Twitter Thread by <u>librehash</u>



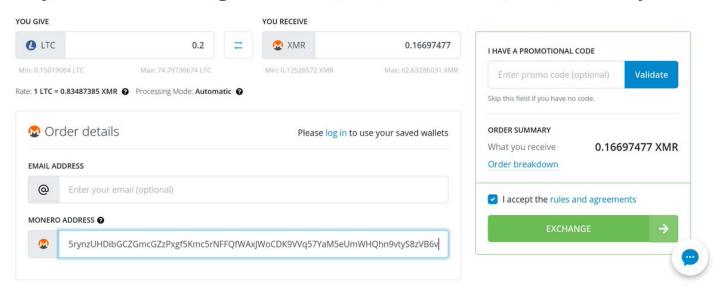


1/ Wrote an article here about an exchanger that allows you to swap several different cryptocurrencies for Monero without KYC or logins at all

2/ Being the eternal skeptic, wanted to test if this website was actually legitimate (there are a lot of crypto scams out there; way too many)..

So we start off visiting the main website and set up a LTC:XMR conversion.

Buy, Sell and Exchange Litecoin (LTC) to Monero (XMR) instantly



3/ The Monero address that you see in the picture above was created using this "mindwallet" altered tool created by Pactito (https://t.co/KArylCXgWR)

○ Bitcoin ○ B	Ethereum O Litecoin O Monero
Passphrase	
Email: [?]	use at least 8 character
	Generate

You are online. For maximum security is better that you clone this page and generate the address in a computer disconnected from the internet.

MindWallet is a deterministic cryptocurrency address generator, it is a fork of MemWallet which itself is inspired by WarpWallet, but it uses the Argon2 hashing function instead of scrypt. You never have to save or store your private key anywhere. Just pick a really good password - many random words, for example - and never use it for anything else.

3a/ Wouldn't recommend creating a Monero wallet this way, specifically, but this tool generates addresses deterministically with Argon2 as its KDF using BIP32 + BIP38

The algorithm behind MindWallet:

```
b = 1 for Bitcoin, 2 for Litecoin, 3 for Ethereum and 4 for Monero seed<sub>1</sub> = argon2(key=(passphrase||b), salt=(salt||b), N=2<sup>18</sup>, r=8, p=1, dkLen=32) seed<sub>2</sub> = pbkdf2(key=(passphrase||(b+1)), salt=(salt||(b+1)), c=2<sup>16</sup>, dkLen=32, prf=SHA256) wallet = generate_wallet(seed=(seed<sub>1</sub> ⊕ seed<sub>2</sub>))
```

3b/ You can try it yourself. Password for this wallet = librehash

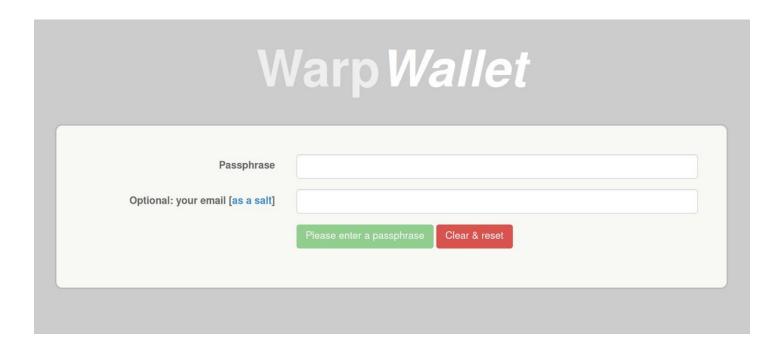
E-mail (salt) = librehash@test.com

You'll generate the exact same addresses and keys as you see here.

Benefit = in theory, you never need to have your private key stored anywhere, ever.

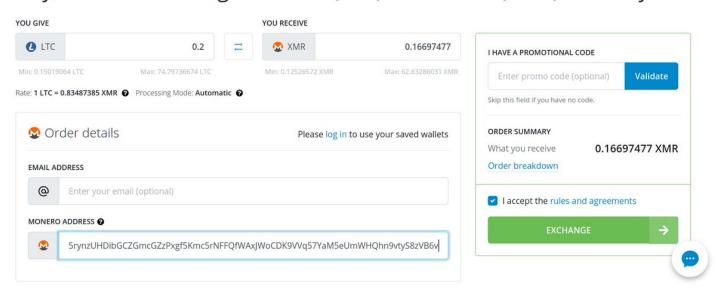
○ Bitcoin ○ Ethereum ○ Litecoin ○ Monero	
Passphrase	•••••
Email: [?]	librehash@test.com
Running argon2 This may take up to 1	or 2 minutes. Use the Golang version for a faster version.

