



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

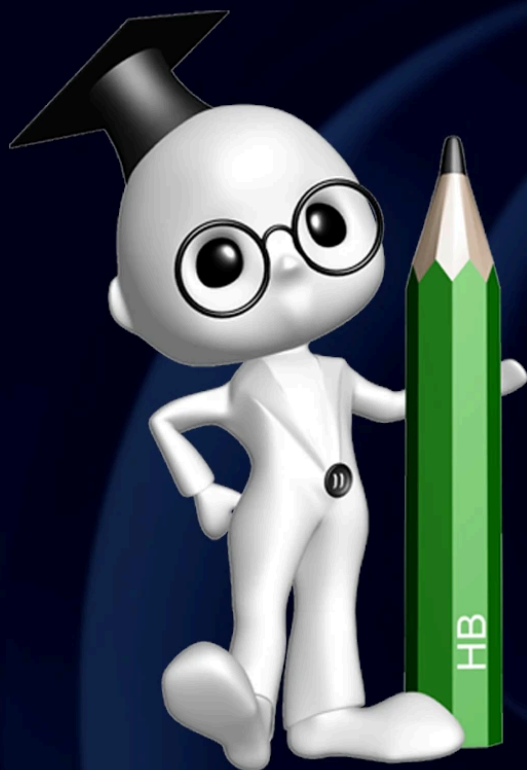
mememe

Come va il recupero
del wallet?

Io:



Piacenza ≤  ≤ Parma - 21 febbraio 2026



UN MOMENTO!

