"I REATI "CRIPTOVALUTARI""

1 aprile 2021

Video Conference

GLI ASPETTI TECNICI DELL'INDAGINE PENALE SULLE CRIPTOVALUTE

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, F.F.O.O.
- Albo CTU e Periti del Tribunale di Torino, Periti ed Esperti CCIAA TO
- Piccole Docenze a Contratto @UniTO e @UniMI
- Tra i fondatori dell'Associazione ONIF (www.onif.it)
- Socio IISFA, Tech & Law, Clusit, Assob.It, AIP

Un ripasso veloce

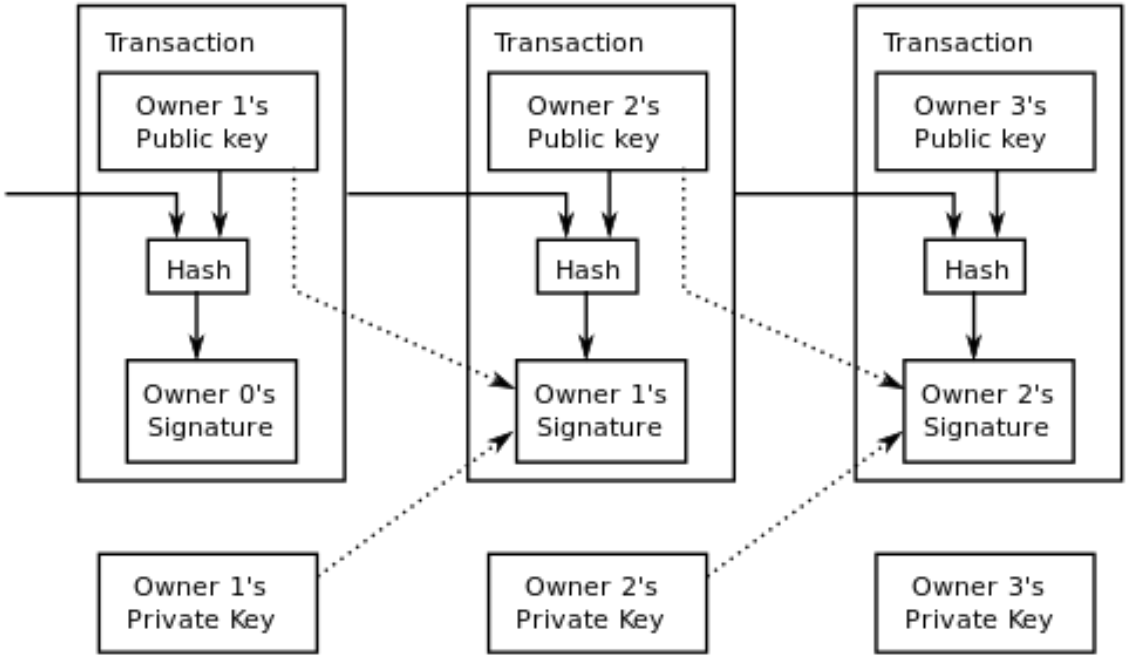
- La maggior parte delle notizie ed informazioni su Bitcoin e criptovalute si basano su errate percezioni, bufale, leggende metropolitane e scarsa comprensione dello strumento.

Un ripasso veloce

- **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. Gli indirizzi vengono derivati dalle chiavi pubbliche dell'utente, derivate dalle chiavi private.

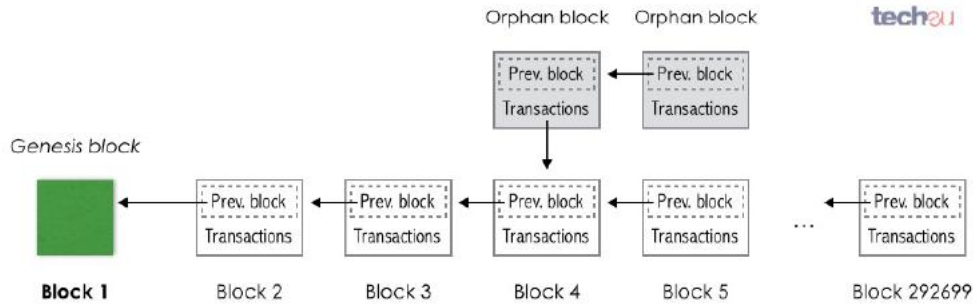
Un ripasso veloce

- **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



Un ripasso veloce

- **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.

Quando non si ha nulla da nascondere

- La blockchain è «trasparente», mantiene i legami tra le transazioni
- Si riesce a fare aggregazione (clustering) degli indirizzi
- Gli utenti non si nascondono dietro indirizzi IP anonimi (VPN, Tor, etc…)
- Le transazioni non avvengono tramite mixer/tumble
- Gli utenti mantengono gli stessi wallet

Le difficoltà dell'indagine penale sulle criptomonete

- Le transazioni possono essere tutte slegate tra di loro
- Difficile aggregare indirizzi e ricostruire wallet
- Gli indirizzi IP utilizzati dagli utenti sono spesso anonimi
- Vengono semre più spesso utilizzati sistemi di anonimizzazione come mixer/tumbler
  - bitcoinmix.org
- Esistono wallet che mixano i bitcoin
  - Samourai Wallet con Whirpool
  - Wasabi Wallet
- Gli utenti cambiano continuamente indirizzi e wallet

