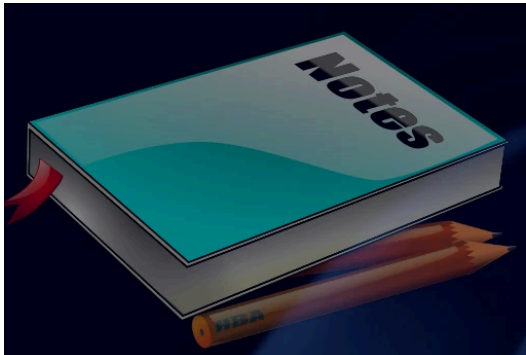



# PREPARARSI AL RECUPERO DEL WALLET

Piacenza ≤ SATOSHI SPRITZ ≤ Parma - 21 febbraio 2026

# Agenda

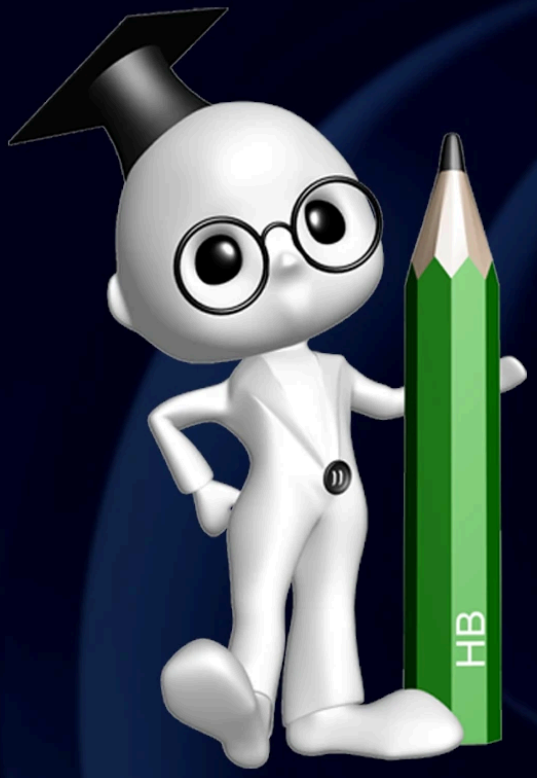
- Breve esercitazione pratica:
  - *ripristino wallet dalla mnemonica*
- Come funziona il wallet
- Elementi essenziali
- Strumenti

# meme

Come va il recupero del wallet?

Io:


Piacenza ≤ SATOSHI SPRITZ ≤ Parma - 21 febbraio 2026




# UN MOMENTO!

... ho il backup della recovery phrase, cosa può andar storto?

Piacenza ≤ SATOSHI SPRITZ ≤ Parma - 21 febbraio 2026

# Ripristino di un wallet

| | |
|---|---|
| 1 emotion | 7 ostrich |
| 2 bring | 8 knock |
| 3 charge | 9 correct |
| 4 arctic | 10 journey |
| 5 knock | 11 hybrid |
| 6 double | 12 resource |

