#CrypTO

Webinar, 12 marzo 2021

Problematiche tecniche, metodologie e best practice del sequestro di criptomonete

Paolo Dal Checco

Consulente Informatico Forense

Chi sono

- PhD @UniTO nel gruppo di Sicurezza delle Reti e degli Elaboratori
- Passato di R&D su crittografia e sicurezza delle comunicazioni
- Consulente Informatico Forense: Perizie Informatiche per Privati, Aziende, Avvocati, Procure, Tribunali, FFOO
- Attività di digital forensics su PC, smartphone, reti, social network, dispositivi elettronici, mail, PEC, scatole nere, OSINT e… da alcuni anni anche cryptocurrency, in particolare Bitcoin
- Albo CTU e Periti del Tribunale di Torino, Periti ed Esperti CCIAA TO
- Piccole docenze a contratto per UniTO, UniMI e UniGE
- Socio fondatore ONIF (www.onif.it), socio IISFA, Tech & Law, Clusit, Assob.It, AIP, Lab4INT, Persone & Privacy

Un ripasso veloce

- La maggior parte delle notizie ed informazioni su Bitcoin e criptovalute si basano su errate percezioni, bufale, leggende metropolitane e scarsa comprensione dello strumento.

Un ripasso veloce (Bitcoin)

- **Chiave privata**: 256 bit, il codice da cui viene generato l'indirizzo, passando tramite la chiave pubblica generata da quella privata. Posso dimostrare di averla firmando un messaggio.
- **Chiave pubblica**: 512 bit, derivata dalla chiave privata tramite algoritmo a chiave pubblica/privata ECDSA a Curve Ellittiche. Posso verificare un messaggio firmato con chiave privata.
- **Indirizzi/address bitcoin**: 160 bit, 27-34 caratteri alfanumerici eccetto alcuni, dal 2020 nuovi indirizzi Bech32 segwit che iniziano per «bc». Gli indirizzi vengono derivati dalle chiavi pubbliche dell'utente, derivate dalle chiavi private.

Private Key (Wallet Import Format)

SECRET

5KkrPXWACDU6JnRi6kuEokPr1rEFAF6pJdLQzExxSFwD5oicaVP

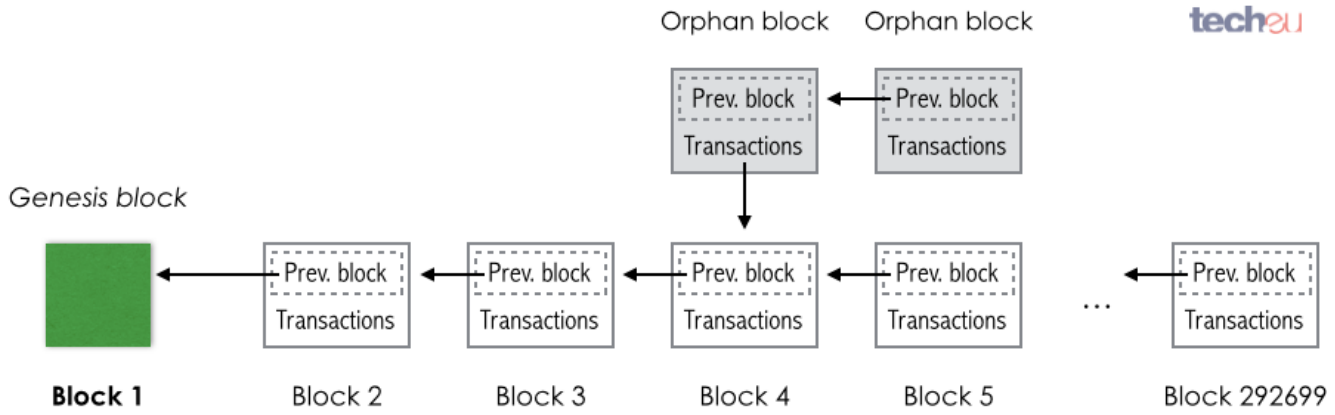
Bitcoin Address

SHARE

12St5js5pT18iMybf1TxghbAzLsH4yqYng

Un ripasso veloce (Bitcoin)