Come vengono “ripuliti” i bitcoin

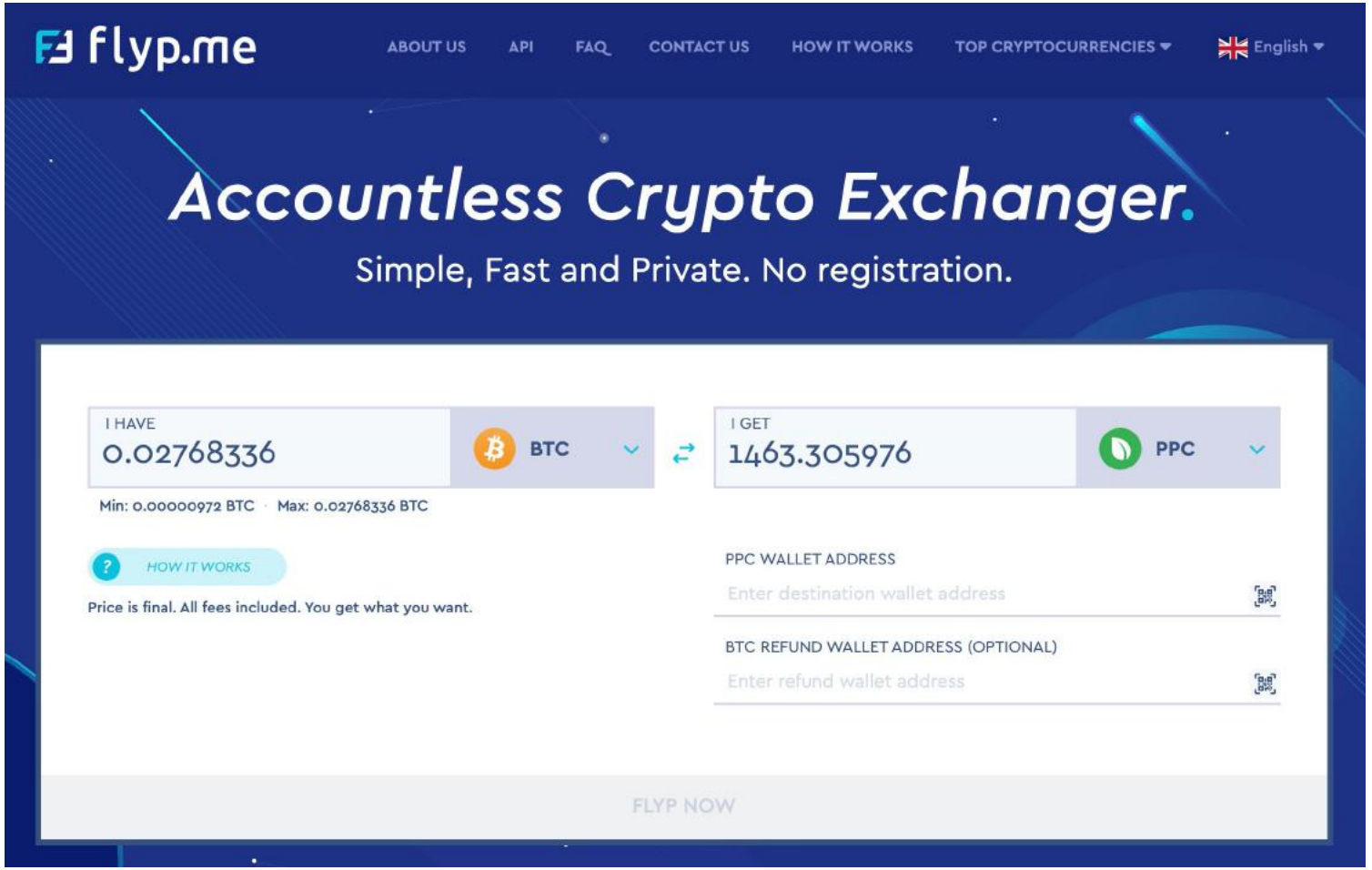
- Tumblers/Mixers via web anche su Tor con Onion address
- Attenzione che non tutti i tumbler funzionano
- Attenzione che non si sa chi ci sia dietro i tumbler

