Come creare un wallet SegWit: paper wallet e software wallet con Electrum (non bech32)

scritto da Alberto De Luigi | 4 Marzo 2018

Questa guida spiega come creare un wallet SegWit in 5 minuti, mostrando tutti i passaggi necessari per creare un brain wallet, un paper wallet e un software wallet (Electrum non bech32). Spiega inoltre come ricevere e monitorare i pagamenti sul paper wallet (watch only wallet), anche senza l'uso di un client software.

Per i più esperti, la guida è riassunta in 6 passaggi, riportati sinteticamente nel seguente elenco puntato. Proseguendo la lettura, ogni punto è approfondito con numerosi suggerimenti e gli screenshot guidano il lettore passo a passo.

1. Aprite il seed generator BIP39 di Iancoleman
2. Selezionate 12 word e create il seed
3. Scaricate Electrum (3.0.6 o superiore): create uno standard wallet -> I already have a seed -> incollate il seed
4. Cliccate su “Options” e flaggate “BIP39 seed”
5. Come Derivation specificate m/49’/0’/0′ (quella di default è m/44’/0’/0′). Nelle versioni più recenti di Electrum ci sono tre opzioni possibili, selezionate p2sh-segwit (p2wpkh-p2sh)
6. Congratulazioni, ora avete un wallet Electrum con indirizzi SegWit non bech32

NOTA IMPORTANTE: per l’import su **Electrum mobile**, anziché “I already have a seed” selezionare **“Use public or private keys**” e incollare la **master private key**, su Iancoleman è l’**Account extended private key**). Eventualmente potete provare questo metodo secondario anche per importare il wallet su altri software alternativi a Electrum

Prima della guida completa, che trovate scorrendo sotto, è bene fare una premessa sulle ragioni per cui conviene usare SegWit, che è una modifica del protocollo Bitcoin (un fork) avvenuta ad agosto 2017. Da agosto, wallet e servizi Bitcoin che eseguono l’upgrade possono ottenere i benefici di SegWit, fra cui il costo inferiore di commissione pagata a ogni transazione.

Recentemente ci sono state buone notizie per Bitcoin poiché numerosi servizi hanno iniziato non solo ad adottare SegWit, ma anche a fare batching di transazioni: fra questi Coinbase (il web wallet ed exchange più utilizzato al mondo), ShapeShift (che rappresenta il 2% delle transazioni della rete), Bitpanda e altri. **Fare batching permette di ridurre fino all’85% i costi di transazione** e lo spazio occupato sulla blockchain. Si veda la voce di glossario per informazioni sul batching: albertodeluigi.com/glossario-bitcoin/

Grazie a batching e SegWit, numerosi servizi hanno potuto abbassare i costi che vengono richiesti all'utente per spostare i bitcoin. I due più grossi exchange al mondo per volumi in euro e dollari, rispettivamente Kraken e Bitfinex, hanno ridotto le commissioni a 0.0005btc il primo e 0.0004btc il secondo. Al prezzo attuale di bitcoin sono circa 5 dollari per transazione. Se il costo appare comunque alto, bisogna considerare che l'exchange non solo paga la commissione al miner, ma deve coprire numerosi altri costi. Infatti l'exchange tenendo i nostri fondi si assume la responsabilità della loro sicurezza, adottando tutte le misure necessarie, aggiorna il software agli upgrade del protocollo bitcoin, implementa nuovi clients per l'airdrop di coin dai fork, fa supporto clienti, si occupa delle pratiche burocratiche e degli aspetti legali, incluse le verifiche AML KYC, paga il personale per tutte queste mansioni etc.

Se vogliamo evitare di pagare tutti questi costi, minimizzando le commissione di transazione e pagando quindi solo la fee al miner, dobbiamo utilizzare un nostro wallet personale, che è anche la soluzione migliore in quanto a privacy e sicurezza. Ci sono però moltissimi software in circolazione poco efficienti e sicuri. Per questo motivo in questa guida si spiega come creare un wallet che abbia i seguenti vantaggi:

1) **è un wallet SegWit**, per cui nell'invio di bitcoin pagherete **commissioni più basse** rispetto a un wallet tradizionale
2) è utilizzabile solo come **paper wallet** oppure **importabile su un client software**, a discrezione dell'utente
3) il client utilizzato è **Electrum**, wallet **open source considerato uno dei più sicuri**
4) al contrario dell'impostazione standard di Electrum con SegWit, con questo metodo non creerete un wallet bech32, perciò **non rischierete incompatibilità in ricezione**. Bech32 è un'ottima tecnologia, ma ad oggi per gli utenti meno esperti costituisce un boomerang, per via delle incompatibilità in

ricezione con la maggior parte degli altri wallet
5) nell'invio di bitcoin, Electrum permette di impostare una **commissione per il miner a piacimento**, con un **buon algoritmo che prevede quando la transazione sarà validata**
6) Electrum **permette Replace By Fee**, ovvero è possibile impostare una fee molto bassa e, solo qualora ci si accorga che non è sufficiente a confermare la transazione entro i tempi richiesti, si può aumentare la fee a piacere in seguito, rimpiazzando la transazione
7) Electrum **permette import ed export di seed e chiavi private**, così da poter esportare il wallet altrove senza dover effettuare una transazione, e **facilita anche il recupero dell'altcoin in caso di fork** della blockchain
8) per i più paranoici della sicurezza, Electrum **permette di creare e firmare le transazioni su un device che rimane sempre offline**, poi la transazione viene esportata su un altro device (quest'ultimo online), per essere trasmessa alla rete

Nonostante la convenienza, SegWit è ad oggi effettivamente adottato in meno del 15% delle transazioni della rete. Solo quando tutti utilizzeremo quasi esclusivamente indirizzi SegWit, lo spazio occupabile nella blockchain sarà di circa 2mb ogni 10 minuti , il doppio rispetto al limite che avevamo fino ad agosto prima del fork. **Utilizzare SegWit è quindi non solo conveniente per l'utente o il servizio, ma anche un dovere nei confronti della community**, poiché permette a tutta la rete di transare più velocemente e a costi inferiori.