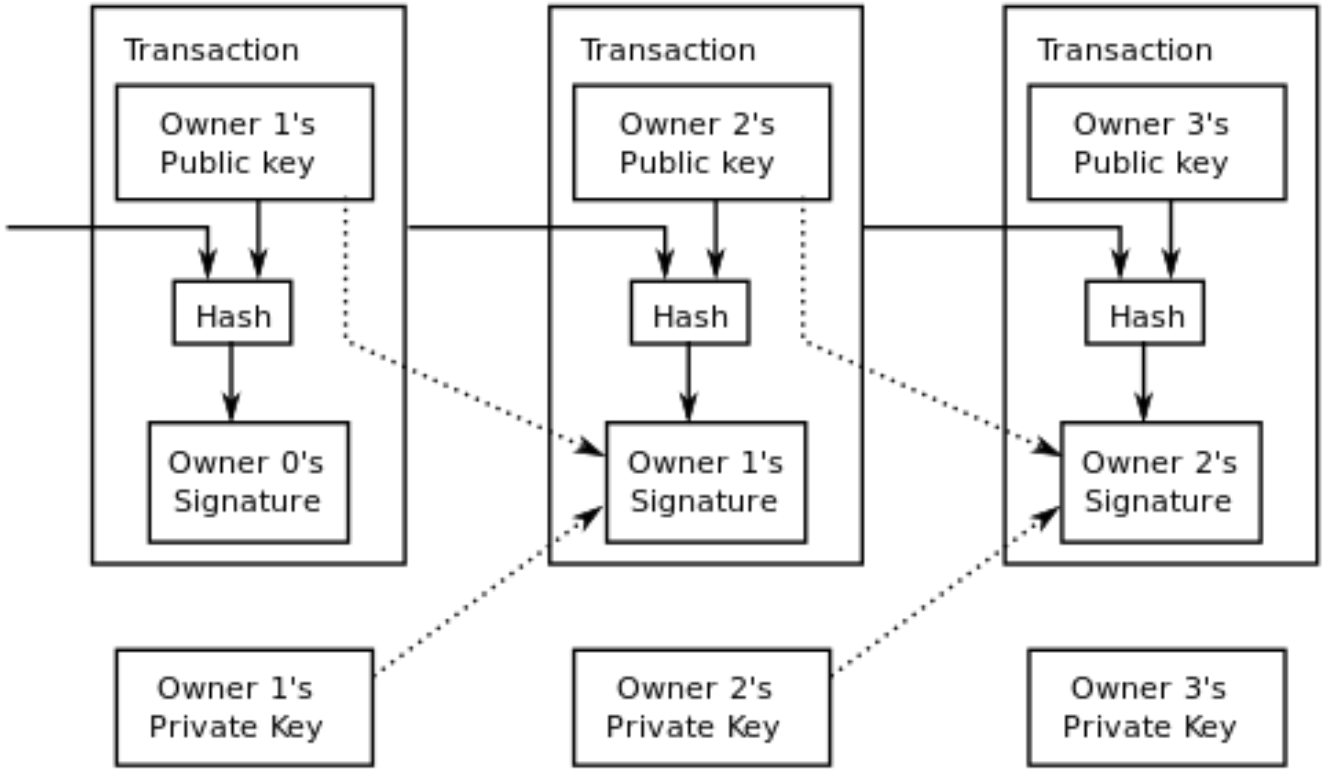
- **Blockchain**: il libro mastro delle transazioni, pubblico, condiviso, decentralizzato, viene composto autonomamente in base al concetto di "proof of work"



- **Wallet**: Il portafoglio che raccoglie i diversi indirizzi/address bitcoin, più facile da gestire rispetto a lavorare direttamente con gli indirizzi. In genere protetto da password. Può essere gerarchico deterministico.

