



# WALLET HARDWARE E CRIPTOVALUTE: dal sequestro dei dispositivi al tracciamento delle transazioni

Luca Cadonici

ONIF – Osservatorio Nazionale sull'Informatica Forense



# Criptovalute

- Rappresentazioni digitali di valore basata sulla **crittografia**, consistenti 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.

Luca Cadonici

ONIF – Osservatorio Nazionale sull'Informatica Forense



# 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
- **Seed** valore 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.

Luca Cadonici

ONIF – Osservatorio Nazionale sull'Informatica Forense



# Wallet di criptovalute

Wallet	Caratteristiche	Esempi	Pro	Contro
Web	<ul style="list-style-type: none"> <li>- Login tramite portale web</li> <li>- La chiave privata viene conservata sul server del fornitore del servizio</li> </ul>	<a href="#">COINBASE</a> <a href="#">XAPO</a> <a href="#">UPHOLD</a> <a href="#">COINAPULT</a>	<ul style="list-style-type: none"> <li>- Massima facilità di accesso</li> <li>- Possibilità di accedere con qualsiasi dispositivo</li> </ul>	<ul style="list-style-type: none"> <li>- Livello di sicurezza ridotto rispetto agli altri wallet</li> <li>- La chiave privata è memorizzata su server di terze parti.</li> </ul>
Software	<ul style="list-style-type: none"> <li>- Installazione di apposito applicativo su PC o mobile</li> <li>- Chiave privata su hard disk</li> </ul>	<a href="#">ELECTRUM</a> <a href="#">JAXX BLOCKCHAIN WALLET</a> <a href="#">GREEN ADDRESS</a> <a href="#">BITCOIN CORE</a> <a href="#">BITGO</a> <a href="#">ARMONY</a>	<ul style="list-style-type: none"> <li>- Facilità di accesso</li> <li>- Livello di sicurezza più alto rispetto ai wallet web</li> </ul>	<ul style="list-style-type: none"> <li>- Necessita della disponibilità fisica del dispositivo su cui è installato il software.</li> <li>- Vulnerabile ad attacchi informatici</li> </ul>
Paper	<ul style="list-style-type: none"> <li>- Supporto cartaceo sul quale la chiave viene stampata sotto forma di stringa alfanumerica o QR code</li> </ul>	<a href="http://www.bitaddress.org">www.bitaddress.org</a> <a href="http://www.bitcoinpaperwallet.com">www.bitcoinpaperwallet.com</a> <a href="http://www.walletgenerator.net">www.walletgenerator.net</a>	<ul style="list-style-type: none"> <li>- Massima sicurezza logica (immune ad attacchi informatici)</li> </ul>	<ul style="list-style-type: none"> <li>- Chiave stampata in chiaro</li> <li>- Necessità delle massime misure di sicurezza fisica</li> <li>- La sottrazione del wallet corrisponde alla sottrazione del conto.</li> </ul>

Luca Cadonici

ONIF – Osservatorio Nazionale sull'Informatica Forense



# Wallet hardware

- **Esigenze di sicurezza crescenti nella conservazione delle chiavi**
- *Mt. Gox* - fallita nel 2014 per un ammanco di **450 milioni di dollari in bitcoin**
- *Quadriga CX* - **166 milioni di dollari** in varie criptovalute inaccessibili dopo la morte del fondatore nel 2019
- *Bitgrail* - fallita nel 2018 registrando un ammanco di **150 milioni di euro** in criptovaluta *Nano*

Luca Cadonici

ONIF – Osservatorio Nazionale sull'Informatica Forense



# Wallet hardware

- **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*)
- 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.

Luca Cadonici

ONIF – Osservatorio Nazionale sull'Informatica Forense



# Wallet hardware

- **Dimensioni ridotte**
- La sicurezza fisica dei wallet può essere infine incrementata attraverso misure quali l'occultamento o la conservazione in cassaforte o in cassette di sicurezza.
- 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).