Ricordiamo inoltre che SegWit permette la tecnologia Lightning Network. Fra un paio di anni si può ipotizzare che avremo una rete LN ben sviluppata e che permetterà un numero esponenzialmente maggiore di transazioni, a parità di spazio occupato sulla blockchain. Qualche "temerario" che sta già usando LN c'è, come il buon vecchio **Laszlo Hanyecz**. Laszlo aveva già "scritto la storia" di Bitcoin facendo la prima famosa compravendita in bitcoin per beni reali, cedendo **10.000**

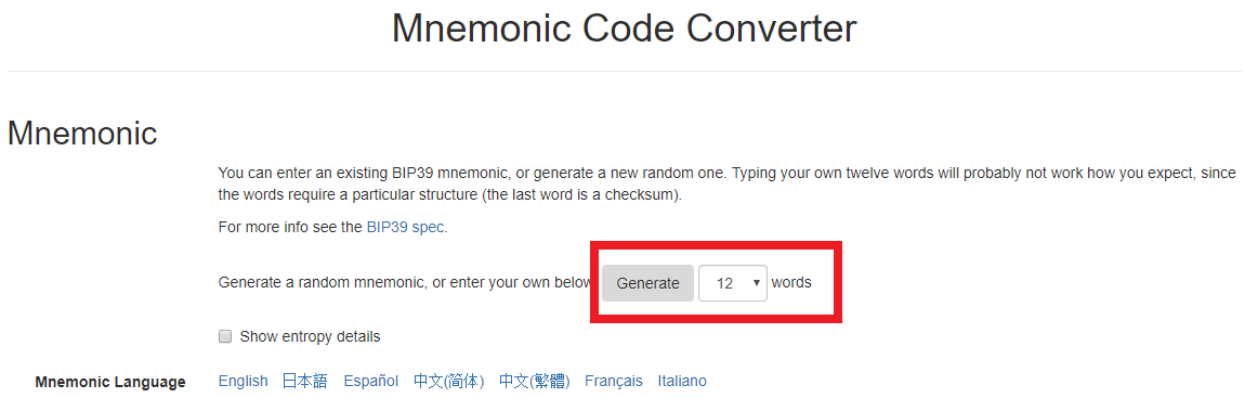
btc per due pizze, nel lontano maggio 2010 (vedi qui). Di recente, è stato il primo a **comprare due pizze con Lightning Network**. Immaginiamo però che non le abbia pagate più 10.000btc come allora, dato che al giorno d'oggi sarebbero oltre 100 milioni di dollari.

GUIDA DETTAGLIATA: CREARE UN WALLET SEGWIT (in 5-10 minuti)

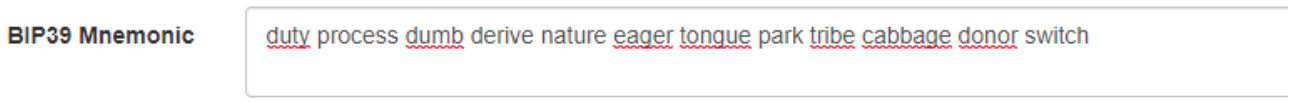
Per prima cosa è necessario creare il seed, ovvero la "frase mnemonica" che sta alla base del wallet, poiché da essa sono derivate tutte le chiavi private. Per farlo, aprite il **generatore di seed BIP39** (è un tool web open source). Potete scaricarlo qui (link diretto al download), o aprire la pagina web dal sito iancoleman.io/bip39 .

nota: per una maggiore sicurezza, se non volete usare il tool online, potete scaricare la pagina in html (cliccate col destro -> salva con nome) e aprire il file in browser quando siete disconnessi da internet, o addirittura da un pc che non è mai stato connesso a internet

2) una volta aperta la pagina, selezionate "12 words" e generate il vostro seed cliccando su "Generate".



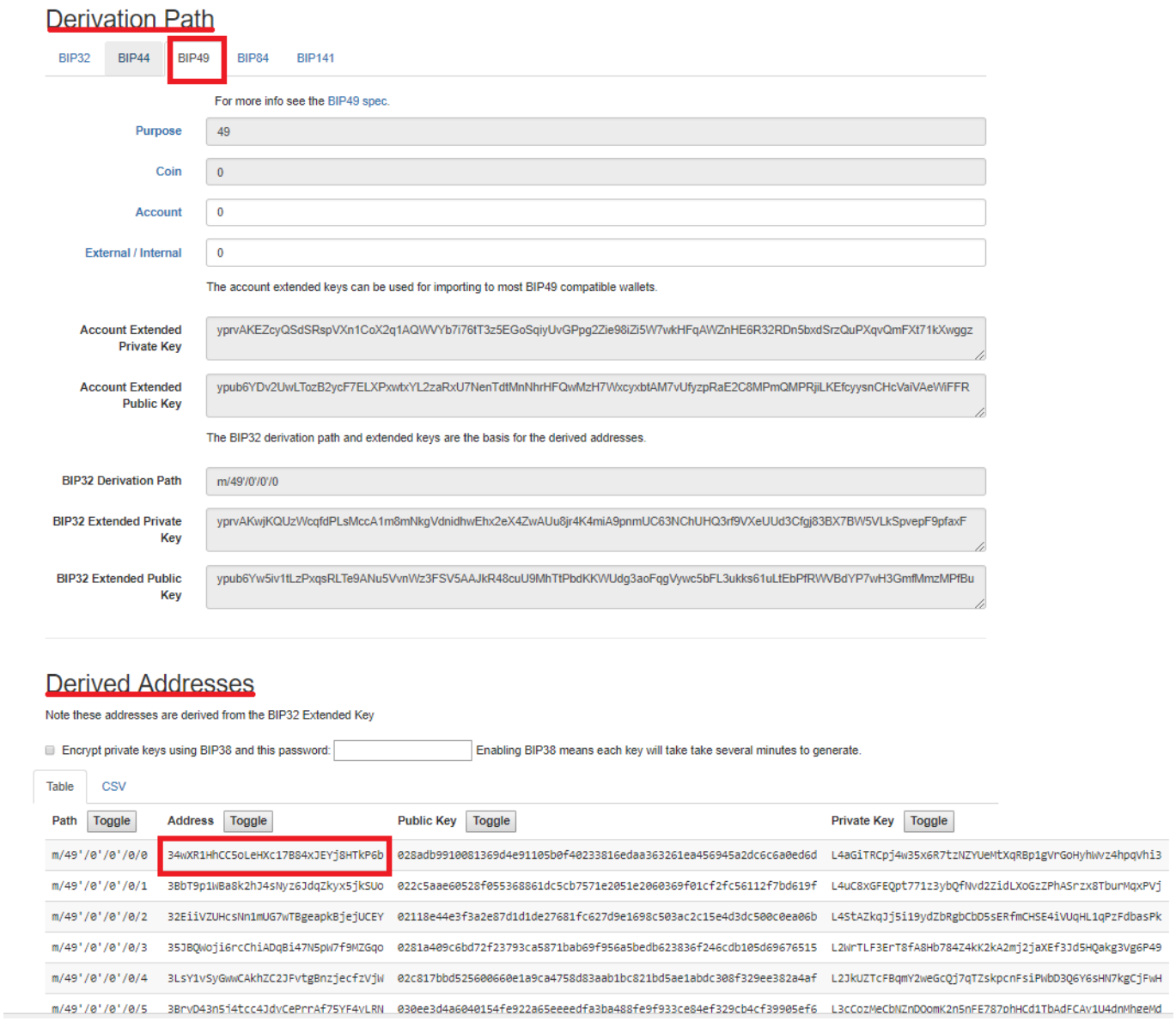
Apparirà quindi la vostra mnemonica nel campo nominato “BIP39 Mnemonic”. Quella frase è il vostro wallet, abbiatene cura.



