

CREAZIONE DI UN WALLET OFF LINE E DEL SUO WALLET DI SOLA VISUALIZZAZIONE

Questo "sistema" costituito da un wallet che sta perennemente offline ed il suo corrispondente wallet di sola visualizzazione, che invece sta perennemente online, è un metodo utile ed economico per creare la propria "cassaforte2".

Il wallet OFFLINE servirà per tenere la chiave privata (derivante dalla mnemonica) al riparo da furti provenienti dalla rete (esfiltrazione), mentre quello ONLINE ci consentirà di ricevere fondi e vedere cronologia e saldo (ma NON di spendere).

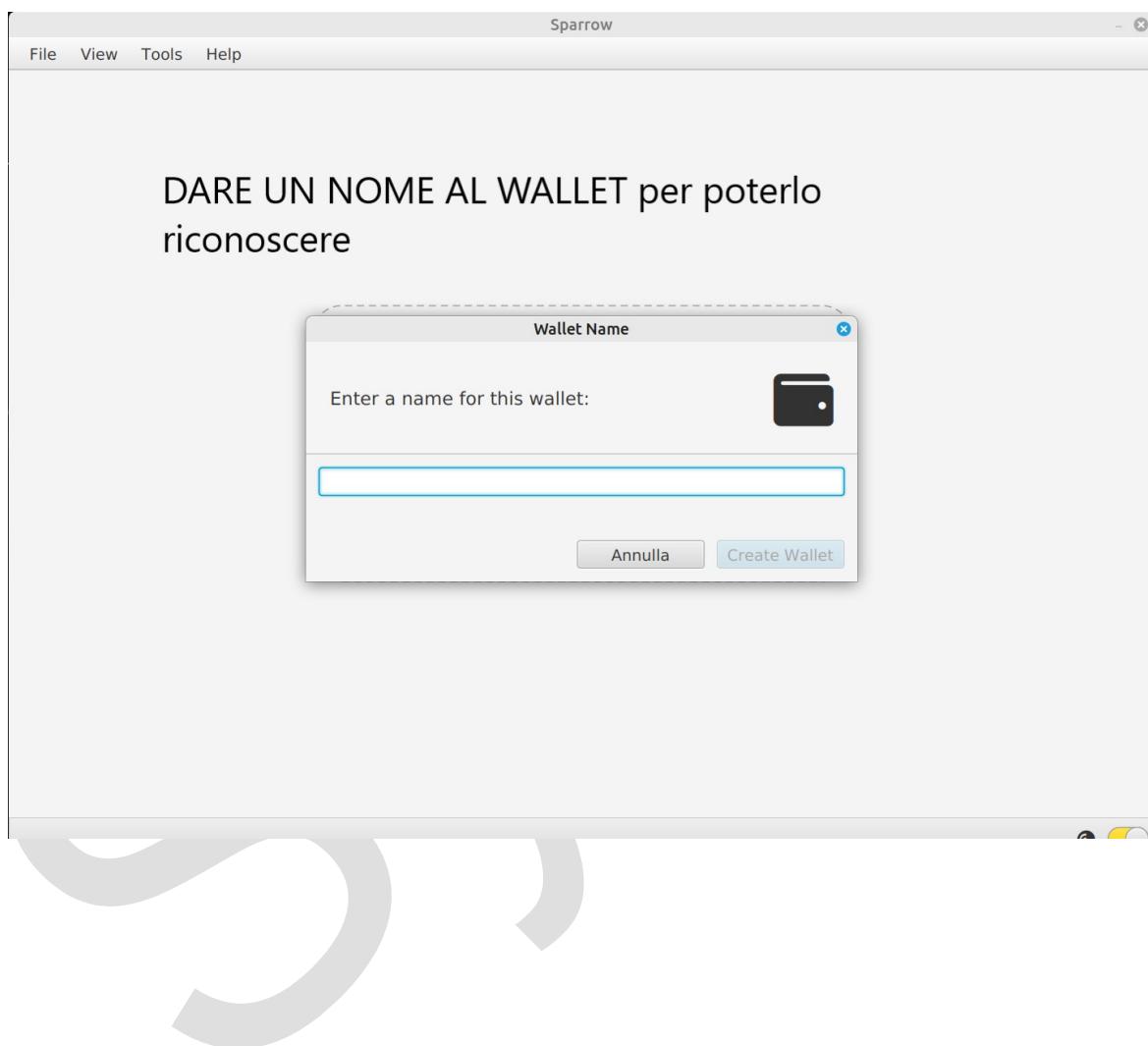
In questo modo anche se qualcuno dovesse vedere il wallet di sola visualizzazione, non potrebbe rubare i nostri fondi, per il cui spostamento è necessario dimostrarne la proprietà, cosa fattibile solo possedendo la chiave privata.

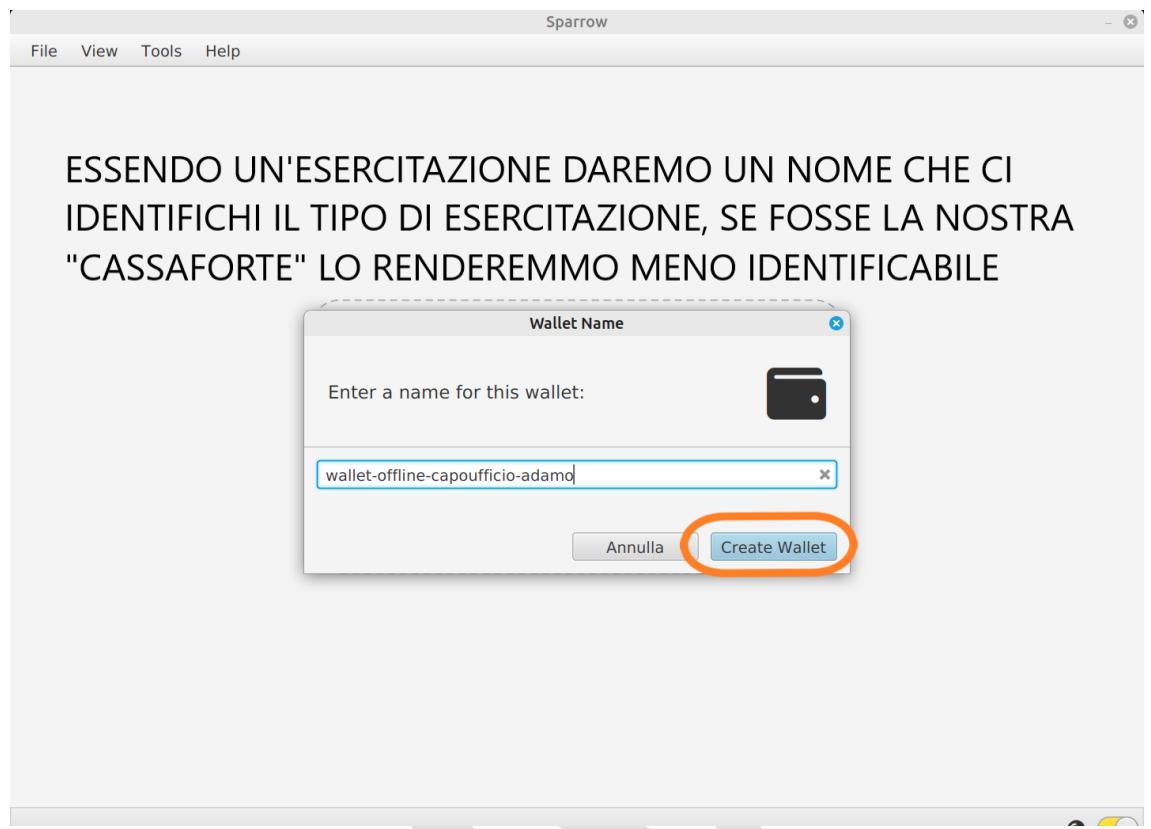
E' un po' come se avessimo un capo-ufficio ed una segretaria. La segretaria può vedere i saldi dei conti correnti aziendali, può comunicare l'IBAN quando riuchiesto e può anche compilare i moduli bancari per fare bonifici a dipendenti e fornitori, ma dovrà rivolgersi al capo-ufficio per firmare i moduli ed autorizzare il trasferimento dei fondi stessi.

Finché non si deve spendere, il capo-ufficio non viene interpellato.

CREAZIONE WALLET OFFLINE

(capo-ufficio /
Adamo)