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

Piacenza ≤  ≤ 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 |

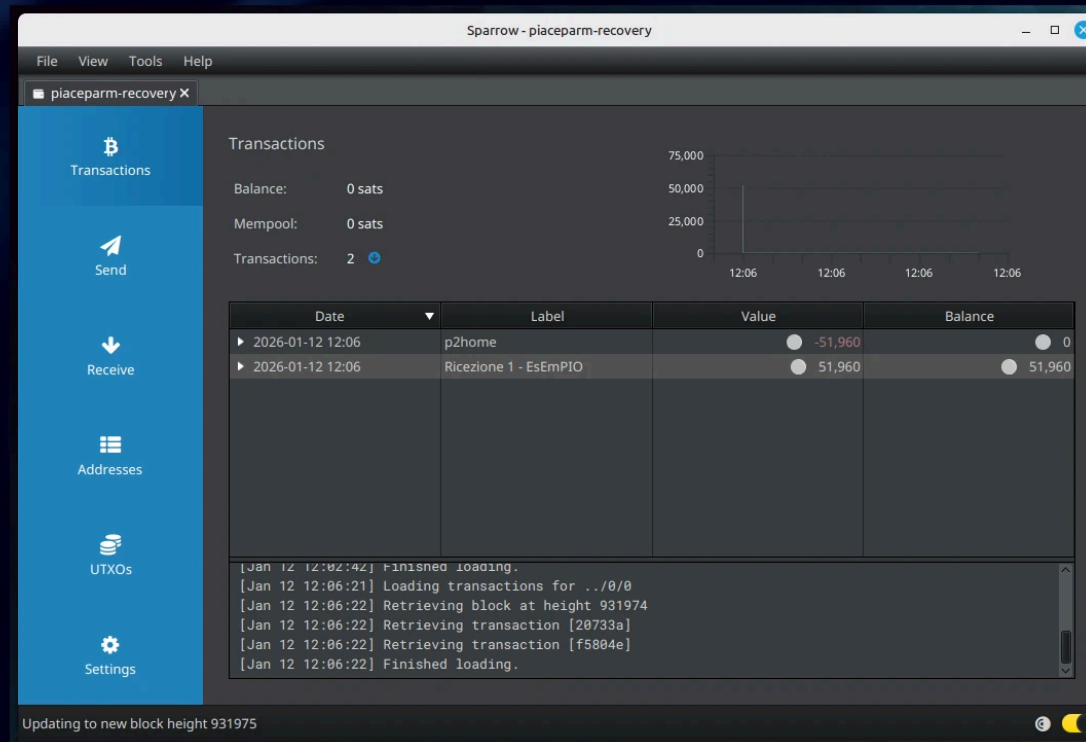
Ripristino di un wallet

bc1qmptm8zdpku1dx2get
dey2ngf36902a3w16zs2t

bc1qrn08evw65yz42xc6s
3maw2e4170qceva01rngs

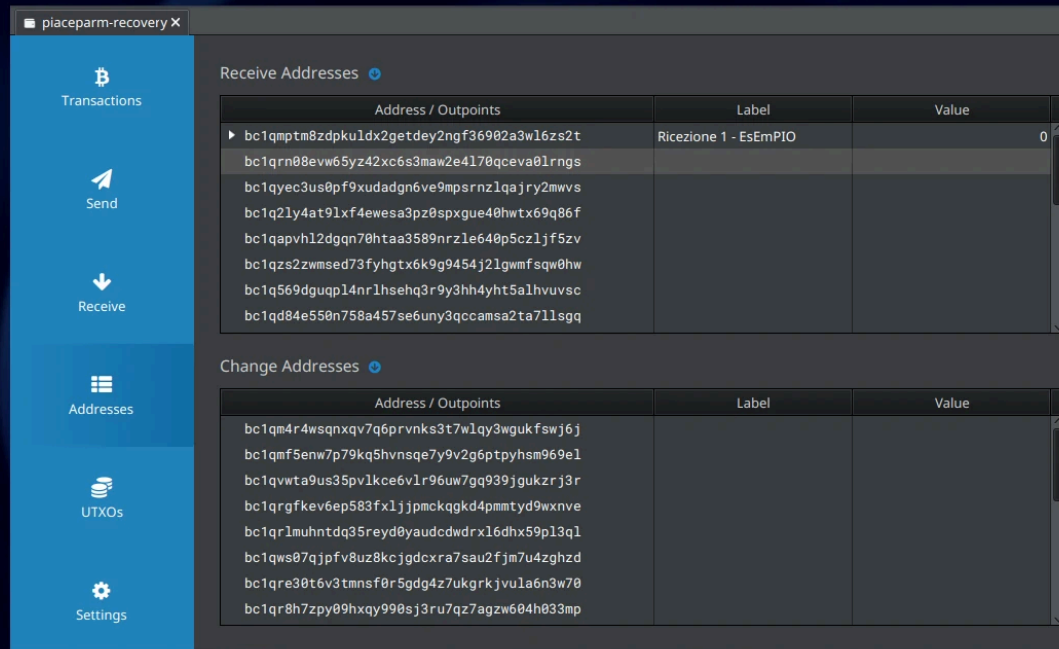
bc1qyec3us0pf9xudadgn
6ve9mps rnz1qaj ry2mwvs