Un ripasso veloce (Bitcoin)

- **Transazione**: passaggio irreversibile di una certa quantità di bitcoin da un indirizzo all'altro, che viene trasmessa dal client alla rete, inserita nella blockchain e diventa pubblica

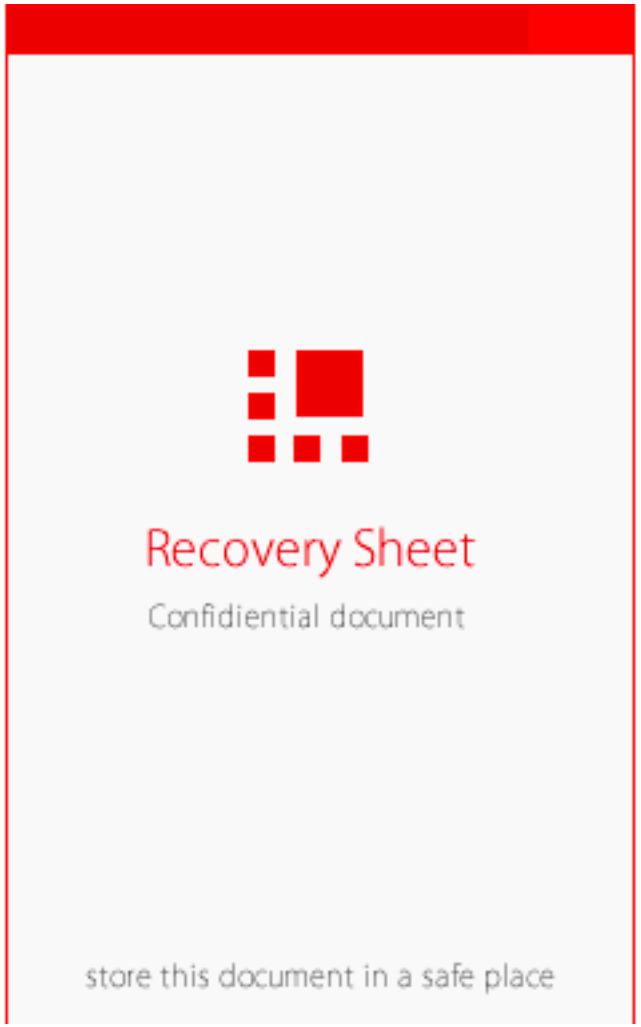


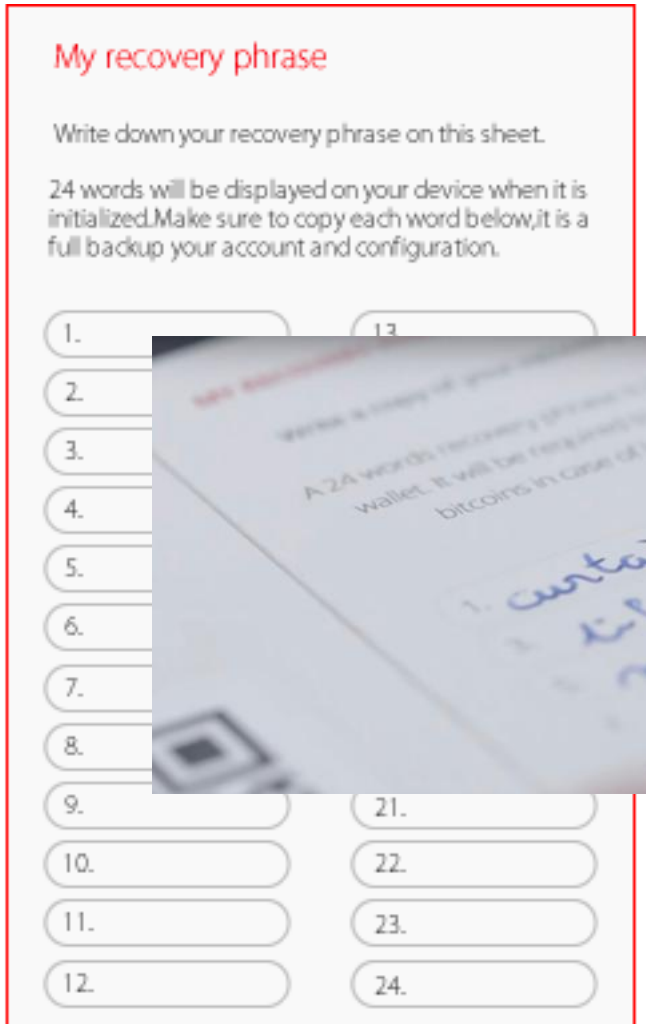
Sequestro durante perquisizione

- La prima: durante le attività di sequestro/perquisizione
- Anche durante descrizioni (non con finalità di sequestro ma di descrizione)
- Poco tempo per pianificare
- Spesso non si sa bene con cosa/chi si ha a che fare (i Bitcoin possono spuntare fuori in indagini «normali»)
- Se il soggetto non è collaborativo bisogna cercare

Cosa si può trovare durante perquisizione o descrizione?

Cosa si può trovare durante perquisizione o descrizione?





Cosa si può trovare durante perquisizione o descrizione?

Cosa si può trovare durante perquisizione o descrizione?