Piacenza ≤ SATOSHI SPRITZ ≤ Parma - 21 febbraio 2026

# Ripristino di un wallet

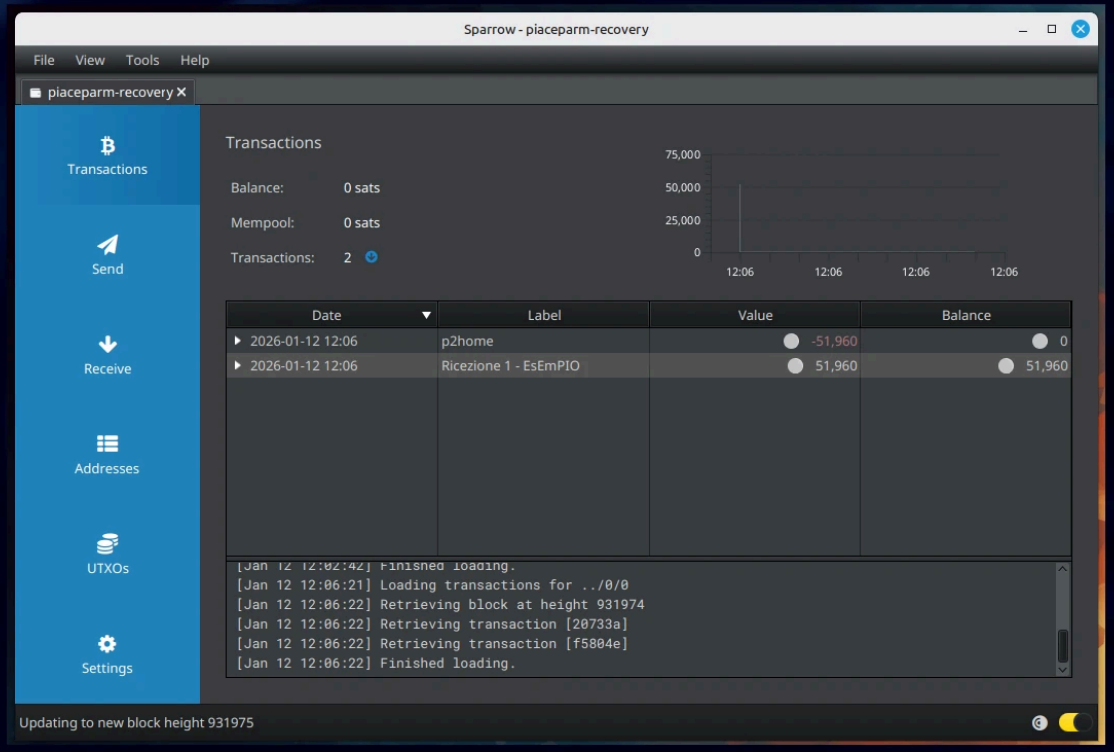
bc1qmptm8zdpkuldx2get
dey2ngf36902a3wl6zs2t

bc1qrn08evw65yz42xc6s
3maw2e4l70qceva0lrngs

bc1qyec3us0pf9xudadgn
6ve9mpsrnzlqajry2mwvs

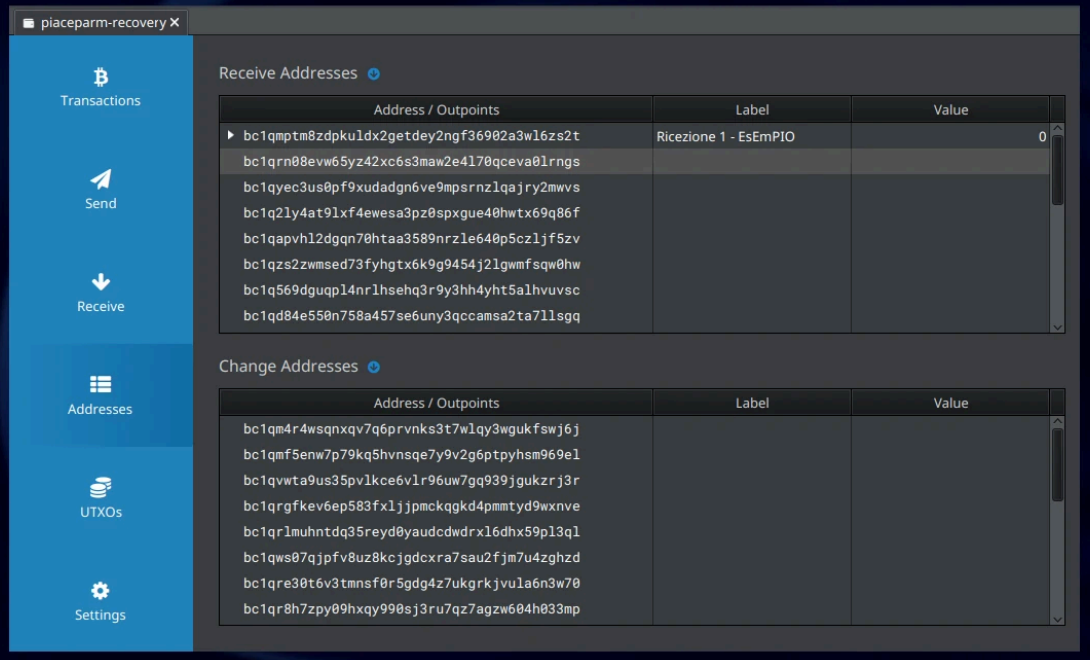
Piacenza ≤ SATOSHI SPRITZ ≤Parma - 21 febbraio 2026

