

# No Hardware Wallet, No Problem!

Riccardo Casatta

2024

# How do you make transactions?

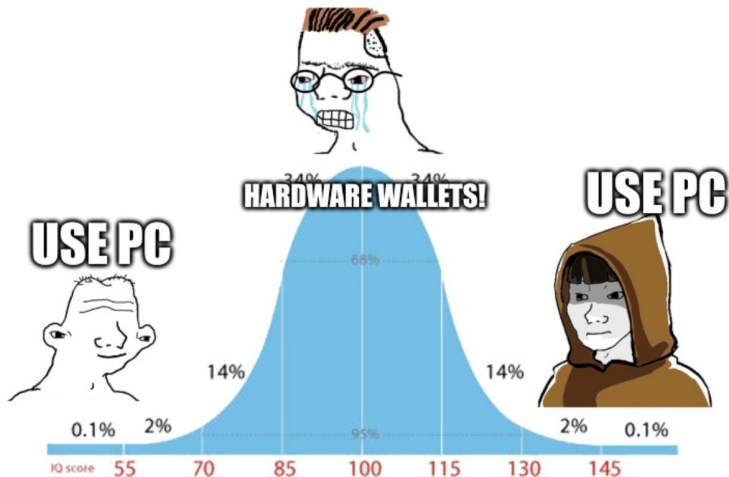


Figure 1: Gauss meme

## General purpose offline signing

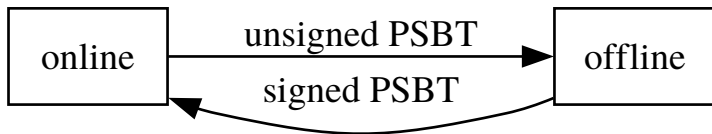


Figure 2: Online offline diagram

# The problem

How to transfer information?

- keyboard (glacier protocol<sup>1</sup>, rusty's protocol)
- cable (usb/ethernet)
- radio (blueetooth/wifi)
- memory (sd card)
- animated QR codes

---

<sup>1</sup><https://glacierprotocol.org/>



Figure 3: General purpose barcode scanner

# Comparison

Feature	HWW	GP offline signing
User experience	✓	
Review	✓	
Cost		✓
Accountability		✓
Centralization		✓
Flexibility		✓

# Tools

- firma2<sup>2</sup> - PSBT signer
  - derive
  - sign
  - addresses
- multiqr<sup>3</sup> - QR codes
- age<sup>4</sup> - Encryption tool
- bitcoin core<sup>5</sup> - Node/Wallet watch-only
- nix<sup>6</sup> - Packaging and more

---

<sup>2</sup><https://github.com/RCasatta/firma2>

<sup>3</sup><https://github.com/RCasatta/multiqr>

<sup>4</sup><https://github.com/FiloSottile/age>

<sup>5</sup><https://github.com/bitcoin/bitcoin>

<sup>6</sup><https://nixos.org>

# Nix - VM

## Run

```
git clone https://github.com/RCasatta/firma2  
cd firma2/vm  
nix run .#vm
```



# Nix - Physical

## Create image

```
git clone https://github.com/RCasatta/firma2  
cd firma2/build-raspi4-image  
nix build .#image.rpi4
```

## Burn on the key

```
sudo pv result/sd-image/nixos-sd-image-...img \  
-Yo /dev/disk/by-id/usb-MXT-USB_Storage_Device_-0:0
```

# Split mnemonic

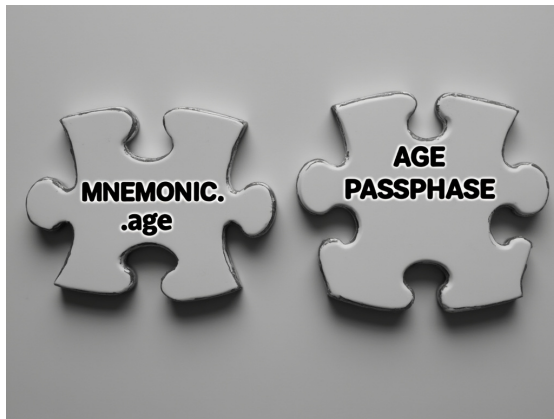


Figure 4: Split mnemonic

Out of scope how to generate the mnemonic, the coolest way is codex32<sup>7</sup>

---

<sup>7</sup><https://www.secretcodex32.com/>



Figure 5: MNEMONIC.age.base32

```
cat - | age -e -p -o MNEMONIC.age  
cat MNEMONIC.age | base32 | multiqr --bmp MNEMONIC.age.bmp
```



Figure 6: AGE\_PASSPHRASE

```
cat - | multiqr --bmp AGE_PASSPHRASE.bmp
```

# Create descriptors (offline)

## Offline

```
vim MNEMONIC.age # scan QR code
export NETWORK=signet

export DESCRIPTOR=$(cat MNEMONIC.age | age -d | derive | \
jq -r .singlesig.bip86_tr.multipath)
```

## Online

```
export IMPORT=$(cat MNEMONIC.age | age -d | derive | \
jq -r .singlesig.bip86_tr.import_descriptor)
```

## Bitcoin core (online)

```
alias bcli="bitcoin-cli --chain=signet -named"
```

```
bcli createwallet wallet_name=lugano blank=true \  
  disable_private_keys=true
```

```
bcli importdescriptors $IMPORT
```

```
bcli getnewaddress address_type=bech32m
```

```
bcli walletcreatefundedpsbt \  
inputs='[{"txid":"2e6425eb67549e638503d541fb1e1fb64f01a5d7dd75'  
outputs='[{"tb1pvsdpz8cucqz4tylmgtemn2qp6l9e8mptn36emnd6w6ntz8'  
| tee psbt_json
```



Figure 7: PSBT part 1

```
cat psbt_json | jq -r .psbt | multiqr --qr-version 10
```



Figure 8: PSBT part 2



## Sign (offline)

```
vim psbt # scan QR code  
cat MNEMONIC.age | age -d | sign psbt | tee result
```

# Broadcast (online)

```
vim tx # scan QR code  
bitcoin-cli sendrawtransaction $(cat tx)
```