di Luca Cadonici

WALLET HARDWARE E CRIPTOVALUTE NELLE OPERAZIONI DI POLIZIA GIUDIZIARIA: DAL SEQUESTRO DEI DISPOSITIVI AL TRACCIAMENTO DELLE TRANSAZIONI

LUCA CADONICI si è laureato all'Università di Pisa avvicinandosi alla Sicurezza Informatica ed ottenendo la qualifica europea di Tecnico esperto della gestione dei servizi e della sicurezza della rete - liv.4 EQF (European Qualification Framework). È iscritto all'Albo dei Periti presso la Camera di Commercio di Pisa e opera come Consulente Tecnico di Parte, Ausiliario di Polizia Giudiziaria e Consulente Tecnico del Pubblico Ministero. Ha collaborato come Ausiliario di Polizia Giudiziaria e Consulente Tecnico del Pubblico Ministero nelle operazioni di Polizia Giudiziaria con i reparti di D.I.A., Polizia Postale, N.A.S e Nuclei Investigativi (CC), Nuclei valutari e tributari (GDF).

Il presente articolo è nato a seguito di esperienze professionali che hanno visto lo scrivente operare come Ausiliario di Polizia Giudiziaria in supporto al personale della Guardia di Finanza, e sviluppa le tematiche presentate nel corso della quinta edizione dell'evento annuale organizzato dall'Osservatorio Nazionale sull'Informatica Forense, tenutosi nella giornata del 18 ottobre 2019 ad Amelia, vicino Terni. Al personale di Polizia Giudiziaria presente, che ringrazio per l'attenzione e la partecipazione, vanno queste righe, sperando di poter offrire informazioni utili e spunti operativi in un ambito non ancora normato, in particolare dal punto di vista procedurale, durante le delicate fasi di perquisizione e sequestro.

Con il termine "criptovaluta", traduzione letterale dell'inglese *cryptocurrency*, si indica una rappresentazione digitale di valore basata sulla crittografia, consistente in un insieme di asset digitali paritari e decentralizzati di cui i *Bitcoin* sono ad oggi l'esempio più conosciuto e diffuso.
A differenza delle monete tradizionali, regolamentate e centralizzate da autorità riconosciute quali le banche centrali, le criptovalute utilizzano tecnologie di tipo *peer-to-peer (p2p)* su reti i cui nodi risultano costituiti da computer di utenti, paritari tra loro e situati in tutto il globo.

La sicurezza di gestione di questo sistema di scambio basato sulla crittografia asimmetrica è strettamente legata alla conservazione della *chiave privata*, il codice identificativo di ciascun conto che può essere usato per movimentare le criptovalute presenti nei vari DLT (*distributed ledger technology*), i registri pubblici alla base del sistema di scambio di criptomonete, prima fra tutti la *blockchain*, contenente lo storico delle movimentazioni dei *Bitcoin*, dalla loro creazione in poi.

1. Wallet di criptovalute

Con il termine **wallet** si indicano comunemente i sistemi hardware e software utilizzati per conservare le **chiavi pubbliche** e **private** necessarie per realizzare le transazioni in criptovaluta: le prime utilizzate per produrre indirizzi comunicabili a terzi al fine di effettuare le transazioni sui conti e le seconde utilizzate per firmare le transazioni in uscita. A monte della generazione delle *chiavi pubbliche* e *private* però, i sistemi di criptovalute generano un solo grande numero, il *seed* da cui derivano in modo differenti coppie multiple di *chiavi pubbliche* e *private* utilizzate sui *wallet*.
Chiunque sia in possesso del *seed* è in possesso dei *wallet* di criptomonete corrispondenti, in quanto può a sua volta generare le **chiavi pubbliche** o **private** che ne derivano.

Se il *seed* viene rubato o smarrito, di conseguenza, le monete custodite nei *wallet* diventano inaccessibili. Sintetizzando al massimo possiamo dire che ogni *wallet* non è altro che una coppia di chiavi, **pubblica** e **privata**, che possedere un *wallet* significa custodire queste chiavi e che un *hardware wallet* è un dispositivo che custodisce *wallet* di criptomonete.

Oltre ai *wallet hardware* che andremo a trattare dettagliatamente più avanti, le tipologie di *wallet* oggi presenti si possono riassumere nelle seguenti categorie:

Tipologia wallet	Caratteristiche	Esempi	Pro	Contro
Web	- Login tramite portale web - La chiave privata viene conservata sul server del fornitore del servizio	COINBASE XAPO UPHOLD COINAPULT	- Massima facilità di accesso - Possibilità di accedere con qualsiasi dispositivo	- Livello di sicurezza ridotto rispetto agli altri wallet - La chiave privata è memorizzata su server di terze parti.
Software	- Installazione di apposito applicativo su PC o dispositivo mobile - Chiave privata conservata su hard disk	ELECTRUM JAXX BLOCKCHAIN WALLET GREEN ADDRESS BITCOIN CORE BITGO ARMONY	- Facilità di accesso - Livello di sicurezza più alto rispetto ai wallet web	- Necessita della disponibilità fisica del dispositivo su cui è installato il software. - Vulnerabile ad attacchi informatici
Paper	- Supporto cartaceo sul quale la chiave privata viene stampata sotto forma di stringa alfanumerica o QR Code	www.bitaddress.org www.bitcoinpaperwallet.com www.walletgenerator.net	- Massima sicurezza logica (immune ad attacchi informatici)	- Chiave stampata in chiaro - Necessità delle massime misure di sicurezza fisica - La sottrazione del wallet corrisponde alla sottrazione del conto.

2. Wallet hardware

Data la maggior diffusione ed il crescente valore sul mercato, negli ultimi anni le criptovalute sono divenute il principale bersaglio di numerose minacce informatiche. Si sono registrati casi non solo di utenti, ma anche di portali dedicati i quali, a causa di una capacità di gestione non adeguata, hanno perso irrecuperabilmente l'accesso a fondi di criptovalute del valore di milioni di euro.

Significativi a tal proposito sono i casi della giapponese *Mt. Gox* (fallita nel 2014 per un ammanco di 450 milioni di dollari in bitcoin), della Canadese *Quadriga CX* (166 milioni di dollari in varie criptovalute inaccessibili dopo la morte del fondatore nel 2019) nonché dell'italiana *Bitgrail* (fallita nel 2018 registrando un ammanco di 150 milioni di euro in criptovaluta *Nano*).

Per rispondere all'esigenza di segretezza relativa alle **chiavi private**, sono stati introdotti sul mercato una serie di dispositivi elettronici denominati *hardware wallet*, utili ad accedere ai conti in criptomoneta senza dover in alcun modo rivelare o digitare il codice consistente nella *chiave privata associata* che resta occultata all'interno dell'hardware per l'intero ciclo di vita del dispositivo.

Ad oggi infatti i *wallet hardware* offrono infatti il più alto livello di sicurezza disponibile, eliminando i rischi di sottrazione della chiave dovuti alla memorizzazione su *hard disk (wallet software)* o su *server* di terze parti *(web wallet)* e offrendo comunque misure di sicurezza logica non presenti nei *paper wallet* quali appunto l'*occultamento* della chiave e l'autenticazione tramite PIN.