È a vostra discrezione come salvarla. Potete memorizzarla (brain wallet) oppure scriverla su un foglio (paper wallet) o inciderla da qualche parte. Potete scriverne solo una parte e ricordarvi il resto, oppure scrivere metà in un luogo e metà altrove. Se avete paura che qualcuno possa trovare la frase, è possibile scriverla modificando alcune parole o lettere o invertirle di posto, a patto che poi vi ricordiate quella originale. Sono tutti metodi che, qualora qualcuno riuscisse a fare breccia in casa vostra o nel vostro computer, vi possono dare il tempo di trasferire i fondi altrove, prima che lo faccia il “ladro”. Ho sentito di persone derise da qualche gradasso perché scrivevano la chiave privata modificando alcuni caratteri (ad esempio sostituendo ogni 0 in 1, o cose di questo tipo) come se fosse una pratica ingenua. Per quanto possa non essere un metodo particolarmente raffinato, dato che basta un cifrario per decodificare la chiave privata originale e un software può farlo in fretta, è comunque un metodo che, nella sua semplicità, potrebbe fare la differenza e dare il tempo al proprietario di spostare i fondi altrove. In qualunque modo decidiate di conservare il seed, ricordate sempre che il numero di coloro che perde i propri bitcoin

perché messi “troppo in sicurezza” e non più accessibili, è molto più grande rispetto al numero di quanti vengono effettivamente derubati. Insomma non complicatevi troppo la vita e, soprattutto, se iniziate ad avere un discreto gruzzolo, pensate anche a come passarlo in eredità.

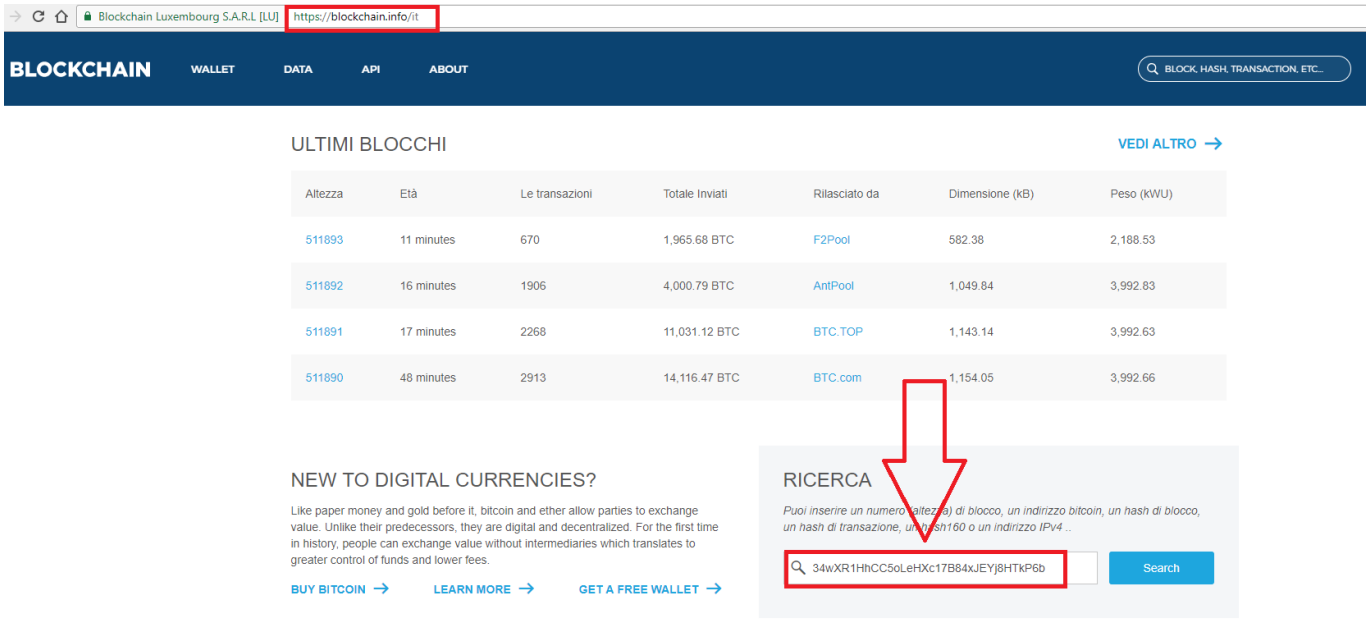
Come ricevere bitcoin sul proprio paper/brain wallet? Nel tool di iancoleman, scorrete nella pagina verso il basso, fino a “Derivation Path”, quindi **selezionate BIP49** (è molto importante questo passaggio, altrimenti non creerete un wallet SegWit). Nella sezione più in basso “Derived Addresses” compariranno una serie di indirizzi.