Come vengono “ripuliti” i bitcoin

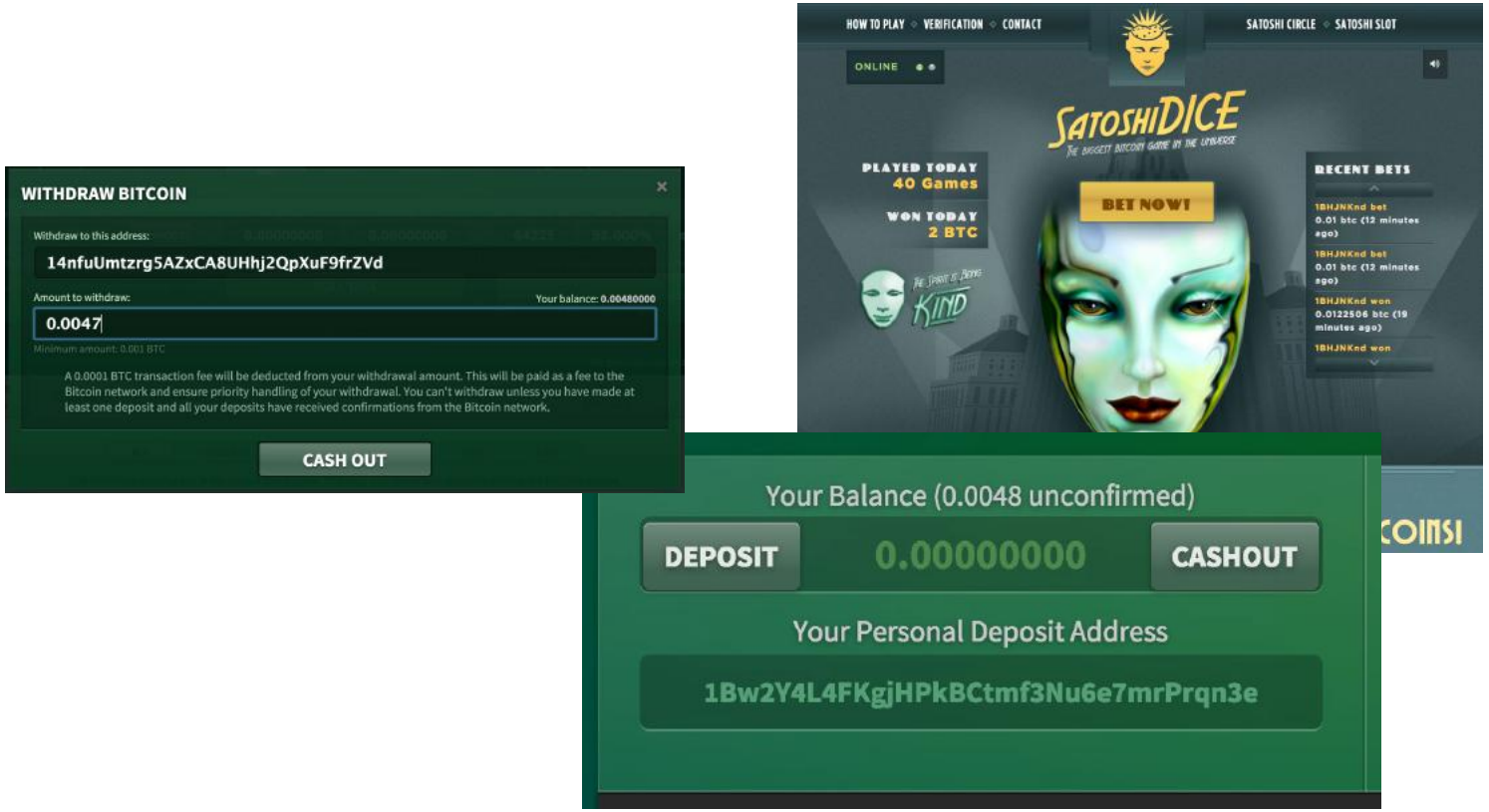
MIXER PER BITCOIN

Bitcoin Mixer (Blender) è qualcosa che ti aiuta a rimescolare i tuoi bitcoin utilizzando i nostri algoritmi e a proteggere la tua identità.

Come vengono “ripuliti” i bitcoin



Come venivano “ripuliti” i bitcoin in origine



Le transazioni sono comunque complesse

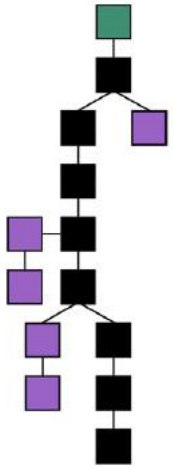
12EFijBVj3PEQZyoBBVr3ocQe1XFYJqxqz (€ 3,159.91 - Output)
1AiN1RxRXmBhZSPZdoi8goABP7UTZgrbFL (€ 2.74 - Output)
1NTaCpQQ3v6QZauVTxSeyDMeQFeVKtuLCW (€ 2.88 - Output)
145dDzvALbGUcJnhM1LRTGXU8EsaVQEvFa (€ 2,812.75 - Output)