Le possibilità di interazione sono ridotte al minimo per incrementare le misure di sicurezza. Sono quindi comunemente assenti *Bluetooth*, *Wi-Fi*, alimentazione a batteria, lettore di impronte digitali e, solitamente, *touch screen*.

Inoltre gli *hardware wallet*, anche se collegati a un computer connesso a Internet, conservano le chiavi private in un'area del dispositivo a prova di manomissione. In questo modo le chiavi private restano *offline* anche se il dispositivo comunica con un computer collegato a Internet.

La sicurezza fisica dei *wallet* può essere infine incrementata attraverso misure quali l'occultamento o la conservazione in cassaforte o in cassette di sicurezza, agevolata dalle ridotte dimensioni dei suddetti, comprese tra la grandezza di una comune pendrive USB (es. *Ledger Nano* S 56,95 mm x 17,4 mm x 9,1 mm) fino a misure leggermente superiori, per dispositivi aventi schermo tra i 2,5 e 3,5 pollici (*Ledger Blue* 97 mm x 68 mm x 10 mm o *KeepKey* 38 mm x 93.5 mm x 12.2 mm).

Tipologia hardware	Sicurezza logica	Sicurezza fisica	Memorizzazione chiave	Vulnerabilità ad attacchi informatici	Cifratura chiave
Hardware	PIN	Cassaforte	Wallet	Ridotta	Sì
Web	Login	/	Cloud	Phishing Software malevolo Vulnerabilità applicative Vulnerabilità del provider	Sì
Software	Login	Locali protetti	Hard disk	Phishing Software malevolo Vulnerabilità applicative	Sì
Paper	/	Cassaforte	Supporto cartaceo (stringa alfanumerica e QR Code)	/	No

Tipologia hardware	Cifratura chiave	Disponibilità offline	Massima sicurezza logica	Massima sicurezza fisica	Memorizzazione esclusiva della chiave
Hardware	X	X	X	X	X
Web	X				
Software	X	X			X
Paper		X		X	X

3. Principi di funzionamento

Alla prima accensione di ogni dispositivo viene chiesto di immettere un PIN numerico che verrà richiesto ad ogni successiva accensione. Il PIN, di norma compreso tra le 4 e le 8 cifre, permette un numero massimo di tentativi, superati i quali il dispositivo viene resettato. In tal caso l'accesso ai fondi collegati potrà essere effettuato solo tramite la *recovery phrase* generata al momento della creazione del conto, ovvero della generazione della chiave privata.

La r*ecovery phrase* infatti è costituita da elenco di 12, 18 o 24 parole a seconda del dispositivo le quali, "tradotte" tramite opportuno algoritmo, contengono tutte le informazioni necessarie per ricostruire una chiave privata. Al momento della creazione del conto il dispositivo *hardware* genera una *recovery phrase* o *seed phrase* e invita l'utente a scriverla su carta. In questo modo, in caso di furto, manomissione o compromissione del dispositivo, si può importare la chiave in un nuovo *wallet*.

È essenziale quindi conservare la *recovery phrase* con le stessa cautele dei *wallet*, essendone a tutti gli effetti, un *backup* cartaceo. Una volta connesso il dispositivo al computer (o al dispositivo mobile se supportato e se si è il possesso di cavo OTG), si può procedere al *download* dell'apposito *software* di gestione quale *Ledger Live* o *Trezor Bridge*, con cui viene gestita la creazione e la gestione dei conti. Prioritaria alla gestione di ogni diversa tipologia di criptovaluta è il *download* dell'apposita *app*. Il *wallet* così configurato è infine pronto per la gestione dei conti.

4. La generazione dei report

Le *app* di gestione dei vari dispositivi presentano capacità di reportistica che sono fondamentali per costruire le attività dei fondi. L'accesso alle app di gestione dei *wallet*, assieme ai *report* che è possibile creare per ogni fondo, consente infatti di acquisire i seguenti elementi chiave per l'analisi dei fondi:

- account collegati
- nome account
- ID account (sui *Ledger* in formato *xpub*[1])
- tipologia di criptovalute dei fondi
- importo totale fondi
- storico delle transazioni
- ID di transazione
- indirizzi di ricezione e invio

1 Il formato *xPub* (*extended Public Key*) consiste in un'unica stringa alfanumerica che consente una visualizzazione completa per tutte le transazioni, gli indirizzi e i saldi in un portafoglio specifico, permettendo di generare gli indirizzi utilizzati per le transazioni senza rivelare la chiave pubblica utilizzata. Concettualmente può essere considerato una visualizzazione in "sola lettura" del portafoglio.

- data e ora delle transazioni
- importo delle transazioni
- tipo di operazione (invio o ricezione)

Si riportano di seguito alcuni esempi di report forniti dagli applicativi associati ai *wallet* presi fin qui in esame.
La differenza principale tra la reportistica dei due *wallet* leader del mercato è l'inclusione dell'ammontare totale del fondo nei report *Trezor*, assente nei *Ledger* che invece riportano il valore delle commissioni[2] e *l'account ID* in forma *xpub*.