Luca Cadonici

ONIF – Osservatorio Nazionale sull'Informatica Forense



# Wallet hardware



**Trezor One**

Luca Cadonici

ONIF – Osservatorio Nazionale sull'Informatica Forense



# Wallet hardware



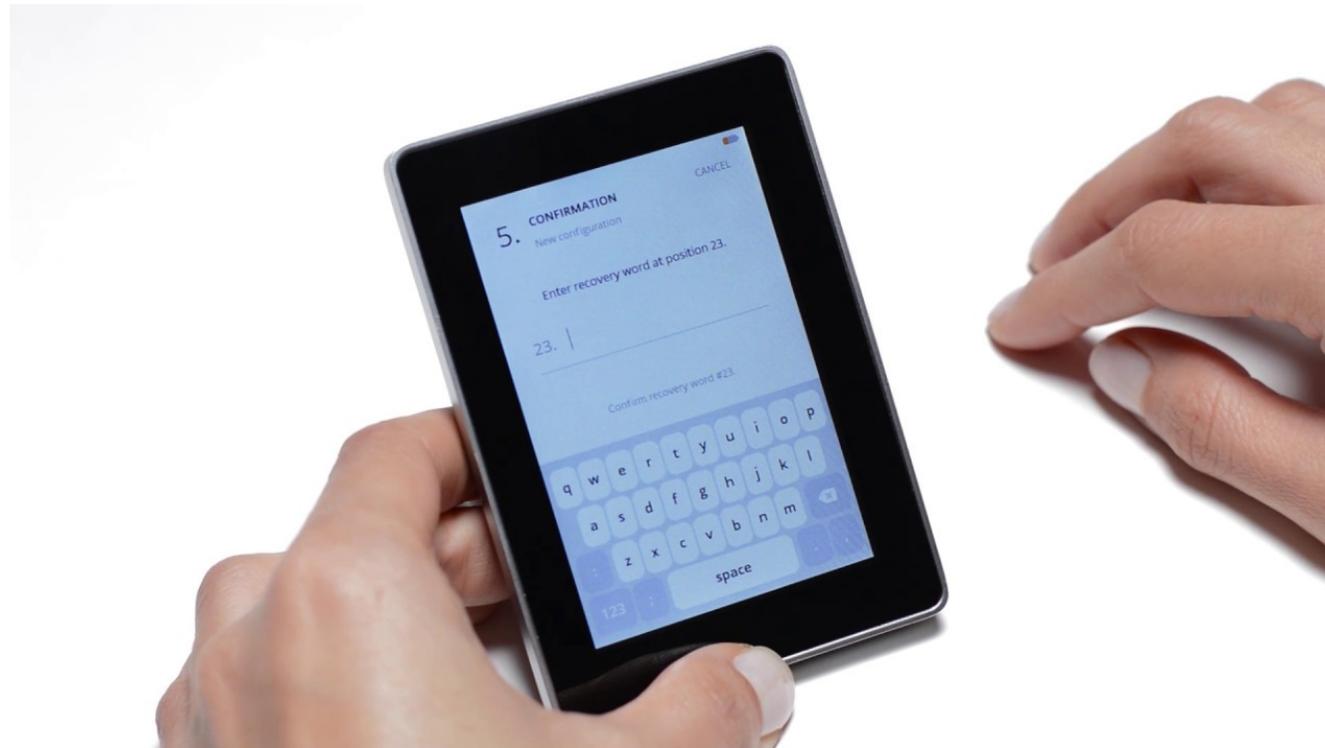
Ledger Nano S

Luca Cadonici

ONIF – Osservatorio Nazionale sull'Informatica Forense



# Wallet hardware



**Ledger Blue**

Luca Cadonici

ONIF – Osservatorio Nazionale sull'Informatica Forense



# Wallet hardware

- **Principi di funzionamento**
- Immissione di PIN, di norma compreso tra le 4 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.
- 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.

Luca Cadonici

ONIF – Osservatorio Nazionale sull'Informatica Forense



# Wallet hardware

- **Recovery phrase**
- 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.

Luca Cadonici

ONIF – Osservatorio Nazionale sull’Informatica Forense



# I principali wallet hardware

Luca Cadonici

ONIF – Osservatorio Nazionale sull'Informatica Forense



# Trezor



**Trezor One**



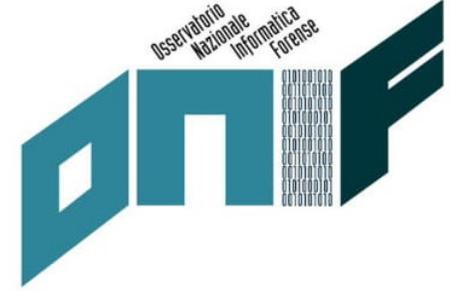
**Trezor Model T**

Luca Cadonici

ONIF – Osservatorio Nazionale sull'Informatica Forense



# Trezor



- *Bootloader* protetto da scrittura e una verifica del *firmware* all'accensione che avvertono l'utente di un'eventuale compromissione.
- I dispositivi **Trezor** utilizzano solo hardware e software *open source*, e supportano la protezione tramite PIN.
- L'interazione viene gestita per la gran parte tramite l'applicazione associata **Trezor Bridge**, mentre il dispositivo hardware viene utilizzato per confermare le transazioni. Sono presenti **estensioni Google Chrome Trezor**, che aumentano la facilità di gestione del dispositivo e dei conti associati.