1FBmDBUgS1gTSd7G8AE4H3wrHz81M1NcNL - (Spesi)	€ 333.16
1CozRs4pzTFFZjbKGd2XNRJpeqMWqts7Wp - (Spesi)	€ 2.74
1Bgvrh2i3FNFReXukACZgfVpKk1f1LuZt - (Spesi)	€ 381.21
1BDbraoxzHJGdoP5xXW3hXTch55cCBPCsQ - (Spesi)	€ 2.82
1CnsCszPrnRGyvfmokLbVFvNGfPB8LBjAs - (Spesi)	€ 368.27
1NVcLCk34d1UXADadwsNobXZxmYDfdcZZT - (Non spesi)	€ 2.74
1KgznLvPB2EVhFQk1KAn2jugkwHhVfXqon - (Spesi)	€ 349.21
14shDhLhJ4czVxwA6yDhimFPcvKnggb65V - (Spesi)	€ 3.01
13yUQQwUuAkQEWSMmRYbbL9skzDSNYHTC9 - (Spesi)	€ 2.47
1AL6QDpoKDSr6TQ3zeVwYgQTcQ2QkCU2yi - (Spesi)	€ 348.56
1EBC2k92WtHbDWVY5wkZyL3NCeHLdeoUGb - (Spesi)	€ 3.01
1N53PG9SsXqf9NNjsMNZR2Bk76UcpAqWqe - (Spesi)	€ 348.84
1K2YSRBAUiR2Xwjy171jUfoWP4xhy5MKfp - (Spesi)	€ 369.20
1Kh3QaxseBiRcsjojYHkdHRMNmgdDQgjAt - (Spesi)	€ 353.46
1GY844iv59QSACfD7XomGcf4iZeCnv2YRZ - (Non spesi)	€ 341.82
1LkRypTeoD5c2wgnvvTAWy9VGDWcU4xcfR - (Spesi)	€ 366.81
1zFBsknwMiPMs2h5ZNyWy8SWMysHts5fU - (Spesi)	€ 342.22
15xzXZCVyVuNkzthSXjc4NWPYZqKGWjFCM - (Spesi)	€ 343.16
1DWaA1n54bGeCs2AXTpV9x4a7GbvSKjQE8 - (Spesi)	€ 3.04
13YamD7pp8wxKhue4AcMiT1Q92R3sS7knp - (Spesi)	€ 347.17
1QELDPd1uuAqQY5hL1oVWWa8TtHuUEghPN - (Spesi)	€ 347.47
192BKs5fAGs74oGXRNvYZErc87RkpcMtvN - (Spesi)	€ 324.26
15nrUxmtYTgkxGaPzhXH2HfGDFFLnUuj6W - (Spesi)	€ 328.22
1N6Ubr1Ziqf9Rf7XXYhGvPdk9CZgSczR9p - (Spesi)	€ 365.34

4 Conferme | € 2.74

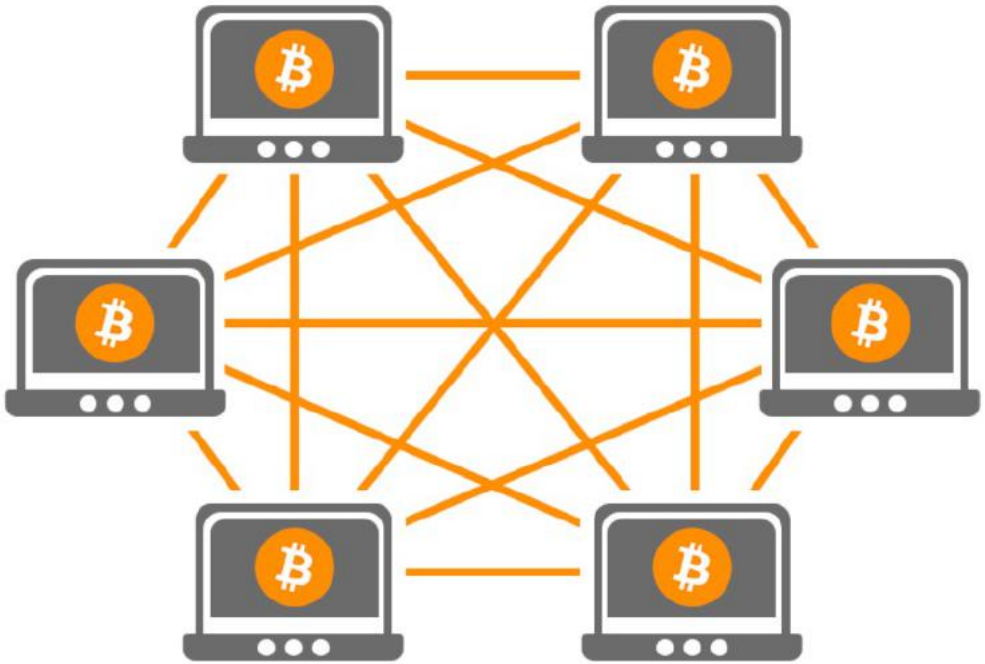
Bitcoin Forensics

- Sottoinsieme della **Digital Forensics**
- Deriva dalla Computer, Network, Mobile, Video, Audio, etc… Forensics
- Applicazione delle best practices e workflow di digital forenscis alle indagini sulle criptomonete.
  - **Elementi tradizionali** e “locali” (es. analisi di un PC su cui è stato installato un wallet)
  - **Elementi innovativi** (intelligence su transazioni presenti nella blockchain)



