Bitcoin Wallets

For when you don't want to wait 10 days to sync the entire Bitcoin network.

Christian Grewell Follow
Oct 28, 2018 · 5 min read

A Bitcoin wallet is the first step to using Bitcoin, but before we begin…

Warning!

Just like in your real life, your funds and wallet must be secured. Bitcoin makes it possible to transfer value anywhere in a very easy way and it allows you to be in control of your money. These features also come with great security concerns. **So always be on guard.** At the same time, Bitcoin can provide very high levels of security if used correctly. **Always remember that it is your responsibility to adopt good practices in order to protect your money**.

```
always type links rather than merely clicking them!
```

What is a Wallet?

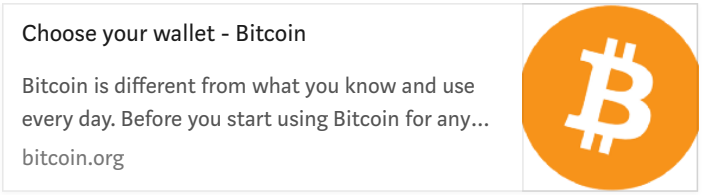
A "wallet" is basically the Bitcoin equivalent of a bank account. It allows you to receive bitcoins, store them, and then send them to others. You can think of a wallet as your personal user interface to the Bitcoin network of nodes, similar to how your online bank account is an interface to the regular monetary system.

Bitcoin wallets contain **private keys**; secret codes that allow you to spend your bitcoins. In reality, it's not bitcoins that need to be stored and secured, but the *private keys* that give you access to them.

In short, a Bitcoin wallet is simply an app, website, or device that manages Bitcoin private keys for you.

Choosing a Bitcoin Wallet

I highly *highly* `highly` recommend choosing a trusted source for your Bitcoin wallet. The best source for wallet information in my opinion, is www.bitcoin.org



Electrum

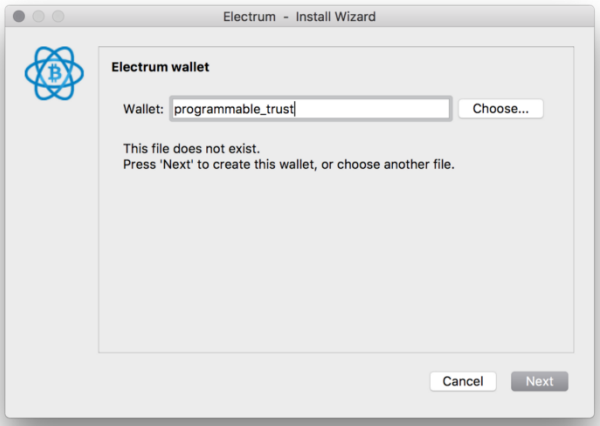
In our case, we'll start with a desktop wallet, Electrum, which does not use a lot of resources, and allows you to recover your wallet from a secret phrase. We'll use mobile wallets for Android and iOS later in the course.

1. Download electrum here: https://electrum.org/#download

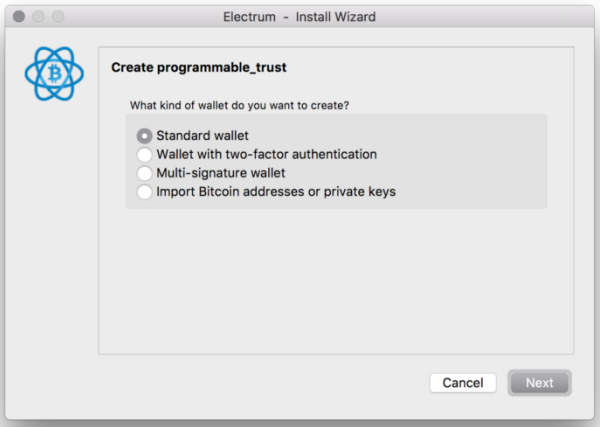
```
always check links before you click on them. you know who
you are...
```