Luca Cadonici

ONIF – Osservatorio Nazionale sull'Informatica Forense



# Trezor



- **Trezor**
- Dispositivi di autenticazione a due fattori (FIDO U2F)
- Password manager

Il gestore di password di Trezor può essere associato a i servizi cloud *Google Drive* e *Dropbox* per salvare le password in forma criptata. Il più recente **Model T** permette inoltre di salvare le password su microSD dedicata ottenendo uno storage totalmente locale

Luca Cadonici

ONIF – Osservatorio Nazionale sull'Informatica Forense



# Trezor



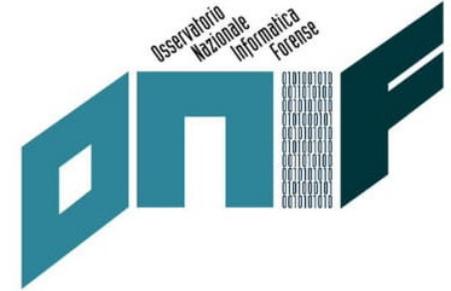
- **Trezor model T**
- Modello più recente
- Schermo di dimensioni maggiori (utile per verificare gli indirizzi)
- Inserimento dati tramite *touch screen* come misura di sicurezza aggiuntiva
- Dati cifrati su cloud o microSD (*password manager*)

Luca Cadonici

ONIF – Osservatorio Nazionale sull'Informatica Forense



# Ledger Nano



Ledger Nano S



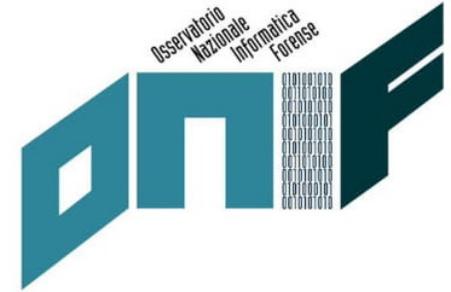
Ledger Nano X

Luca Cadonici

ONIF – Osservatorio Nazionale sull'Informatica Forense



# Ledger Nano



- Forma e dimensioni corrispondenti a una pendrive USB
- *Secure element* - hardware isolato da attacchi esterni, costituito da un chip di sicurezza in cui sono memorizzate le chiavi private
- Protezione tramite PIN
- Interazione tramite due tasti meccanici presenti su lato del dispositivo
- Indirizzo transazione visualizzato sul display
- Conferma tramite pressione simultanea dei due tasti.

Luca Cadonici

ONIF – Osservatorio Nazionale sull'Informatica Forense



# Ledger Nano



- Sblocco computer host tramite *Windows Hello*
- Cifratura mail tramite *OpenPGP*
- Autenticazione a due fattori (FIDO U2F)
- App *password manager* (password memorizzate su dispositivo)

Luca Cadonici

ONIF – Osservatorio Nazionale sull'Informatica Forense



# Ledger Nano



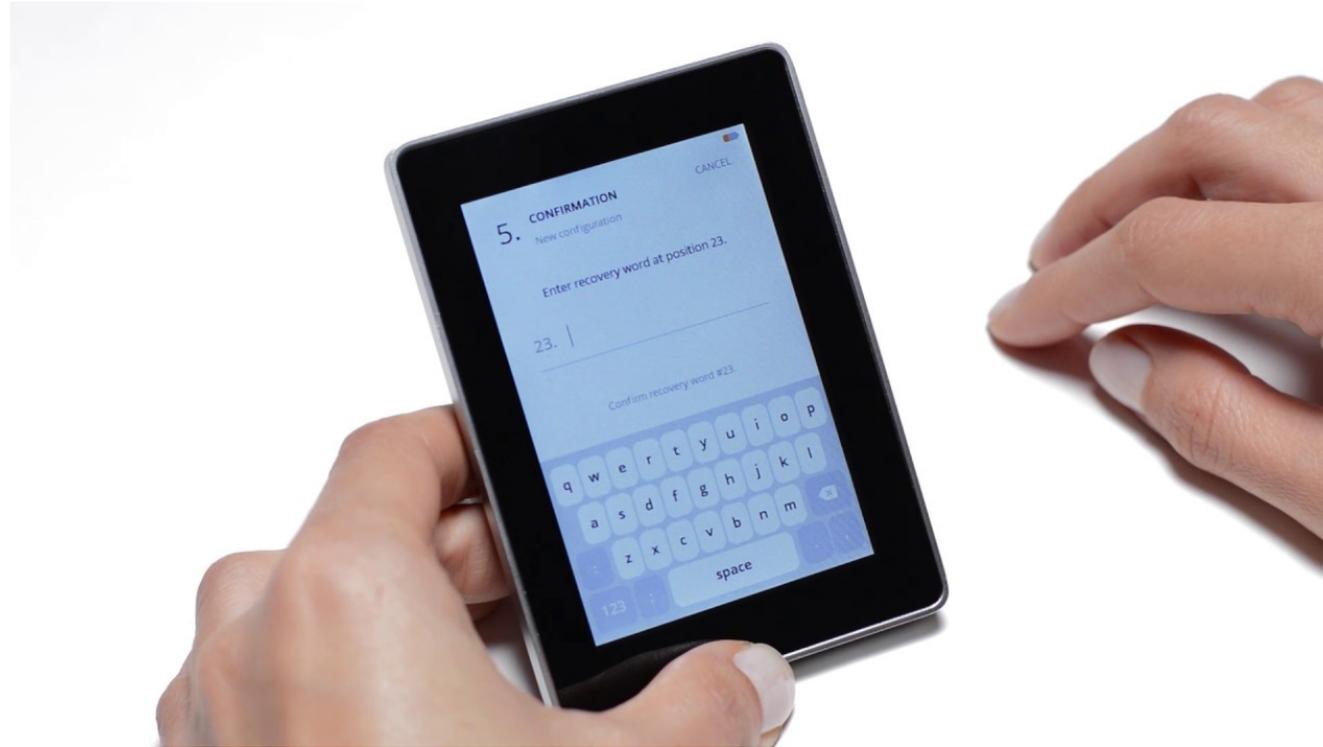
- **Ledger Nano X**
- Maggior numero di app supportate (100 rispetto alle 20 del Nano S)
- Schermo di dimensioni maggiori (240x64 pixel contro i 128x32 del Nano S)
- Comunicazione con dispositivi mobili con crittografia end-to-end
- Bluetooth
- Batteria