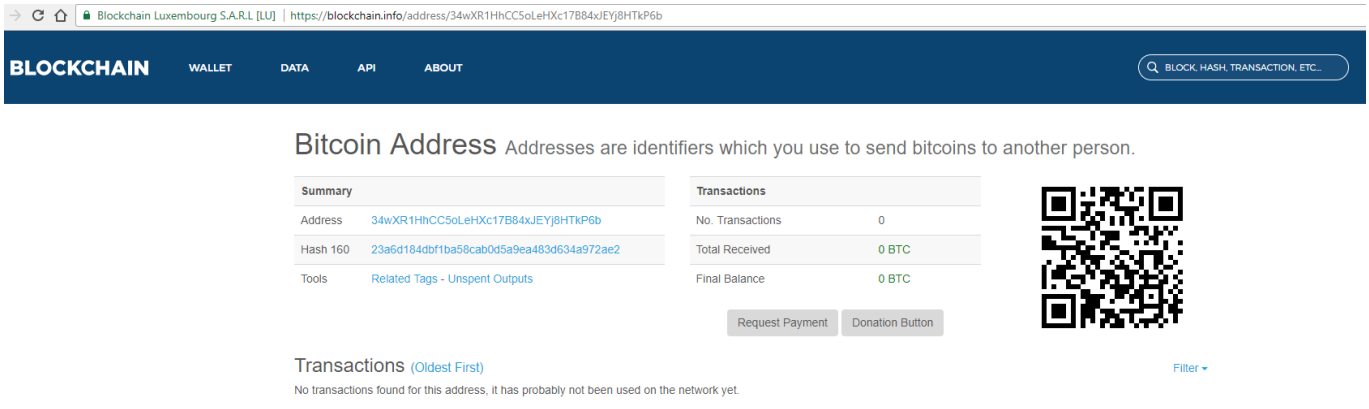
Se avete fatto tutto correttamente, gli indirizzi inizieranno

con il “3” poiché sono indirizzi SegWit. Potete ricevere bitcoin a uno qualsiasi di quegli indirizzi. Potrete copiare il primo della lista e utilizzarlo come vostro indirizzo primario e mostrarlo a chiunque per ricevere pagamenti. L’importante è non mostrare a nessuno il seed, né la private key corrispondente a ciascun indirizzo.

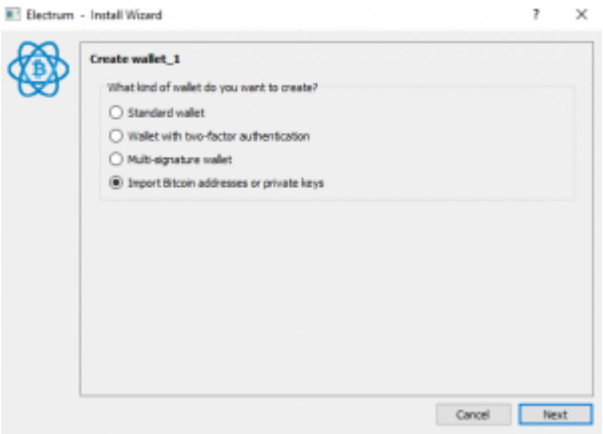
Se volete monitorare quanti soldi sono stati inviati al vostro indirizzo, potete incollare l’indirizzo in un qualsiasi blockexplorer come blockchain.info, quindi cliccare su “Search”



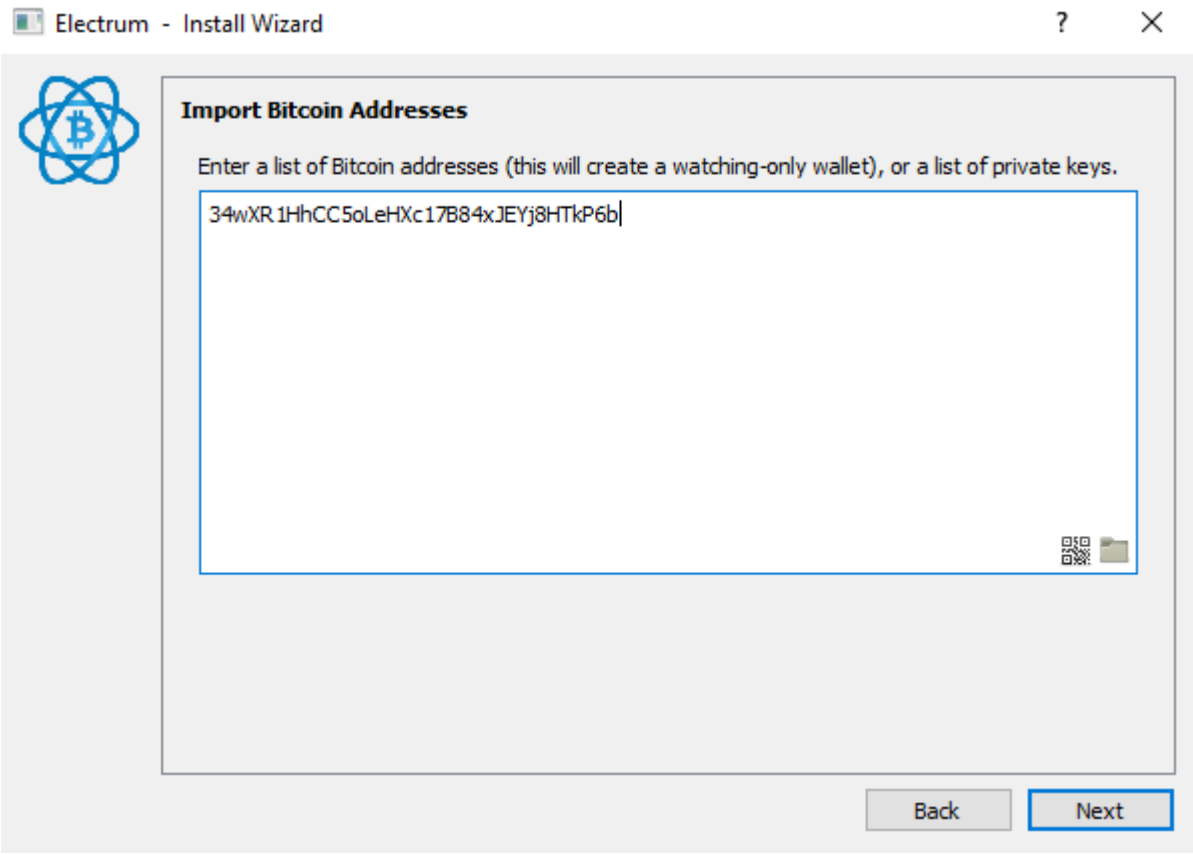
Da qui è possibile vedere quanti btc sono su quell’indirizzo e anche il QR code, che si può usare per ricevere pagamenti come alternativa all’invio della stringa di testo.