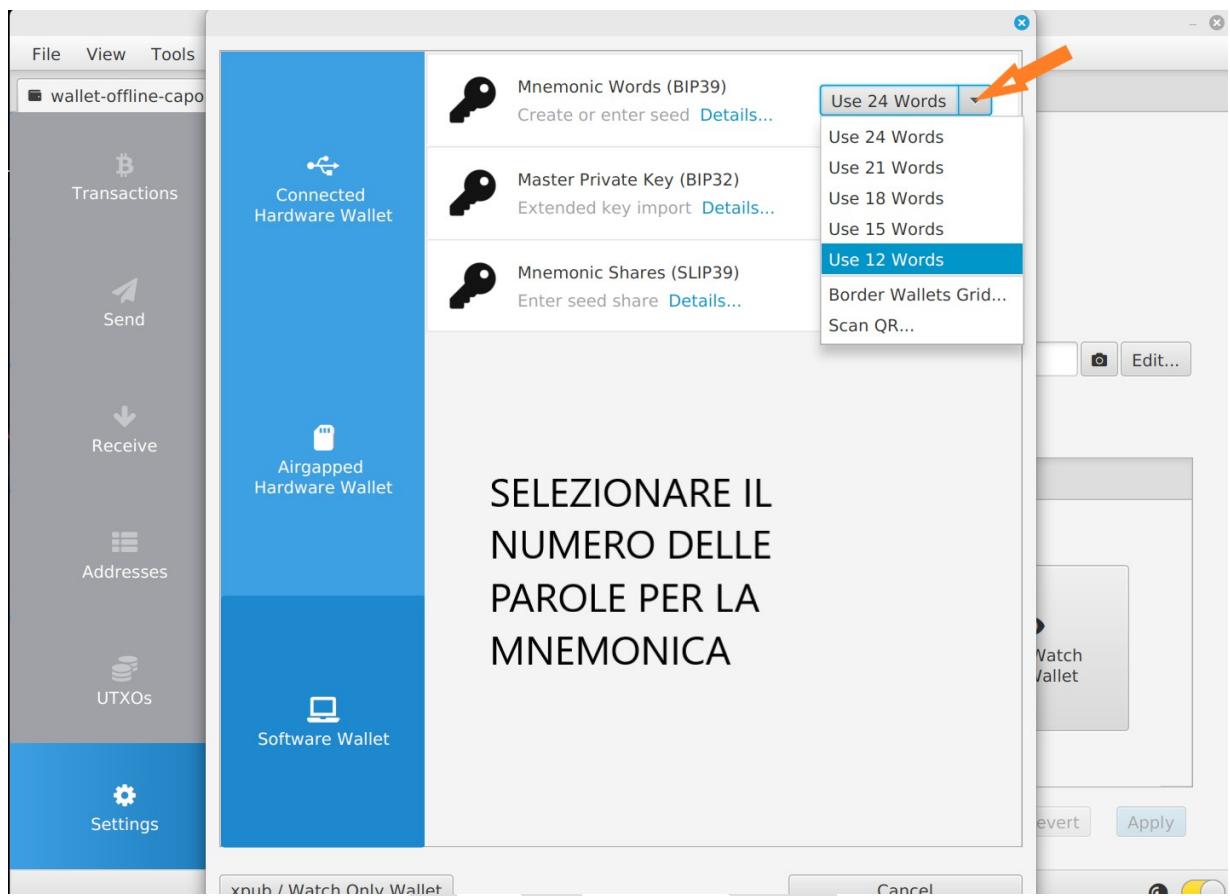




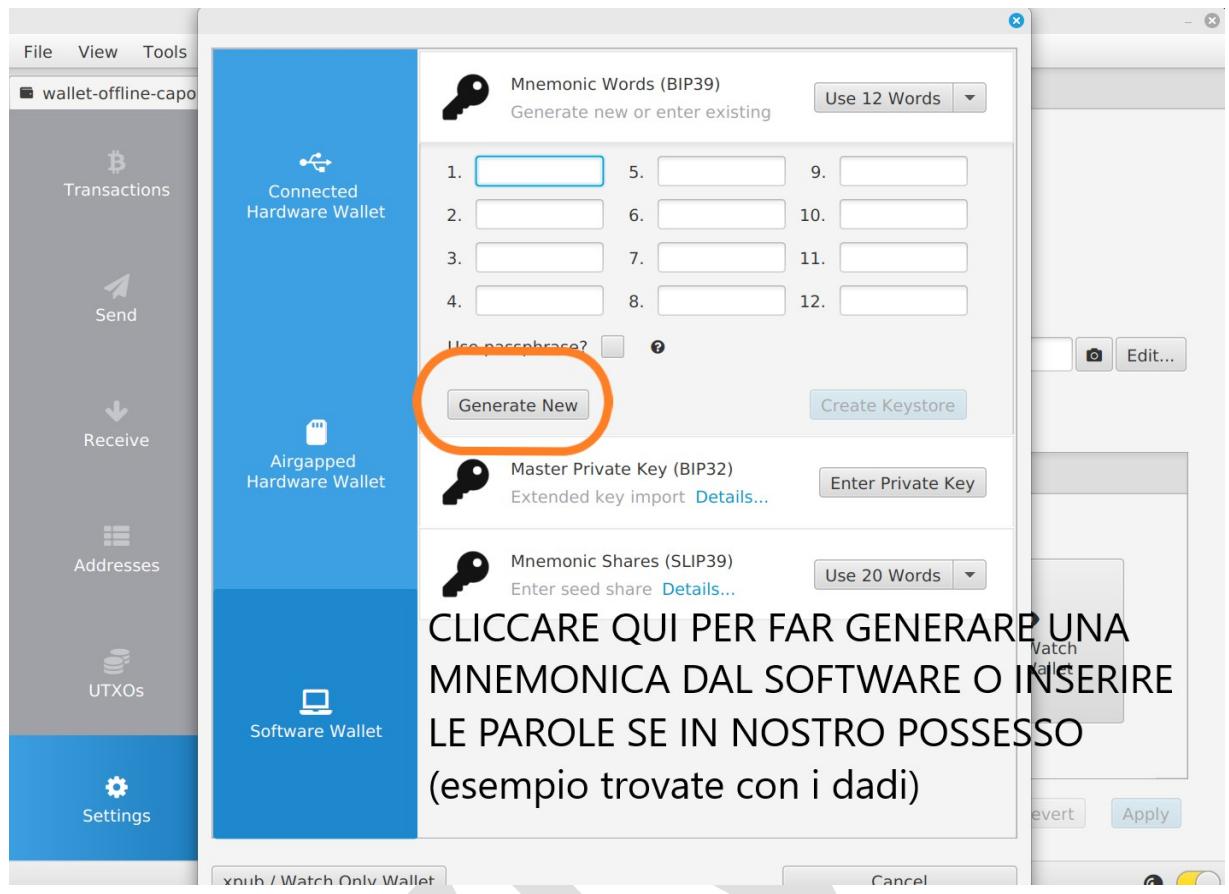
TIPO DI WALLET (singolo o Multi)