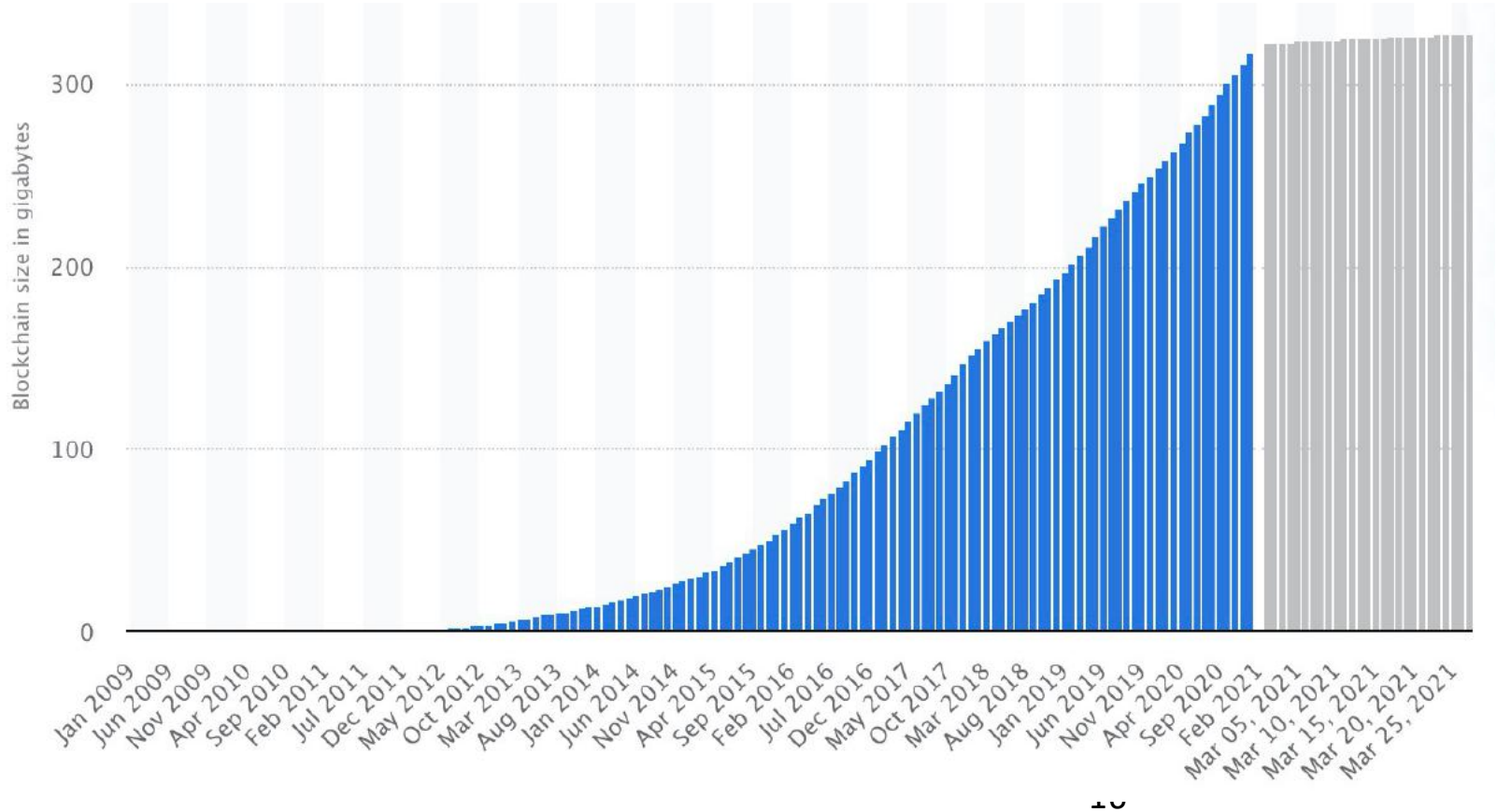
Bitcoin Forensics

- **Blockchain**: la prova è pubblica, immutabile, già “forense”
- Dove si trova la blockchain? Su tutti i nodi dei partecipanti alla rete (minatori o utenti che hanno installato un «nodo» e non soltanto un wallet «leggero»



Bitcoin Forensics

- Problema: **dimensione della blockchain**



Bitcoin Forensics

BitcoinCore

Bitcoin Forensics

BitcoinCore

- Per indicizzare tutte le transazioni (non soltanto quelle nel proprio wallet) è necessario impostare **txindex=1** nel config

```
txindex=1
rpcuser=[redacted]
rpcpassword=[redacted]
Library/Application\ Support/Bitcoin/bitcoin.conf (END)
```

- Si può così interrogare la blockchain per qualsiasi TX

22:04:05 getrawtransaction
f8d55fec6057a5e0d6ced7ec5b7f21171b4a25061f863d2dd2caa312fc7d0ee4

22:04:06
010000000128c2f19a1e046d6e3bae09070249f22bebc94a5abc9d8371ec3796fa59e90b
b6450000004847304402026e82f93fd7cbab04debc9cc3b018f6042304c48f8da4ecdc7
e46f4a45ff0011022050559fd0bb3d94c7c5631729341c59407585e38c567d1da96a929af
05908a06001ffffffff02e8030000000000001976a914a72b2649da2ad8a8bf92e00f01e7a2
950a1be76c88ac00000000000000000446a4245572044616920646961 6d616e7469206e
6f6e206e61736365206e69656e74652c2064616c6c6120626c6f636b636861696e206e61
73636f6e6f20692066696f726900000000

Bitcoin Forensics

- E dalla raw transaction, ottenere la versione “in chiaro”

```
22:04:49  decoderawtransaction
010000000128c2f19a1e046d6e3bae09070249f22bebc94a5abc9d8371ec3796fa59e90b
b6450000004847304402202...
```