Ripristino di un wallet



Piacenza ≤  ≤ Parma - 21 febbraio 2026

Ripristino di un wallet



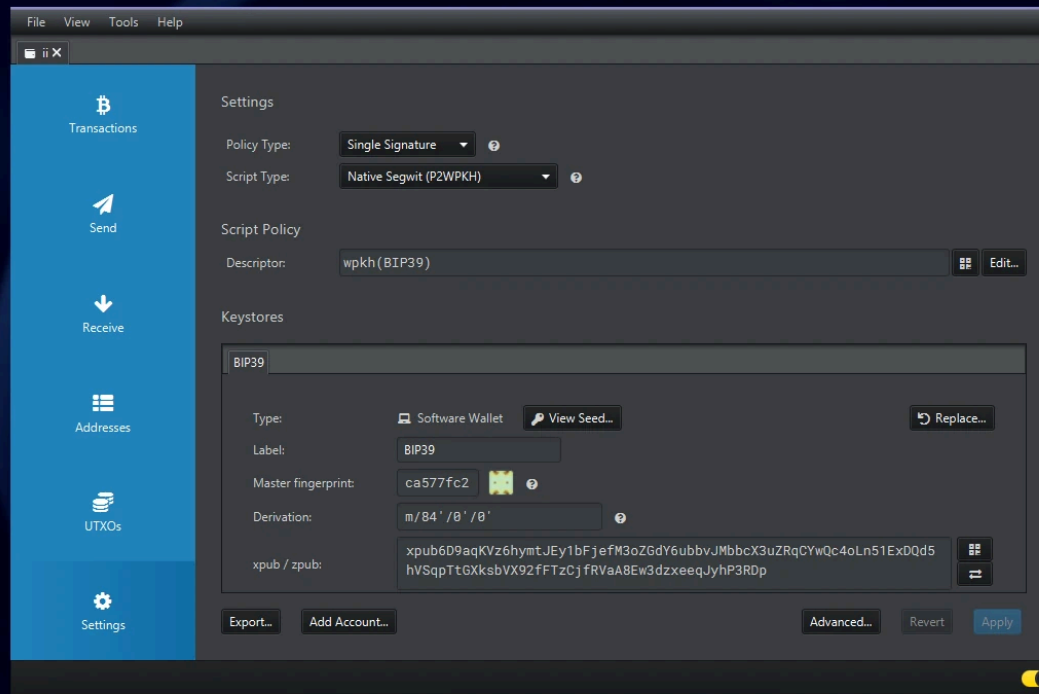
The screenshot shows a Bitcoin wallet recovery interface with a sidebar on the left and two main panels. The sidebar contains icons for Transactions, Send, Receive, Addresses, UTXOs, and Settings. The 'Receive Addresses' panel displays a table with columns for Address / Outpoints, Label, and Value. The 'Change Addresses' panel displays a similar table.

Address / Outpoints	Label	Value
bc1qmptm8zdpkuldx2getdey2ngf36902a3w16zs2t	Ricezione 1 - EsEmPIO	0
bc1qrn08evw65yz42xc6s3maw2e4170qceva01rnsgs		
bc1qyec3us0pf9xudadgn6ve9mpsrnz1qajry2mwws		
bc1q21y4at91xf4ewesa3pz0spxgue40hwtx69q86f		
bc1qapvh12dgn70htaa3589nrz1e640p5cz1jf5zv		
bc1qzs2zwmse73fyhgtx6k9g9454j21gwmfsgw0hw		
bc1q569dguqp14nr1hsehq3r9y3hh4yht5a1hvuvsc		
bc1qd84e550n758a457se6uny3qccamsa2ta71lsgq		

Address / Outpoints	Label	Value
bc1qm4r4wsqnxv7q6prvnks3t7w1qy3wgukfswj6j		
bc1qmF5enw7p79kq5hvnsqe7y9v2g6ptpyhsm969e1		
bc1qvwta9us35pv1kce6v1r96uw7gq939jgukzrj3r		
bc1qrgfkev6ep583fx1jpmckqgkd4pmmtyd9wxnve		
bc1qr1muhntdq35reyd0yauddwdrx16dhx59p13q1		
bc1qws07qjpfv8uz8kcjgdcxra7sau2fjm7u4zghzd		
bc1qre30t6v3tmnsf0r5gdg4z7ukgrkjvu1a6n3w70		
bc1qr8h7zpy09hxqy990sj3ru7qz7agzw604h833mp		

Piacenza ≤  ≤ Parma - 21 febbraio 2026

Ripristino di un wallet



Piacenza ≤  ≤ Parma - 21 febbraio 2026

Funzionamento interno del wallet



Master fingerprint

ca577fc2

Piacenza ≤  ≤ Parma - 21 febbraio 2026

Generazione del wallet

(Mnemonic)

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



→ (Seed)



(Master Keys)



(Purpose: scelta script)



(Network)



