To do a long-term cold storage for cryptocurrencies.

Do this ceremony

First **generate**,
Then **test**,
Then **verify**,
Then **transport**,
Finally **store**.

Applying these rules

3 copies of data
2 different media
1 backup copy offsite

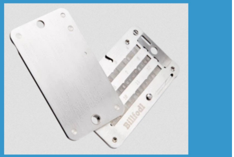
First, we **generate**

A 24 words **mnemonic code**
Split in **2 groups** of 12 words
Secured by **1 passphrase**

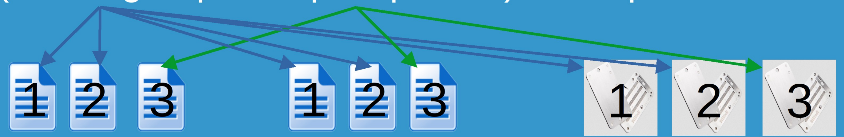
With a Ledger or a Trezor
Using :

- BIP39 mnemonic code
- BIP38 passphrase encryption
- BIP32 Extended public keys **XPUB**

And write **3** numbered copies of data of the **2 groups** of 12 words and the **1 passphrase**
Onto **2** different media
Notebooks + bitfodl



(2 wordgroups + 1 passphrase) x 3 copies = 9 media



Extended public keys **XPUB** can be written anywhere.
They do not need cold storage but remain **private** !

Then, we **test**

First,

Send a
minimal test amount
on an address
generated with your
XPUB

Never reuse an address, generate another one

Then,

On a **new or reset** Ledger or Trezor,
Enter the 24 words **mnemonic code**
from the **2 groups** of 12 words and unlock
the device with the **1 passphrase**

If you see your funds : it works.
If not : review the **generate** step

Then, we **verify**

On a **new** Ledger or Trezor

By entering the 24 words
mnemonic code
from the **2 groups** of 12 words
And unlock the device with the
1 passphrase

This is the *recovery procedure*

Repeat these operations with the **3** copies, notebooks and billfodl.

For each of the **3** copies,
Send a test amount
From the ledger/trezor
To an address on which
You can acknowledge reception.

On success, reset the ledger/trezor

Then, we **transport**

You have **3** numbered copies of data of the **2 groups** of 12 words and the **1 passphrase** Written on **2** different media

- Seal them with uniquely numbered seals
- Do not keep them in one place anymore.
- Do not make them traveling together.
- Do make them travel on different people and by different paths.

Finally, we **store**

Once arrived at the destination check that all the seals are in place

The 9 data backups must be stored in 9 different safes/vaults/jurisdictions.

Think about :

- natural disasters
- political risks.
- Funds seizure
- **1** backup copy offsite

passphrases must have :

- access control
- verification of identity.

Takeaway

NEVER transfer crypto to these accounts (Extended public keys XPUB) until:

- Backups have been verified
- The Ledger/Trezor has been formatted, reset or destroyed
- You have verified backups arrived sealed and are safely stored.

FAMILY !

- Should have access to the recovery of funds
- Must know the 3 storage locations of the passphrase
- Train them to understand and to be able to do the recovery procedure.