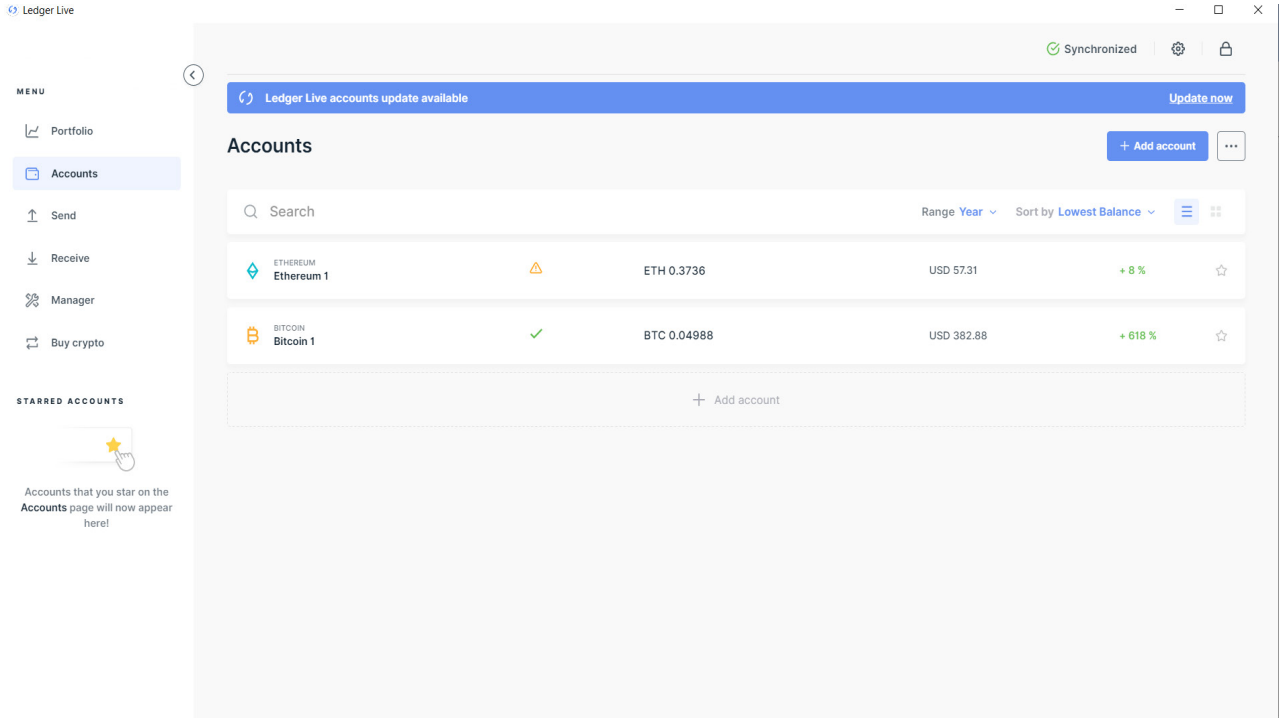


Fig.1 - Ledger live

Operation Date	Currency Ticker	Operation Type	Operation Amount	Operation Fees	Operation Hash	Account Name	Account id
2019-10-13T20:30:18.000Z	BTC	OUT	0.00130488	0.00000488	8305b8232eeb28580035338b3e6de8fea860970c3269b6b17663688c3c4ed8cf	Bitcoin 1	xpub6DFyHAUFP4vYGw8Jj1kB958mwdiEDNeht5Hy6FFpR9CUAeduJ4hBaZjRNGufhFq5idWRC4HihbW1mNBYmIdO7fvNxmtSKH6TrNxUjbj9Y23
2019-05-03T11:02:33.000Z	BTC	IN	0.018488	0.00006309	e3a38f6e4dec1eb28f4457e1e3175c631728e029c036bc926a6e03d0c769e8fc	Bitcoin 1	xpub6DFyHAUFP4vYGw8Jj1kB958mwdiEDNeht5Hy6FFpR9CUAeduJ4hBaZjRNGufhFq5idWRC4HihbW1mNBYmIdO7fvNxmtSKH6TrNxUjbj9Y23
2019-04-10T12:30:39.000Z	BTC	OUT	0.0024036	0.0003036	06df838694dc34df2a216b52ff5a1e465002f15cfcb2d9a049ae611894f69a1a	Bitcoin 1	xpub6DFyHAUFP4vYGw8Jj1kB958mwdiEDNeht5Hy6FFpR9CUAeduJ4hBaZjRNGufhFq5idWRC4HihbW1mNBYmIdO7fvNxmtSKH6TrNxUjbj9Y23
2019-03-31T00:31:50.000Z	BTC	OUT	0.00110736	0.00010736	c4e38c8bce22f8a070f955a1c813ec16421be4c8413bec9e36182a8f9b856774	Bitcoin 1	xpub6DFyHAUFP4vYGw8Jj1kB958mwdiEDNeht5Hy6FFpR9CUAeduJ4hBaZjRNGufhFq5idWRC4HihbW1mNBYmIdO7fvNxmtSKH6TrNxUjbj9Y23
2019-03-30T16:23:00.000Z	BTC	OUT	0.00289028	0.00009028	eb21d528cca8127035f6031b07cded5299ce4aad49d041f1a9c32f1298bb0308	Bitcoin 1	xpub6DFyHAUFP4vYGw8Jj1kB958mwdiEDNeht5Hy6FFpR9CUAeduJ4hBaZjRNGufhFq5idWRC4HihbW1mNBYmIdO7fvNxmtSKH6TrNxUjbj9Y23
2019-03-27T14:34:45.000Z	BTC	IN	0.00114007	0.00005993	692c68d07f677814b6f3be709c56a866388b29bc5583e8eb5565984a4ec89be4	Bitcoin 1	xpub6DFyHAUFP4vYGw8Jj1kB958mwdiEDNeht5Hy6FFpR9CUAeduJ4hBaZjRNGufhFq5idWRC4HihbW1mNBYmIdO7fvNxmtSKH6TrNxUjbj9Y23
2019-03-27T13:53:38.000Z	BTC	OUT	0.00253156	0.00008052	57ed1f57c380fc8f001a6026da286a89ab4214134dd297041a05b84c53a1d1c5	Bitcoin 1	xpub6DFyHAUFP4vYGw8Jj1kB958mwdiEDNeht5Hy6FFpR9CUAeduJ4hBaZjRNGufhFq5idWRC4HihbW1mNBYmIdO7fvNxmtSKH6TrNxUjbj9Y23
2019-03-27T13:04:04.000Z	BTC	IN	0.026523	0.00004106	3190d0f114eb6f8cdce9aba0740dc1abcf74aa6019a3ac928239795518cfb191	Bitcoin 1	xpub6DFyHAUFP4vYGw8Jj1kB958mwdiEDNeht5Hy6FFpR9CUAeduJ4hBaZjRNGufhFq5idWRC4HihbW1mNBYmIdO7fvNxmtSKH6TrNxUjbj9Y23
2019-03-25T19:59:38.000Z	BTC	IN	0.013664	0.00001397	05cfa55611114e7c0029b3763a6478c5d38382a984834c9d0c5b8fd0fd67c4ac	Bitcoin 1	xpub6DFyHAUFP4vYGw8Jj1kB958mwdiEDNeht5Hy6FFpR9CUAeduJ4hBaZjRNGufhFq5idWRC4HihbW1mNBYmIdO7fvNxmtSKH6TrNxUjbj9Y23

Fig.2 - Report Ledger live

2 Corrispettivo dell'inglese *fees* con cui si indicano le tariffe pagate ad un *miner* per l'inclusione della transazione nella *blockchain*.