3c/ If you're wondering if this is legit or not, check out the <u>@KeybaseIO</u> implementation at <u>https://t.co/sUJpIZEWAf</u>; as you can see, a simple 8-character alphanumeric password with 20+ btc in it has yet to be solved 3-4 years later (salt already given)

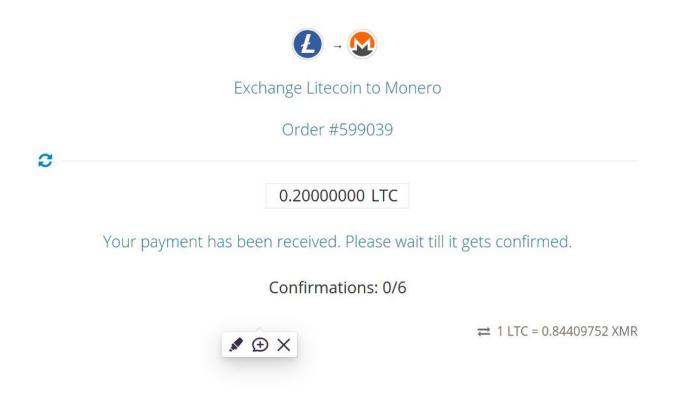


4/ Back to the site, we tested out a simple \$LTC #Litecoin to \$XMR #Monero transfer

Buy, Sell and Exchange Litecoin (LTC) to Monero (XMR) instantly



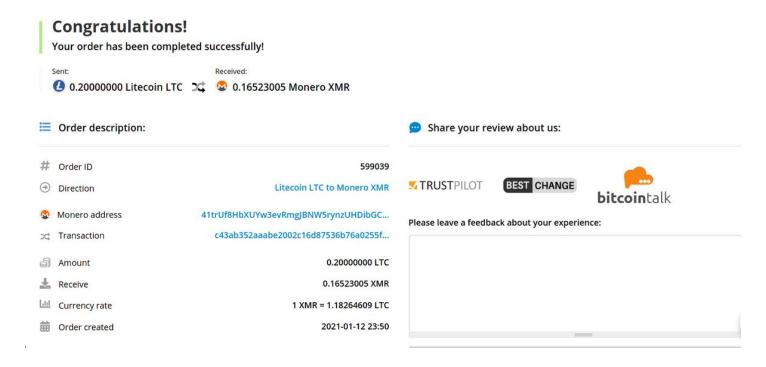
5/ Elected to send about \$20 worth of \$LTC at the time. Enough of an amount to where it felt like a legitimate test. The 6 confirmation wait screen is pretty standard. Cool.



6/ Once that was finished, we were given this screen.

\$XMR Monero is diff from other cryptocurrencies (obviously). We need to visit the transaction link.

https://t.co/MTck2Nsxdp



7/ The link from above takes us here. Notice the two stealth addresses with question marks for 'amount'.

If we want to see ours, we need to use our reg. \$XMR addy + priv. view key.



8/ Upon doing so, we can see that the correct output has been matched. Cross referencing it with what the site told us (and what we agreed to), we can see that the values match.

So this gets the stamp of approval right now.

Tx hash: c43ab352aaabe2002c16d87536b76a0255f8b576c7b20ca01915d4fa08dfce06

 $Tx\;public\;key:\;120a41918f04de04352b7230d4467e6e699e3bbd867d351d5f4aefbd5acf12ef$

Timestamp [UCT]: 2021-01-12 21:10:02 Block: 2273162

Age [y:d:h:m:s]: 00:000:03:45:00

Fee: 0.000015880000 Tx size: 1.9189 kB

Checking which outputs belong to the given address and viewkey

 $address:\ 41 tr Uf8 HbXUYw3 evRmgJBNW5 rynz UHDibGCZGmcGZzPxgf5Kmc5 rNFFQfWAxJWoCDK9VVq57 YaM5 eUmWHQhn9vtyS8zVB6varders. Authorized the company of the co$

Outputs (2)

output public key

00: 433fee59a3d8b7424402fd32e65a1fe16fdc7002848792a40f4135c53729deb7

01: 7c9fdd4d42b0fe6cf5ebbf817667950445d3dbb60c3ba692ab28ddd9dcc8f3da

0.165230050000

false

Sum XMR from matched outputs (i.e., incoming XMR): 0.165230050000

link to this page