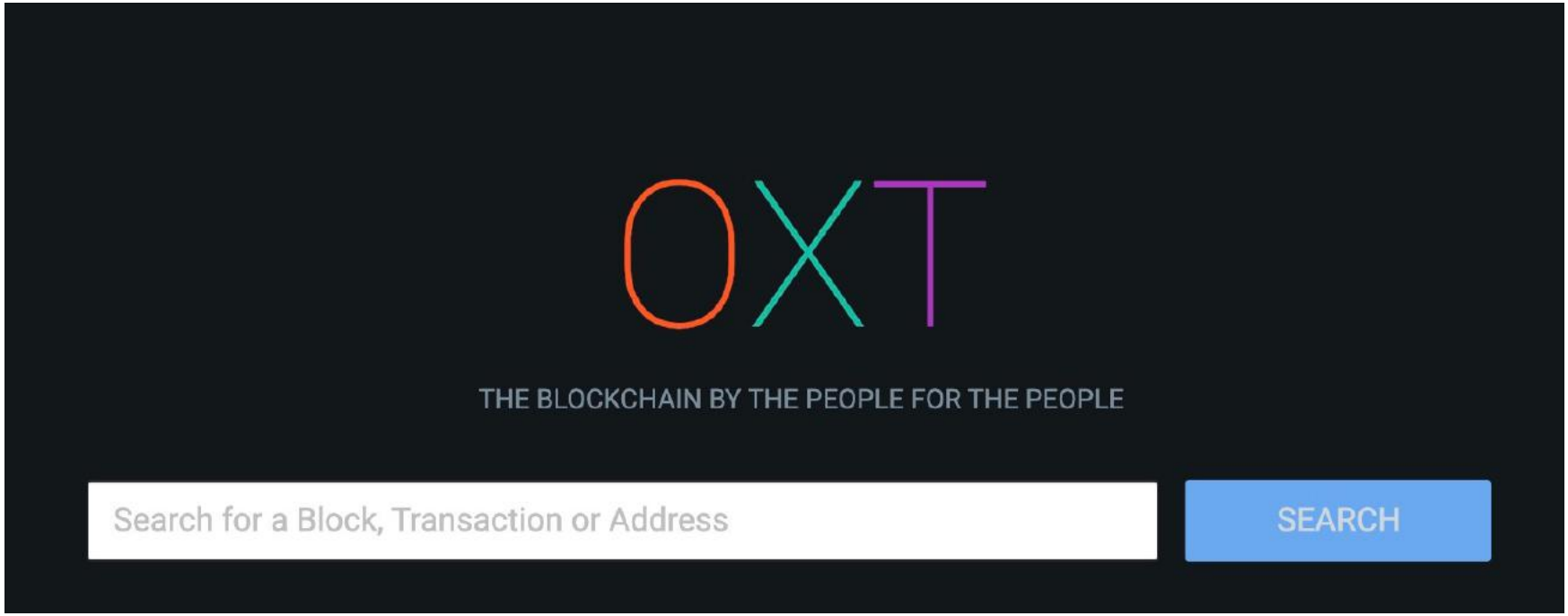
- Inclusi dati eventualmente contenuti all’interno

```
"scriptPubKey" : {
"asm" : "OP_RETURN
45572044616920646961 6d616e7469206e6f6e206e61736365206e69656e74652c20646
16c6c6120626c6f636b636861696e206e6173636f6e6f20692066696f7269",
"hex" :
"6a4c4545720446169206469616d616e7469206e6f6e206e61736365206e69656e74652c
```

- Che convertiti da hex ad ascii potrebbero avere un significato

```
PMB:~ Paolo$ echo 45572044616920646961 6d616e7469206e6f6e206e61736365206e69656e746
52c2064616c6c6120626c6f636b636861696e206e6173636f6e6f20692066696f7269 | xxd -r -p
EW Dai diamanti non nasce niente, dalla blockchain nascono i fioriPMB:~ Paolo$
```