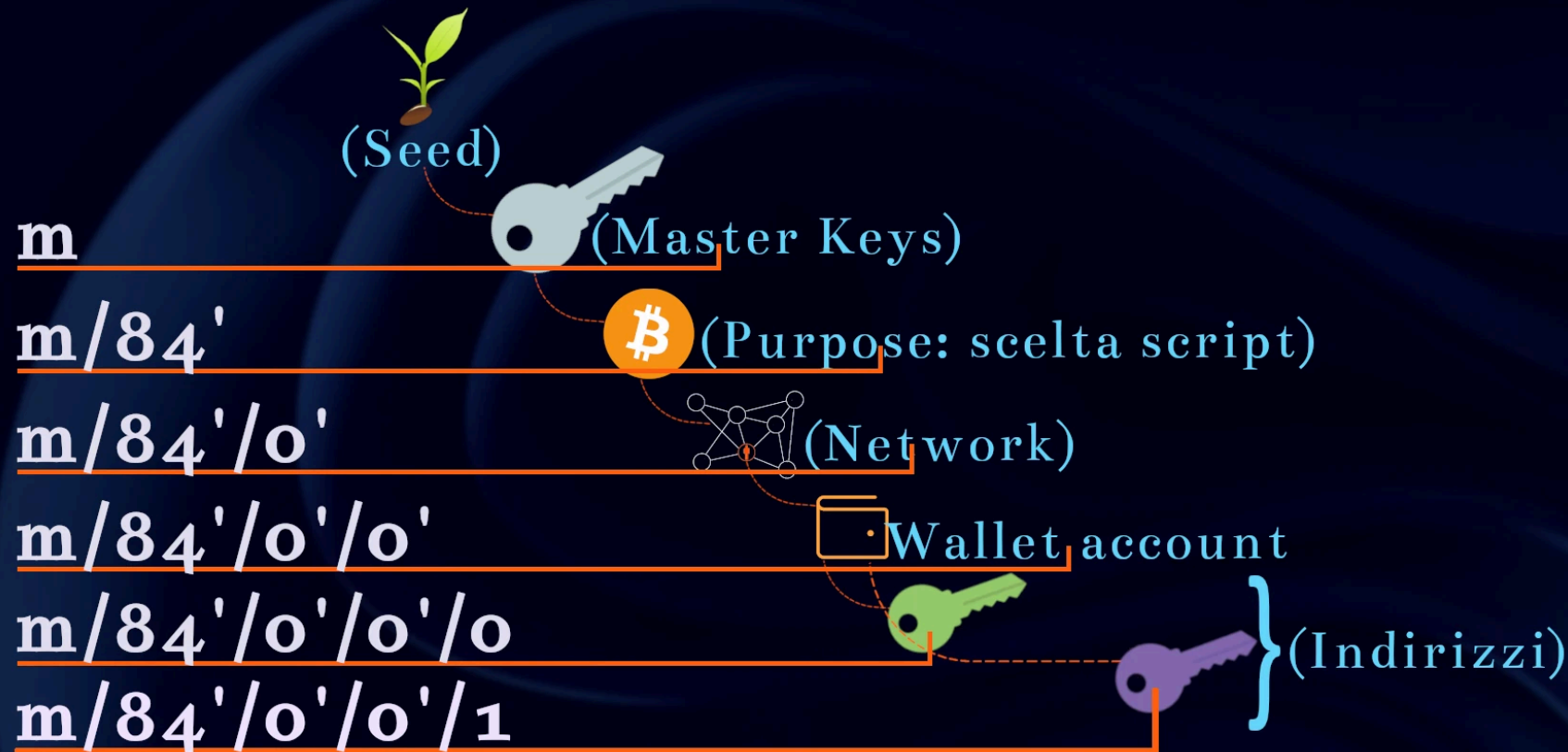
Wallet account



(Indirizzi)

Piacenza ≤  **SATOSHI
SPRITZ** ≤ Parma - 21 febbraio 2026

Derivation Path



Wallet HD

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

(Mnemonic)

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



La gerarchia è
stabilita dal
derivation path

Wallet HD


Cosa significa
esattamente

DETERMINISTICO?