Bither

breadwallet

Electrum

GreenBits

Mycelium

Airbitz

ArcBit

Armory

Bitcoin Core

Bitcoin Knots

BitGo

Bither

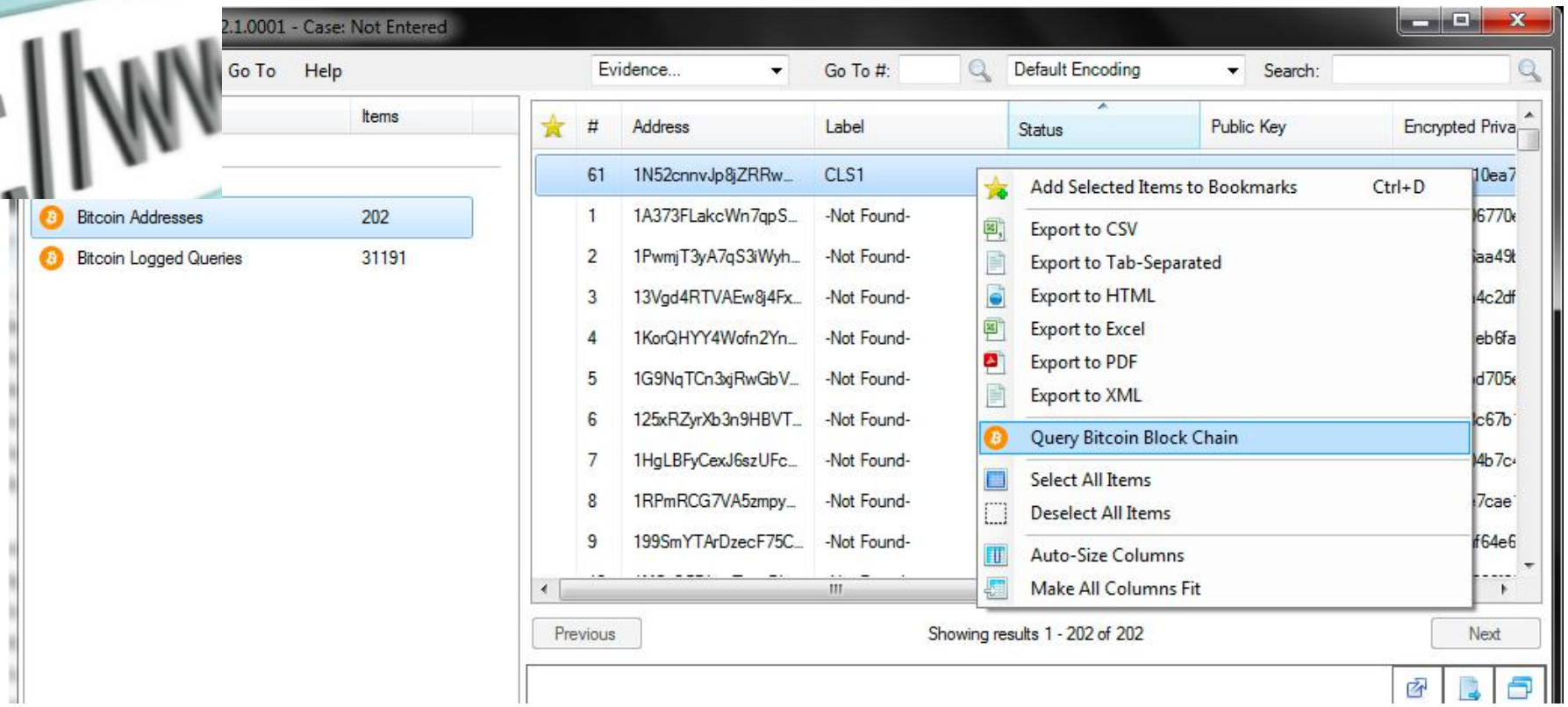
Electrum

Coin.Space

Green Address

Simple Bitcoin

Cosa si può trovare durante perquisizione o descrizione?



Sequestro successivo (es. conservativo, probatorio, preventivo, confisca)

- **Si può pianificare la modalità migliore**
- **Si può fare in contraddittorio**
- **Possibilità di avere a che fare con più criptomonete**
- **<u>Non c'è una banca cui chiedere supporto/esecuzione</u>**
- Se presenti exchange, può essere richiesto il «congelamento» dei fondi
  - E loro possono non rispondere (exchange cinesi, etc…)
  - Se l'exchange risponde ed esegue, i fondi congelati possono poi essere spostati/confiscati con i metodi descritti in seguito

Le richieste che potrebbero arrivare…

- **Sequestrare il «server Bitcoin»**
- **Chiedere alla «Bitcoin Society Inc.» ;-) di «congelare» il wallet o informazioni sul proprietario**

Le richieste che potrebbero arrivare…

- **Sequestrare il PC/Smartphone del soggetto**
- **Fare copia forense del PC/Smartphone/Wallet**
- **Cambiare la password del wallet (prima bisogna trovarla con bruteforce o farsela comunicare)**

Le richieste che potrebbero arrivare…

- **Farsi consegnare le chiavi private (valutare se non può invece rappresentare un rischio)**

TREZOR

Not your keys, not your coins.