# Ripristino di un wallet



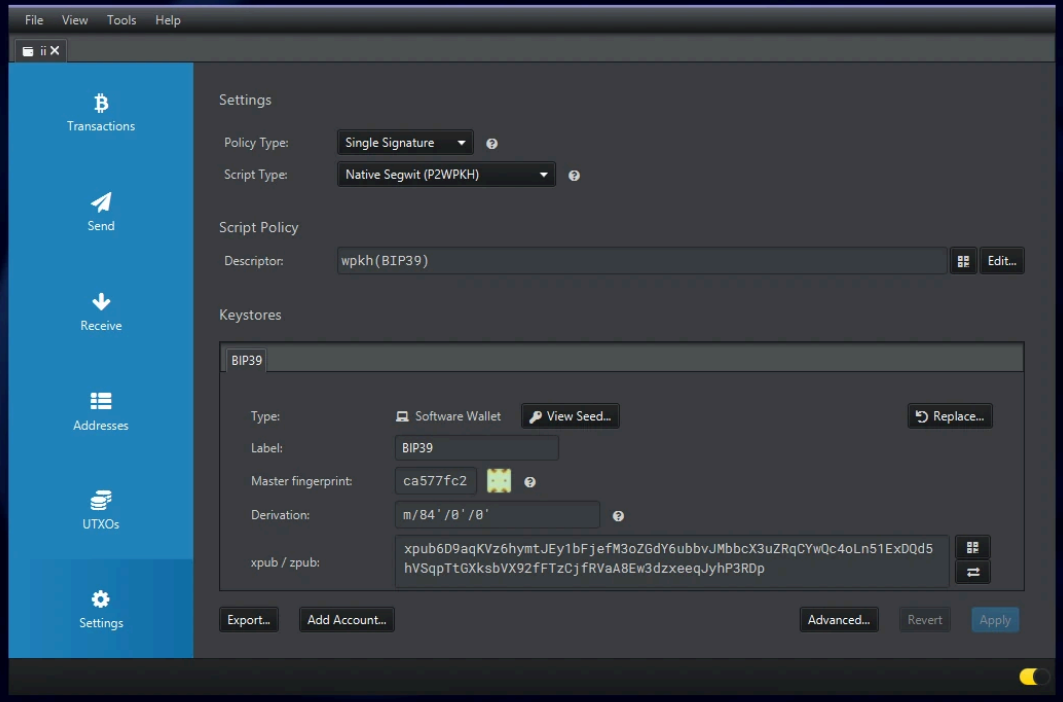

Piacenza ≤ SATOSHI SPRITZ ≤ Parma - 21 febbraio 2026

# Ripristino di un wallet




Piacenza ≤ SATOSHI SPRITZ ≤ Parma - 21 febbraio 2026

# Ripristino di un wallet




Piacenza ≤ SATOSHI SPRITZ ≤ Parma - 21 febbraio 2026

# Funzionamento interno del wallet

Master fingerprint

ca577fc2

Piacenza ≤ SATOSHI SPRITZ ≤Parma - 21 febbraio 2026

# Generazione del wallet

(Mnemonica)

emotion bring charge
arctic knock double
ostrich knock correct
journey hybrid resource

(Seed)

(Master Keys)

(Purpose: scelta script)

(Network)

Wallet account

(Indirizzi)

Piacenza ≤ SATOSHI SPRITZ ≤ Parma - 21 febbraio 2026

# Derivation Path

(Seed)

m (Master Keys)

m/84' (Purpose: scelta script)

m/84'/0' (Network)

m/84'/0'/0' Wallet account

m/84'/0'/0'/0

m/84'/0'/0'/1

(Indirizzi)

Piacenza ≤ SATOSHI SPRITZ ≤ Parma - 21 febbraio 2026

# Wallet HD

## Il "segreto" risiede nel backup del wallet gerarchico-deterministico

(Mnemonica)

emotion bring charge
arctic knock double
ostrich knock correct
journey hybrid resource

→  (Seed)

La gerarchia è stabilita dal derivation path

Piacenza ≤ SATOSHI SPRITZ ≤ Parma - 21 febbraio 2026

# Wallet HD

# Cosa significa esattamente DETERMINISTICO?

Piacenza ≤ SATOSHI SPRITZ ≤ Parma - 21 febbraio 2026

# Crittografia

(Mnemonica)

emotion bring charge
arctic knock double
ostrich knock correct
journey hybrid resource

(Seed)

Questo "semplice" passaggio è solo un esempio della crittografia applicata nel protocollo Bitcoin