Luca Cadonici

ONIF – Osservatorio Nazionale sull'Informatica Forense



# Ledger



Ledger Blue



Luca Cadonici

ONIF – Osservatorio Nazionale sull'Informatica Forense



# Ledger Blue



- Meno diffuso rispetto ai due *Nano*
- Schermo touch screen 3,5 pollici a colori.
- PIN
- *Secure chip*
- Supporta fino a 30 criptovalute e 11 app

Luca Cadonici

ONIF – Osservatorio Nazionale sull'Informatica Forense



# KeepKey



KeepKey

Luca Cadonici

ONIF – Osservatorio Nazionale sull'Informatica Forense



# KeepKey



- Principale alternativa al duopolio di Trezor e Ledger
- Schermo OLED a 3,12 pollici (non richiede elementi aggiuntivi per essere illuminato)
- Gestione tramite connessione a portale <https://beta.shapeshift.com/> o estensione per Chrome
- Interazione quasi interamente via computer.
- L'unico tasto presente viene usato per confermare le operazioni tramite pressione prolungata.
- Support fino a 8 criptovalute + Token ERC-20

Luca Cadonici

ONIF – Osservatorio Nazionale sull'Informatica Forense



# La generazione dei report

Luca Cadonici

ONIF – Osservatorio Nazionale sull'Informatica Forense



# La generazione dei report



- account collegati
- nome account
- ID account in formato (sui *Ledger* in formato *xpub*)
- tipologia di criptovalute dei fondi
- importo totale fondi
- storico delle transazioni
- ID di transazione
- indirizzi di ricezione e invio
- data e ora delle transazioni
- importo delle transazioni
- tipo di operazione (invio o ricezione)

Luca Cadonici

ONIF – Osservatorio Nazionale sull'Informatica Forense



# La generazione dei report



- **Xpub**
- 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.
- Permette di visualizzare gli indirizzi utilizzati per le transazioni senza rivelare la chiave pubblica utilizzata.
- Concettualmente può essere considerato una visualizzazione in “sola lettura” del portafoglio.

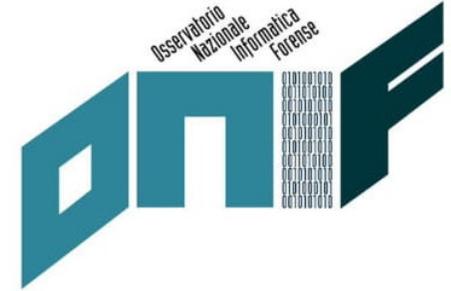
Luca Cadonici

ONIF – Osservatorio Nazionale sull'Informatica Forense



# La generazione dei report

- Ledger vs Trezor
- Balance (*Trezor*)
- Account ID in forma di xpub (*Ledger*)
- Commissioni (*Ledger*)

