# Twitter Thread by librehash

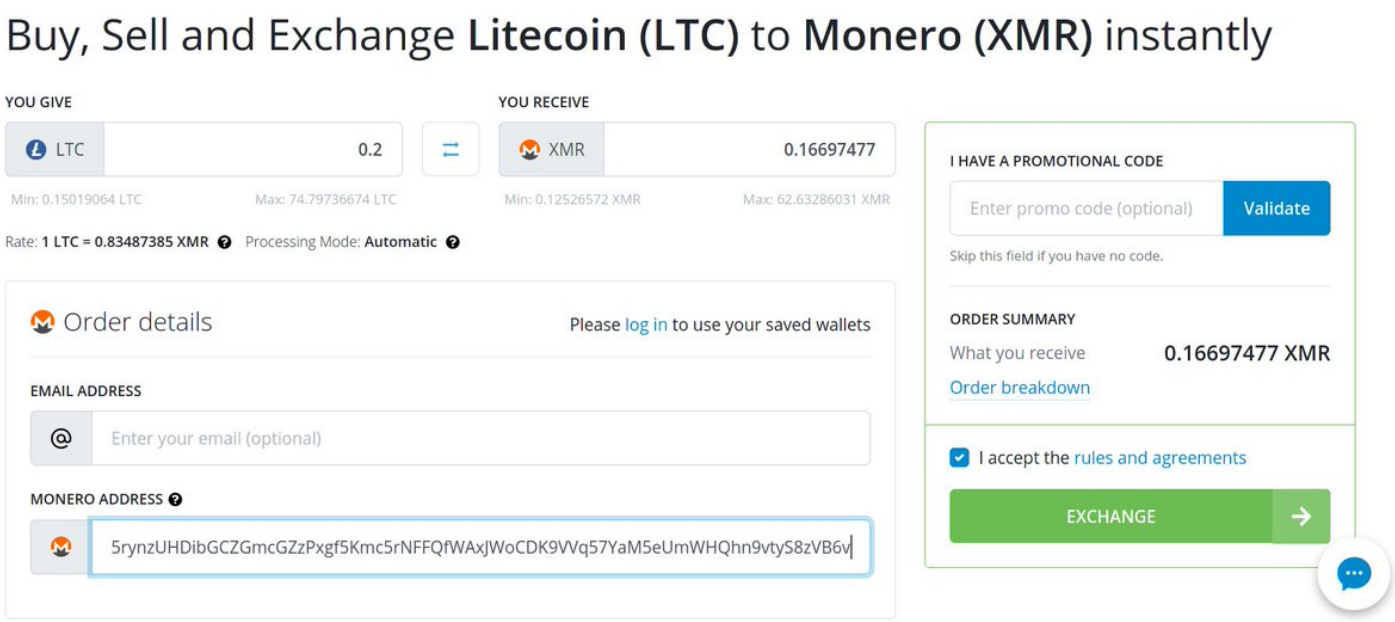


**librehash**
@librehash

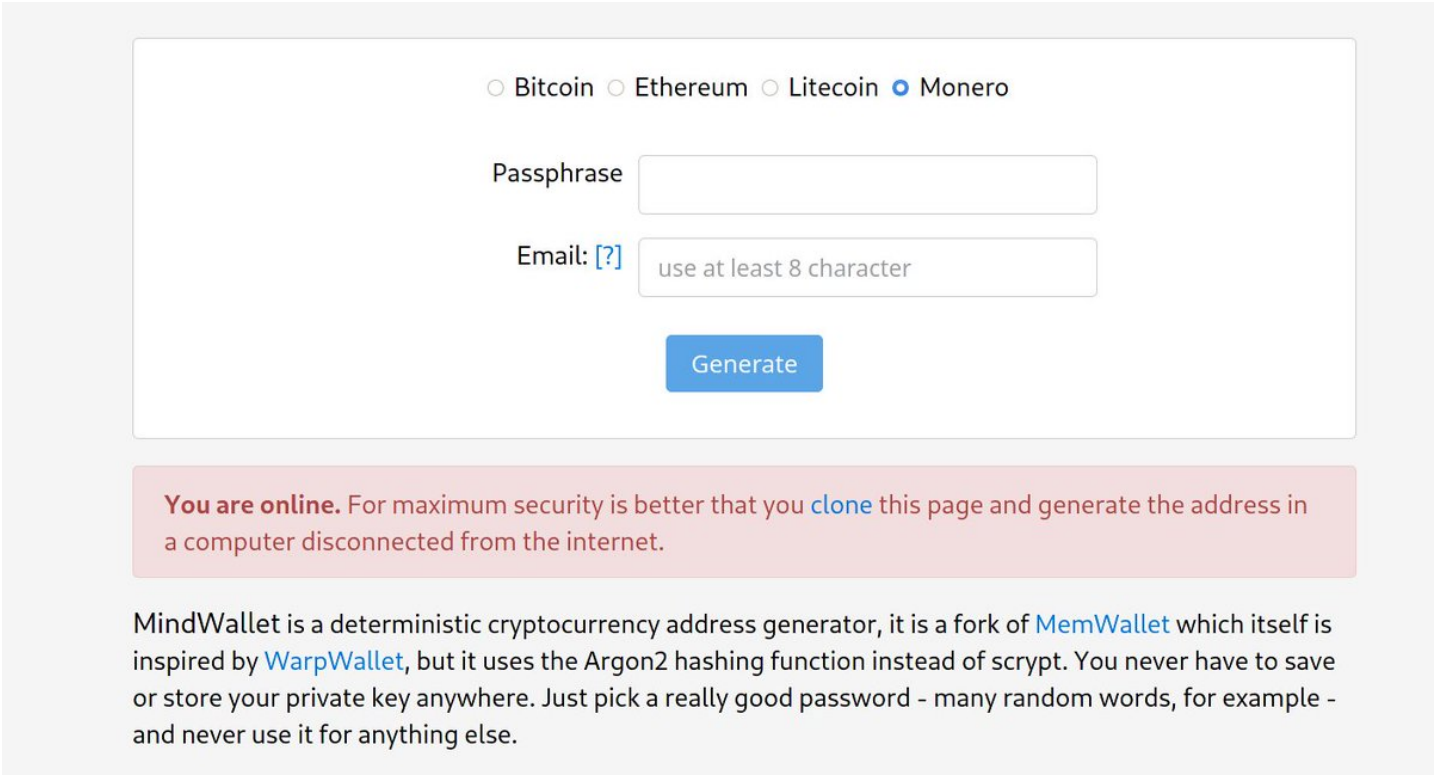
## 1/ Wrote an article here about an exchanger that allows you to swap several different