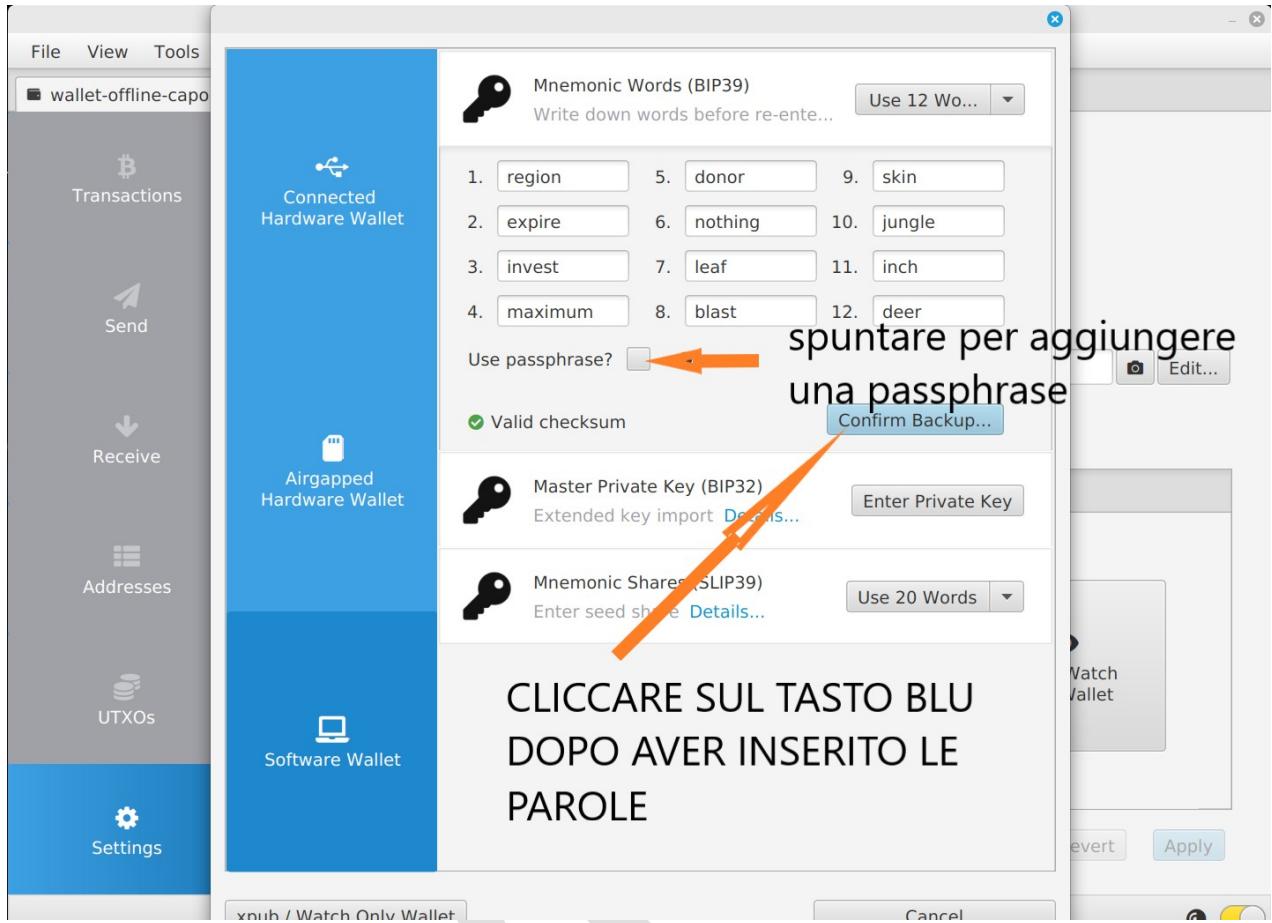
TIPO DI INDIRIZZO

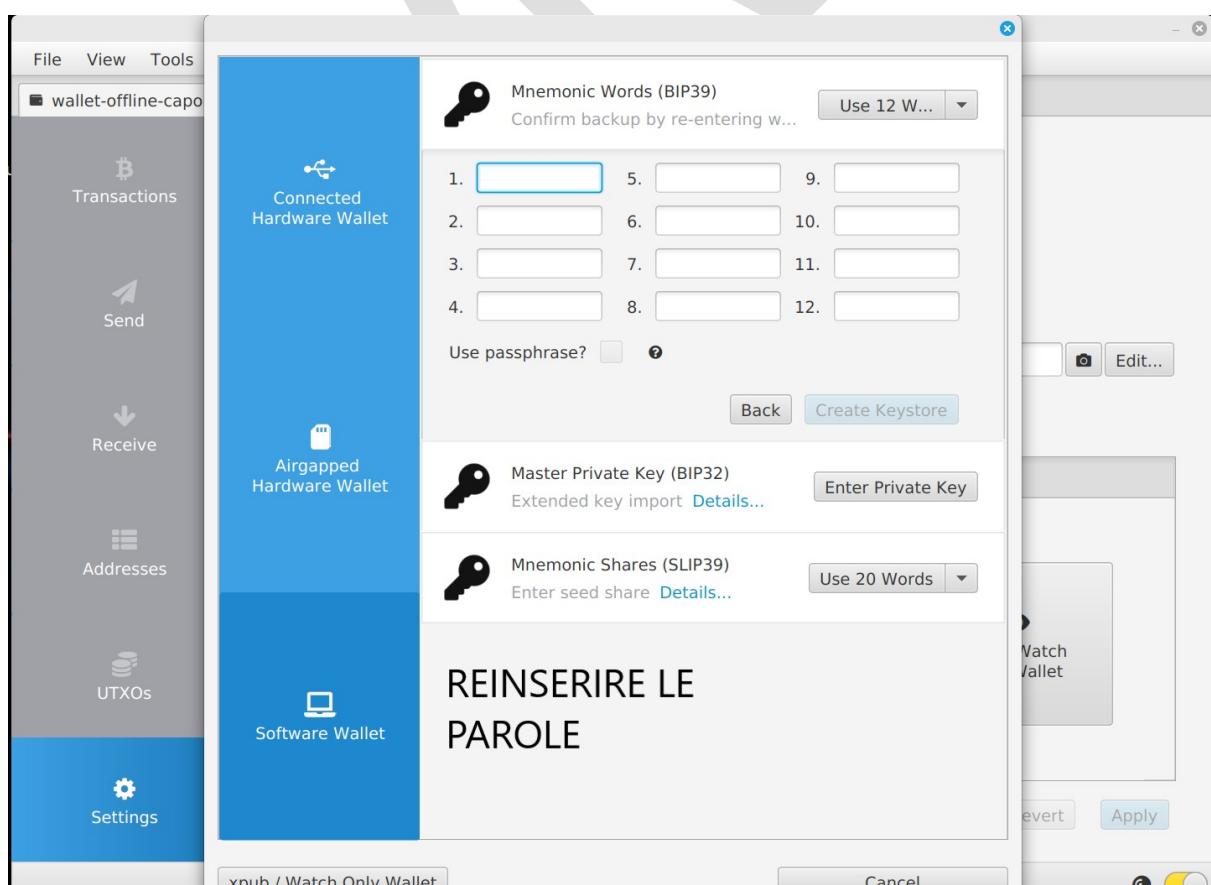
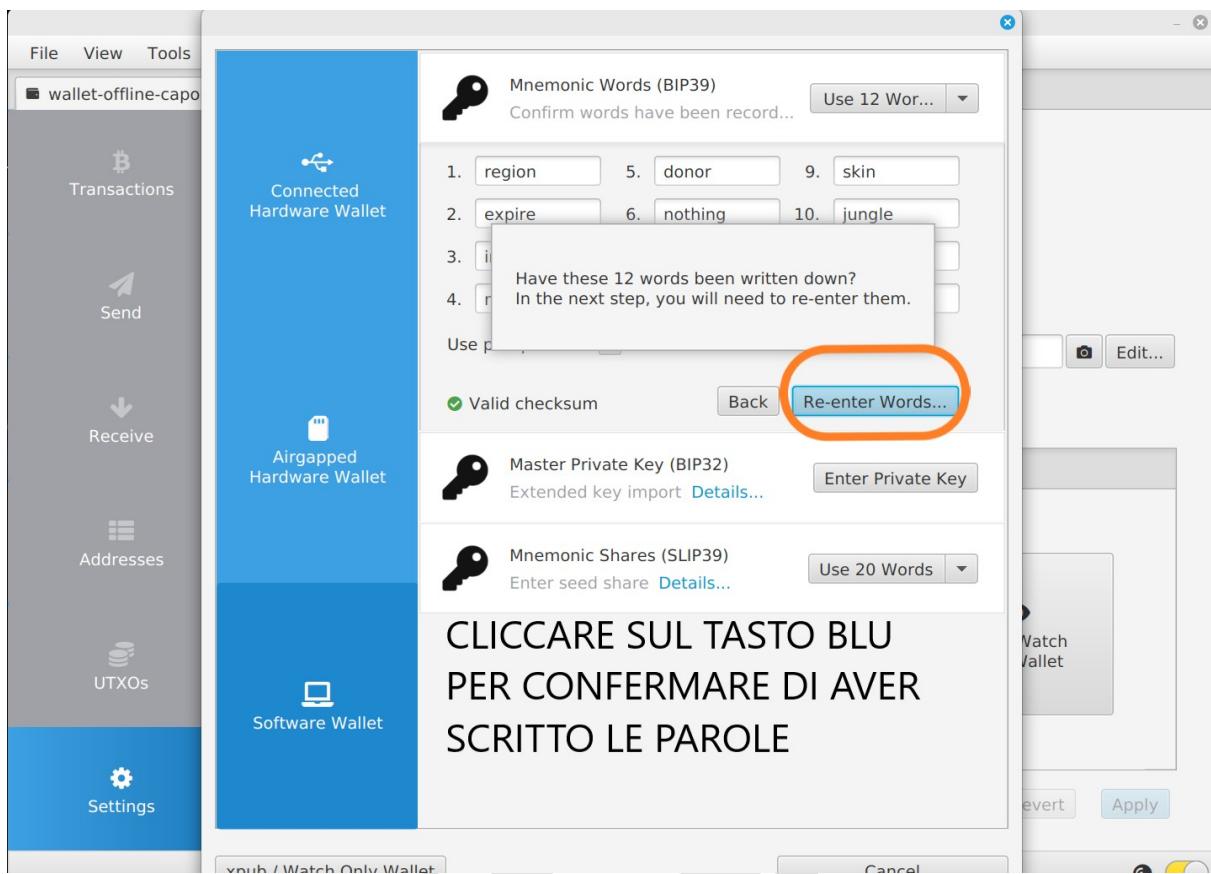
The screenshot shows the Sparrow wallet settings interface for the 'wallet-offline-capoufficio-adamo' wallet. On the left sidebar, there are icons for Transactions, Send, Receive, Addresses, UTXOs, and Settings. The 'Settings' icon is selected. In the main area, under 'Settings', there are dropdown menus for 'Policy Type' (set to 'Single Signature') and 'Script Type' (set to 'Native Segwit (P2WPKH)'). Under 'Script Policy', there is a descriptor field with 'wpkh(Keystore1)'. Under 'Keystores', there is a section titled 'Keystore 1' with four options: 'Connected Hardware Wallet', 'Airgapped Hardware Wallet', 'New or Imported Software Wallet' (which is circled in orange), and 'xPub / Watch Only Wallet'. At the bottom of the screen are buttons for 'Export...', 'Add Account...', 'Advanced...', 'Revert', and 'Apply'.