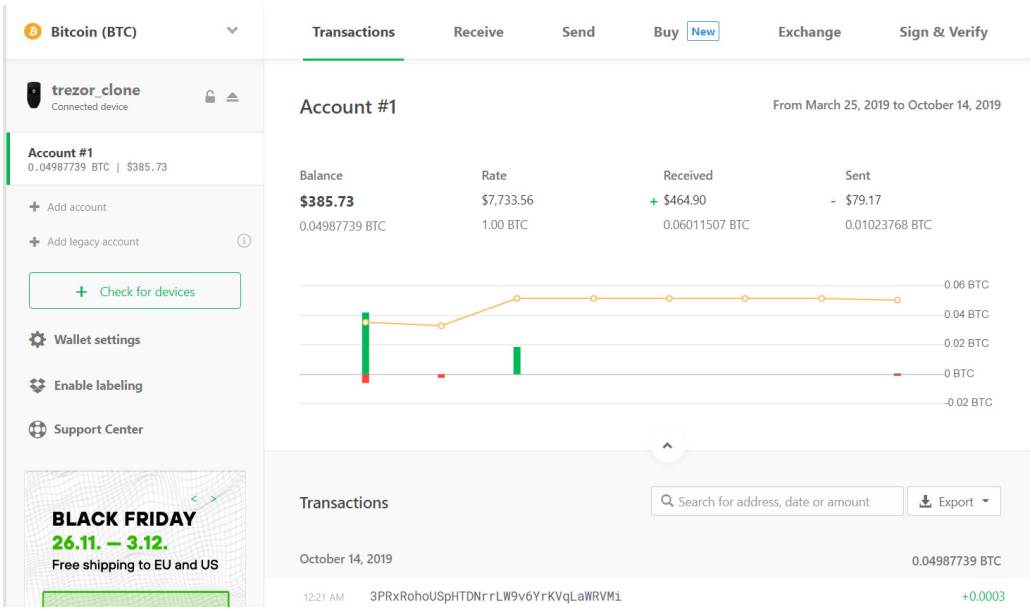


Fig.3 - Trezor Chrome Extension

TREZOR

Account #1 - BTC

Date	Time	TX id	Address	TX type	Value	TX total	Balance
2019-10-14	00:21:34	8d482e4c0ef42146c8a133018fb22c9207e58e2bc50727c991cb734532c603f9	3PRxRohoUSpHTDNrrLW9v6YrKVqLaWRVMi	IN	0.0003	0.0003	0.04987739
2019-10-13	21:49:50	8305b8232eeb28580035338b3e6de8fea860970c3269b6b17663688c3c4ed8cf	1Fd9ottDK1rqLZLCGnXac6XsY37HvRWRF4	OUT	0.0013	-0.00130488	0.04957739
2019-05-03	12:03:26	e3a38f6e4dec1eb28f4457e1e3175c631728e029c036bc926a6e03d0c769e8fc	3FG9xvTY2Jyqgqp5ch6YNCRhuMGH3XSzKo	IN	0.018488	0.018488	0.05088227
2019-04-10	13:34:10	06df838694dc34df2a216b52ff5a1e465002f15cfcb2d9a049ae611894f69a1a	3H1XqcwDrMqGXv7cumf2rFDWgdUjH8yrG5	OUT	0.0021	-0.0024036	0.03239427
2019-03-31	01:32:28	c4e38c8bce22f8a070f955a1c813ec16421be4c8413bec9e36182a8f9b856774	1LJFJZRpB7n28uS1ozWjpF8GzP5K94KQpS	OUT	0.001	-0.00110736	0.03479787
2019-03-30	17:41:59	eb21d528cca8127035f6031b07cded5299ce4aad49d041f1a9c32f1298bb0308	3C9ncBfwhs1Cdjm2dQXjUrYMoYBeHjk9BZ	OUT	0.0028	-0.00289028	0.03590523
2019-03-27	15:36:43	692c68d07f677814b6f3be709c56a866388b29bc5583e8eb5565984a4ec89be4	3AB74BJoxNfUw1CiNTRMrd1iJuM1pszBNs	IN	0.00114007	0.00114007	0.03879551
2019-03-27	15:28:33	3190d0f114eb6f8cdce9aba0740dc1abcf74aa6019a3ac928239795518cfb191	3FG9xvTY2Jyqgqp5ch6YNCRhuMGH3XSzKo	IN	0.026523	0.026523	0.03765544
2019-03-27	15:22:52	57ed1f57c380fc8f001a6026da286a89ab42141344dd297041a05b84c53a1d1c5	3C8k9aKFNvrdnMVY1BxpVgrxqAM1k7kzM6	OUT	0.00245104	-0.00253156	0.01113244
2019-03-25	21:26:35	05cfa55611114e7c0029b3763a6478c5d38382a984834c9d0c5b8fd0fd67c4ac	3FG9xvTY2Jyqgqp5ch6YNCRhuMGH3XSzKo	IN	0.013664	0.013664	0.013664

Fig.4 - Report Trezor Chrome Extension

5. I wallet hardware nelle operazioni di Polizia Giudiziaria

I *wallet hardware* sequestrati possono essere utilizzati per l'accesso e la ricostruzione dello storico dei fondi qualora si sia in possesso del PIN o nel caso in cui questo venga comunicato dall'indagato. Qualora il PIN non venga comunicato, è possibile effettuare la clonazione dei *wallet* importando il *seed* su nuovi dispositivi dal PIN concordato. L'operazione è sempre possibile nel caso si riescano ad acquisire i *recovery sheet* associati ad ogni *wallet*. Tale ipotesi operativa è applicabile anche nei casi di distruzione, malfunzionamento o di mancato rinvenimento dei *wallet*.

Composto da 12, 18 o 24 parole il *seed* permette di ricostruire la *Master Key* da cui sono derivate le chiavi in un *wallet* in ordine deterministico. Alla base di ciò sta il concetto di «portafoglio deterministico gerarchico». Nello specifico si considera un portafoglio deterministico, qualsiasi portafoglio per il quale una determinata chiave privata può essere recuperata se si è in possesso di due elementi:

- il *seed*
- l'identificativo/numero di sequenza della chiave

Un portafoglio deterministico gerarchico inizia con una singola coppia di chiavi principale in cui la chiave privata è il *seed*: a partire da essa saranno generate tutte le successive chiavi figlie. È possibile quindi, ricostruendo la chiave principale, generare nuovamente tutte le chiavi che ne sono derivate.

6. I principali standard dei seed: BIP32, BIP39 e BIP44

BIP32 è stato il primo *standard* di *seed* per *wallet* deterministici gerarchici. Ad esso sono seguiti i più recenti standard **BIP39**, **BIP44**. **BIP32**, lo standard alla base dei *wallet hardware*, è costituito da una stringa esadecimale di 512 bit in grado di generare la *master key* di un *wallet*. **BIP 44** è un'ulteriore implementazione dello *standard* che permette di creare più account di criptovalute a partire da un'unica *master key*. **BIP39** invece costituisce lo *standard* "mnemonico" a partire dal quale è possibile utilizzare una sequenza di parole per generare la stringa esadecimale a 512 bit alla base dei seed **BIP32** e **BIP44**.
Il processo di conversione della *passphrase* dello *standard* **BIP39** nei valori esadecimali alla base degli standard **BIP32** e **BIP34** può essere effettuato tramite il *Mnemonic Code Converter* sviluppato da Ian Coleman e reperibile al seguente indirizzo: https://iancole-

man.io/bip39/. La conversione *offline*, preferibile dal punto di vista della sicurezza, è possibile tramite apposita versione scaricabile da *Github*: https://github.com/iancoleman/bip39