2. Install electrum and create your personal wallet

Choose autoconnect

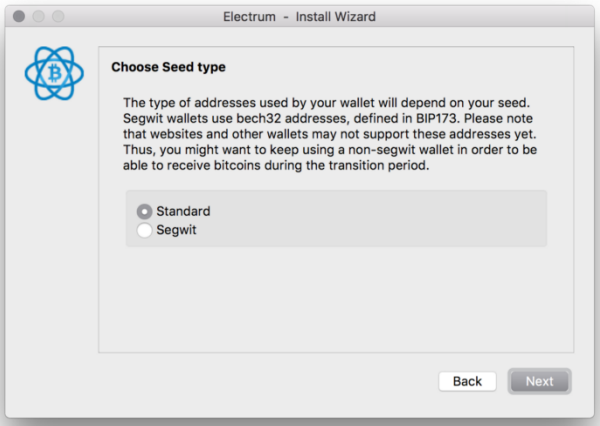


name it something useful

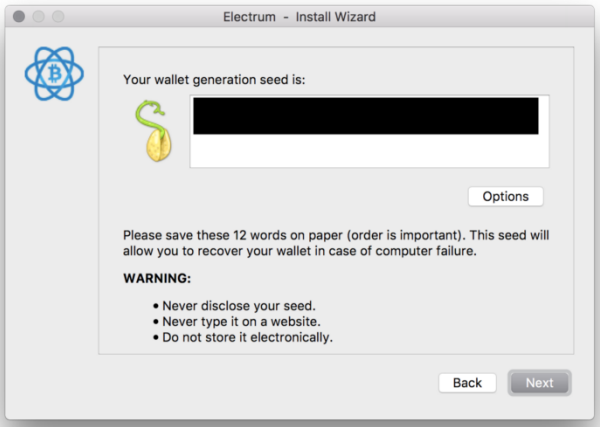


choose a standard wallet

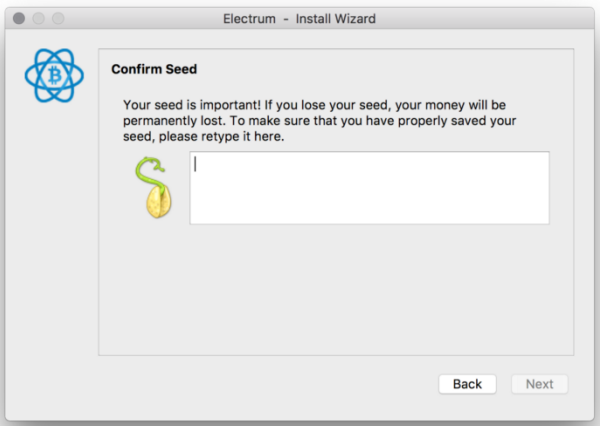
create a new seed



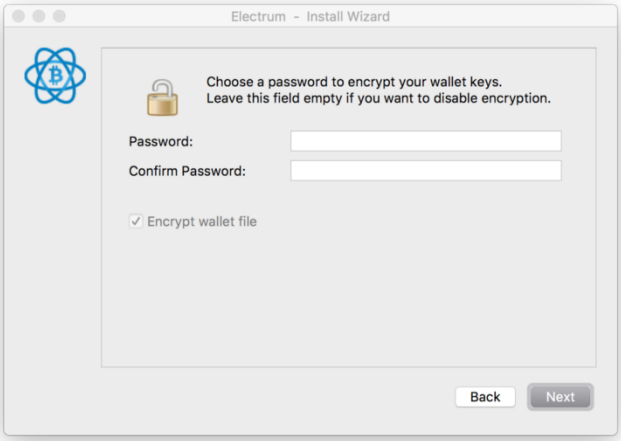
Choose a standard seed type



WRITE YOUR SEED PHRASE ON A PIECE OF PAPER, **DO NOT DISCLOSE IT TO ANYONE!**



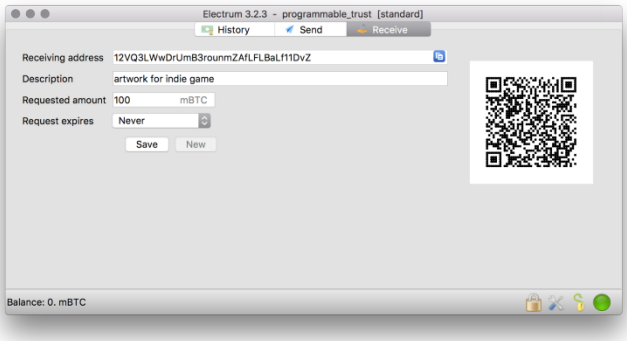
now re-type it to verify you wrote it down correctly



choose a password to encrypt your keys. you can always generate these keys again using your seed, but if you do not encrypt your private keys, your wallet is easily stolen.