cryptocurrencies for Monero without KYC or logins at all

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)..

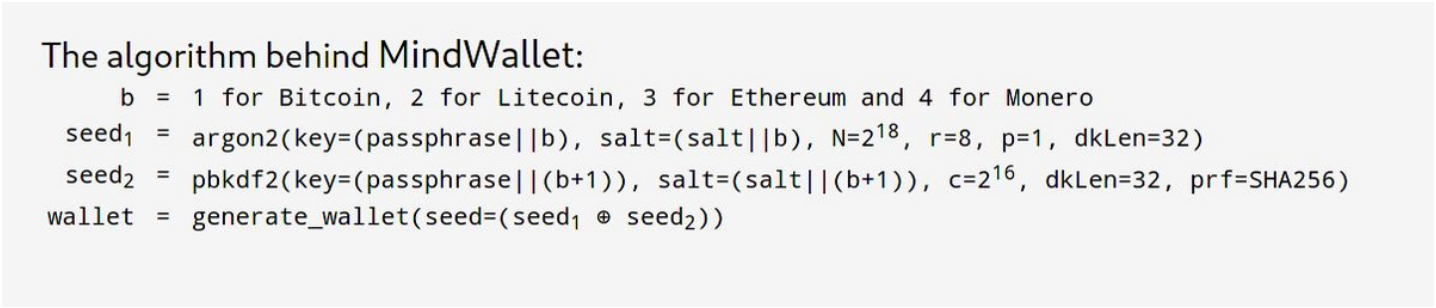
So we start off visiting the main website and set up a LTC:XMR conversion.