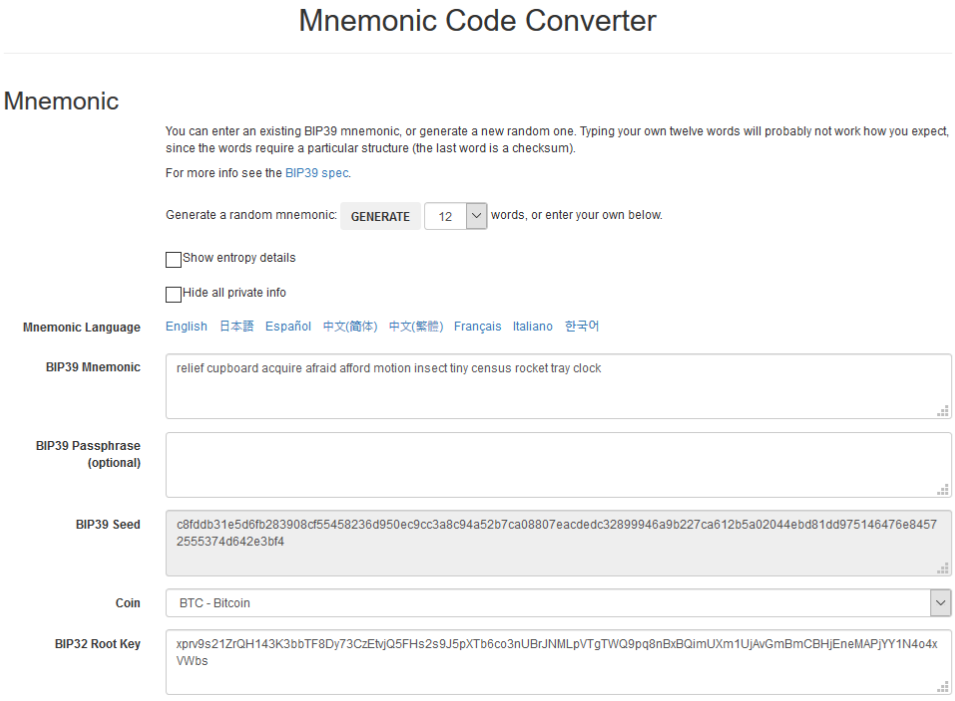


Fig.5 - Esempio di stringa di 12 parole convertita usando lo standard BIP39

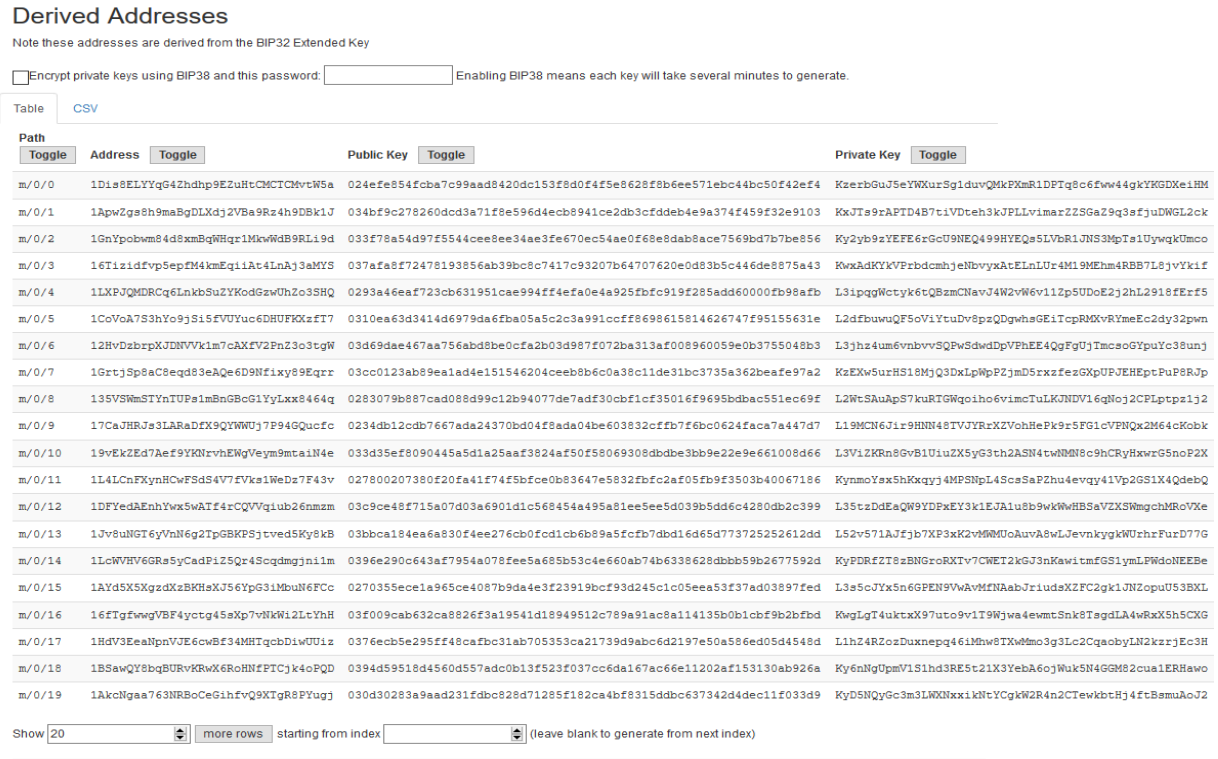
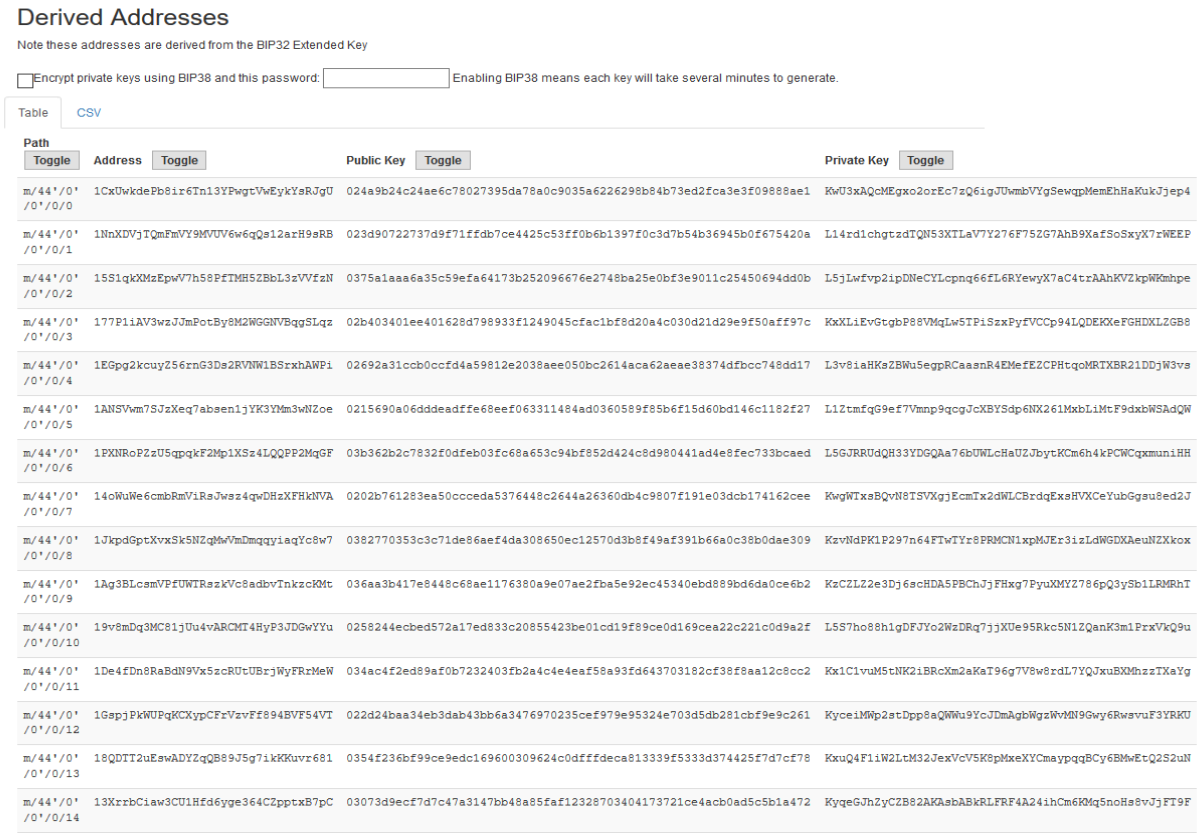


