Basic Bitcoin Tech: Securing your Bitcoin

Host - SimplestBitcoinBook w/ PortlandHODL

- Overview -

- What Bitcoins Are
- The Private Key
- Custody (Ownership Types)
  - Custodial
  - Self-Custodial
- Types of security
  - Physical
  - Software
  - Social
  - Hardware (Cold)
  - Software (Hot)

What are Bitcoins?

1. bitcoins are Data

- bitcoins are the unit of account on the timechain.
- bitcoins are represented as the number of ‘satoshis’ in a UTXO (sent but not spent)
- UTXOs can be combined or split up.

2. Data storage

- bitcoins are stored across the Bitcoin network of nodes.
- This is not a problem because even though the bitcoins are stored across thousands of computers, those bitcoins all have a lock on them that is impossible to crack without the key.

3. Spending

- All bitcoins have a lock on them.
- This lock in most cases needs the private key.
- Without the key the bitcoins don’t move and can’t be spent, so be sure to secure the private key!

The timechain visualized - An analogy

- One can imagine an address as a safe deposit box on a wall of 2^256 safe deposit boxes.
- Each safe deposit box has a keyhole and a slit to deposit into (*if bitcoins were physical)*.
- Anyone can put bitcoins into an address (box) by passing them through the slit on the box, but the slit is so small it's impossible for anyone to take anything out of the box unless they have the key. **This is where privacy is involved.**
- The only way for someone to get into that box and spend the bitcoins (*transfer them to another box*) is to have the key to the safe deposit box. **This is where security is involved.**

THE PRIVATE KEY - DO NOT SHARE!

- The private key is the code/password/key needed to spend bitcoins from a specific address.
- This password is up to and should be 2^256 bits long.
- It is often translated to a set of 12 or 24 words, known as a s**eed phrase.**

ALWAYS SECURE THIS KEY AND NEVER SHARE IT WITH ANYONE EVER! WHOEVER HAS IT CAN SPEND YOUR BITCOIN

Visualized - If a bitcoin private key was a real key it would be roughly this long:

How many keys are there?

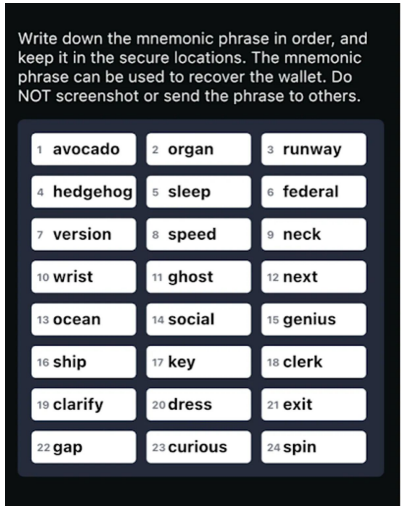
115,792,089,237,316,195,423,570,985,008,687,907,853,269,984,665,640,564,039,457,584,007,913,129,639,936 - So there are surely enough digital locks and keys for everyone for a very long time!

There are more possible bitcoin keys than atoms in the known universe.
(6×10^79 atoms)

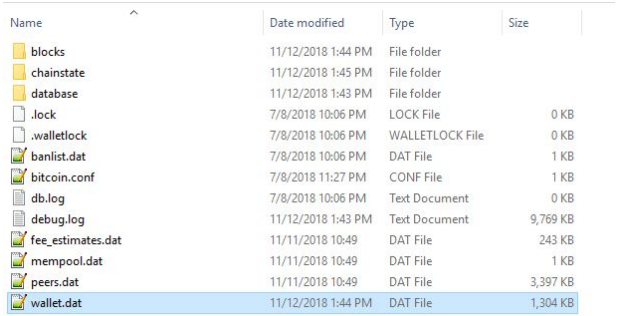
Types and Forms of Private Keys

More Common ← → **Less Common**

12/24 Word Seed Phrase



Wallet File (xpriv/HD)



WIF - Paper Wallet Private Key

Custody - Who owns the keys owns the coins

In Bitcoin possession is ten tenths of the law. You either have your keys or you don't.

SELF-CUSTODY - You have your keys, and thus you own your own bitcoin.