Piacenza ≤  ≤ Parma - 21 febbraio 2026

Crittografia

(Mnemonic) → (Seed)
emotion bring charge
arctic knock double
ostrich knock correct
journey hybrid resource



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

(Mnemonic)

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



(Seed)

Testo in chiaro
(INPUT)

Algoritmo

Testo cifrato
(OUTPUT)

Piacenza ≤  ≤ 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**

Piacenza ≤  ≤ Parma - 21 febbraio 2026

Backup essenziale



Wallet singlesig

- Mnemonica
- Derivation Path
- Master Fingerprint

Piacenza ≤  ≤ 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 ≤  ≤ 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 ≤  ≤ Parma - 21 febbraio 2026

Descriptor

Receive and change descriptor (BIP389):

```
wsh(sortedmulti(2,[00000000/48h/0h/0h/2h]xpub6BgH84e9idEukj256KRCQ8ZgZiQdNrbH6mvz1FgVTxeJ8ZFjn6LUNtFsMKWxEo4hQgdB47wtBXWgEPWb6WDVwAirvjiP8jbc0LAZCbTuBV6/<0;1>/*, [e84ccbeb/48h/0h/0h/2h]xpub6FJQ9zaj6ycVmHHePqjX5XmvmcmP4NSsXuvB4m8BZ69E4AzoF1jaC9nwMpsDUidxpA6u3E7gj5PSq1Q3izho7PtEXRdXt4ZRBMn7hww5ymg/<0;1>/*))#97ednkq3
```

Receive descriptor (Bitcoin Core):

```
wsh(sortedmulti(2,[00000000/48h/0h/0h/2h]xpub6BgH84e9idEukj256KRCQ8ZgZiQdNrbH6mvz1FgVTxeJ8ZFjn6LUNtFsMKWxEo4hQgdB47wtBXWgEPWb6WDVwAirvjiP8jbc0LAZCbTuBV6/0/*, [e84ccbeb/48h/0h/0h/2h]xpub6FJQ9zaj6ycVmHHePqjX5XmvmcmP4NSsXuvB4m8BZ69E4AzoF1jaC9nwMpsDUidxpA6u3E7gj5PSq1Q3izho7PtEXRdXt4ZRBMn7hww5ymg/0/*))#ef7elezj
```

Change descriptor (Bitcoin Core):

```
wsh(sortedmulti(2,[e84ccbeb/48h/0h/0h/2h]xpub6FJQ9zaj6ycVmHHePqjX5XmvmcmP4NSsXuvB4m8BZ69E4AzoF1jaC9nwMpsDUidxpA6u3E7gj5PSq1Q3izho7PtEXRdXt4ZRBMn7hww5ymg/1/*, [00000000/48h/0h/0h/2h]xpub6BgH84e9idEukj256KRCQ8ZgZiQdNrbH6mvz1FgVTxeJ8ZFjn6LUNtFsMKWxEo4hQgdB47wtBXWgEPWb6WDVwAirvjiP8jbc0LAZCbTuBV6/1/*))#njh76c7h
```

Piacenza ≤  ≤ Parma - 21 febbraio 2026

Descriptor

```
# Receive and change descriptor (BIP389):  
wsh(sortedmulti(2, [00000000/48h/0h/0h/2h]xp  
ub6BgH84e9idEukj256KRCQ8ZgZiQdNrbH6mvz1FgVT  
xeJ8ZFjn6LUNtFsMKWxEo4hQgdB47wtBXWgEPWb6WDV  
wAirvjiP8jbc0LAZCbTuBV6/<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 ≤  ≤ Parma - 21 febbraio 2026

DOMANDE?



Piacenza ≤  ≤ Parma - 21 febbraio 2026



QUESTA PRESENTAZIONE È DISTRIBUITA SOTTO LA
LICENZA CREATIVE COMMONS CC BY-SA 4.0.



LE IMMAGINI UTILIZZATE SONO PROPRIETÀ
DEI RISPETTIVI AUTORI E SONO INCLUSE
SOLO A FINI EDUCATIVI E ILLUSTRATIVI.








MAY THIS PRESENTATION INSPIRE YOU
TO BECOME MORE SELF-SOVEREIGN!

Piacenza ≤  ≤ 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>



PREPARARSI AL RECUPERO DEL WALLET

Piacenza ≤ **SATOSHI
SPRITZ** ≤ Parma - 21 febbraio 2026



Thank you!

Piacenza ≤ SATOSHI SPRITZ ≤ Parma - 21 febbraio 2026