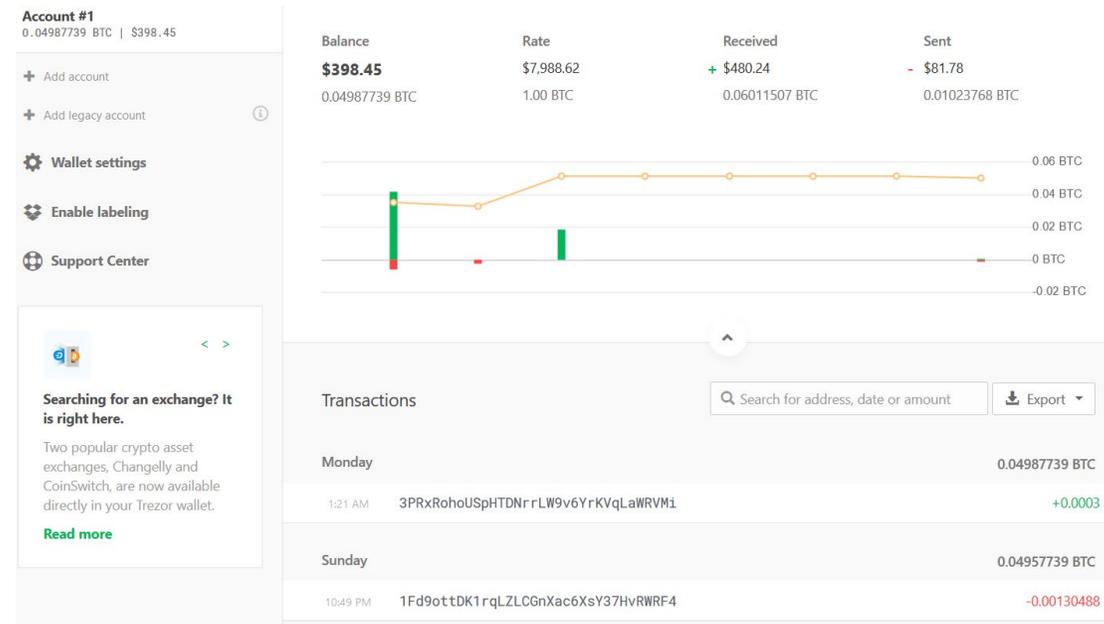


Luca Cadonici

ONIF – Osservatorio Nazionale sull'Informatica Forense



# La generazione dei report



## Trezor Chrome Extension

Luca Cadonici

ONIF – Osservatorio Nazionale sull'Informatica Forense



# La generazione dei report



## Account #1 - BTC

Date	Time	TX id	Address	TX type	Value	TX total	Balance
2019-10-14	01:21:34	8d482e4c0ef42146c8a133018fb22c9207e58e2bc50727c991cb734532c603f9	3PRxRohoUSpHTDNrLW9v6YrKVqLaWRVMI	IN	0.0003	0.0003	0.04987739
2019-10-13	22:49:50	8305b8232eeb28580035338b3e6de8fea860970c3269b6b17663688c3c4ed8cf	1Fd9ottDK1rqlZLCGnXac6XsY37HvRWRf4	OUT	0.0013	-0.00130488	0.04957739
2019-05-03	13:03:26	e3a38f6e4dec1eb28f4457e1e3175c631728e029c036bc926a6e03d0c769e8fc	3FG9xvTY2Jyqqp5ch6YNCRhuMGH3XSzKo	IN	0.018488	0.018488	0.05088227
2019-04-10	14:34:10	06df838694dc34df2a216b52ff5a1e465002f15cfc2d9a049ae611894f69a1a	3H1XqcwDrMqGXv7cumf2rFDWgdUJH8yrG5	OUT	0.0021	-0.0024036	0.03239427
2019-03-31	02:32:28	c4e38c8bce22f8a070f955a1c813ec16421be4c8413bec9e36182a8f9b856774	1LJFJZRpB7n28uS1ozWjpF8GzP5K94KQpS	OUT	0.001	-0.00110736	0.03479787
2019-03-30	18:41:59	eb21d528cca8127035f6031b07cde5299ce4aad49d041f1a9c32f1298bb0308	3C9ncBfwhs1Cdjm2dQXjUryMoYBeHjk9BZ	OUT	0.0028	-0.00289028	0.03590523
2019-03-27	16:36:43	692c68d07f677814b6f3be709c56a866388b29bc5583e8eb5565984a4ec89be4	3AB74BJoxNFUw1CINTRMrd1iJuM1pszBNs	IN	0.00114007	0.00114007	0.03879551
2019-03-27	16:28:33	3190d0f114eb6f8cdce9aba0740dc1abcf74aa6019a3ac928239795518cfc191	3FG9xvTY2Jyqqp5ch6YNCRhuMGH3XSzKo	IN	0.026523	0.026523	0.03765544
2019-03-27	16:22:52	57ed1f57c380fc8f001a6026da286a89ab4214134dd297041a05b84c53a1d1c5	3C8k9aKFNvrdnMVY1BxpVgrxqAM1k7kzM6	OUT	0.00245104	-0.00253156	0.01113244
2019-03-25	22:26:35	05cfa55611114e7c0029b3763a6478c5d38382a984834c9d0c5b8f0fd67c4c	3FG9xvTY2Jyqqp5ch6YNCRhuMGH3XSzKo	IN	0.013664	0.013664	0.013664

## Report Trezor Chrome Extension

Luca Cadonici

ONIF – Osservatorio Nazionale sull'Informatica Forense



# La generazione dei report



The screenshot shows a web application interface for 'Ledger live'. At the top right, there is a 'Synchronized' status indicator, a settings gear icon, and a lock icon. The main heading is 'Accounts', with a '+ Add account' button on the right. Below the heading is a search bar and filters for 'Range year' and 'Sort by Account Balance'. The table lists two accounts:

Account Name	Status	Balance	USD Value	Actions
ETHEREUM Ethereum 1	✓	ETH 0.3736	USD 67.57	—
BITCOIN Bitcoin 1	✓	BTC 0.04957739	USD 408.89	—

At the bottom of the table, there is a '+ Add account' button.