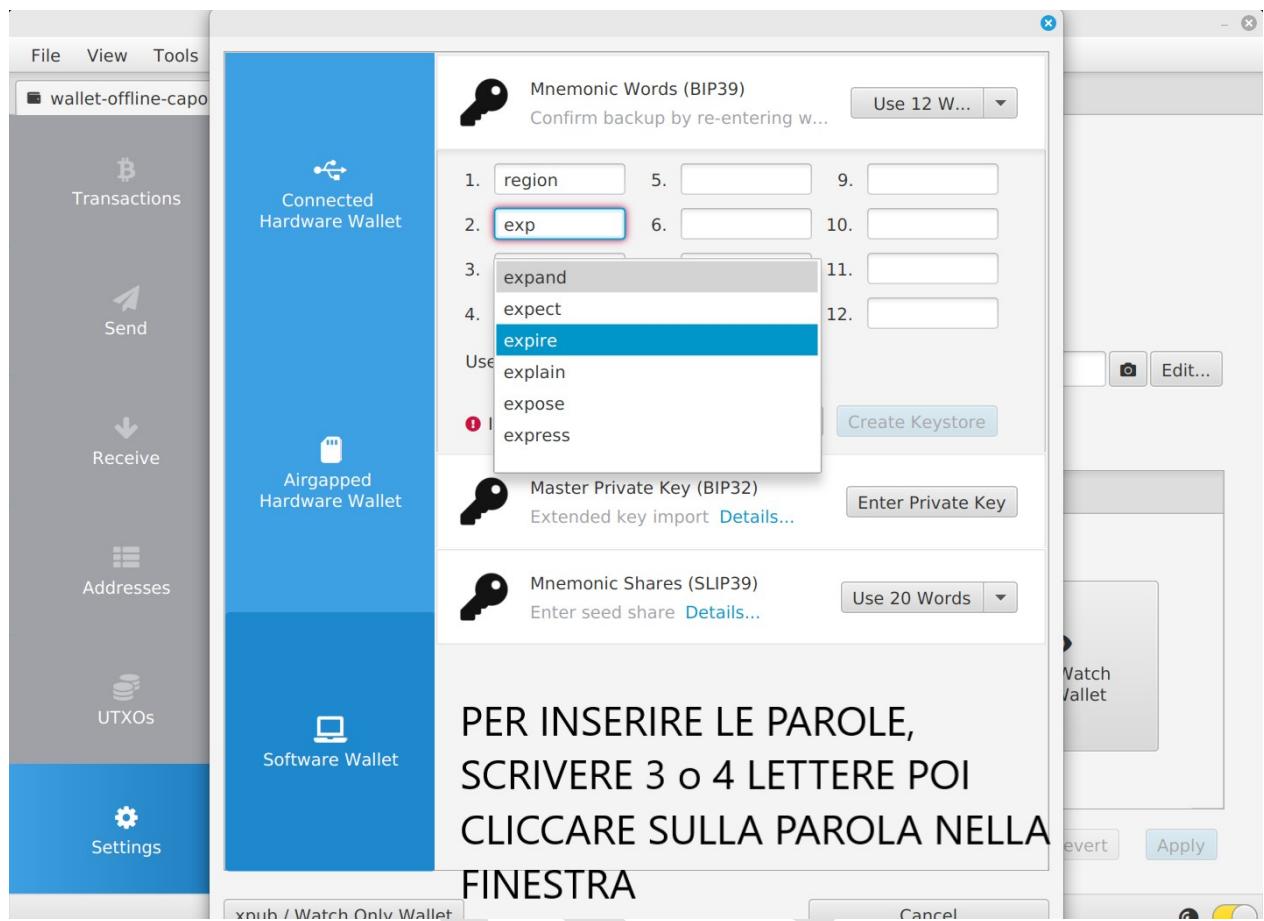


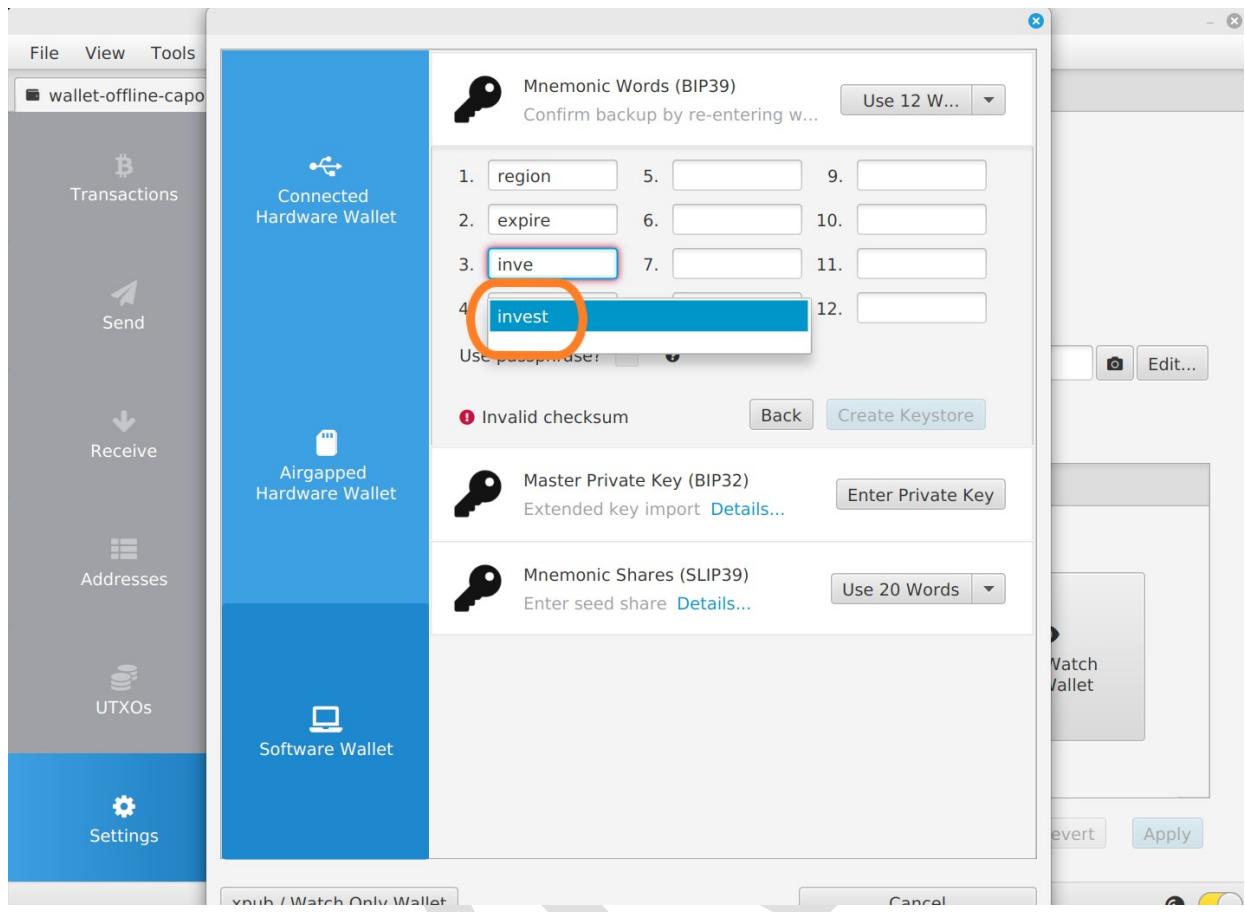
S
Y

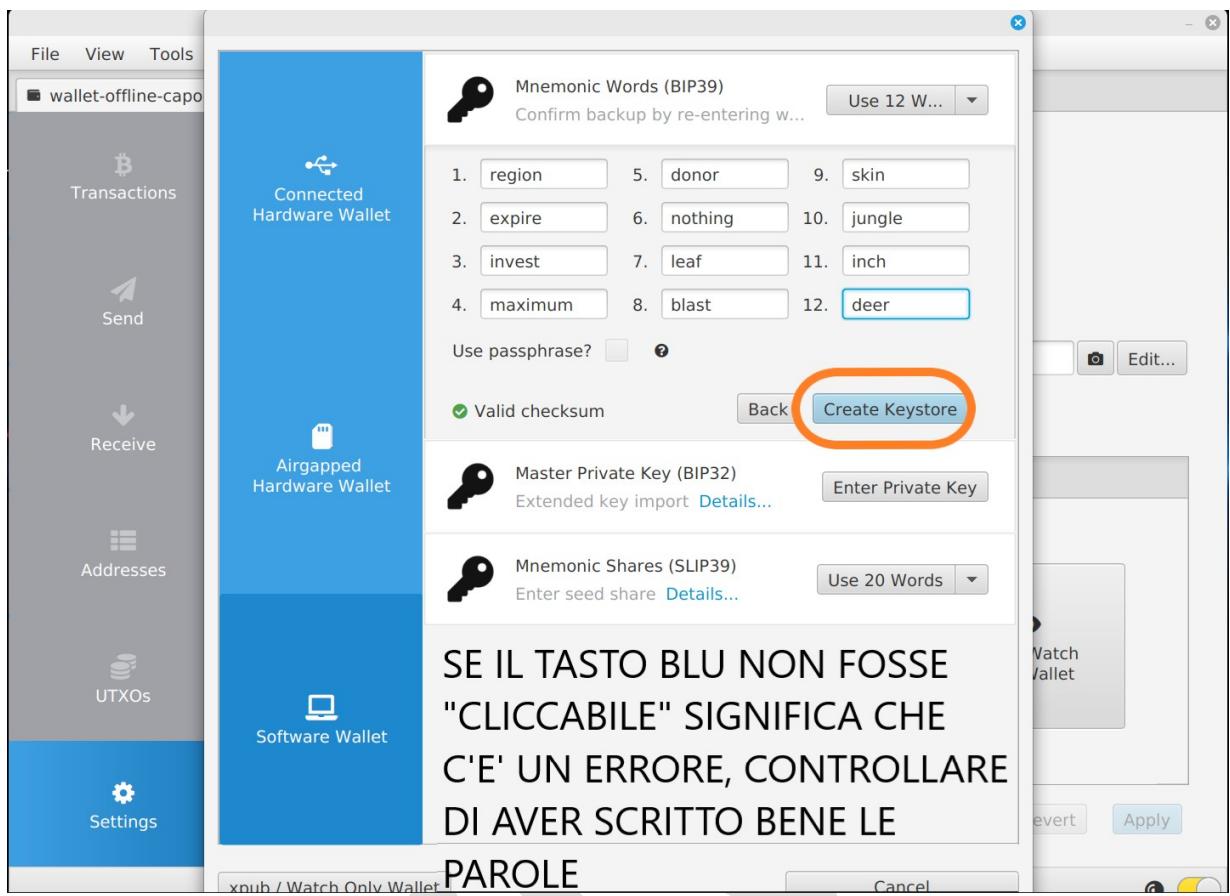


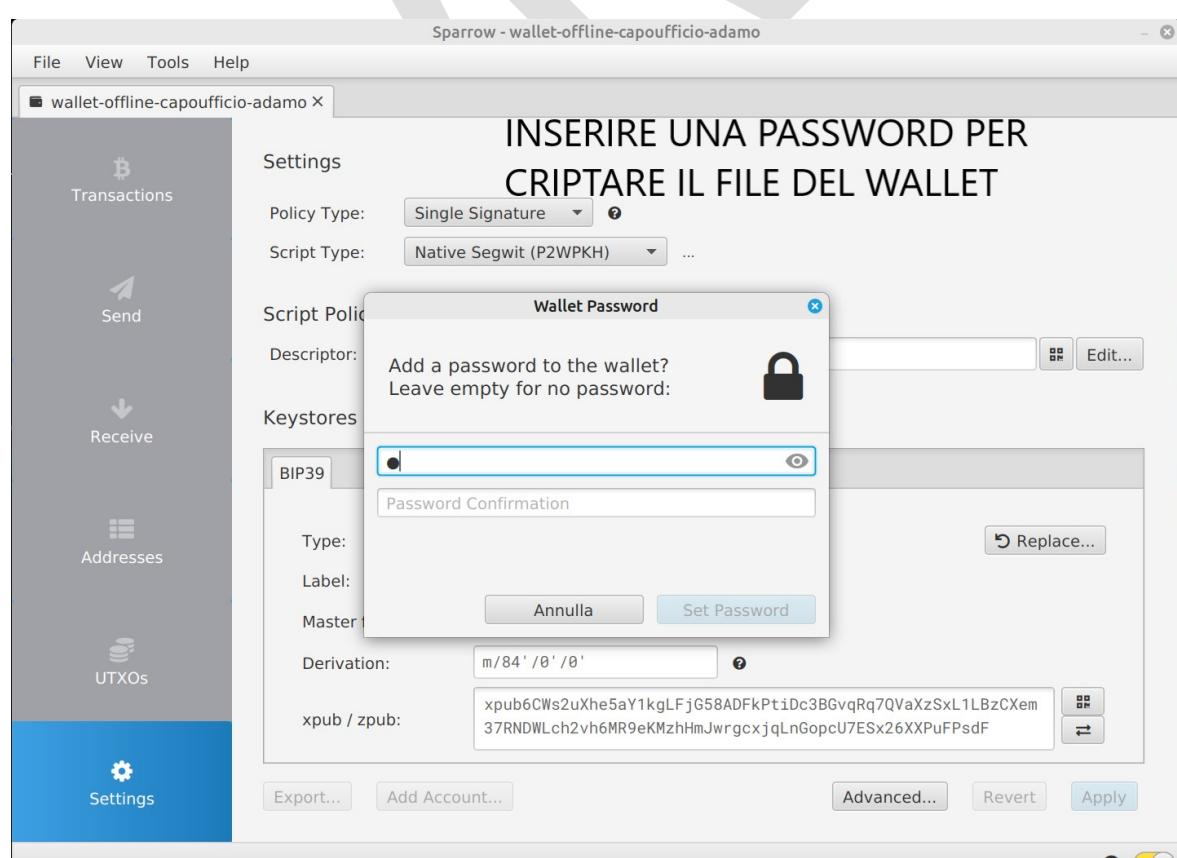
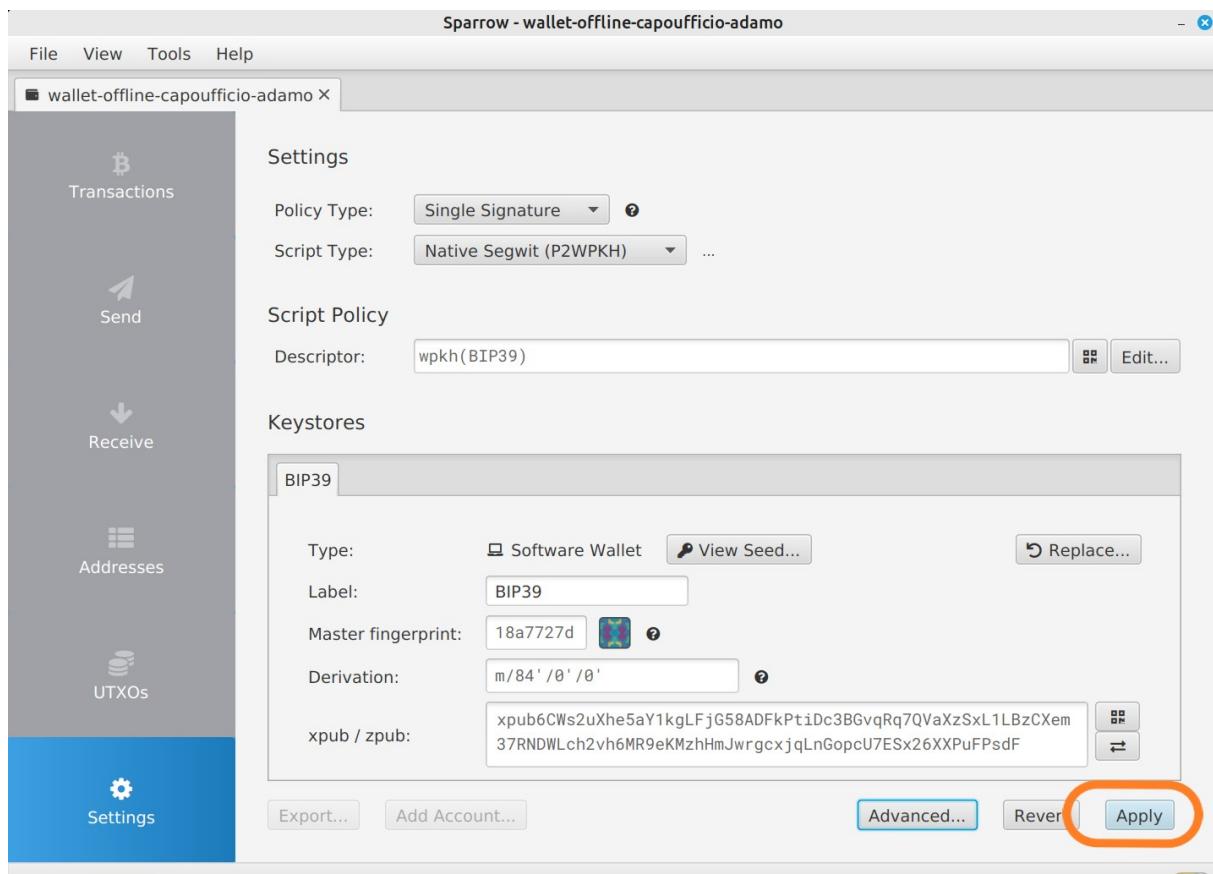