Fig.6 - Conversione della stringa precedente da BIP39 a BIP32



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 several minutes to generate.

Table CSV

Path Toggle	Address Toggle	Public Key Toggle	Private Key Toggle
m/44'/0'/0'/0/0	1CxUwkdePb8ir6Tn13YPwgtVwEykYsRJgU	024a9b24c24ae6c78027395da78a0c9035a6226298b84b73ed2fca3e3f09888ae1	KwU3xAQcMEgxo2orEc7zQ6igJUwmbVYgSewqpMemEhHaKukJjep4
m/44'/0'/0'/0/1	1NnXDVjTQmFmVY9MVUV6w6qQs12arH9sRB	023d90722737d9f71ffdb7ce4425c53ff0b6b1397f0c3d7b54b36945b0f675420a	L14rd1chgtzdTQN53XTLaV7Y276F75ZG7AhB9XafSoSxyX7rWEEP
m/44'/0'/0'/0/2	15S1qkXMzEpwV7h58PfTMH5ZBbL3zVVfzN	0375a1aaa6a35c59efa64173b252096676e2748ba25e0bf3e9011c25450694dd0b	L5jLwfvp2ipDNeCYLcpnq66fL6RYewyX7aC4trAAhKVZkpWKmhpe
m/44'/0'/0'/0/3	177P1iAV3wzJJmPotBy8M2WGGNVBqgSLqz	02b403401ee401628d798933f1249045cfac1bf8d20a4c030d21d29e9f50aff97c	KxXLiEvGtgbP88VMqLw5TPiSzxPyfVCCp94LQDEKXeFGHDXLZGB8
m/44'/0'/0'/0/4	1EGpg2kcuyZ56rnG3Ds2RVNW1BSrxhAWPi	02692a31ccb0ccfd4a59812e2038aee050bc2614aca62aeae38374dfbcc748dd17	L3v8iaHKsZBWu5egpRCaasnR4EMefEZCPHtqoMRTXBR21DDjW3vs
m/44'/0'/0'/0/5	1ANSVwm7SJzXeq7absen1jYK3YMm3wNZoe	0215690a06dddeadffe68eef063311484ad0360589f85b6f15d60bd146c1182f27	L1ZtmfqG9ef7Vmnp9qcgJcXBYSdp6NX261MxbLiMtF9dxbWSAdQW
m/44'/0'/0'/0/6	1PXNRoPZzU5qpqkF2Mp1XSz4LQQPP2MqGF	03b362b2c7832f0dfeb03fc68a653c94bf852d424c8d980441ad4e8fec733bcaed	L5GJRRUdQH33YDGQAa76bUWLcHaUZJbytKCm6h4kPCWCqxmuniHH
m/44'/0'/0'/0/7	14oWuWe6cmbRmViRsJwsz4qwDHzXFHkNVA	0202b761283ea50ccceda5376448c2644a26360db4c9807f191e03dcb174162cee	KwgWTxsBQvN8TSVXgjEcmTx2dWLCBrdqExsHVXCeYubGgsu8ed2J
m/44'/0'/0'/0/8	1JkpdGptXvxSk5NZqMwVmDmqqyiaqYc8w7	0382770353c3c71de86aef4da308650ec12570d3b8f49af391b66a0c38b0dae309	KzvNdPK1P297n64FTwTYr8PRMCN1xpMJEr3izLdWGDXAeuNZXkox
m/44'/0'/0'/0/9	1Ag3BLcsmVPfUWIRszkVc8adbvTnkzcKMt	036aa3b417e8448c68ae1176380a9e07ae2fba5e92ec45340ebd889bd6da0ce6b2	KzCZLZ2e3Dj6scHDA5PBChJjFHxg7PyuXMYZ786pQ3ySb1LRMRhT
m/44'/0'/0'/0/10	19v8mDq3MC81jUu4vARCMT4HyP3JDGwYYu	0258244ecbed572a17ed833c20855423be01cd19f89ce0d169cea22c221c0d9a2f	L5S7ho88h1gDFJYo2WzDRq7jjXUe95Rkc5N1ZQanK3m1PrxVkQ9u
m/44'/0'/0'/0/11	1De4fDn8RaBdN9Vx5zcRUtUBrjWyFRrMeW	034ac4f2ed89af0b7232403fb2a4c4e4eaf58a93fd643703182cf38f8aa12c8cc2	Kx1C1vuM5tNK2iBRcXm2aKaT96g7V8w8rdL7YQJxuBXMhzzTXaYg
m/44'/0'/0'/0/12	1GspjPkWUPqKCXypCFrVzvFf894BVF54VT	022d24baa34eb3dab43bb6a3476970235cef979e95324e703d5db281cbf9e9c261	KyceiMWp2stDpp8aQWWu9YcJDmAgbWgzWvMN9Gwy6RwsvuF3YRkU
m/44'/0'/0'/0/13	18QDTT2uEswADYZqQB89J5g7ikKKuvr681	0354f236bf99ce9edc169600309624c0dfffdeca813339f5333d374425f7d7cf78	KxuQ4F1iW2LtM32JexVcV5K8pMxeXYCmaypqqBCy6BMwEtQ2S2uN
m/44'/0'/0'/0/14	13XrrbCiaw3CU1Hfd6yge364CZpptxB7pC	03073d9ecf7d7c47a3147bb48a85faf12328703404173721ce4acb0ad5c5b1a472	KyqeGJhZyCZB82AKAsbABkRLFRF4A24ihCm6KMq5noHs8vJjFT9F

Fig.7 - Conversione della stringa precedente da BIP39 a BIP44 (account 0)

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 several minutes to generate.