Ledger live

Luca Cadonici

ONIF – Osservatorio Nazionale sull'Informatica Forense



# La generazione dei report



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	xpub6DFyHAUFP4vYgW8Jj1k8958mwdiEDNeht5Hy6FFpR9CUAeduJ4hBaZjRNGuFhfQ5idWRC4HihbW1mNBYmldO7fvNxmTSKH6TrNxUjbj9Y23
2019-05-03T11:02:33.000Z	BTC	IN	0.018488	0.00006309	e3a38f6e4dec1eb28f4457e1e3175c631728e029c036bc926a6e03d0c769e8fc	Bitcoin 1	xpub6DFyHAUFP4vYgW8Jj1k8958mwdiEDNeht5Hy6FFpR9CUAeduJ4hBaZjRNGuFhfQ5idWRC4HihbW1mNBYmldO7fvNxmTSKH6TrNxUjbj9Y23
2019-04-10T12:30:39.000Z	BTC	OUT	0.0024036	0.0003036	06df838694dc34df2a216b52ff5a1e465002f15cfcb2d9a049ae611894f69a1a	Bitcoin 1	xpub6DFyHAUFP4vYgW8Jj1k8958mwdiEDNeht5Hy6FFpR9CUAeduJ4hBaZjRNGuFhfQ5idWRC4HihbW1mNBYmldO7fvNxmTSKH6TrNxUjbj9Y23
2019-03-31T00:31:50.000Z	BTC	OUT	0.00110736	0.00010736	c4e38c8bce22f8a070f955a1c813ec16421be4c8413bec9e36182a8f9b856774	Bitcoin 1	xpub6DFyHAUFP4vYgW8Jj1k8958mwdiEDNeht5Hy6FFpR9CUAeduJ4hBaZjRNGuFhfQ5idWRC4HihbW1mNBYmldO7fvNxmTSKH6TrNxUjbj9Y23
2019-03-30T16:23:00.000Z	BTC	OUT	0.00289028	0.00009028	eb21d528cca8127035f6031b07cdded5299ce4aad49d041f1a9c32f1298bb0308	Bitcoin 1	xpub6DFyHAUFP4vYgW8Jj1k8958mwdiEDNeht5Hy6FFpR9CUAeduJ4hBaZjRNGuFhfQ5idWRC4HihbW1mNBYmldO7fvNxmTSKH6TrNxUjbj9Y23
2019-03-27T14:34:45.000Z	BTC	IN	0.00114007	0.00005993	692c68d07f677814b6f3be709c56a866388b29bc5583e8eb5565984a4ec89be4	Bitcoin 1	xpub6DFyHAUFP4vYgW8Jj1k8958mwdiEDNeht5Hy6FFpR9CUAeduJ4hBaZjRNGuFhfQ5idWRC4HihbW1mNBYmldO7fvNxmTSKH6TrNxUjbj9Y23
2019-03-27T13:53:38.000Z	BTC	OUT	0.00253156	0.00008052	57ed1f57c380fc8f001a6026da286a89ab4214134dd297041a05b84c53a1d1c5	Bitcoin 1	xpub6DFyHAUFP4vYgW8Jj1k8958mwdiEDNeht5Hy6FFpR9CUAeduJ4hBaZjRNGuFhfQ5idWRC4HihbW1mNBYmldO7fvNxmTSKH6TrNxUjbj9Y23
2019-03-27T13:04:04.000Z	BTC	IN	0.026523	0.00004106	3190d0f114eb6f8cde9aba0740dc1abcf74aa6019a3ac928239795518c8b191	Bitcoin 1	xpub6DFyHAUFP4vYgW8Jj1k8958mwdiEDNeht5Hy6FFpR9CUAeduJ4hBaZjRNGuFhfQ5idWRC4HihbW1mNBYmldO7fvNxmTSKH6TrNxUjbj9Y23
2019-03-25T19:59:38.000Z	BTC	IN	0.013664	0.00001397	05cfa55611114e7c0029b3763a6478c5d38382a984834c9d0c5b8fd0fd67c4ac	Bitcoin 1	xpub6DFyHAUFP4vYgW8Jj1k8958mwdiEDNeht5Hy6FFpR9CUAeduJ4hBaZjRNGuFhfQ5idWRC4HihbW1mNBYmldO7fvNxmTSKH6TrNxUjbj9Y23