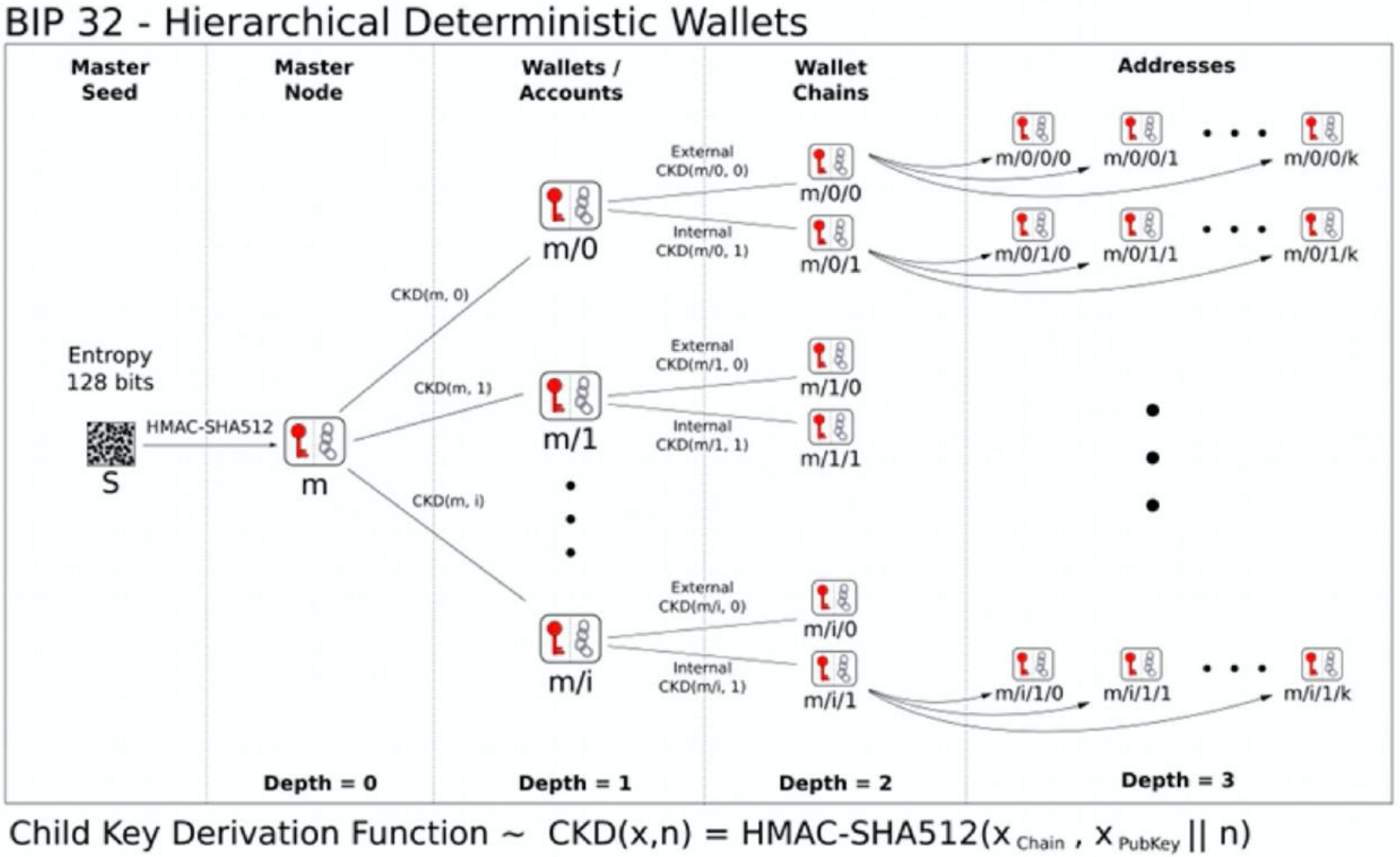
Brought to you by SATOSHILABS

I wallet ormai sono protetti da crittografia a diversi livelli

- Wallet su smartphone (es. iPhone) → Crittografia OS
- File contenente il wallet (es. Electrum) → Crittografia simmetrica
  - Contengono chiavi private o generatori di interi wallet tramite protocolli gerarchici
- File contenenti mnemonic → Crittografia simmetrica (spesso container Veracrypt, GPG, etc…)
- Esistono tool per far brute force di wallet:
  - github.com/gurnec/btcrecover

Come interpretare le «mnemonic»

- Diversi protocolli di generazione di un wallet con chiavi private e indirizzi a partire da 12-24 parole
- BIP32, BIP 39, BIP 44



Come interpretare le «mnemonic»