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)




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

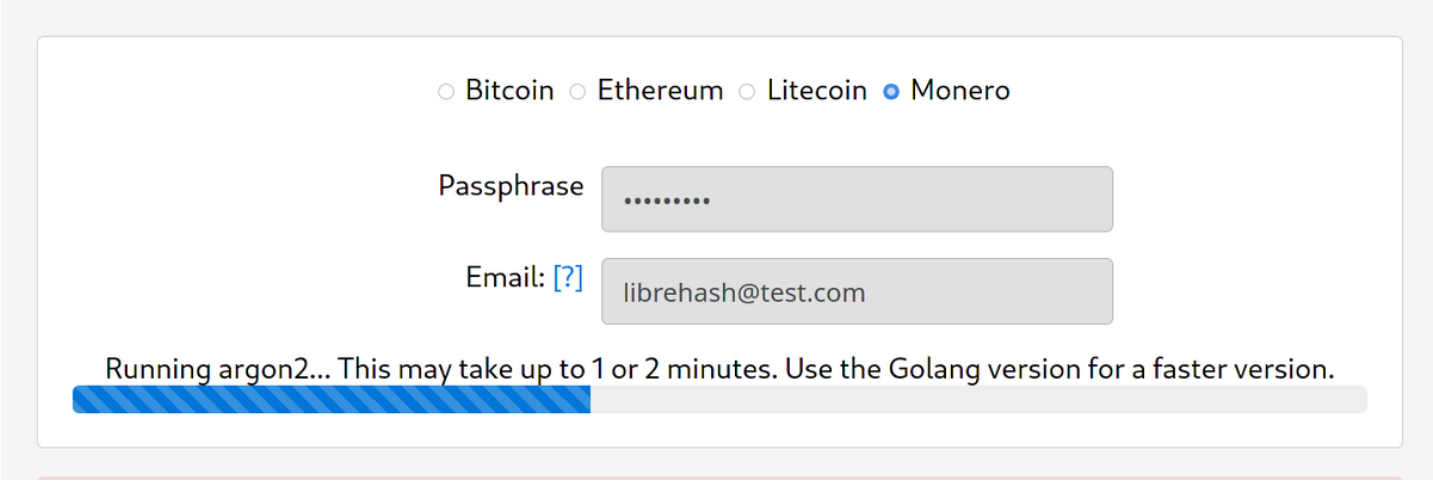



3b/ You can try it yourself. Password for this wallet = librehash