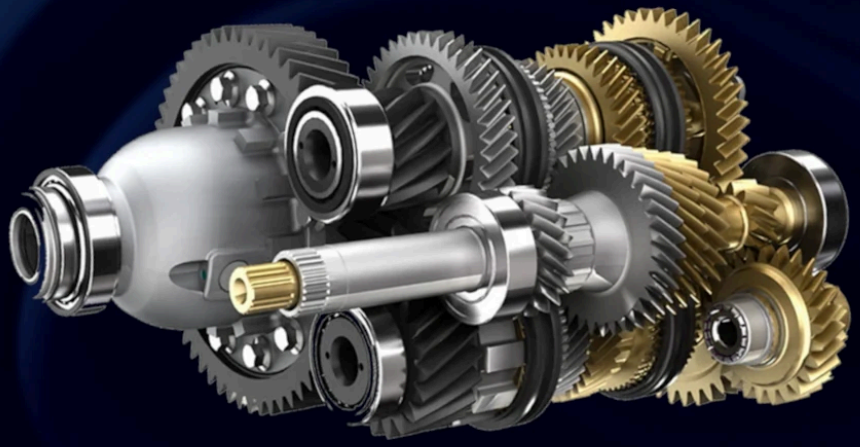
Algoritmi: PBKDF2 + HMAC 512

Piacenza ≤ SATOSHI SPRITZ ≤ Parma - 21 febbraio 2026

# Crittografia

(Mnemonica)

emotion bring charge
arctic knock double
ostrich knock correct
journey hybrid resource



(Seed)

Testo in chiaro

(INPUT)

## Algoritmo

Testo cifrato

(OUTPUT)

Piacenza ≤ SATOSHI SPRITZ ≤ Parma - 21 febbraio 2026

# Crittografia

In crittografia, **deterministico** significa:

- a partire dallo stesso **INPUT**
- applicando gli stessi **algoritmi**
- si ottengono sempre gli stessi **OUTPUT**

**A patto di replicare fedelmente le condizioni**

Nel caso della generazione di un wallet: **lo stesso derivation path**

# Backup essenziale

## Wallet singlesig

- Mnemonica
- Derivation Path
- Master Fingerprint

Piacenza ≤ SATOSHI SPRITZ ≤ Parma - 21 febbraio 2026

# Backup essenziale

## Wallet singlesig

- standard di derivazione - sapere cosa si sta facendo e sapere qual è il risultato che si deve ottenere
- imparare a ripristinare il wallet su più software



Piacenza ≤ SATOSHI SPRITZ ≤ Parma - 21 febbraio 2026

# Backup essenziale

## Wallet singlesig

- fare il backup del file del wallet
  - mantiene le descrizioni associate a ciascun UTXO
  - conservare su supporti cifrati (luks, veracrypt)

**Implica il backup della password con cui il software cifra il file del wallet (e tenerla separata)**

# Backup essenziale

## Wallet multisig

Nuovo standard che si sta diffondendo tra diversi software

DESCRIPTOR che esporta la configurazione del wallet

Piacenza ≤ SATOSHI SPRITZ ≤ Parma - 21 febbraio 2026

# Descriptor

```
# Receive and change descriptor (BIP389):
wsh(sortedmulti(2,[00000000/48h/0h/0h/2h]xpub6BgH84e9idEukj256KR
CQ8ZgZiQdNrbH6mvz1FgVTxeJ8ZFjn6LUNtFsMKWxEo4hQgdB47wtBXWgEPWb6WD
VwAirvjiP8jbcoLAZCbTuBV6/<0;1>/*,[e84ccbeb/48h/0h/0h/2h]xpub6FJQ
9zaj6ycVmHHePqjX5XmvmcmP4NSsXuvB4m8BZ69E4AzoF1jaC9nwMpsDUidxpA6u
3E7gj5PSq1Q3izho7PtEXRdXt4ZRBMn7hww5ymg/<0;1>/*))#97ednkq3

# Receive descriptor (Bitcoin Core):
wsh(sortedmulti(2,[00000000/48h/0h/0h/2h]xpub6BgH84e9idEukj256KR
CQ8ZgZiQdNrbH6mvz1FgVTxeJ8ZFjn6LUNtFsMKWxEo4hQgdB47wtBXWgEPWb6WD
VwAirvjiP8jbcoLAZCbTuBV6/0/*,[e84ccbeb/48h/0h/0h/2h]xpub6FJQ9zaj
6ycVmHHePqjX5XmvmcmP4NSsXuvB4m8BZ69E4AzoF1jaC9nwMpsDUidxpA6u3E7g
j5PSq1Q3izho7PtEXRdXt4ZRBMn7hww5ymg/0/*))#ef7elezj

# Change descriptor (Bitcoin Core):
wsh(sortedmulti(2,[e84ccbeb/48h/0h/0h/2h]xpub6FJQ9zaj6ycVmHHePqj
X5XmvmcmP4NSsXuvB4m8BZ69E4AzoF1jaC9nwMpsDUidxpA6u3E7gj5PSq1Q3izh
o7PtEXRdXt4ZRBMn7hww5ymg/1/*,[00000000/48h/0h/0h/2h]xpub6BgH84e9
idEukj256KRCQ8ZgZiQdNrbH6mvz1FgVTxeJ8ZFjn6LUNtFsMKWxEo4hQgdB47wt
BXWgEPWb6WDVwAirvjiP8jbcoLAZCbTuBV6/1/*))#njh76c7h
```