Table CSV

Path Toggle	Address Toggle	Public Key Toggle	Private Key Toggle
m/44'/0'/1'/0/0	12Y5jTs9FrCWMFmmZwAQGyaFc65bQdK5tc	029daa4ce9d17cb59afc01b3a4cabdf4ce748288763 9a994fbf0a9278aa436cb1d	L2qgh9GWHLAWuTwnyhnBuWthcRJJprWvRnxNjaBEii2N4KTFBA19
m/44'/0'/1'/0/1	1HsrWHrAQ69r3BciWpGeCVWZQ9sEQvZu7A	02328738786e444c8e2334377af199efb4e8238582065c721e84870b6e18d2560e	KxiKcRDFTKQFqB8qT9aDpgEmyffXiYSB7LWkfWz9A6G5Tw1zYBGU
m/44'/0'/1'/0/2	1PTWSLw9poADwxcs8WxnFREAhZ9SYBywkw	02e3f6e5482925436fea43a43ec4379e4d85427a2ec8bff3030456041c290bef4d	KzxgFNiuzEaiaBzD4Rn1jB3TxUQkrTeivfpqCFTXJUYbReiJsd9T
m/44'/0'/1'/0/3	15uDpQpM5wjFDhLYdbaQVqRcJFXyVce4xD	026fe0cb331c748a9a8293a5da2f13e7449d67e7d13df5bef7258f6eb6ea204d6c	L1DKXibkRnBHXjqW3MVnnZRdKuG3CmBCyStzNCvmQJzVkNftmTtp
m/44'/0'/1'/0/4	1KpQk4MfNGKxBwEkjSxd5qBPSgCgyu7pTT	02c6606c9a0836f55756583b1d6e3c8903ff0f5faa461cab3d88bfc6f0579b3dd2	L3Yu4gxTsThxBxMyRd1fcZt9QZBhwALNrTWgJXveZvebFUQzzpYc
m/44'/0'/1'/0/5	1QGuUSaweiU9MyaEuYoxNMwZ5nyetb4hK8	03d8a17c2320f2c34569fa4e9dec878874003e2813151bd2294c6ac8084885c9b2	Kz8Jo6PMJ9Y99rmcp2wREF6g1oYB59fQMh5LcAaa6cr4yeajNcKT
m/44'/0'/1'/0/6	14PgzTCuzWHKWjiUX6o9CSNzcrAYLsp6P5	02de83a19901db84a5a57d00ccae78fb1eb9f4b8a97f896e0b35d6cc677e8e32bc	L2MeNqZ3SW9gzwfgQU3JWs1Z8EedyeHD9iLRC6m4ZxZVvufxwfGc
m/44'/0'/1'/0/7	1AU6xAatBbQovP9R6khe9EiEpGX5Zf5p8o	025d41f983c2d4f621327894bd9c3ef0cf7e1c9e4c73f722c5b0f4291ee98b4079	KzPjQTUZLUyti5LwULirPTRkfVgthqGekSHFHaMXXKDJF6LqJ1du
m/44'/0'/1'/0/8	1G8RTgpLK4XZbBqpfFKoWVWHKJCro36hgw	020f9090cc3dea5f17088d3163684a92df2cd145ed6cda3c6f0ba0b1c041a2b3b5	L4GBybGFgdvumtkENvQGoLHGd9o4ERnnKneeVbZ76dJ4DzDR1RCi
m/44'/0'/1'/0/9	1LF8DqTE8YFKWQF1eDXMonYoffCeeGnuRx	025ee854e3efe59489c9671b8025a8026463be9825c550a699fb8423c24e954bbc	KwzKaF2vh2Uy55r1qz6eDtqu6nzMhsm5ra5j534GjYyX3oLgwxAa
m/44'/0'/1'/0/10	1PuBibN4DRCBfGX1tGT4Qh6sBVR7vMJEaK	03e88d21dbc9f2a36e49fae94f537879a1653c56b92a898ab126fe2a52614308d4	L17ki9iPqkEqF1sCjMxkgf2w28d55wJuttn9Y3we1Ejx7W7eajav
m/44'/0'/1'/0/11	16FqmLJyJP6GuU8DBG8HqZ9tXCdJJwFQxi	035c469e6cf66fdbb3af4a03a4cfe23133dade476ed6d4566967cdad89e6093d1a	L3hWbUttYs5ft9KMHGcDaecqRqVxgvxbefxquGKxMeNFe8bWonr8
m/44'/0'/1'/0/12	1Ehht5Wa6HQUjahh4CLR4AgiwJYkg4jxBc	02fc14a0bdcec5fe40ee465637c670eb8e2b527c39e5554e1013fdb96ee7dad793	L1snyt9J6RiBUD6rPcbjGSD6BpKKhrcyA2bcG5TY55zgQQUDaSuo
m/44'/0'/1'/0/13	1GaDP82Yco9f4mggTD8Ym6YTWQchkXzQr8	03397dd76a2090bf33260305ba11042611c4039fc65971fae7516d322064f3724e	KxPGsG7aSwaxysXBtodEVQN8SrQYdDydPNT1c5KuVi7huxAEUKgA
m/44'/0'/1'/0/14	17zgarNt7swio7ZBdkFE8BIndUaEXXAbpX	025d9d6c1df4a4a0bbc5e0a6724bd3b4bd4363d1c45caad08e637ed0b9b782df77	KW8mGVRcd4mf9iPhQkFCMHhL4vS9WfvnfRNPPxNFVjYWBYA3ntBt

Fig.8 - Conversione della stringa precedente da BIP39 a BIP44 (account 1)

In questo modo, conoscendo gli *standard* supportati dai *wallet* è possibile ricostruire il *seed*, la *master key*, le chiavi private e pubbliche e, in ultimo, gli indirizzi utilizzati a partendo da semplici liste di parole memorizzate sui *recovery sheet*. Gli standard **BIP32/**

BIP39/BIP44 sono supportati da tutti i *wallet* presi in esame.

7. Note tecniche di acquisizione: sequestro e importazione dei seed

Possiamo suddividere le procedure di acquisizione dei *wallet* durante le operazioni di Polizia Giudiziaria nelle seguenti fasi:

8. individuazione
9. messa in sicurezza
10. repertazione
11. sequestro
12. acquisizione del PIN

(comunicato dall'indagato, via *social engineering*, tramite nota cartacea o memorizzato su computer/dispositivo mobile)

13. individuazione dei conti associati
14. generazione di reportistica tramite *software* associato

Nei casi di malfunzionamento, distruzione o mancata acquisizione del PIN o del dispositivo stesso, è possibile ricostruire il *seed* a partire dai *recovery sheet* importandolo su un nuovo dispositivo per verificare le chiavi pubbliche e private associate, l'importo dei conti, le criptovalute associate e lo storico delle transazioni. Nonostante l'importazione del *seed* possa generare uno o più cloni del dispositivo originale, che potrebbe in questo modo restare totalmente inalterato, la verifica sui dispositivi sequestrati è imprescindibile, in quanto non vi sono elementi certi che associno un *recovery sheet* ad un *wallet*: l'associazione di solito è effettuata sulla base di etichette o cartellini cartacei; pertanto anche un'unica accensione e connessione al dispositivo *host* è sempre indicata, qualora possibile.