È possibile monitorare uno o più indirizzi anche su Electrum, creando un watch only wallet. In quel caso, quando installerete Electrum (vedi dettagli più sotto) e create un nuovo wallet, selezionate “Import bitcoin addressess or private keys”,



Quindi incollate l’indirizzo all’interno

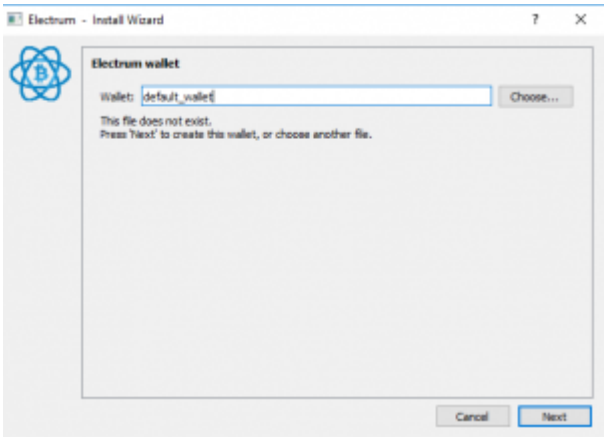


Ogni volta che aprirete il wallet Electrum watch only potrete quindi controllare quanti soldi avete ricevuto. Un wallet di questo tipo può essere comodo per esempio da tenere su un

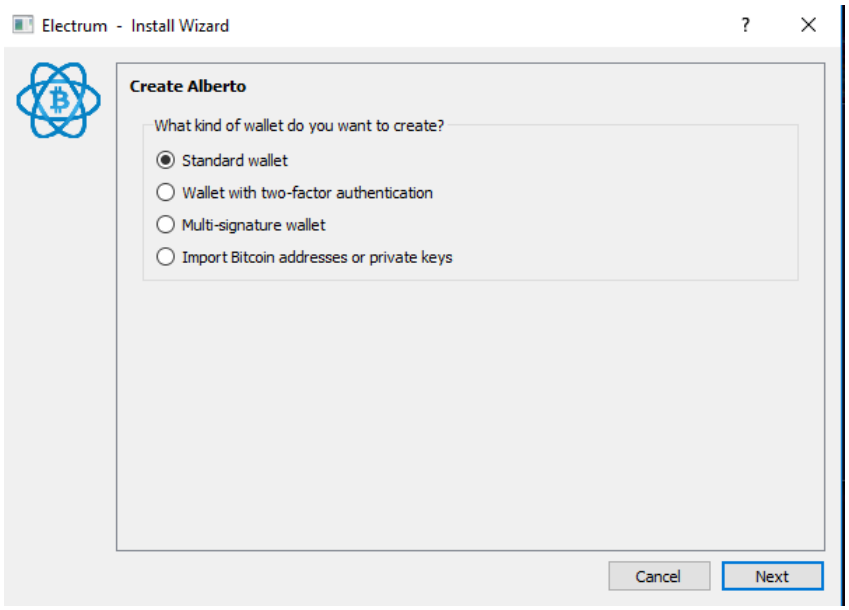
device secondario, o sullo smartphone che abbiamo sempre con noi per controllare il nostro saldo. Se però volete anche spendere i vostri soldi, è necessario creare un wallet vero e proprio con tutte le sue funzionalità in invio e ricezione. Dovrete quindi importare il seed, non l'indirizzo, su Electrum.

Per importare il seed su Electrum creando il vostro software wallet con indirizzi SegWit non bech32, dovrete iniziare ovviamente scaricando Electrum, dal sito ufficiale (versione desktop). Installatelo, apritelo e alla prima schermata selezionate "Auto connect" e passate alla schermata successiva.

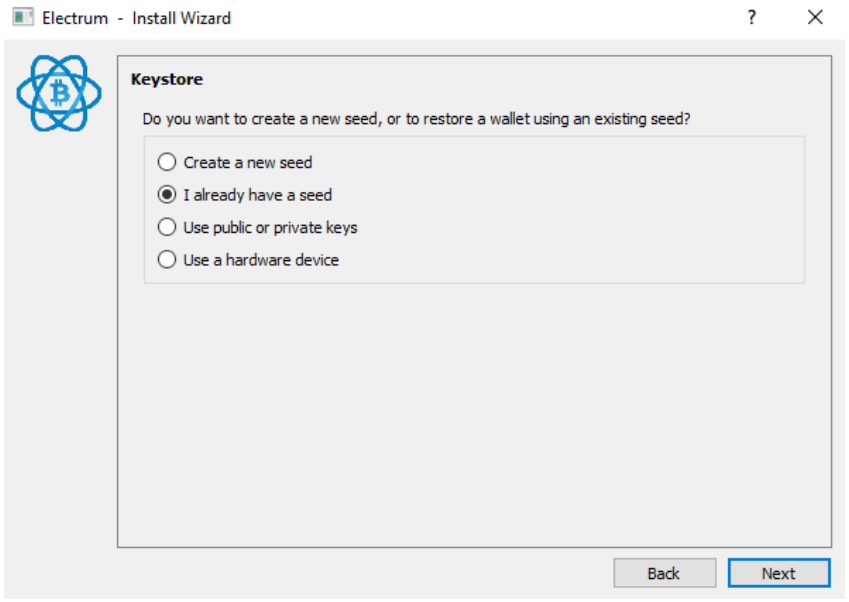
Potete dare al wallet il nome che desiderate, ad esempio lasciare default_wallet o mettere "Alberto" o qualsiasi altra cosa

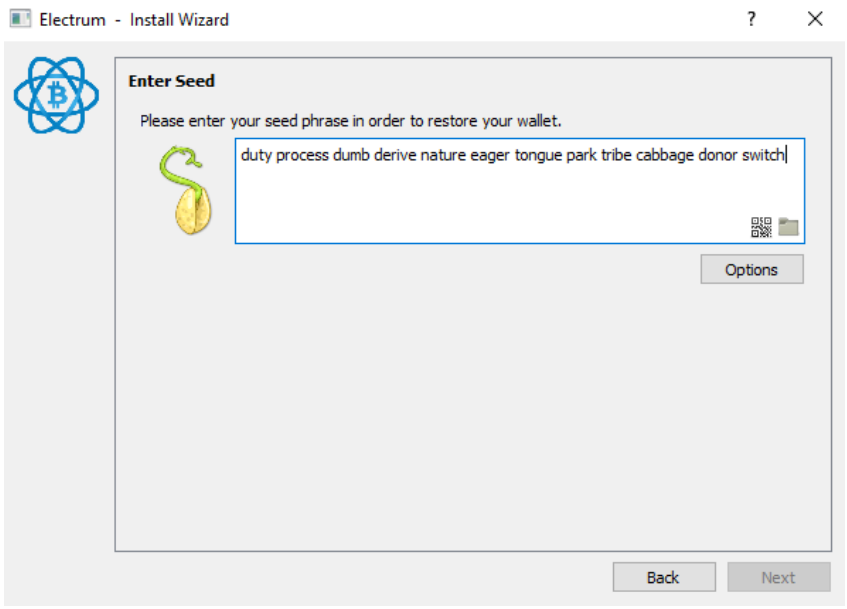


Una volta cliccato su "Next", nella schermata successiva selezionate "Standard Wallet"