Piacenza ≤ SATOSHI SPRITZ ≤ Parma - 21 febbraio 2026

# Descriptor

```
# Receive and change descriptor (BIP389):
wsh(sortedmulti(2,[00000000/48h/0h/0h/2h]xp
ub6BgH84e9idEukj256KRCQ8ZgZiQdNrbH6mvz1FgVT
xeJ8ZFjn6LUNtFsMKWxEo4hQgdB47wtBXWgEPWb6WDV
wAirvjiP8jbcoLAZCbTuBV6/<0;1>/*,[e84ccbeb/
48h/0h/0h/2h]xpub6FJQ9zaj6ycVmHHePqjX5Xmvmc
mP4NSsXuvB4m8BZ69E4AzoF1jaC9nwMpsDUidxpA6u3
E7gj5PSq1Q3izho7PtEXRdXt4ZRBMn7hww5ymg/<0;1
>/*))#97ednkq3
```

# Descriptor

Stringa testuale che descrive completamente come verranno spesi i fondi legati al wallet

Elimina la necessità di memorizzare script complessi

Standardizzato (BIP380) e portabile

# Vantaggi del Descriptor

**Portabilità**: stesso descriptor funziona con diversi wallet

**Sicurezza**: non è necessario esportare le chiavi private

**Flessibilità**: supporta script complessi e timelock

**Standardizzazione**: compatibilità tra diversi software

# Strumenti di backup

## Cosa ci serve per un buon backup?

- Backup fisico (carta, metallo)
- Accessori adatti (punzoni, blockmit, satoshi corner)

# Strumenti di backup


Piacenza ≤ SATOSHI SPRITZ ≤ Parma - 21 febbraio 2026

# Strumenti di backup

## Cosa non ci serve per un buon backup?

- mettere l'entropia su un computer
- fotografare la mnemonica
- salvare nel cloud
- condividere il segreto

soprattutto con noi del Satoshi Spritz

Piacenza ≤ SATOSHI SPRITZ ≤ Parma - 21 febbraio 2026

# DOMANDE?

May this presentation inspire you to become more self-sovereign!

Piacenza ≤ SATOSHI SPRITZ ≤ Parma - 21 febbraio 2026


SATOSHI
SPRITZ
• 💻 Federazione di gruppi locali di bitcoiner
• 🎓 Eventi gratuiti e privacy oriented
• 🤖 BITCOIN ONLY
• 📖 Orientato all'apprendimento della self-sovereign
• 🔧 Satoshi Spritz Connect online settimanale
https://satoshispritz.it
https://t.me/SatoshiSpritzConnect


OFFICINE BITCOIN
Comunità Italiana di Bitcoiners, totalmente gratuita
BITCOIN ONLY
Focus su educazione e sviluppo di progetti
progetti:
Sviluppo nodi Bitcoin
Uso di Hardware Wallet
Filosofia open source
Installazione di Debian
Mnemoniche & Dadi
... e molto altro
https://officinebitcoin.it


Notes
PREPARARSI AL RECUPERO DEL
WALLET
Piacenza ≤ SATOSHI SPRITZ ≤Parma - 21 febbraio 2026


Notes
Thank you!
Piacenza ≤ SATOSHI SPRITZ ≤ Parma - 21 febbraio 2026