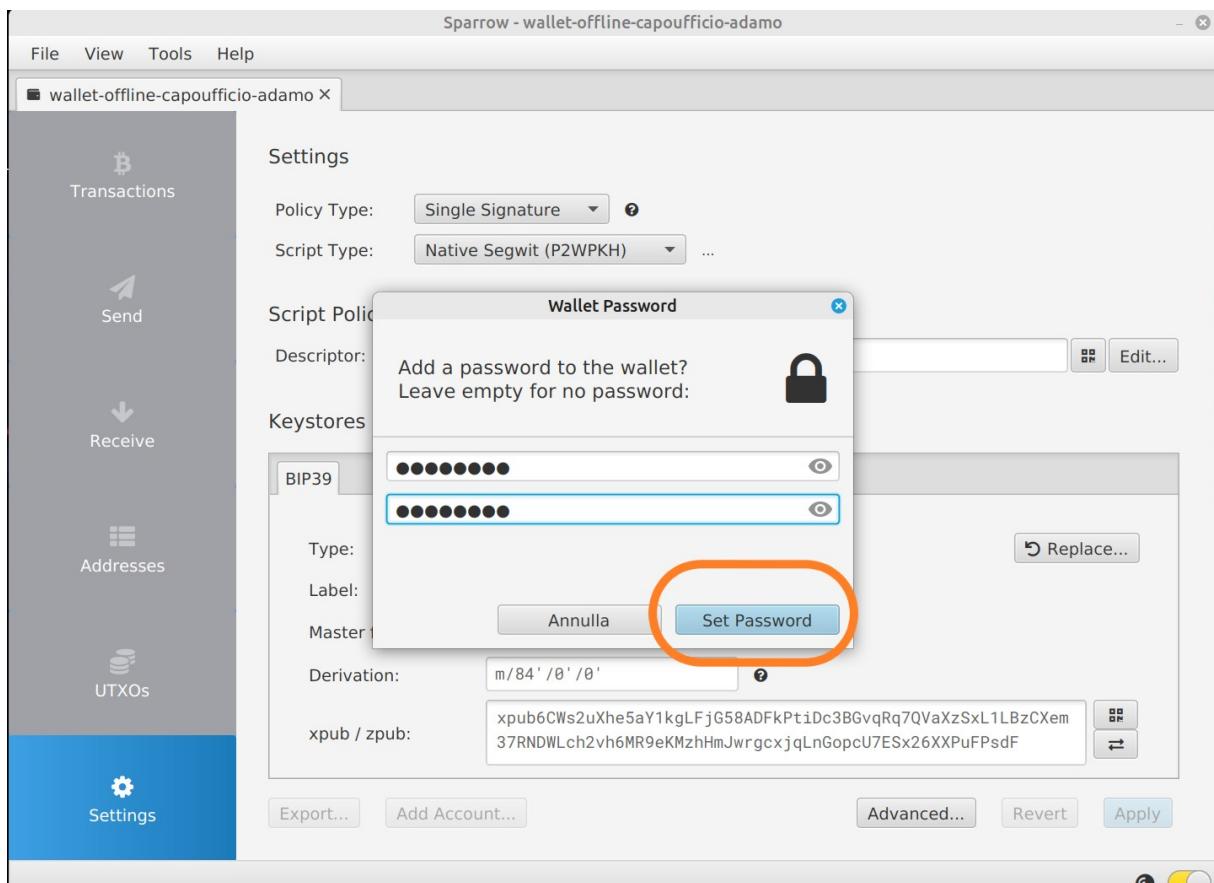


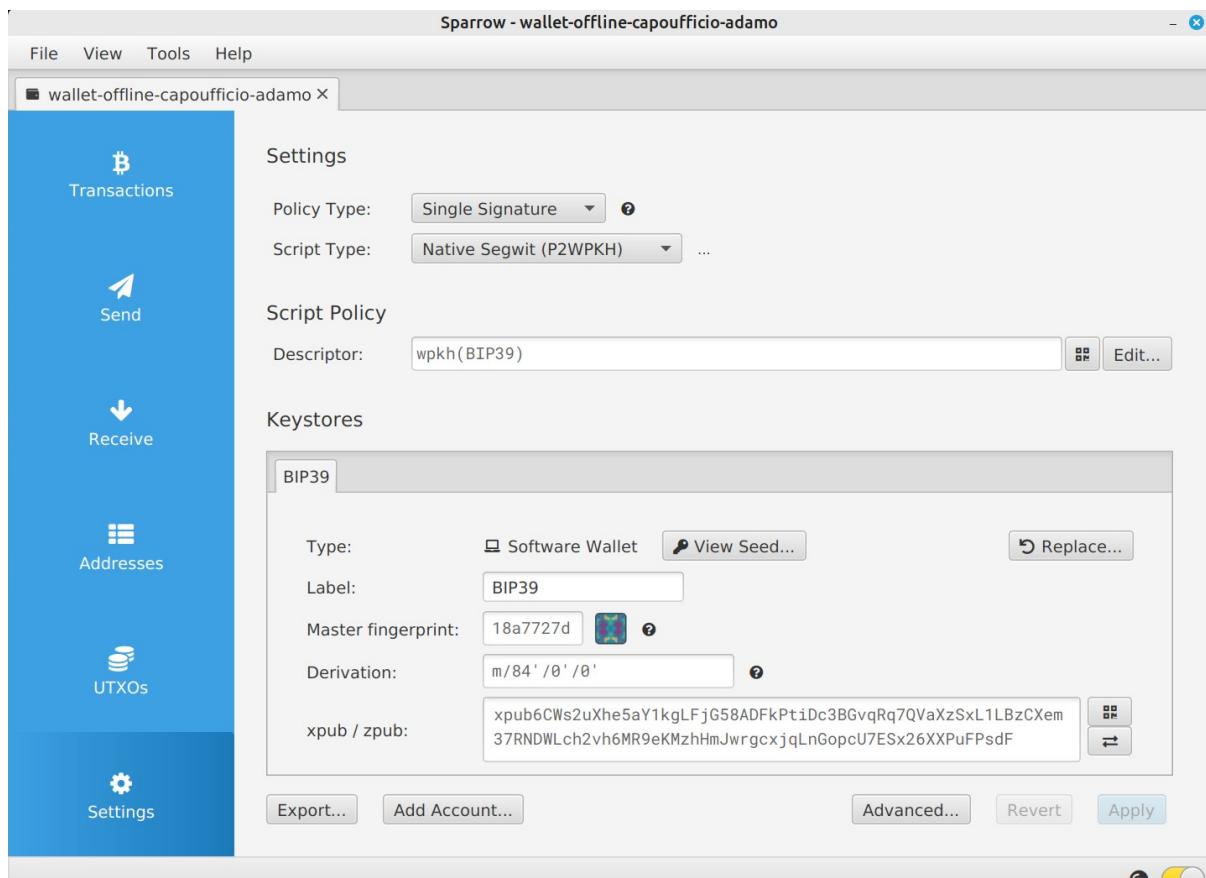












Il wallet OFFLINE o capo-ufficio è pronto!

Ora vi devo raccontare un'altra storia per farvi ricordare come si fa il wallet di visualizzazione.

Vi ricordate di Adamo ed Eva?

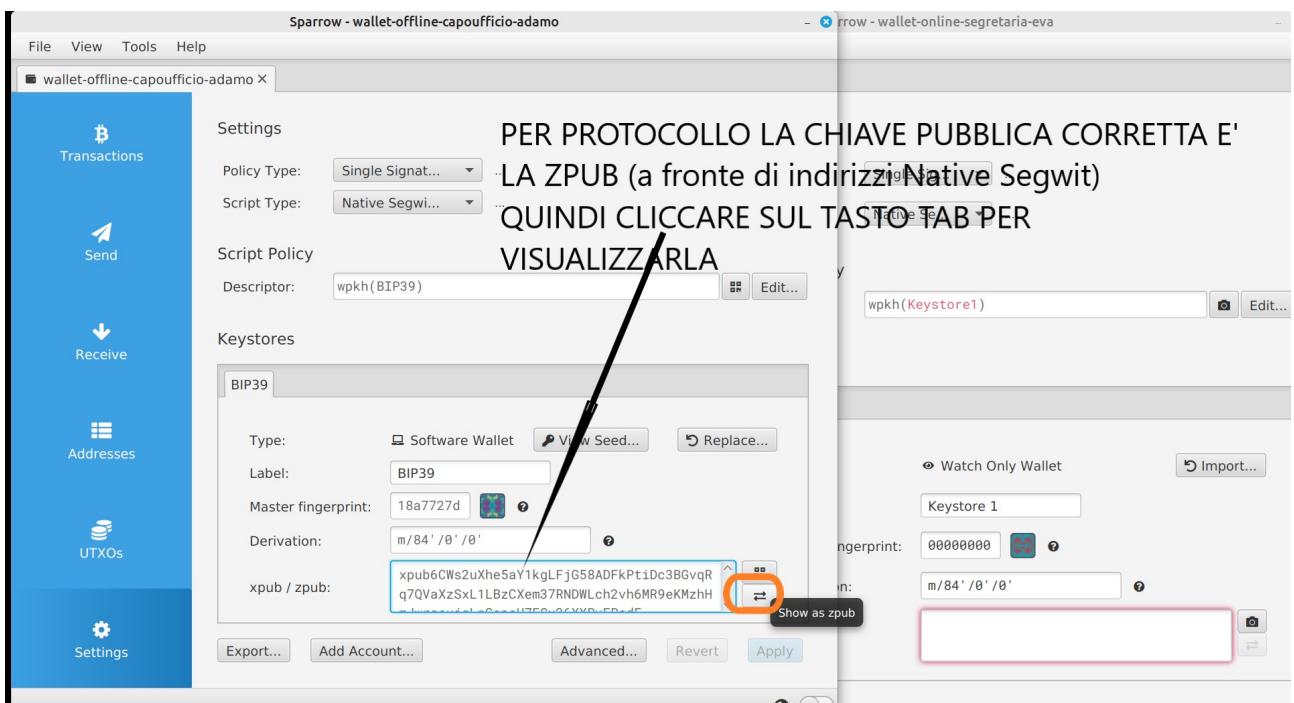
Dio fece una statuetta con la terra e le diede vita, questo fu Adamo. (voi avete creato una mnemonica, questo è il vostro Adamo).