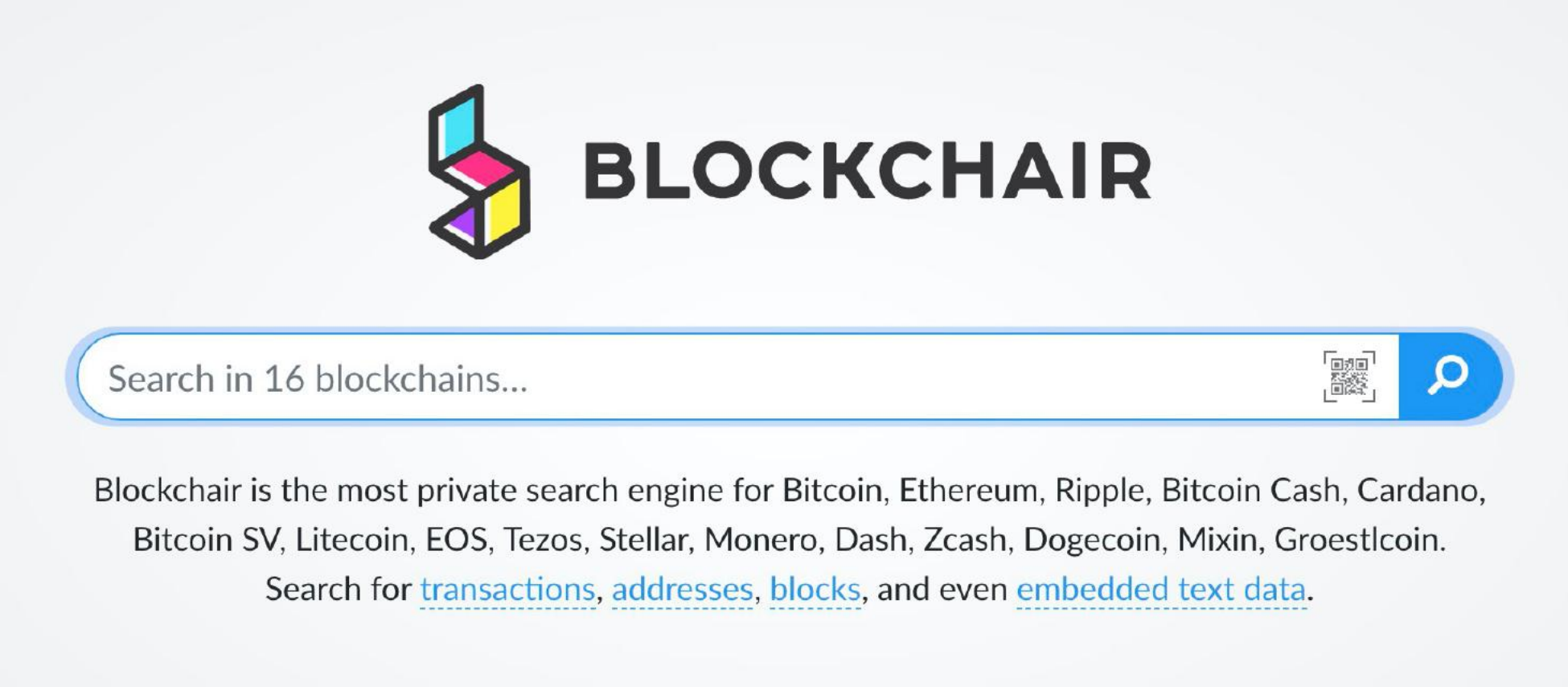
Strumenti Online: block explorer



oxt.me

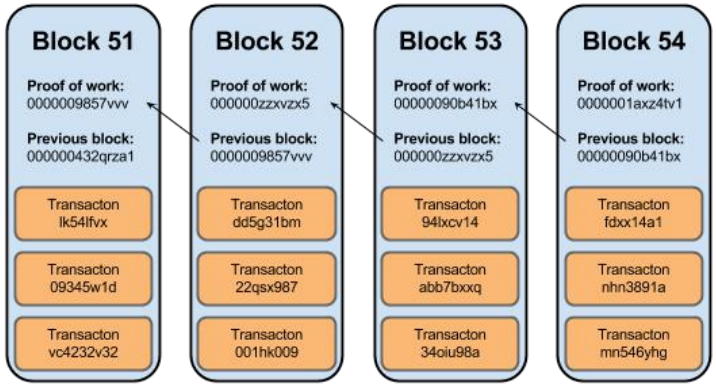
(prova pratica: 17YKd1iJBxu616JEVo15PsXvk1mnQyEFVt)

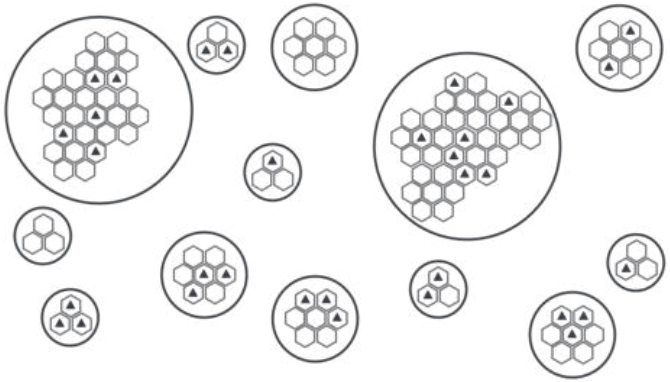
Strumenti Online: block explorer



blockchair.com

Bitcoin Intelligence: Clustering

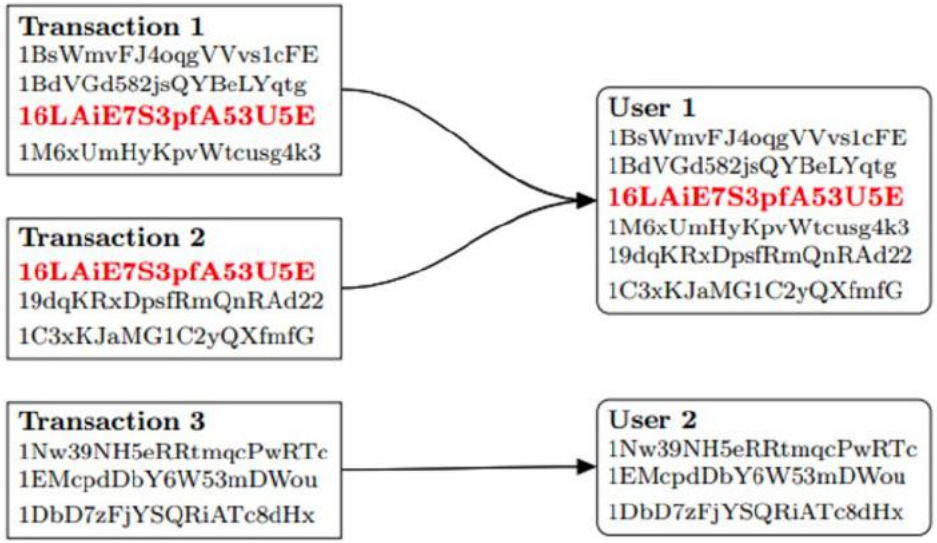




- La blockchain è un mero elenco di transazioni da indirizzo a indirizzo
- Con la Blockchain Intelligence si tenta di costruire relazioni tra gli indirizzi, le transazioni e i wallet, raggruppando gli indirizzi in wallet tramite tecniche di “clustering”
- Con li clustering non otteniamo (direttamente) indirizzi IP, numeri di telefono, email, ma possiamo arrivare a deanonimizzare degli indirizzi o meglio dei wallet
- Per la classificazione, utilizziamo la ricerca di Jonas Nick