CUSTODIAL - The ‘bank’ or the exchange has the keys, and the bitcoin

Pros and Cons

Self-Custody

- Pros
  - Ultimate control of your money
  - No counterparty risk
- Cons
  - You lose the key you lose the bitcoins

Custodial

- Pros
  - You won't lose access because of a lost 'password'
- Cons
  - Complete loss of funds if insolvent
  - Custodian is hacked or or loses keys
  - Potential to be locked out of your funds due to regulatory capture

SECURITY

Hot vs Cold Storage (Signing Device)

HOT WALLET - Device is connected to the internet and/or is not air-gapped.

COLD STORAGE uses an air-gapped method to store and secure your seed phrase and sign transactions

- These apps are available on smartphones or desktop computers.
- They are best used as ‘spending’ wallets for smaller amounts of bitcoin.

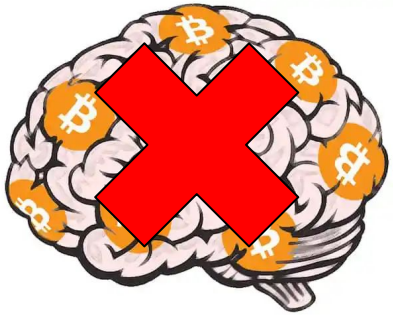
HOT WALLET APPS - Non-Custodial

Muun Wallet, Blue Wallet, Samourai Wallet (Android only), Sparrow Wallet, Green Wallet, Phoenix Wallet

*ALWAYS purchase your cold storage signing device new and direct from the manufacturer, to be certain it has not been tampered with.

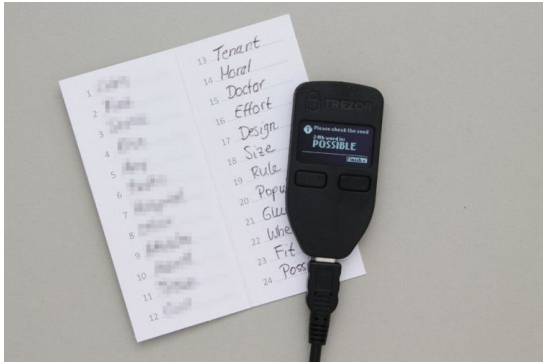
COLD STORAGE WALLETS

Cold Card, Trezor, Passport, Keystone, Blockstream Jade, Seed Signer, Bitbox,



Physical Security - It's all about the backup!

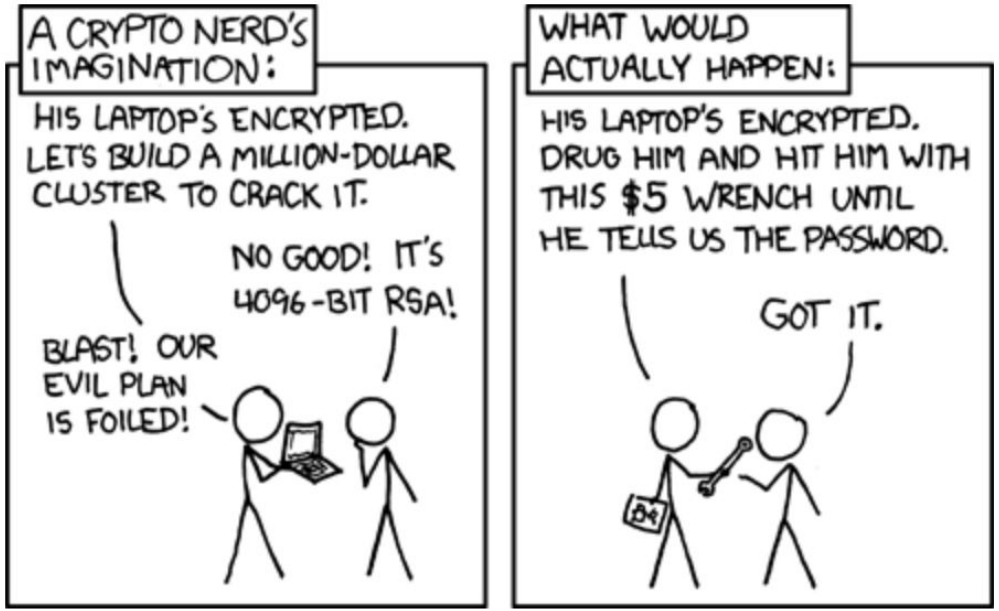
Paper Works - Sub Optimal



Washers are good - Must keep the order intact

Plates are excellent - Must be perfectly legible

Social - DONT TALK ABOUT THE SIZE OF YOUR BITCOIN STACK!



Thanks for listening!

1. Let us know what we can do better.
2. Anything incorrect? Leave a comment.