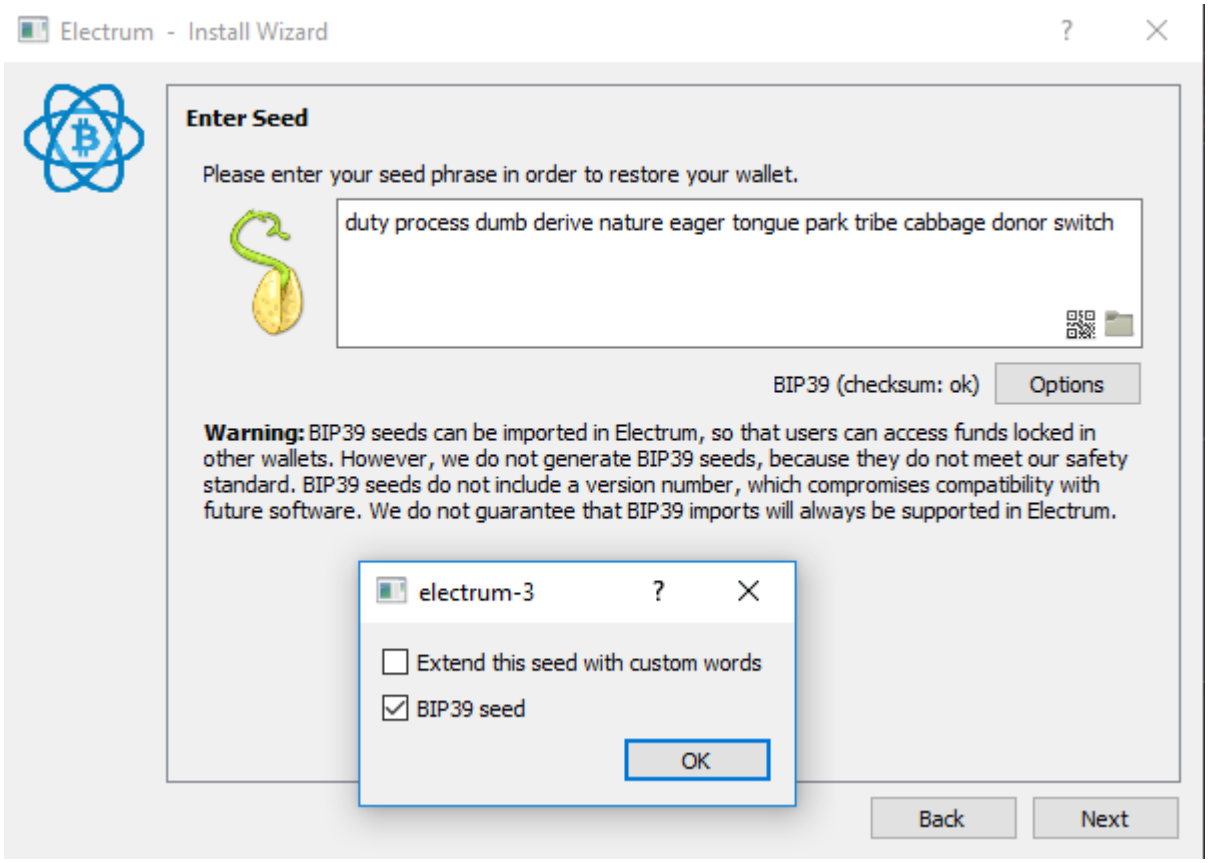


Quindi selezionate “I already have a seed” -> Next e poi incollate all’interno dello spazio le 12 parole del seed