Ma Eva? Fece un'altra statuetta e fu Eva... **NO** se no sarebbe stata un'entità a sé, senza legami con Adamo. Dio prese una costola di Adamo e con quella fece Eva. In questo modo creò un'entità separata ma in qualche modo "collegata".

Lo stesso faremo noi con i nostri wallet:

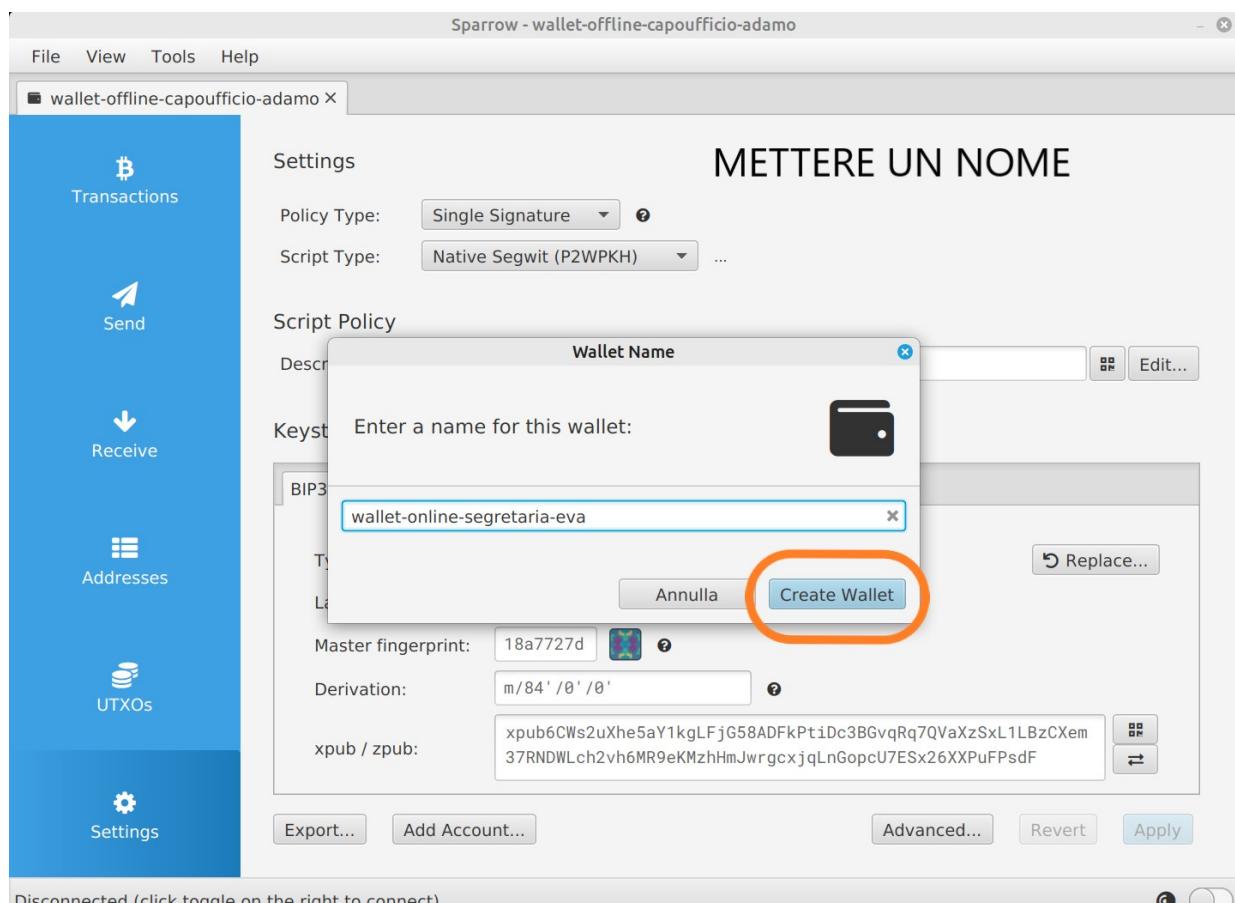
Prenderemo una "costola" dal wallet Offline/capo-ufficio/Adamo cioè la CHIAVE PUBBLICA PRINCIPALE e usando quella creeremo il nostro wallet di sola visualizzazione Online/Segretaria/Eva.

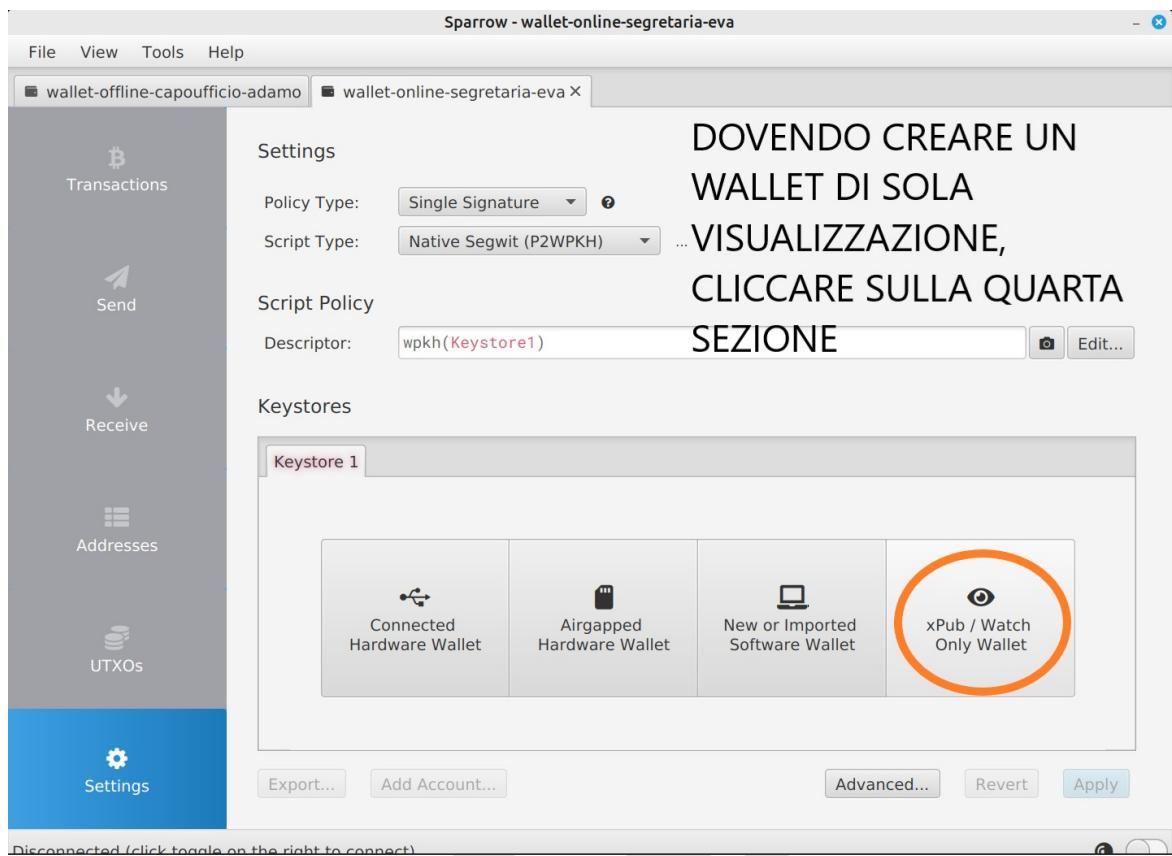
Sparrow non è molto ligio al protocollo Bitcoin, infatti ci mostra la xpub mentre per l'indirizzo standard che abbiamo scelto di usare la versione corretta sarebbe la zpub, quindi dovremo andare a prendere il dato corretto come segue:

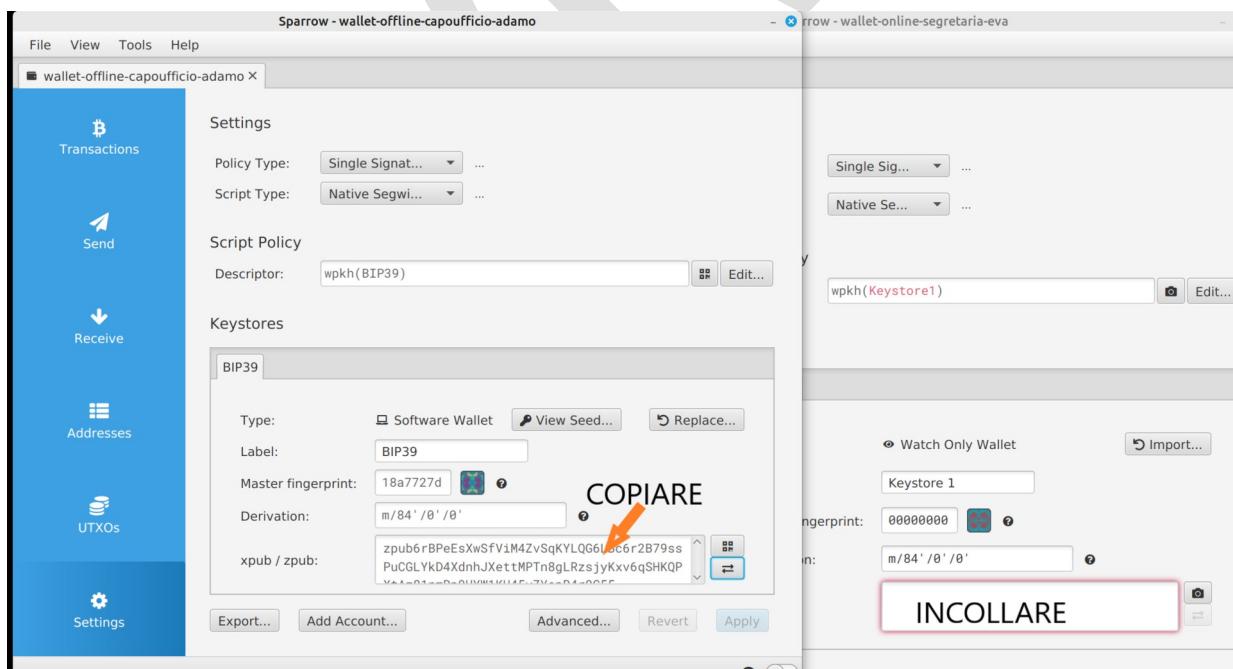
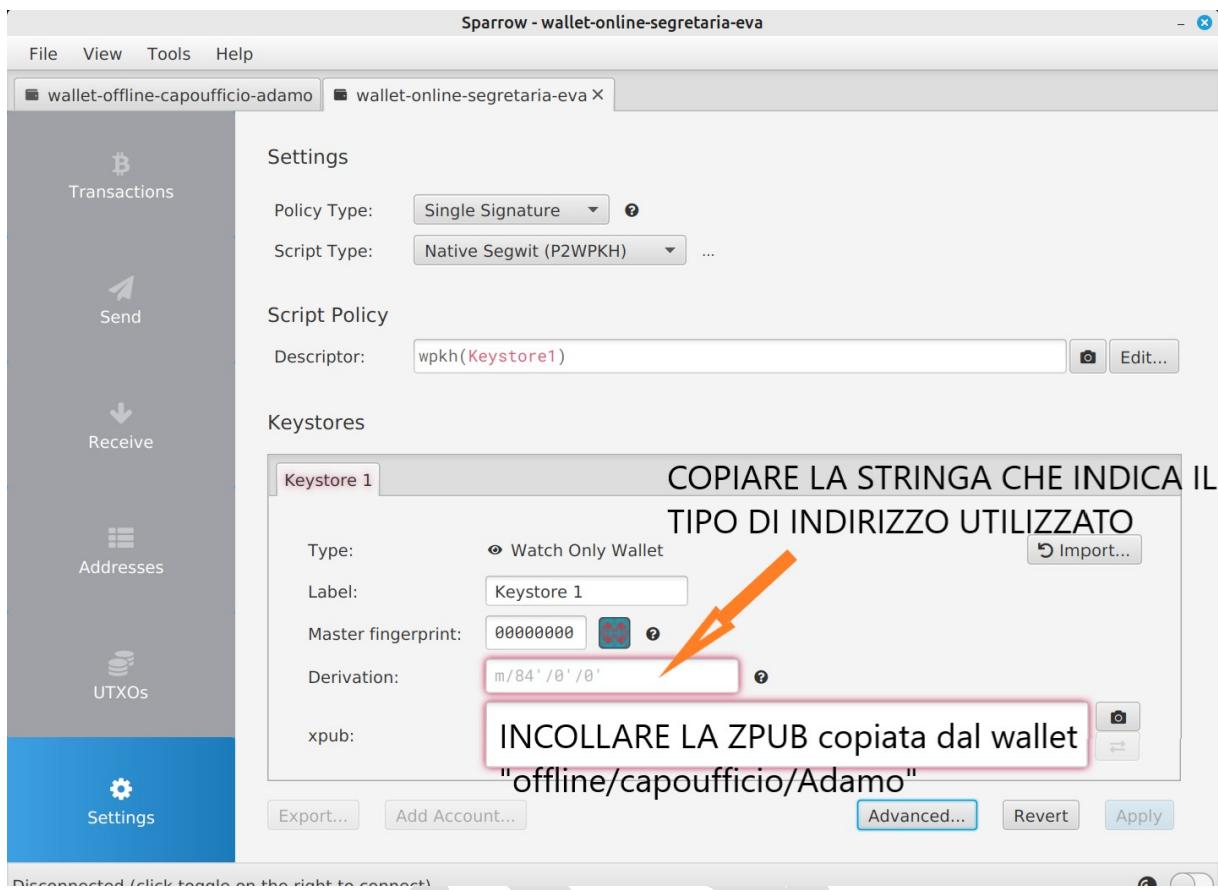