- BIP32, BIP 39, BIP 44
- Tool per derivare indirizzi dalle mnemonic e capire quali hanno fondi
  - https://github.com/dan-da/hd-wallet-addrs
  - https://github.com/dan-da/hd-wallet-derive
- Wallet “Coinomi”
- Siti con raccolte di “regole” di derivazione

Come osservare un wallet tramite le «mnemonic»

- È possible osservare, in maniera “watch only” un wallet HD hardware o software importando le extended public keys
- Si esportano XPUB, YPUB o XPUB e s’importano in un wallet (es. Electrum)

Approccio ragionato per il sequestro di criptomonete

- E' necessario **creare un nuovo indirizzo/wallet**
  - Valutare utilizzo di un wallet HD, in modo da non dover memorizzare chiavi private ma un generatore (mnemonic) e segnare algoritmo di derivazione
  - Meglio usare sistema "live" e offline, per non lasciare tracce e non rischiare leak
    - Rimane il problema della sicurezza del wallet (backdoor, bad RND number generator)
  - Verificare la sicurezza (firma PGP della ISO e del wallet)
  - Fare tutto in modo ripetibile (hash della ISO, hash del software wallet, conservare copia dei software, etc…)
  - Consigliata creazione di **wallet multisig** (es. 3 su 5)
    - Valutare se lasciare chiavi (o copia delle chiavi) ai CT
    - Depositare tutte le chiavi in busta chiusa
  - Generare wallet/indirizzo e testarlo
    - Versare cifra di prova (se non scompare è già un buon segno)
    - Verificare che possano uscire i fondi in futuro (rigenerare chiavi da zero e fare TXOUT)
  - Stampare (e poi distruggere eventuali copie) chiavi private o mnemonic (rischioso se non multisig)

Alcune idee

- E’ necessario **spostare i BTC sul un nuovo indirizzo**
  - Se possibile fare fare la transazione al soggetto
  - Evitare di farsi consegnare le chiavi, si è a rischio per un certo periodo di tempo… a meno che il tutto non avvenga in ambiente controllato e contraddittorio.
  - E’ anche possibile valutare la preparazione e la firma di TX (offline) e poi il broadcast sulla rete Bitcoin
    - La preparazione può farla il soggetto (preparazione, nostra verifica e firma)
    - O possiamo farla noi (preparazione, lui verifica e firma)
    - Dopo accurata verifica, si manda la TX in broadcast

Preparazione, verifica, firma e broadcast di TX

- Transazione non firmata
  - Può generarla chiunque
  - E' verificabile
  - Contiene i dati della transazione ma non può essere «attivata»

010000000576c786beb122e19e20d094edbe20d9abccae8dba7ddb9b76ff2675a54e8c11eb0600000044
01ff4104f265c1434ed9f0c17ea595c878dfdd3fb12c526752243bd8752a49c6ade5b3c11a6c516707220f8
d1592d88a3fb59da051ce9d7ac14a0 c786beb122e19e20d094edbe20d9a
bccae8dba7ddb9b76ff2675a54e8c11 434ed9f0c17ea595c878dfdd3fb12c
526752243bd8752a49c6ade5b3c11a 59da051ce9d7ac14a0fcca71d5a914
70e65f3feffffff76c786beb122e19e20 b9b76ff2675a54e8c11eb080000004
401ff4104f265c1434ed9f0c17ea595 752a49c6ade5b3c11a6c516707220f
8d1592d88a3fb59da051ce9d7ac14a 5c786beb122e19e20d094edbe20d9
abccae8dba7ddb9b76ff2675a54e8c1 1434ed9f0c17ea595c878dfdd3fb12
c526752243bd8752a49c6ade5b3c11 59da051ce9d7ac14a0fcca71d5a914
70e65f3feffffff76c786beb122e19e20 b9b76ff2675a54e8c11eb0a0000004
401ff4104f265c1434ed9f0c17ea595c878dfdd3fb12c526752243bd8752a49c6ade5b3c11a6c516707220f
8d1592d88a3fb59da051ce9d7ac14a0fcca71d5a91470e65f3feffffff01e03c0100000000001976a914c911
d6d4a57721efd4cadb766bc47c6b99b24bec88acc8fb0700