8. Importazione dei seed da recovery sheet: Ledger Nano S

L'importazione del *seed* su nuovo dispositivo è possibile a partire dalla lista di parole riportate nel *recovery sheet*. Una volta acquisita la lista di 12, 18 o 24 parole è possibile realizzarne l'importazione seguendo le procedure richieste da ogni singolo dispositivo. Nel caso in esempio vedremo l'importazione di *seed* da e verso *Ledger Nano S*. Si noti che la conferma di ogni operazione viene fornita dalla simultanea pressione dei due pulsanti del *wallet*.

1. Scaricare l'applicativo *Ledger live*
2. Connettere il *wallet hardware* al dispositivo *host*
3. Premere i due pulsanti simultaneamente come richiesto sul *display*
4. Selezionare *cancel* (tasto sinistro) per *Configure as a New Device?*
5. Selezionare la spunta (tasto destro) per *Restore configuration?*
6. Scegliere il codice PIN
7. Selezionare la lunghezza della frase da immettere
8. Inserire la frase dando conferma con i pulsanti delle prime lettere di ogni parola finché questa non viene riconosciuta
9. Avviare l'applicativo *Ledger live*

Una volta terminata la procedura di importazione, si potranno verificare e analizzare i conti associati al *wallet* tramite l'applicativo *Ledger live*.

Fig.9 - Accesso tramite *Ledger live* e *seed* importato su *Ledger Nano S*

9. Importazione dei seed da recovery sheet: Trezor One

Anche in questo caso è possibile il *seed* sul dispositivo a partire dalla lista di parole riportate nel *recovery sheet*. Nello specifico, useremo lo stesso *seed* dell'esempio precedente, originariamente prodotto da un dispositivo *Ledger Nano S*.

1. Scaricare l'estensione *Trezor* per *browser Chrome*
2. Connettere il *wallet hardware* al dispositivo *host*
3. Effettuare le procedure di inizializzazione tramite *Trezor Chrome Extension*[3]
4. Inserire le parole del *recovery sheet* nell'ordine richiesto dal *wallet*
5. Accedere al *wallet* tramite *Trezor Chrome Extension*

Una volta terminata la procedura di importazione, si potranno verificare e analizzare i conti associati al *wallet* tramite *Trezor Chrome Extension*. ©

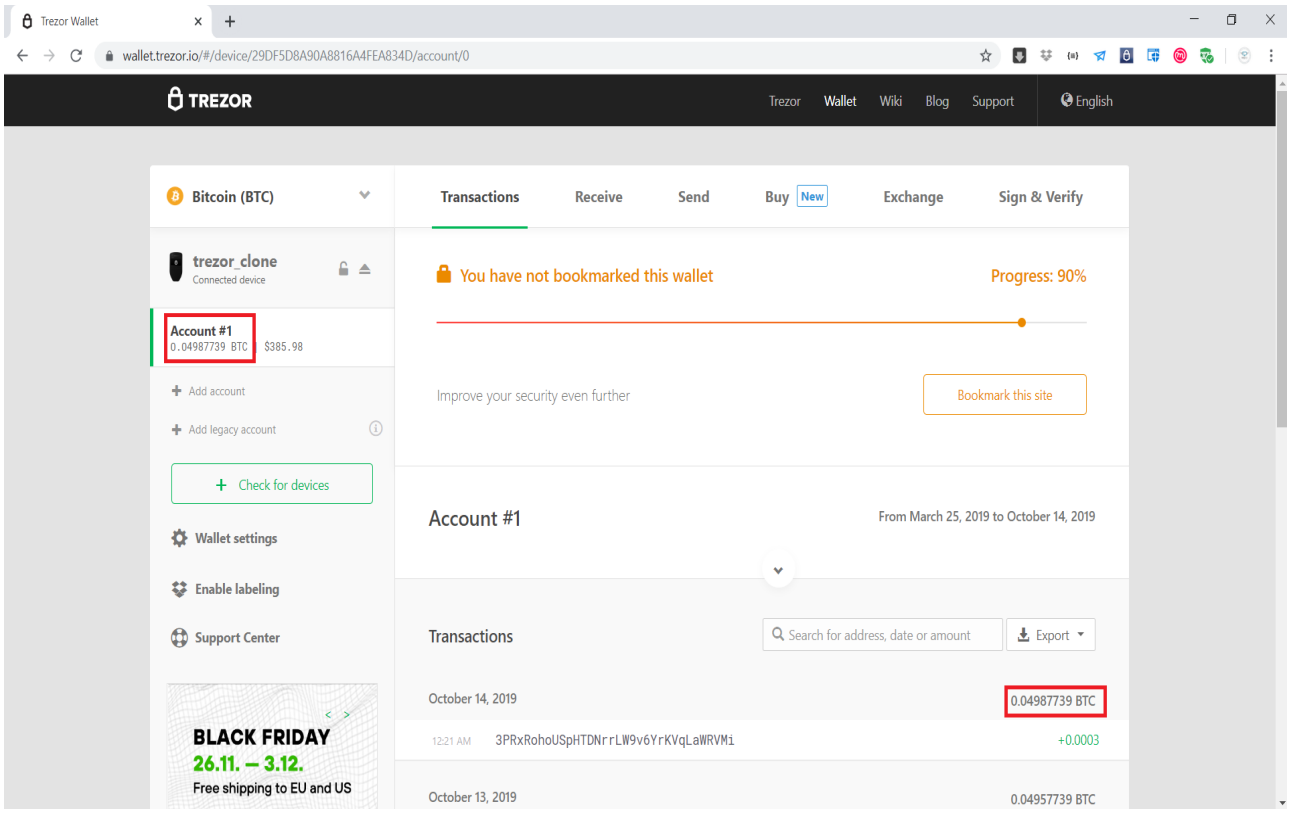


Fig.10 - *Trezor Chrome Extension* – il numero di *bitcoin* coincide con quelli nel *wallet Ledger* (0.04987739 BTC)

3 A differenza dei *Ledger*, nei dispositivi *Trezor* è possibile scegliere se abilitare la protezione tramite PIN e se aggiungere un'ulteriore *passphrase* di cifratura (nei *Ledger* il PIN è obbligatorio, mentre non è possibile inserire la *passphrase* addizionale di cifratura).

RIFERIMENTI

https://blog.trezor.io/satoshilabs-security-philosophy-manifesto-11791ac06f14
https://cryptonomist.ch/2019/06/01/bip32-bip39-bip44-differenze-seed-wallet/
https://www.ilsole24ore.com/art/fallisce-bitgrail-piattaforma-italiana-le-criptovalute-AE9Dg8LH
https://www.ilsole24ore.com/art/bitcoin-muore-fondatore-un-exchange-150milioni-fumo-perche-nessuno-sa-password-AF8cmnF
https://www.kaspersky.it/blog/cryptowallets/15418/
https://www.kaspersky.it/blog/hardware-wallets-hacked/16785/
https://wiki.trezor.io/Open-source_hardware