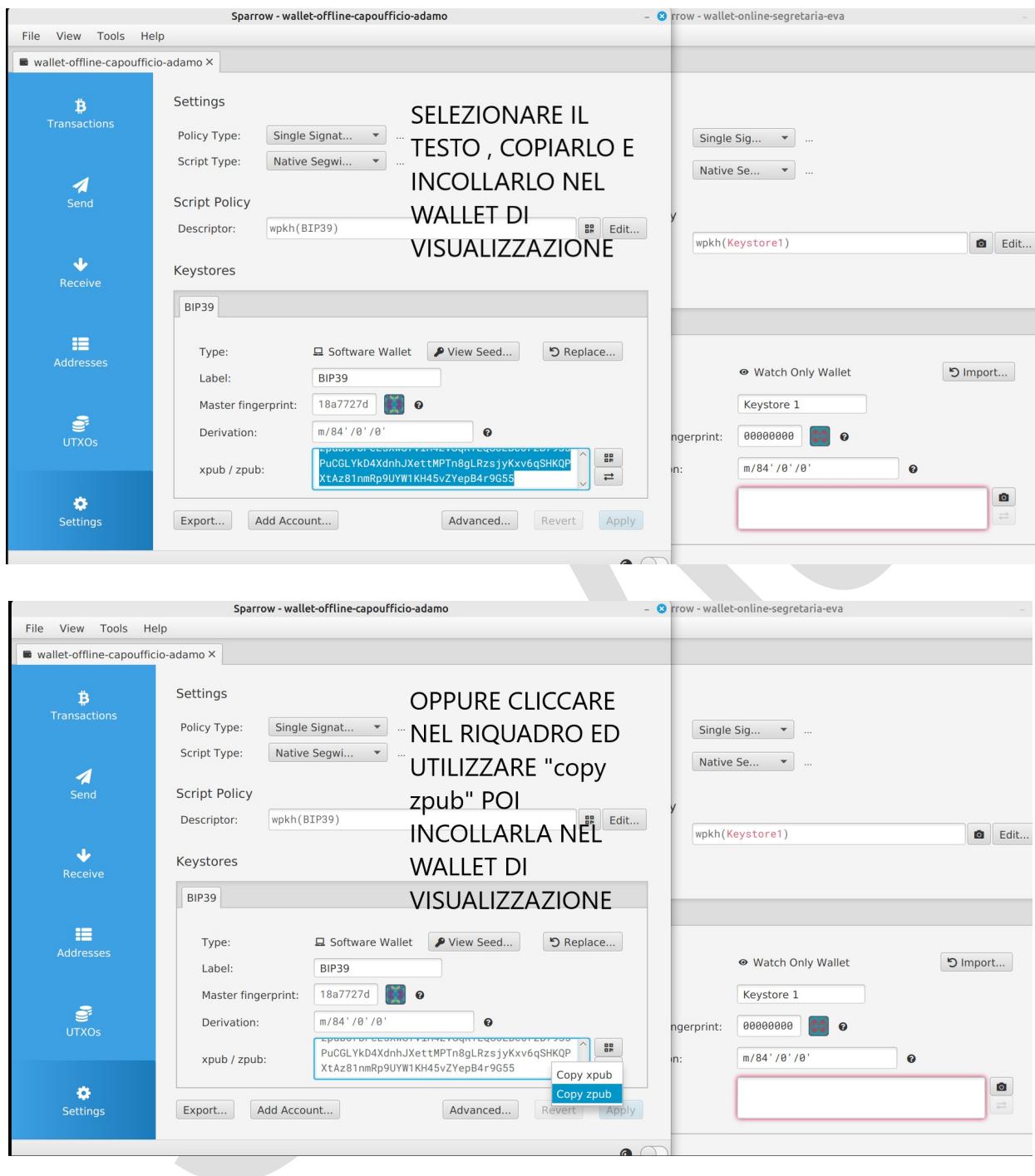
CREAZIONE DEL WALLET DI SOLA VISUALIZZAZIONE (Online/Segretaria/Eva)

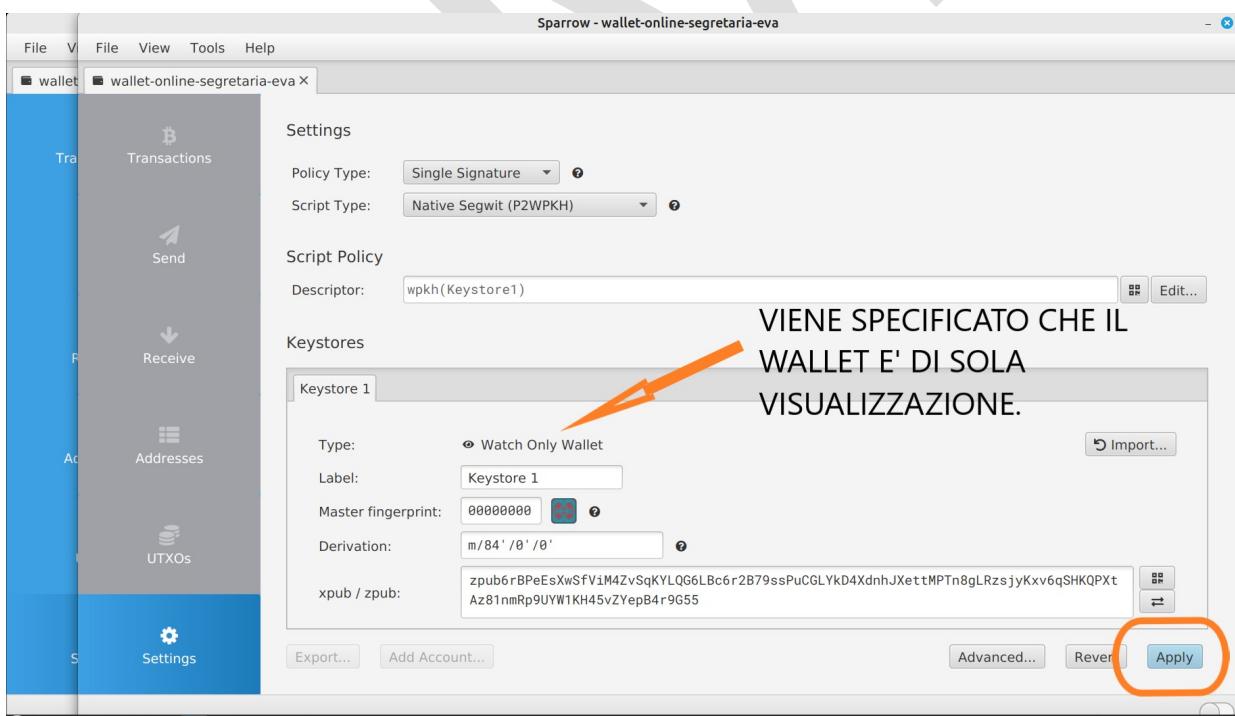
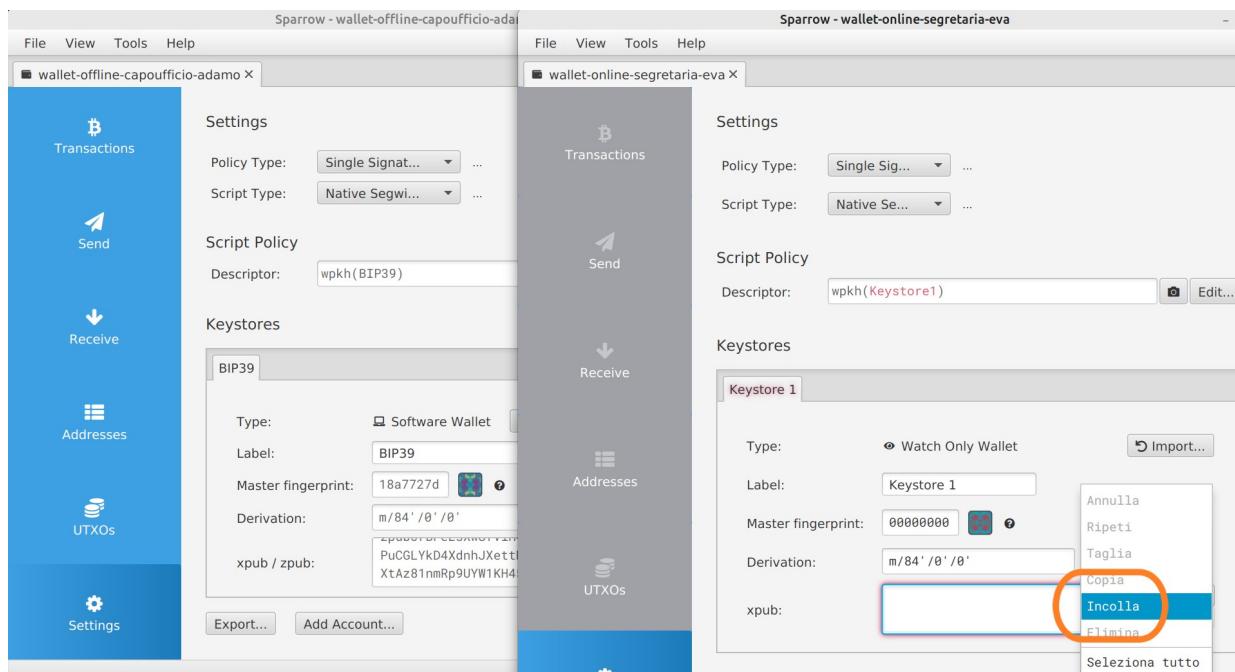
Per creare il nuovo wallet possiamo cliccare su File (in alto a sinistra) --> New se abbiamo il wallet principale aperto oppure sui comandi centrali blu, nella pagina iniziale (se siamo su un altro computer).