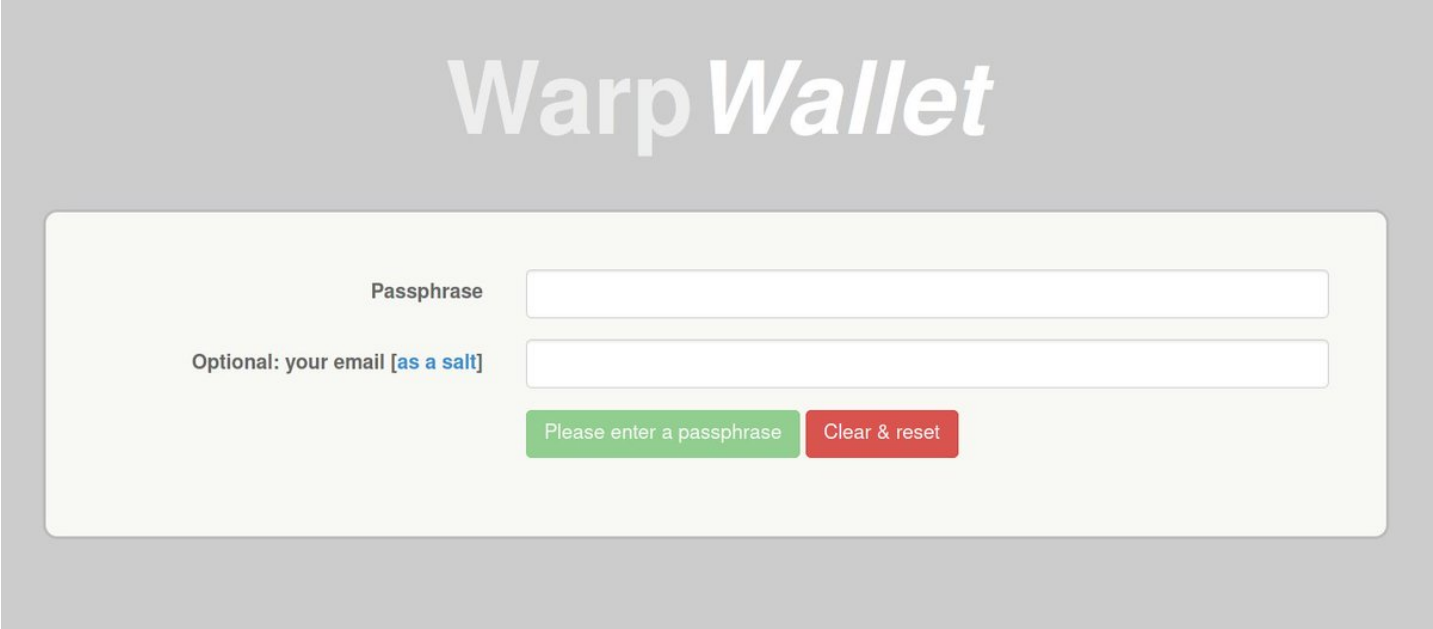
E-mail (salt) = librehash@test.com

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

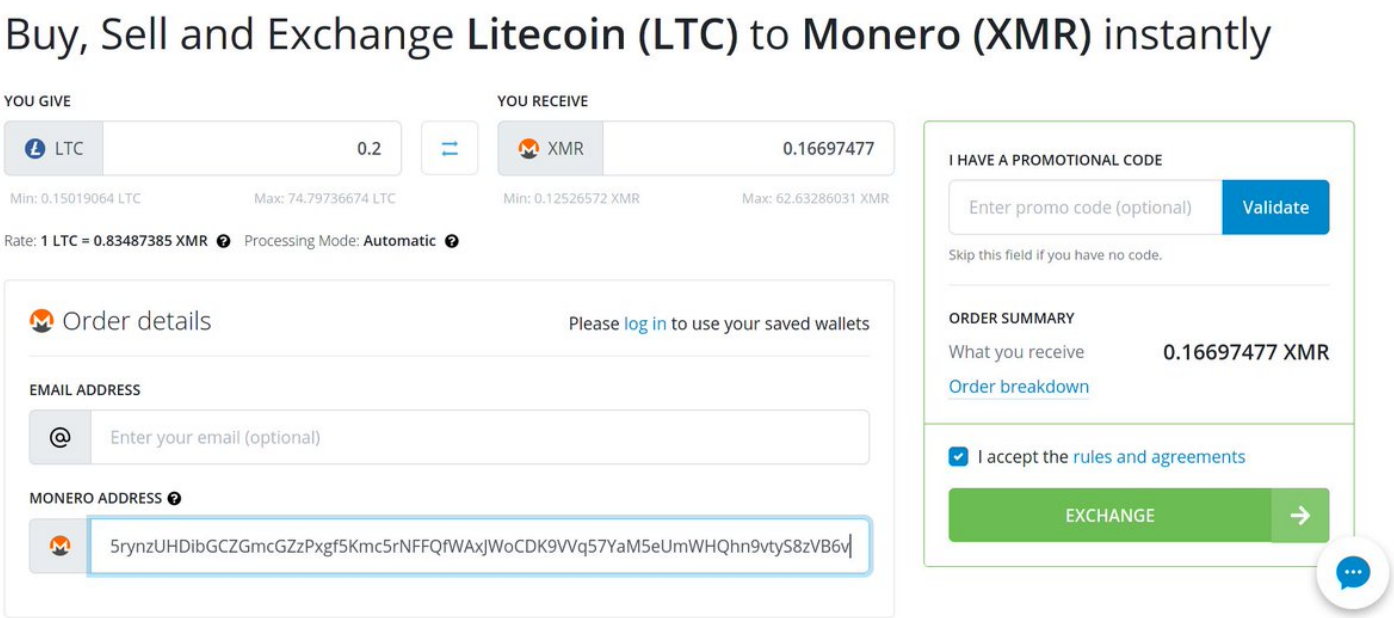
Benefit = in theory, you never need to have your private key stored anywhere, ever.