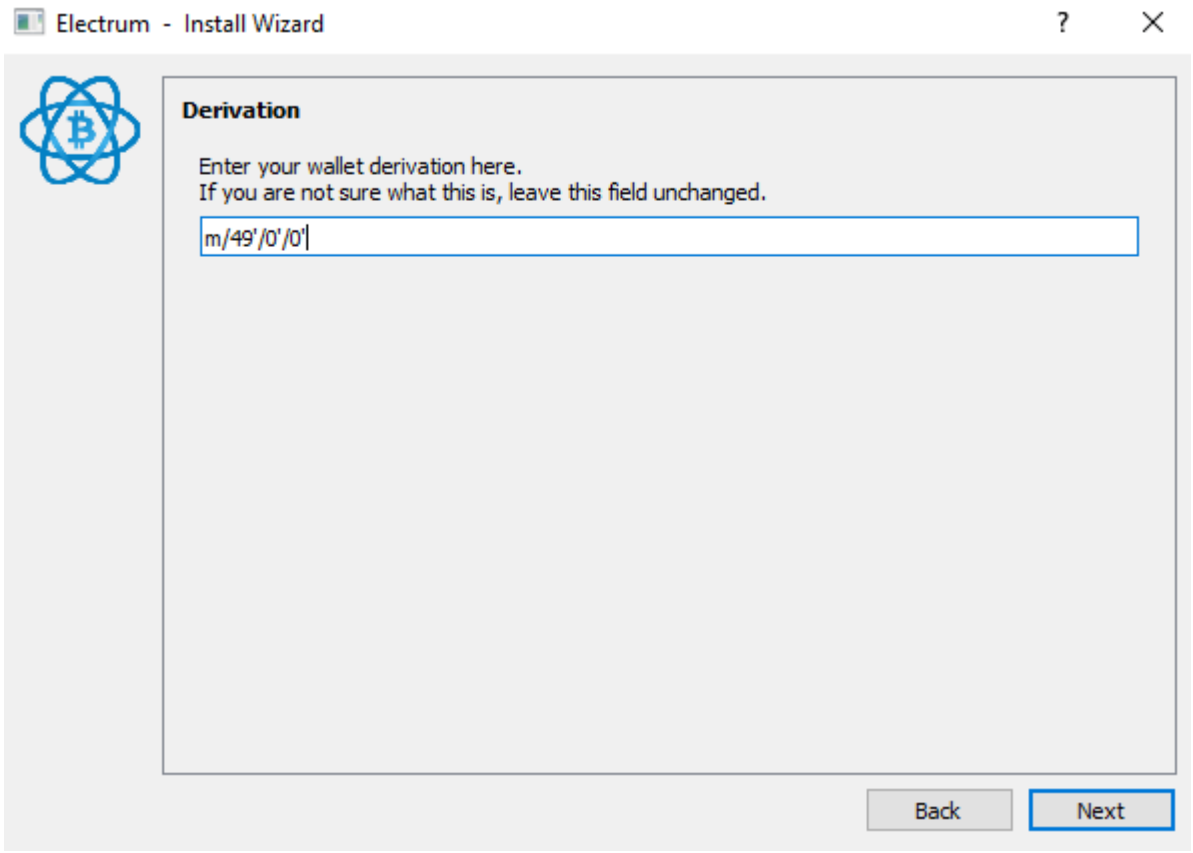




Cliccate su opzioni, quindi cliccate su “BIP39 seed”.

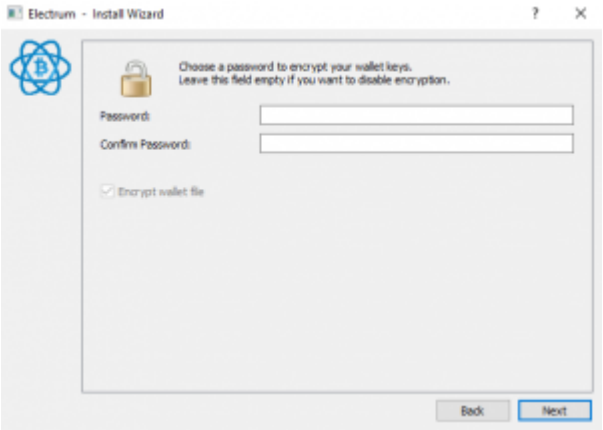


Nella schermata “Derivation” sostituite 44 con 49, di modo che la stringa risulti: m/49’/0’/0′

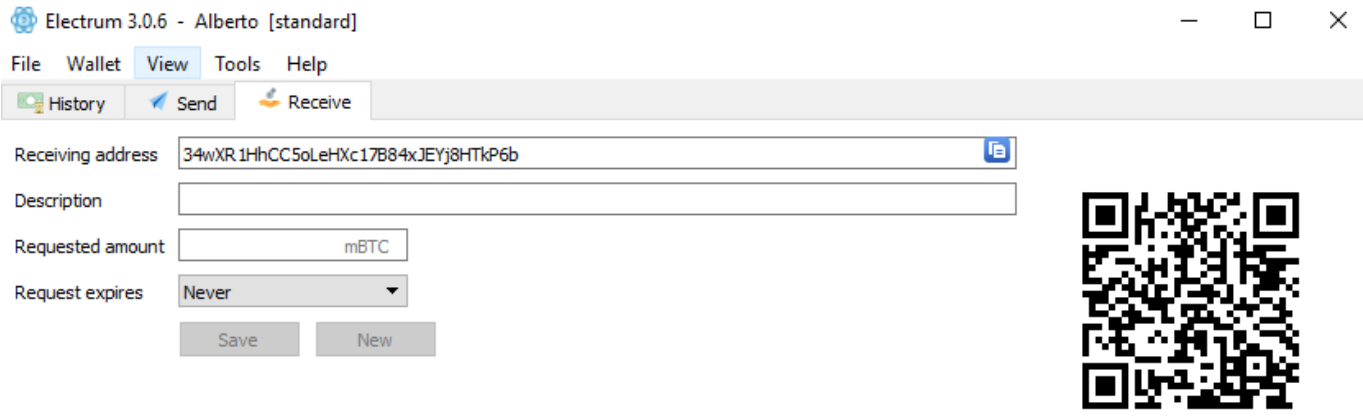


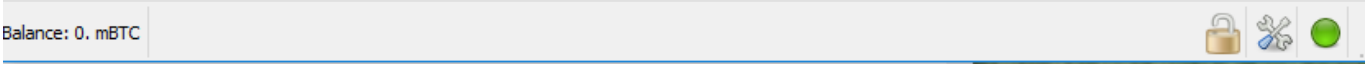
nota: nelle più recenti versioni di Electrum, compaiono tre opzioni, selezionate p2sh-segwit (p2wpkh-p2sh) come da screenshot:

Nella schermata successiva potete aggiungere una password per l’accesso al wallet. Senza password, chiunque abbia accesso al pc in cui è installato Electrum potrebbe aprire il wallet e inviare i soldi.



Complimenti, avete creato il vostro wallet. Se avete svolto correttamente ogni passaggio, andando sul tab “Ricevi” di Electrum dovreste vedere come primo indirizzo suggerito lo stesso presente al primo posto nella lista del tool di iancoleman.io, sotto a Derived Addresses. Nel caso d’esempio l’indirizzo era: 34wXR1HhCC5oLeHXc17B84xJEYj8HTkP6b





Infine, sotto tools -> preferences -> appearence potete modificare la lingua e impostare l’italiano, oppure impostare come unità di misura (Base unit) BTC anziché mBTC, poiché di default Electrum mostra i milli Bitcoin (1000mbtc = 1btc)