Clustering: transazioni con TXIN multiple

- Transazioni con TXIN multiple in ingresso appartengono tutte allo stesso utente/wallet (che deve conoscere le chiavi private di tutti gli indirizzi da cui partono le TXIN)
- Consideriamo il caso di wallet e non di exchange



Strumenti commerciali

- XFlow (coinbase.com) 
- CipherTrace 
- Elliptic (elliptic.co) 
- Chainalyis (chainalysis.com) 
- Blockseer (blockseer.com) 
- Scorechain (scorechain.com) 
- Skry (skry.tech) 
- Blockchaingroup (blockchaingroup.io) 
- Sabr (sabr.io) 

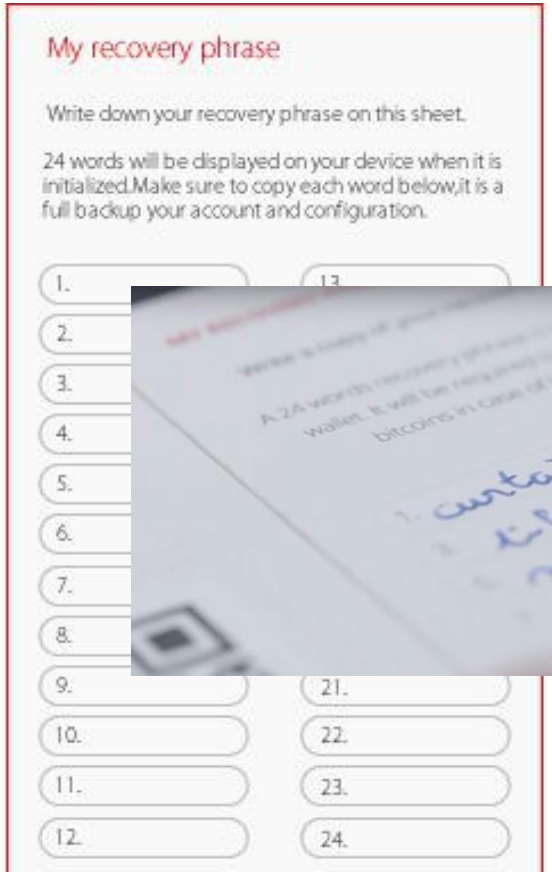
38

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 cercare durante perquisizione o descrizione?

Cosa cercare durante perquisizione o descrizione?



Cosa cercare durante perquisizione o descrizione?

Cosa cercare 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

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

Cosa non è possibile fare

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

Cosa si può fare ma non è utile allo scopo

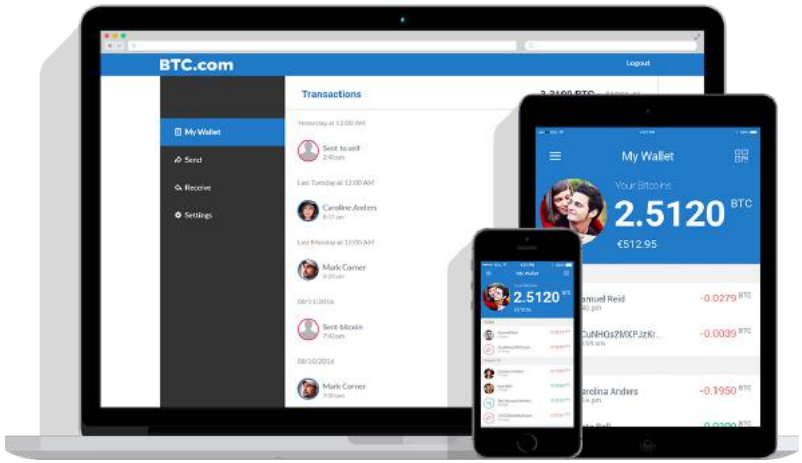
- **Sequestrare il PC/Smartphone del soggetto**
- **Fare copia forense del PC/Smartphone/Wallet**
- **Cambiare la password del wallet (prima bisogna trovarla con bruteforce o farsela dire)**

Cosa può essere persino pericoloso

- **Farsi consegnare le chiavi private**

Alcune ipotesi

- **Versare tutto su un conto intestato a Procura/Tribunale**
  - **Conto… intestato? O_o**
  - **Exchange?**
  - **Custodian?**
  - **Banca?**



Alcune ipotesi

- **Vendere la criptomoneta**
  - **Poi versarla in conto Procura/Tribunale**
  - **Conservarla in contanti**

Una proposta di protocollo

- 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)

Una proposta di protocollo

- 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
- Preferibile creare prima il wallet/indirizzo, metterlo al sicuro e solo dopo trasferire le criptomonete

Se non si conosce il wallet o l'indagato non collabora?

- Forzatura password dei wallet trovati
- Captatore
- Acquisire informazioni tramite intercettazioni tradizionali
- Non si può mai intervenire per bloccare/modificare transazioni, solo eventualmente tracciarla

Grazie per l'attenzione!

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