a243ab76c2b94d40964a24d4cd0b87546943d529183d1e20c24d00000000744830450221008e591ffc1d03fed14d6dbb3d4d8b22233fab5a80c1e1115796cd213464b77e4c02206ac1e1902e06c0f514caaaa43a746afa36d4688031859bad0193c0e38b948bdb012a04601e905ab175210299f20c7c1580c273c7f3a92100e7cfb37c4c249c0af1e25473f279882feeb0bfac0000000001d0fb0100000000001976a9148129c607ca292d6169b139fc183ad565c0b66ea888ac601e905a

Size: 201 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!

Finally, go to the 'Broadcast' tab to paste the signed transaction. The coins will only be sent if the date or block height of the time-locked transaction has expired.



[+ New](#)
[Verify](#)
[Sign](#)
[Broadcast](#)
[Wallet](#)
[About](#)

Broadcast Transaction

into the bitcoin network

Enter your hex encoded bitcoin transaction

010000000166da16875ef2a243ab76c2b94d40964a24d4cd0b87546943d529183d1e20c24d00000000744830450221008e591ffc1d03fed14d6dbb3d4d8b22233fab5a80c1e1115796cd213464b77e4c02206ac1e1902e06c0f514caaaa43a746afa36d4688031859bad0193c0e38b948bdb012a04601e905ab175210299f20c7c1580c273c7f3a92100e7cfb37c4c249c0af1e25473f279882feeb0bfac0000000001d0fb0100000000001976a9148129c607ca292d6169b139fc183ad565c0b66ea888ac601e905a

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!



You'll get an error like this when you try to broadcast before the time-lock expires:

[+ New](#) [✓ Verify](#) [✎ Sign](#) [📡 Broadcast](#) [👛 Wallet](#) [🔔 About](#)

Broadcast Transaction into the bitcoin network

Enter your hex encoded bitcoin transaction

```
010000000166da16875ef2a243ab76c2b94d40964a24d4cd0b87546943d529183d1e20c24d00000000744830450221008e591ffc1d03fed14d6dbb3d4d8b22233fab5a80c1e1115796cd213464b77e4c02206ac1e1902e06c0f514caaaa43a746afa36d4688031859bad0193c0e38b948bdb012a04601e905ab175210299f20c7c1580c273c7f3a92100e7cfb37c4c249c0af1e25473f279882feeb0bfac000000001d0fb010000000001976a9148129c607ca292d6169b139fc183ad565c0b66ea888ac601e905a
```

64: non-final

[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!]

Grab your coins!

Within this message I've made it possible for you to claim my time-lock worth 0.0014 BTC (minus fees). All you need to do is enter the redeem script and private keys, which I've shown in this post.

TL;DR

To create the Time Locked Address:

Go to [Coinb.in](#);

Click on 'New' >> 'Time Locked Address'

Enter your public key (Of the address you created with Electrum)

Enter date + time or block height of when you want your Bitcoins released

Submit

Save the Redeem Script

Send the bitcoins you want to keep locked to the Address generated.



Spend your coins after the time-lock expires.

Go to Coinb.in

Click on: 'New' -> 'Transaction'

Paste your Redeem Script and click Load (it shows every input available to be spent)

Paste the address you want to send the coins to at the "Address" field and the amount in the "Amount" field. The remaining funds will be used as fee. E.g: If your address has 0.015BTC, you can put 0.0014BTC in the

"Amount" field and the fee will be 0.0001BTC (Making 0.0015 in total)

Press 'Submit' and copy the raw transaction

Click on the "Sign" tab

Paste the private key from the Electrum address you created

Paste the raw transaction (you've gotten this from the 'transaction' page.)

Press 'Submit'. Now you've received a 'signed transaction' script

Click on the 'Broadcast' tab and paste the signed transaction script

Transaction is sent! Or not, if you've made an error or if you try to do this before the time-lock has expired.

Reference.

- (1) <https://steemit.com/bitcoin/@daan/how-to-create-time-locked-transactions-with-bitcoin-free-bitcoins-inside>
- (2) www.Coinb.in
- (3) www.ADDRESSKY.com