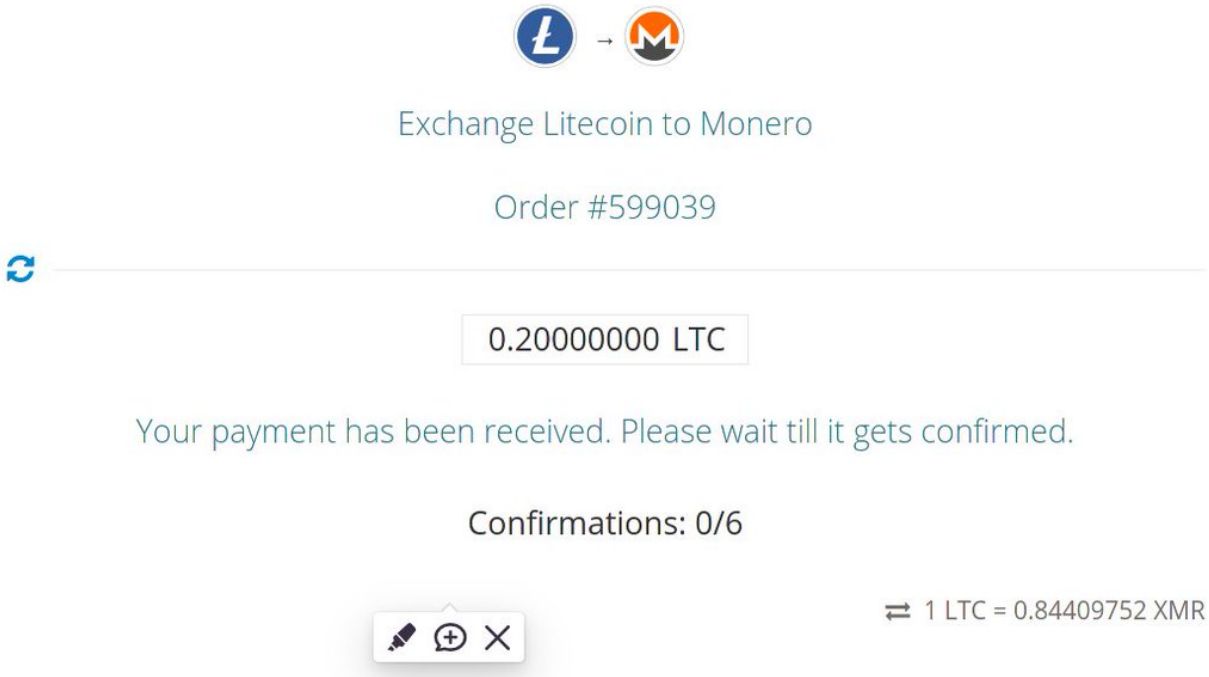

3c/ If you're wondering if this is legit or not, check out the @KeybaseIO implementation at https://t.co/sUJpIZEWAf ; as you can see, a simple 8-character alphanumeric password with 20+ btc in it has yet to be solved 3-4 years later (salt already given)