## Report Ledger live

Luca Cadonici

ONIF – Osservatorio Nazionale sull'Informatica Forense



# I wallet hardware nelle operazioni di Polizia Giudiziaria

Luca Cadonici

ONIF – Osservatorio Nazionale sull'Informatica Forense



# I wallet hardware nelle operazioni di Polizia Giudiziaria



- Accesso e ricostruzione dello storico dei fondi qualora si sia in possesso del PIN o nel caso in cui questo venga comunicato dall'indagato.
- Clonazione dei wallet importando il *seed* su nuovi dispositivi dal PIN concordato.
- Necessari i *recovery sheet* associati ad ogni *wallet*.
- Ipotesi operativa applicabile nei casi di mancata comunicazione del PIN, di distruzione, malfunzionamento o di mancato rinvenimento dei *wallet*.

Luca Cadonici

ONIF – Osservatorio Nazionale sull'Informatica Forense



# I wallet hardware nelle operazioni di Polizia Giudiziaria



- **Seed**
- 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.
- 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

Luca Cadonici

ONIF – Osservatorio Nazionale sull'Informatica Forense



# I wallet hardware nelle operazioni di Polizia Giudiziaria

- **Seed**
- 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.



Luca Cadonici

ONIF – Osservatorio Nazionale sull'Informatica Forense



# I wallet hardware nelle operazioni di Polizia Giudiziaria



- I principali standard dei Seed: BIP32, BIP39, BIP44

- **BIP32**

Stringa esadecimale di 512 bit in grado di generare la *master key* di un *wallet*.

- **BIP 44**

Ulteriore implementazione dello standard che permette di creare più account di criptovalute a partire da un'unica *master key*.

- **BIP39**

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**.

Luca Cadonici

ONIF – Osservatorio Nazionale sull'Informatica Forense



# I wallet hardware nelle operazioni di Polizia Giudiziaria

- Note tecniche di acquisizione: sequestro e importazione dei seed

1. individuazione
2. messa in sicurezza
3. repertazione
4. sequestro
5. acquisizione del PIN

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

6. individuazione dei conti associati
7. generazione di reportistica tramite software associato

Luca Cadonici

ONIF – Osservatorio Nazionale sull'Informatica Forense





# I wallet hardware nelle operazioni di Polizia Giudiziaria

- Note tecniche di acquisizione: sequestro e importazione dei seed
- PIN ignoto
- Malfunzionamento
- Mancato sequestro
- Distruzione del wallet
- Necessario importare il *seed* da *recovery sheet*



