

Twitter Thread by librehash

**librehash**

@librehash



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

YOU GIVE

LTC

0.2

Min: 0.15019064 LTC

Max: 74.79736674 LTC

=

YOU RECEIVE

XMR

0.16697477

Min: 0.12526572 XMR

Max: 62.63286031 XMR

Rate: 1 LTC = 0.83487385 XMR ⓘ Processing Mode: Automatic ⓘ

Order details

Please [log in](#) to use your saved wallets

EMAIL ADDRESS

@

Enter your email (optional)

MONERO ADDRESS ⓘ

5rynzUHDibGCZGmcGZzPxgf5Kmc5rNFFQfWaxjWoCDK9VVq57YaM5eUmWHQhn9vtyS8zVB6v|

I HAVE A PROMOTIONAL CODE

Enter promo code (optional)

Validate

Skip this field if you have no code.

ORDER SUMMARY

What you receive **0.16697477 XMR**

[Order breakdown](#)

☒ I accept the [rules and agreements](#)

EXCHANGE

→

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

☐ Bitcoin ☐ Ethereum ☐ Litecoin ☒ 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
seed1 = argon2(key=(passphrase||b), salt=(salt||b), N=218, r=8, p=1, dkLen=32)
seed2 = pbkdf2(key=(passphrase||(b+1)), salt=(salt||(b+1)), c=216, dkLen=32, prf=SHA256)
wallet = generate_wallet(seed=(seed1 ⊗ seed2))
```

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 [@KeybaseIO](#) implementation at <https://t.co/sUJplZEWaf> ; 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)

Warp Wallet

Passphrase

Optional: your email [\[as a salt\]](#)

Please enter a passphrase

Clear & reset

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

YOU GIVE

LTC

0.2

Min: 0.15019064 LTCMax: 74.79736674 LTC

YOU RECEIVE

XMR

0.16697477

Min: 0.12526572 XMRMax: 62.63286031 XMR

Rate: 1 LTC = 0.83487385 XMRProcessing Mode: Automatic

Order details

Please [log in](#) to use your saved wallets

EMAIL ADDRESS

@

Enter your email (optional)

MONERO ADDRESS

M

5rynzUHDibGCZGmcGZzPxf5Kmc5rNFFQfWAXjWoCDK9VVq57YaM5eUmWHQhn9vtyS8zVB6v

I HAVE A PROMOTIONAL CODE

Enter promo code (optional)

Validate

Skip this field if you have no code.

ORDER SUMMARY

What you receive0.16697477 XMR

[Order breakdown](#)

☒ I accept the [rules and agreements](#)

EXCHANGE

→

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.

L

→

M

Exchange Litecoin to Monero

Order #599039

↺

0.20000000 LTC

Your payment has been received. Please wait till it gets confirmed.

Confirmations: 0/6

✎

+

✕

⇄ 1 LTC = 0.84409752 XMR

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>

Congratulations!

Your order has been completed successfully!

Sent: 0.20000000 Litecoin LTC Received: 0.16523005 Monero XMR

Order description:

# Order ID	599039
➔ Direction	Bitcoin LTC to Monero XMR
👤 Monero address	41trUf8HbXUYw3evRmgjBNW5rynzUHDibGC...
🔗 Transaction	c43ab352aaabe2002c16d87536b76a0255f...
📄 Amount	0.20000000 LTC
📄 Receive	0.16523005 XMR
📊 Currency rate	1 XMR = 1.18264609 LTC
📅 Order created	2021-01-12 23:50

Share your review about us:

TRUSTPILOT

BEST CHANGE



Please leave a feedback about your experience:

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.

Autorefresh is OFF

Tx hash: c43ab352aaabe2002c16d87536b76a0255f8b576c7b20ca01915d4fa08dfce06
Tx prefix hash: 950d35a54ca46c331727e3b3a49adc51c7b0a8168d35cc5657a8893bcb0214ab
Tx public key: 120a41918f04de04352b7230d4467e6e699e3bbd867d351d5f4aefbd5acf12ef
Payment id (encrypted): d72dd238c2751e73

Timestamp: 1610485802

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

Age [y:d:h:m:s]: 00:000:03:40:13

Block: 2273162

Fee (per_kB): 0.000015880000 (0.000008275379)

Tx size: 1.9189 kB

Tx version: 2

No of confirmations: 96

RingCT/type: yes/5

Extra: 01120a41918f04de04352b7230d4467e6e699e3bbd867d351d5f4aefbd5acf12ef020901d72dd238c2751e73

2 output(s) for total of ? xmr

	stealth address	amount	amount idx
00:	433fee59a3d8b7424402fd32e65a1fe16fdc7002848792a40f4135c53729deb7	?	25815400 of 25825019
01:	7c9fdd4d42b0fe6cf5ebbf817667950445d3dbb60c3ba692ab28dd9dcc8f3da	?	25815401 of 25825019

code outputs

Prove sending

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

Payment id (decrypted): 0000000000000000 (value incorrect if you are not the recipient of the tx)

Block: 2273162 Timestamp [UCT]: 2021-01-12 21:10:02 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: 41trUf8HbXUYw3evRmgJBW5rynzUHDibGCZGmcGZzPxf5Kmc5rNFFQfWaxJWoCDK9VVq57YaM5eUmWHQhn9vtyS8zVB6v

viewkey: c25*****06

Outputs (2)

output public key	amount	output match?
00: 433fee59a3d8b7424402fd32e65a1fe16fdc7002848792a40f4135c53729deb7	0.165230050000	true
01: 7c9fdd4d42b0fe6cf5ebbf817667950445d3dbb60c3ba692ab28ddd9dcc8f3da	?	false

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

[link to this page](#)