Manca la firma…

Preparazione, verifica, firma e broadcast di TX

- **Transazione firmata**
  - **Può generarla solo il proprietario della chiave privata**
  - **E' verificabile**
  - **Chiunque può inviarla alla rete Bitcon e «attivarla»**

010000000576c786beb122e19e20d094edbe20d9abccae8dba7ddb9b76ff2675a54e8c11eb060000008b483045022100ce19
14e4d60c4070640f19e3b577c0e31be7bf67254b6daaca478be1e20fa9fb02206f5bea4ad2fa80effcbbb5203d1fb325fccc2d38
bad56324855da692625b8bb9014104f265c1434ed9f0c17ea595c878dfdd3fb12c526752243bd8752a49c6ade5b3c11a6c516
707220f8d1592d88a3fb59da051ce9d7ac14 6beb122e19e20d094edbe20d9abccae8db
a7ddb9b76ff2675a54e8c11eb070000008b 96e8644c3a394dd42f010a1e20a9270e1e4
2e9b2b3d8d022077dc451015b4dc844f457 78e9452e0597b014104f265c1434ed9f0c17
ea595c878dfdd3fb12c526752243bd8752a4 2d88a3fb59da051ce9d7ac14a0fcca71d5a9
1470e65f3feffffff76c786beb122e19e20d09 75a54e8c11eb080000008b483045022100
dd1a9ac7452f536190bf1d5a699a551c0f88 0736713570292f7ce6d80d279853a2cb979
76dd1c5df3bb2aa2968d4ac6dc9657014104 fb12c526752243bd8752a49c6ade5b3c11a
6c516707220f8d1592d88a3fb59da051ce9c 76c786beb122e19e20d094edbe20d9abcc
ae8dba7ddb9b76ff2675a54e8c11eb090000 0d42fe7bd37b74ef7ff3af2bfa4f1985ec11cd
4960fd99870220526961ae50e1d8fbf0955b 9c5fba8f2439014104f265c1434ed9f0c17e
a595c878dfdd3fb12c526752243bd8752a49 d88a3fb59da051ce9d7ac14a0fcca71d5a91
470e65f3feffffff76c786beb122e19e20d094edbe20d9abccae8dba7ddb9b76ff2675a54e8c11eb0a0000008b483045022100b
660bf4655bd8ba1f723672c6a86889664965107c832c3ed1bba5b1cdbd9d404022073200b33d6c9e7b47a95bd2f179d24e8c
c80910c8373f0993087404de85f52bb014104f265c1434ed9f0c17ea595c878dfdd3fb12c526752243bd8752a49c6ade5b3c11
a6c516707220f8d1592d88a3fb59da051ce9d7ac14a0fcca71d5a91470e65f3feffffff01e03c0100000000001976a914c911d6d
4a57721efd4cadb766bc47c6b99b24bec88acc8fb0700

Si può mandare in broadcast
https://coinb.in/#broadcast

Idee?

- Valutare **wallet alternativi**
  - Trezor, Ledger
    - Ottima perché supporta numerose criptomonete
    - Backup? Dove archiviamo le 24 parole dello mnemonic?
  - OpenDime
    - Ottima perché non ha backup key/phrase: chi possiede l'hardware ha i BTC.
    - Se si rompe?
    - Suddividere importo in modo da limitare le perdite?
  - Web Wallet/Exchange
    - Custodian?
    - Se fallisce o perde i fondi?
    - Se permette export di chiavi private torniamo al problema iniziale?

Grazie per l'attenzione!

Paolo Dal Checco
paolo@dalchecco.it
@forensico
www.dalchecco.it. www.bitcoinforensics.it
www.ransomware.it, www.osintbook.it