Luca Cadonici

ONIF – Osservatorio Nazionale sull'Informatica Forense



# I wallet hardware nelle operazioni di Polizia Giudiziaria

## ■ Importazione dei seed da recovery sheet: Ledger Nano S

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*



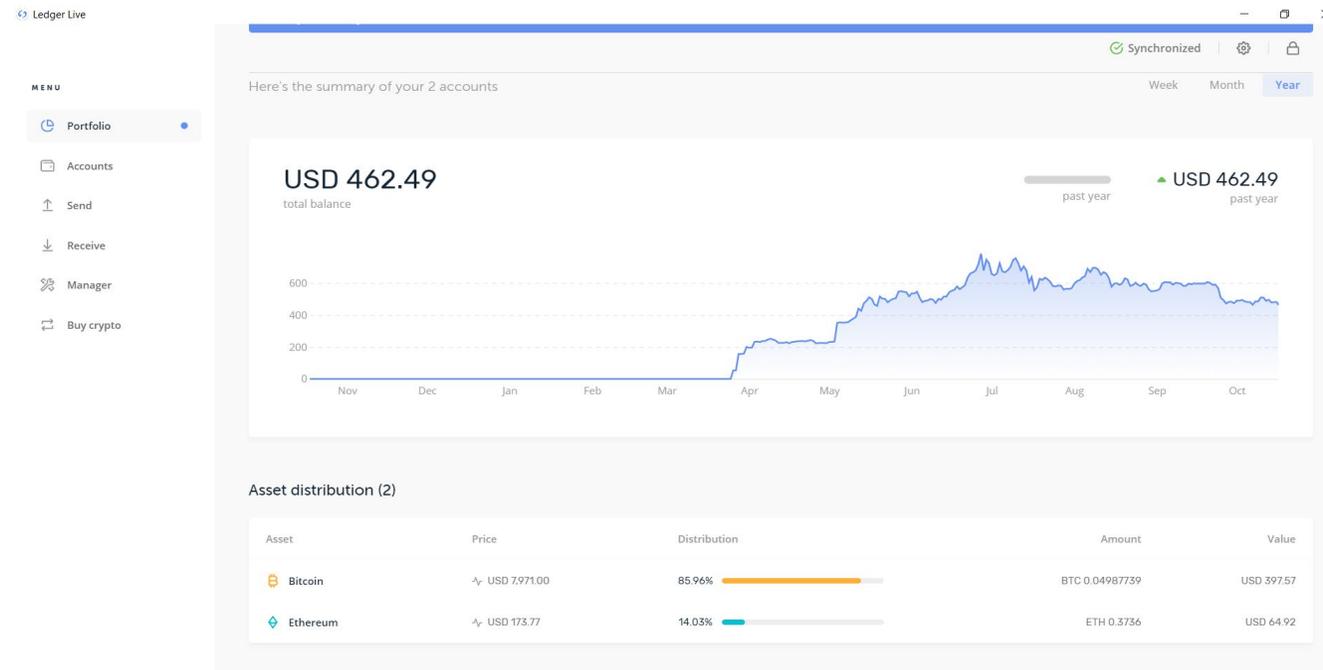
Luca Cadonici

ONIF – Osservatorio Nazionale sull'Informatica Forense



# I wallet hardware nelle operazioni di Polizia Giudiziaria

- Importazione dei seed da recovery sheet: Ledger Nano S



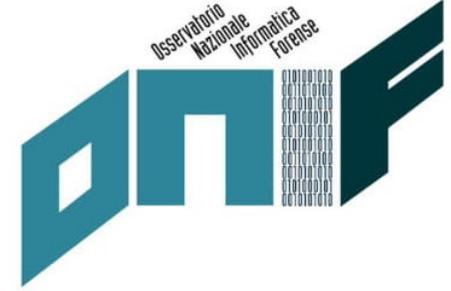
Accesso tramite *Ledger live* e *seed* importato su *Ledger Nano S*

Luca Cadonici

ONIF – Osservatorio Nazionale sull'Informatica Forense



# I wallet hardware nelle operazioni di Polizia Giudiziaria



## ■ Importazione dei seed da recovery sheet: Trezor One

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*
4. Scegliere se richiedere codice PIN e password aggiuntiva
5. Selezionare la lunghezza della frase del *seed* da immettere
6. Inserire le parole del seed nell'ordine richiesto dal dispositivo
7. Avviare l'apposita estensione Chrome

Luca Cadonici

ONIF – Osservatorio Nazionale sull'Informatica Forense



# I wallet hardware nelle operazioni di Polizia Giudiziaria



- Importazione dei seed da recovery sheet: Ledger Nano S

The screenshot displays the Trezor Bitcoin wallet interface. The top navigation bar includes 'Transactions', 'Receive', 'Send', 'Buy', 'Exchange', and 'Sign & Verify'. The 'Transactions' tab is active, showing a list of transactions for 'Account #1' (connected device) from March 25, 2019, to Monday. The account balance is 0.04987739 BTC, valued at \$397.92. The transaction list includes:

Date	Time	Address	Amount
Monday			0.04987739 BTC
	1:21 AM	3PRxRohoUSpHTDNrrrLW9v6YrKVqLaWRVM1	+0.0003
Sunday			0.04957739 BTC
	10:49 PM	1Fd9ottDK1rqlZLcGnXac6XsY37HvRWF4	-0.00130488
May 3, 2019			0.05088227 BTC
	1:03 PM	3FG9xvTY2Jyqqp5ch6YNCRhuMGH3XSzKo	+0.018488
April 10, 2019			0.03239427 BTC
	2:34 PM	3H1XqcwDrMqGxv7cumf2rFDWgdUjH8yrG5	-0.0024036

**Accesso tramite Trezor Chrome Extension e seed importato su Trezor One**

Luca Cadonici

ONIF – Osservatorio Nazionale sull'Informatica Forense



# I wallet hardware nelle operazioni di Polizia Giudiziaria



- Importazione dei seed da recovery sheet: Ledger Nano S

Distribution	Amount	Value
85.96% 	BTC 0.04987739	USD 397.57
14.03% 	ETH 0.3736	USD 64.92

*Ledger live*

Bitcoin (BTC) ▼ Transactions Receive Send Buy Exchange New Sign & Verify

**trezor\_ledger**  
Connected device ▲

Account #1 ▼ From March 25, 2019 to Monday

Account #1  
0.04987739 BTC | \$397.92

+ Add account

+ Add legacy account ?

Transactions  Export

Monday 0.04987739 BTC

**Trezor Chrome Extension** – il numero di bitcoin coincide con quello del wallet *Ledger* (0.04987739 BTC)

Luca Cadonici

ONIF – Osservatorio Nazionale sull'Informatica Forense



# I wallet hardware nelle operazioni di Polizia Giudiziaria



# Grazie per l'attenzione.

Luca Cadonici

ONIF – Osservatorio Nazionale sull'Informatica Forense