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



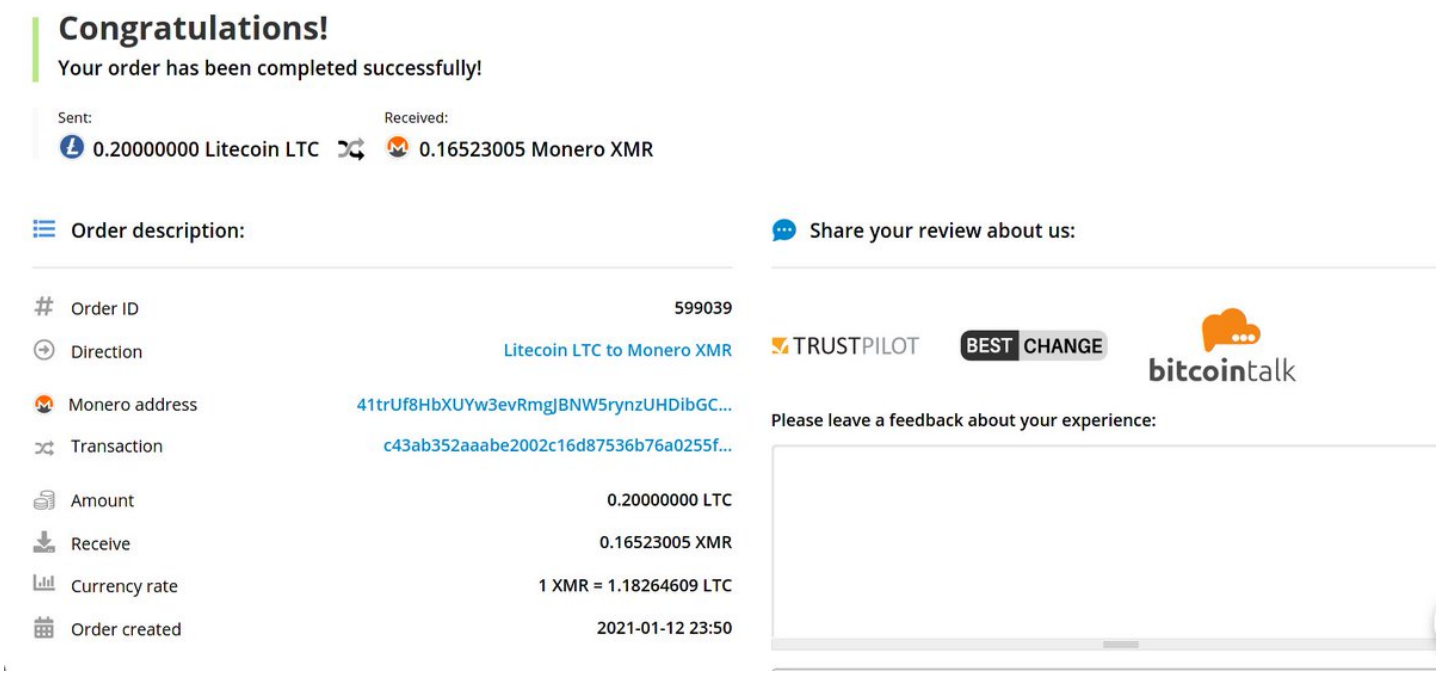

5/ Elected to send about $20 worth of $LTC at the time. Enough of an amount to where it felt like a legitimate test. The 6 confirmation wait screen is pretty standard. Cool.




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

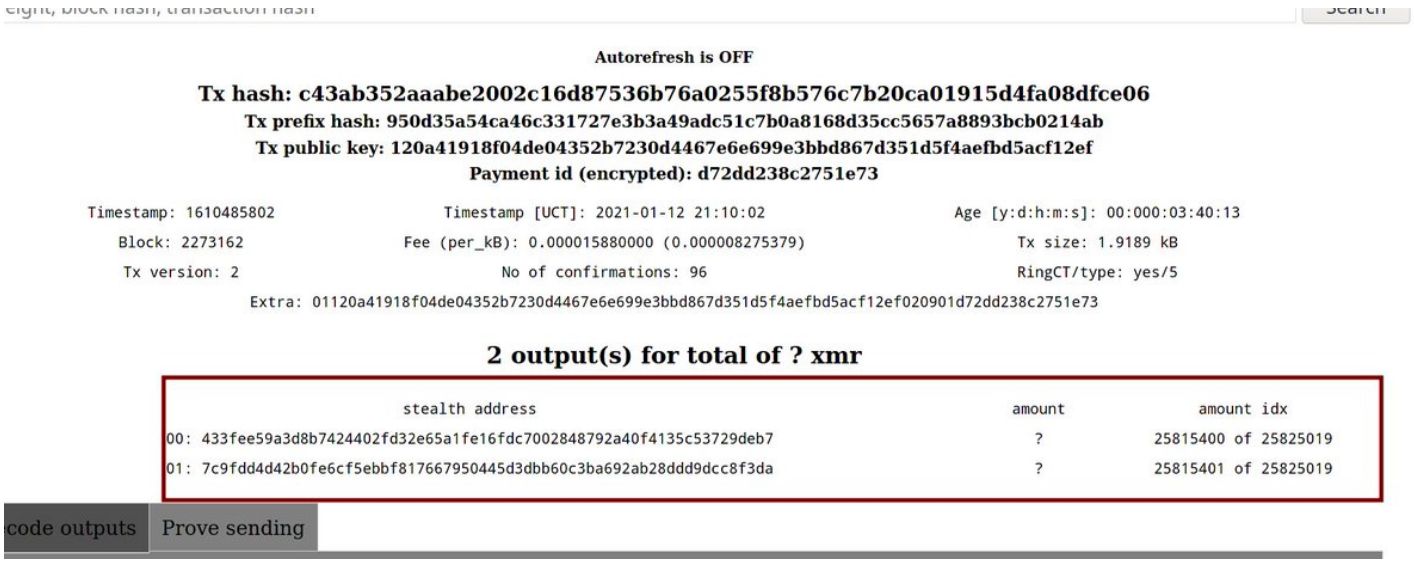
$XMR Monero is diff from other cryptocurrencies (obviously). We need to visit the transaction link.

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**

**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: 41trUf8HbXUYw3evRmgJBNW5rynzUHDibGCZGmcGZzPxgf5Kmc5rNFFQfWAxJWoCDK9VVq57YaM5eUmWHQhn9vtyS8zVB6v**

**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**