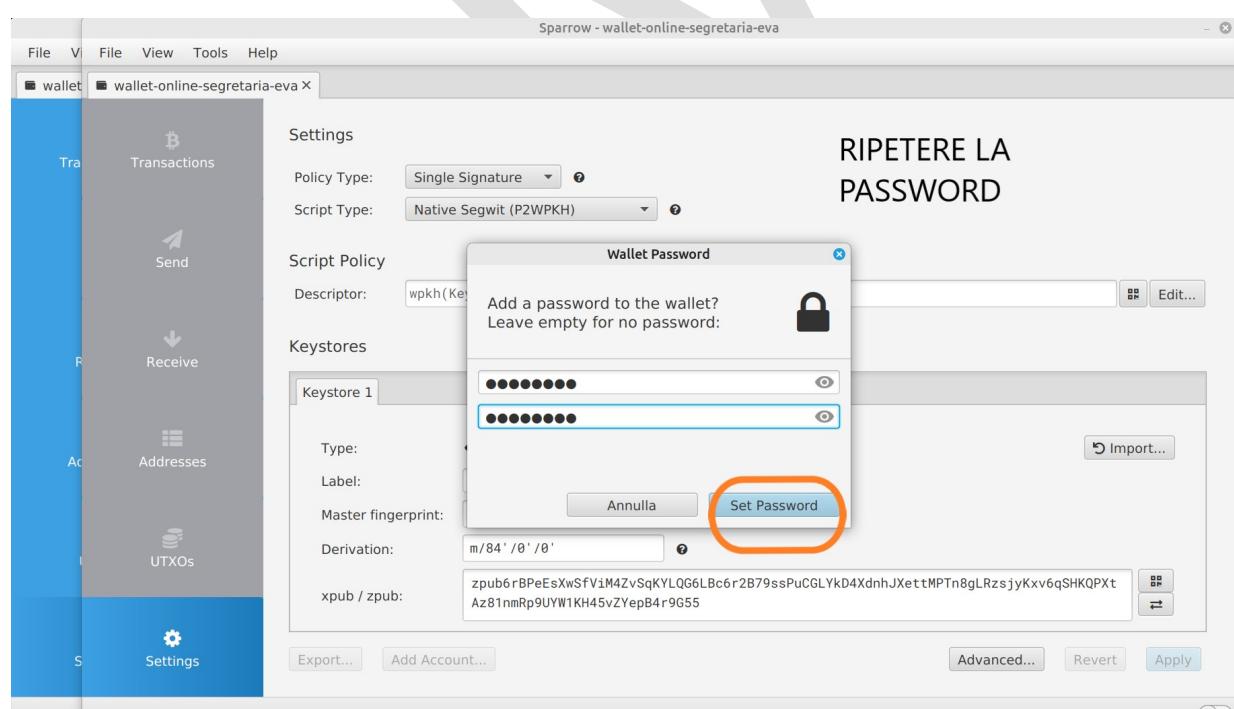
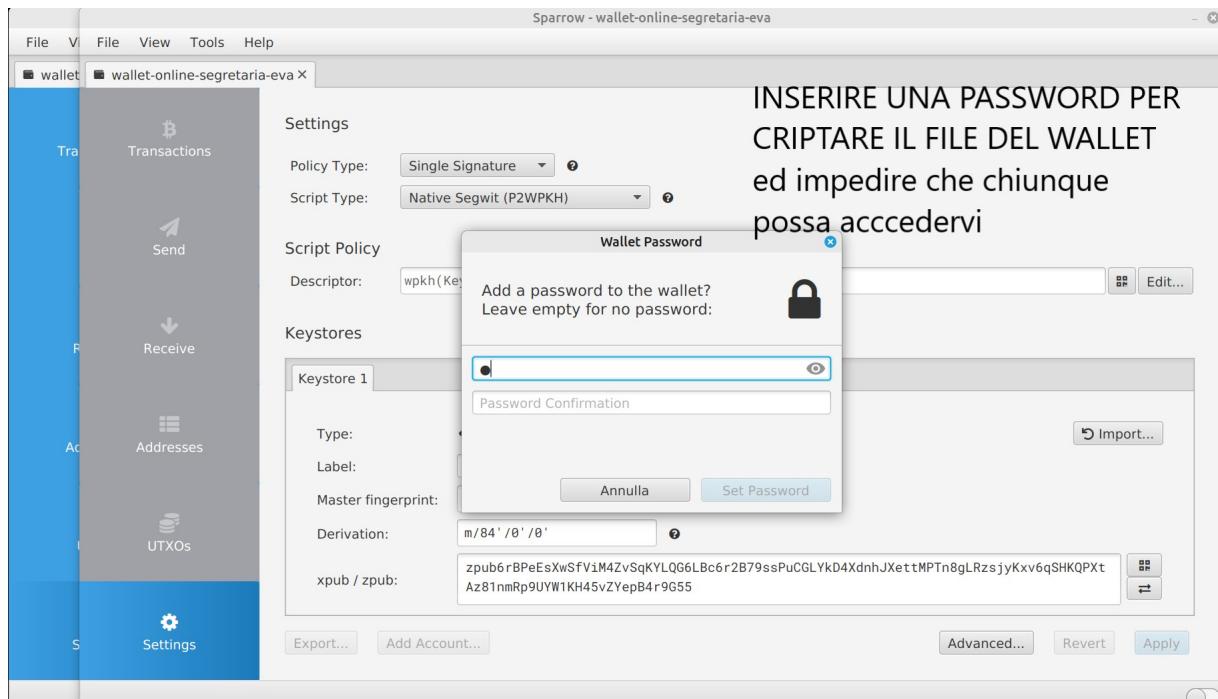






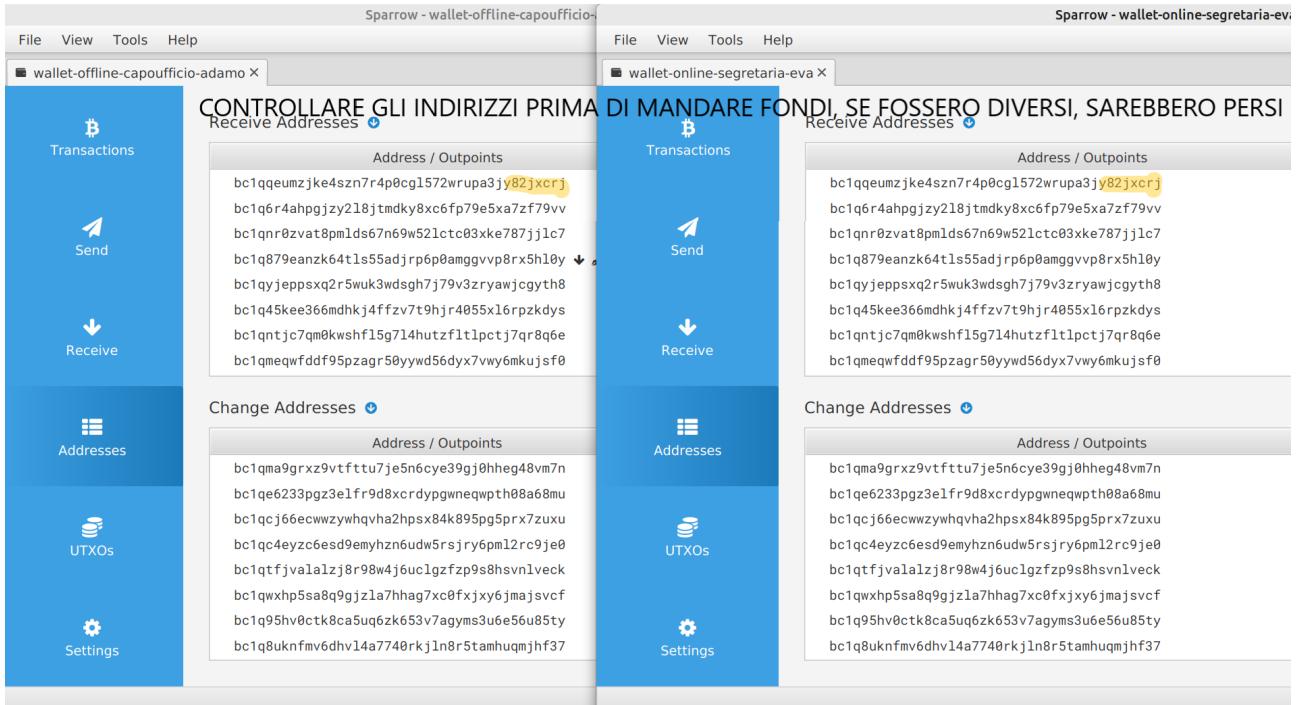






Dopo la conferma della password, il wallet è pronto!

PRIMA DI USARE QUESTI WALLET è **IMPORTANTISSIMO** verificare che i due wallet realmente corrispondano l'uno all'altro, siano la versione **OFFline** e **Online** dello stesso portafoglio! Per far questo dobbiamo confrontare visivamente gli indirizzi generati da entrambi, nella sezione "Addresses"



Basta controllare i primi nella parte iniziale e soprattutto finale.
 Nel caso risultassero diversi, significa che abbiamo sbagliato ad inserire la Chiave Pubblica Principale quindi dobbiamo eliminare il wallet di visualizzazione e rifarlo.
Pena: Perdita irreversibile dei fondi!!!!