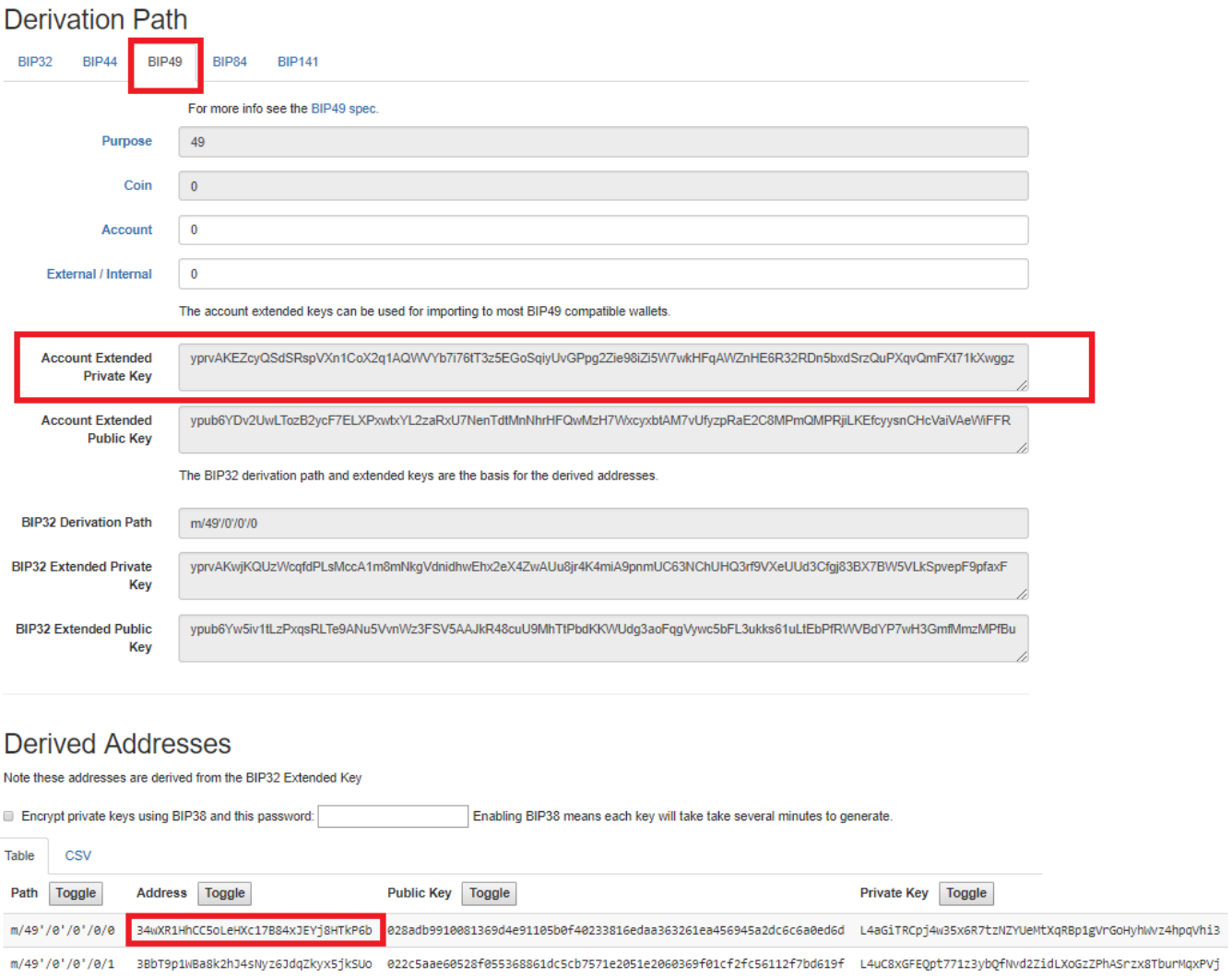
IMPORTARE IL WALLET SULL’APP ELECTRUM PER MOBILE

Sull’applicazione mobile non è possibile importare il wallet con il seed BIP39 con derivation path BIP49, perciò bisogna seguire un altro procedimento, valido sia per desktop che mobile e che ci permette di ottenere o importare lo stesso identico wallet:

1) creare uno standard wallet, ma anziché selezionare “I already have a seed” si selezioni “Use public or private keys”.

2) Quindi si incolli all’interno dello spazio la stringa che nel tool seed generator di Iancoleman è chiamata “**Account Extended Private Key**” (si trova sotto alla sezione Derivation Path, dove bisogna sempre fare attenzione di aver selezionato BIP49). Questa chiave è anche detta Master Private key.

3) Si noterà che importando questa private key il primo indirizzo di ricezione mostrato dall’app Electrum è sempre lo stesso, che nel nostro caso era 34wXR1HhCC5oLeHXc17B84xJEYj8HTkP6b. Fatta questa verifica, abbiamo appurato che il wallet è stato importato correttamente



Derivation Path

BIP32 | BIP44 | BIP49 | BIP84 | BIP141

For more info see the BIP49 spec.

Purpose	49
Coin	0
Account	0
External / Internal	0

The account extended keys can be used for importing to most BIP49 compatible wallets.

Account Extended Private Key	yprvAKEZcyQSdSRspVXn1CoX2q1AQWVYb7i76tT3z5EGoSqiyUvGPpg2Zie98iZi5W7wkHFqAWZnHE6R32RDn5bxdSrzQuPXqvQmFXt71kXwggz
Account Extended Public Key	ypub6YDv2UwLTozB2ycF7ELXPxwtxYL2zaRxU7NenTdtMnNhrHFQwMzH7WxcyxbtAM7vUfyzpRaE2C8MPmQMPRjiLKEfcyysnCHcVaiVAeWiFFR

The BIP32 derivation path and extended keys are the basis for the derived addresses.

BIP32 Derivation Path	m/49'/0'/0'/0
BIP32 Extended Private Key	yprvAKwjKQUzWcqfdPLsMccA1m8mNkgVdnidhwEhx2eX4ZwAUu8jr4K4miA9pnmUC63NChUHQ3rf9VXeUUd3Cfgj83BX7BW5VLkSpvepF9pfaxF
BIP32 Extended Public Key	ypub6Yw5iv1tLzPxqsRLTe9ANu5VvnWz3FSV5AAJkR48cuU9MhTtPbdKKWUdg3aoFqgVywc5bFL3ukks61uLtEbPfRWVBdYP7wH3GmfMmzMPfBu

Derived Addresses

Note these addresses are derived from the BIP32 Extended Key

Encrypt private keys using BIP38 and this password: Enabling BIP38 means each key will take take several minutes to generate.

Table | CSV

Path Toggle	Address Toggle	Public Key Toggle	Private Key Toggle
m/49'/0'/0'/0/0	34wXR1HhCC5oLeHXc17B84xJEYj8HTkP6b	028adb9910081369d4e91105b0f4023816edaa363261ea456945a2dc6c6a0ed6d	L4aGiTRCpj4w35x6R7tzNZYUeMtXqRBp1gVrGoHyhWvz4hpqVhi3
m/49'/0'/0'/0/1	3BbT9p1WBa8k2hJ4sNyz6JdqZkyx5jkSUo	022c5aae60528f055368861dc5cb7571e2051e2060369f01cf2fc56112f7bd619f	L4uC8xGFEQpt771z3ybQfNvd2ZidLXoGzZPhASrzx8TburMqxPVj

Tieniti aggiornato sulle news quotidiane più importanti seguendo la pagina facebook: https://www.facebook.com/albertodeluigi.news

Iscriviti alla newsletter del blog, riceverai una mail ad ogni nuovo articolo pubblicato