

# SFYL Wallet

Satoshi Spritz

Valerio Vaccaro

March 25, 2021



# Table of contents

## 1 Introduzione

- Cos'è?
- Pagine

## 2 Demo

- Spected-desktop
- Bitcoin core

# Cos'è?

Proof-of-concept di un Hardware Wallet.

Caratteristiche:

- basato su pagine HTML servite via WIFI,
- firma esclusivamente PSBT,
- supporta solo bech32,
- supporta solo testnet,
- supporta multipli wallet.

# Cos'è?

## Caratteristiche:

- basato su ESP32,
- display eink,
- hardware disponibile per 23 dollari,
- firmware open source (MIT),
- contiene una copia del whitepaper di Satoshi.

# Cos'è?



# Cos'è?

## Riferimenti:

- Sito: [sfyl.info](https://sfyl.info),
- Gruppo telegram: <https://t.me/sfylwallet>,
- Sorgenti: <https://github.com/valerio-vaccaro/SFYL-Wallet>,

# Pagina Main



## SFYL Wallet

Loaded wallet: default (testnet)

Available wallets: default

### Status

Chip ID: 334fc4

MAC address: c44f337773d

Battery: 100

Heap: 193048


Support and informations on [sfyl.info](#) and on [telegram group](#).

Open source released under MIT license on [github.com/valerio-vaccaro/SFYL-Wallet](#).

Based on uBitcoin lib and tutorial [github.com/micro-bitcoin/uBitcoin](#).

[Bitcoin whitepaper](#)

# Pagina Settings

 **bitcoin**

---

**Network**  
Change network (testnet)  

Testnet

**Mnemonic**  
Change mnemonic  

start tree vicious crash drum meat turn price exile weasel slam hurt

You'll never share your mnemonic with anyone else.

**Passphrase**  
Change passphrase  

Enter a passphrase

**Derivation path**  
Change derivation path  

m/84'/1'/0'

Set new parameters

**Load a wallet from flash**  
Wallet name  

default

  
Password  

Enter a password

Load

**Save a wallet to flash**  
Wallet name  

secret

  
Password  

Enter a password

Save

**Delete a wallet from flash**  
Wallet name  

default

Delete



# Pagina XPub



## Extended pubkey



[7oe3cdf2/84h/0h]xpub62t6tT6XEr8QF65Aa5ctgerQxvrmM76cgu2WJ/Fboop60a52z2pvmRMh4cDwP4TeeDcdNDL0xkxLcRc5cp8BD6zsp866THWk

## Import in Bitcoin Core

Core XPub:

tpub0DmNUCUuFWJcup8FJebhGTH96Cj3Ez3db62StxzD99jyPMGRxe1e9vKJcmvUNk3umT75GN5P5e80DEuA7Damy3UROYQc6A  
Hnnppe

- Create a new wallet [Optional] `bitcoin-cli -testnet createwallet "watcher" true`
- Import descriptors `bitcoin-cli -testnet -rpcwallet="watcher" importmulti [{"desc": "wpub([7e3cdf2/84h/0h]xpub62t6tT6XEr8QF65Aa5ctgerQxvrmM76cgu2WJ/Fboop60a52z2pvmRMh4cDwP4TeeDcdNDL0xkxLcRc5cp8BD6zsp866THWk)", "internal": false, "range": [8, 1000], "timestamp": "now", "keypool": true, "watchonly": true, "desc": "wpub([7e3cdf2/84h/0h]xpub62t6tT6XEr8QF65Aa5ctgerQxvrmM76cgu2WJ/Fboop60a52z2pvmRMh4cDwP4TeeDcdNDL0xkxLcRc5cp8BD6zsp866THWk)", "internal": true, "range": [8, 1000], "timestamp": "now", "keypool": true, "watchonly": true}]}`

Open source released under MIT license (<https://github.com/valerio-vaccaro/SFYL-Wallet>).

Based on ubitcoin lib and tutorial (<https://github.com/micr0-bitcoin/ubitcoin>).


[Bitcoin whitepaper](#)

# Pagina Address

 **bitcoin**


---

**Address**  
Derive a new address.



tb1q8wfbq3yk4yuf2zv4h394jyvmg0ayp34mqga

# Pagina PSBT



### Sign PSBT

- Create a new PSBT `bitcoin-cli -testnet --rpcwallet="watchman" walletcreatefundedpsbt "[1]" "[["ADDRESS":AMOUNT]]" 0 ["includeWatching":true]" true`. Change ADDRESS with destination address and AMOUNT with the amount you want send in Bitcoin.
- Use SFYL Wallet and sign your PSBT.

Unsigned PSBT

Enter a psbt

Sign PSBT

- Combine PSBT `bitcoin-cli -testnet combinepsbt "[*]"`
- Finalize PSBT `bitcoin-cli -testnet finalizepsbt "..."`
- Broadcast transaction `bitcoin-cli -testnet sendrawtransaction "..."`

### Sign message

Sign a message.

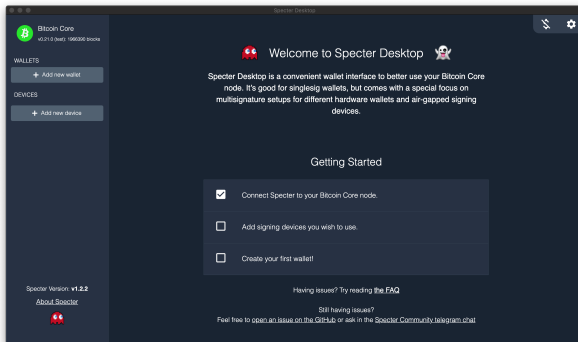
Message

Buy Bitcoin!

mY847T0/0/0

Sign message

# Spected-desktop



# Bitcoin core

I comandi utili sono riportati nelle stesse pagine HTML mostrate da SFYL.