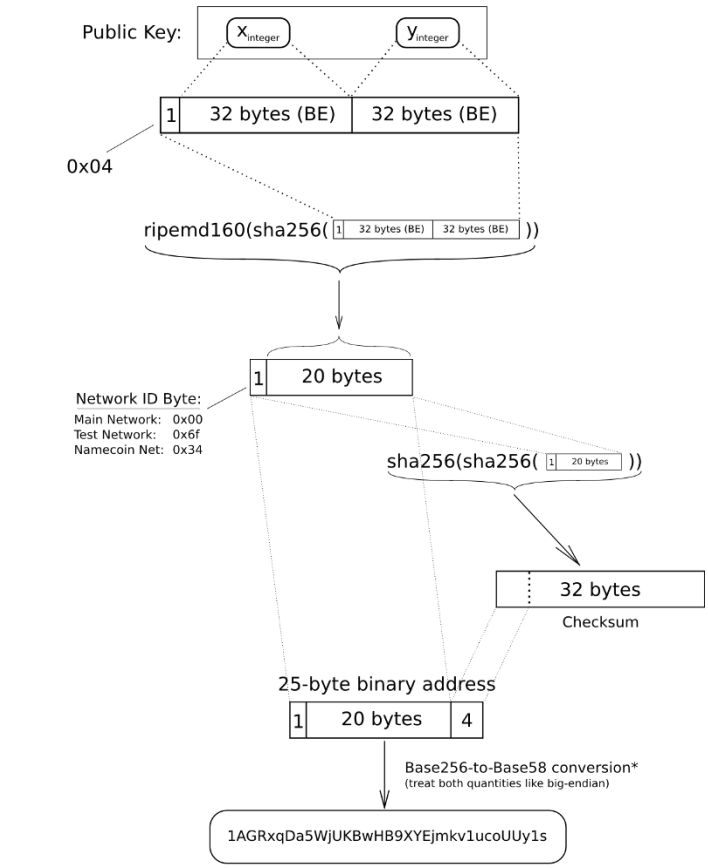
Receiving Bitcoin

If you would like to receive Bitcoin (who doesn't!?) then you need to provide the sender with your wallet address. Electrum can (and does) generate many public wallet addresses



- The `receiving address` is a 160-bit hash of the public portion of a public/private keypair. It's the output of a cryptographic process that converts your public key to a public bitcoin address.

Elliptic-Curve Public Key to BTC Address conversion



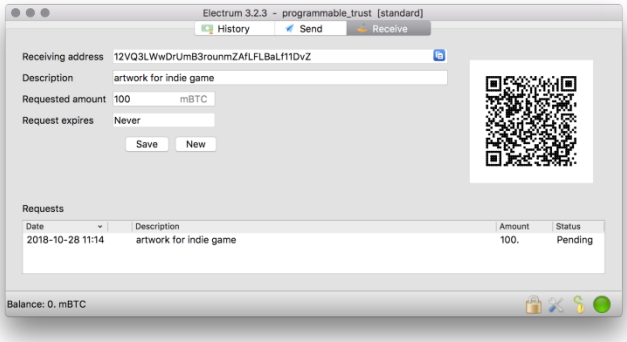
*In a standard base conversion, the 0x00 byte on the left would be irrelevant (like writing '052' instead of just '52'), but in the BTC network the left-most zero chars are carried through the conversion. So for every 0x00 byte on the left end of the binary address, we will attach one '1' character to the Base58 address. This is why main-network addresses all start with '1'

source: https://en.bitcoin.it/wiki/File:PubKeyToAddr.png

- The `description` is just that, a description for the sender to view
- The `amount` is a field denominated in mBTC. **mBTC** is also know as millibitcoin and it also one thousandth of a BTC. 1 **mBTC** = 0.001 BTC. Given that as of this writing, 1 BTC = $6,400 USD, it's handy to denominate things in mBTC.

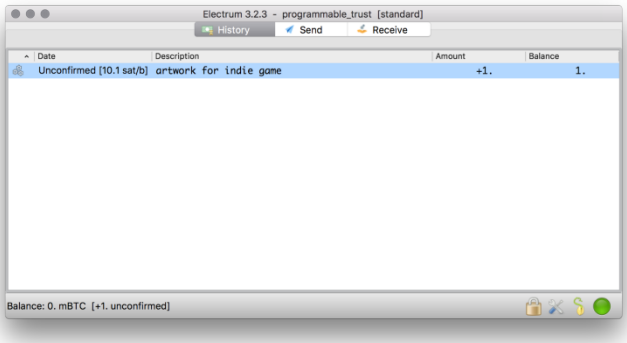
Next, you can provide the sender with either the QR code, or the wallet address directl. In this case: `12VQ3LWwDrUmB3rounmZAfLFLBaLf11DvZ`

Electrum will show these transactions as pending until the bitcoin network confirms that bitcoin was sent to the address.



waiting for a transfer

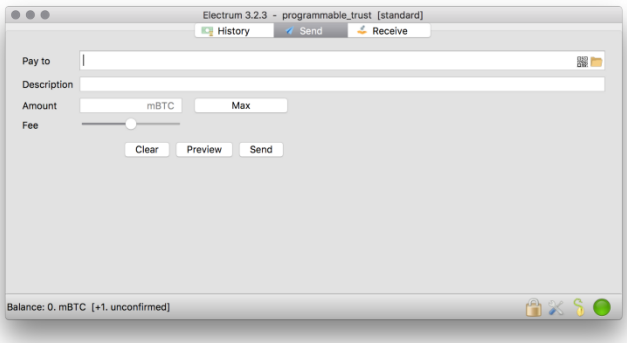
Electrum will notify you immediately once it sees funds have been sent (but they will be unconfirmed until at least the next block is mined - between 0 and 10 minutes).



This transaction has not been confirmed yet by the bitcoin network

Sending Bitcoin

To send bitcoin, you first need a balance in the wallet.



- `Pay to` —this is the Bitcoin wallet you would like to send funds to. **Be very careful to make sure your address is correct!** I've sent untold numbers of BTC throughout the years to bad addresses. It hurts.

- `Fee` —the fee amount will impact how quickly your transaction is confirmed by the bitcoin network. It will generally tell you the estimates time as well. If the network is congested (e.g., many transactions), then a higher fee will incentivize network participants to include your transaction instead of other, lower fee transactions.