E-PRIVACY
XXVI
3-4 OTTOBRE
2019
AUTUNNO
BARI
BIBLIOTECA DELL'ORDINE
DEGLI AVVOCATI DI BARI

Dalle Istituzioni alla Blockchain

Metodologie, procedure e limiti delle indagini forensi e di Polizia Giudiziaria su blockchain ed exchange

Paolo Dal Checco
Consulente Informatico Forense

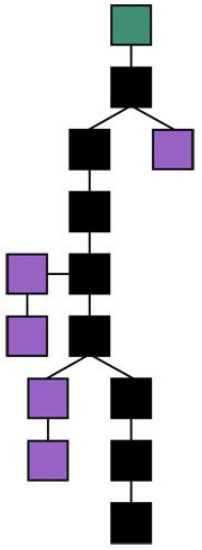
Paolo Dal Checco

- **PhD @UniTO nel gruppo di Sicurezza delle Reti e degli Elaboratori**
- **Collaboratore a contratto in master e perfezionamento presso @UniTO e @UniMI**
- **Cultore della materia in Informatica Giuridica Avanzata (IUS20) @UniMI**
- **Consulente Informatico Forense (Perizie Informatiche e Indagini Digitali) per Privati, Aziende, Avvocati, Procure, Tribunali, F.F.O.O.**
- Socio IISFA, AIP, Coinlex, Tech & Law, Clusit, Assobit
- Tra i fondatori dell'Associazione **ONIF** (www.onif.it)

- ***@forensico / paolo@dalchecco.it***
- ***Web: dalchecco.it, ransomware.it, osintbook.it, bitcoinforensics.it***

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

BitcoinCore

- **Blockchain**: la prova è pubblica, immutabile, già "forense"

```
du -h blocks/
13G     blocks/index
161G    blocks/
```

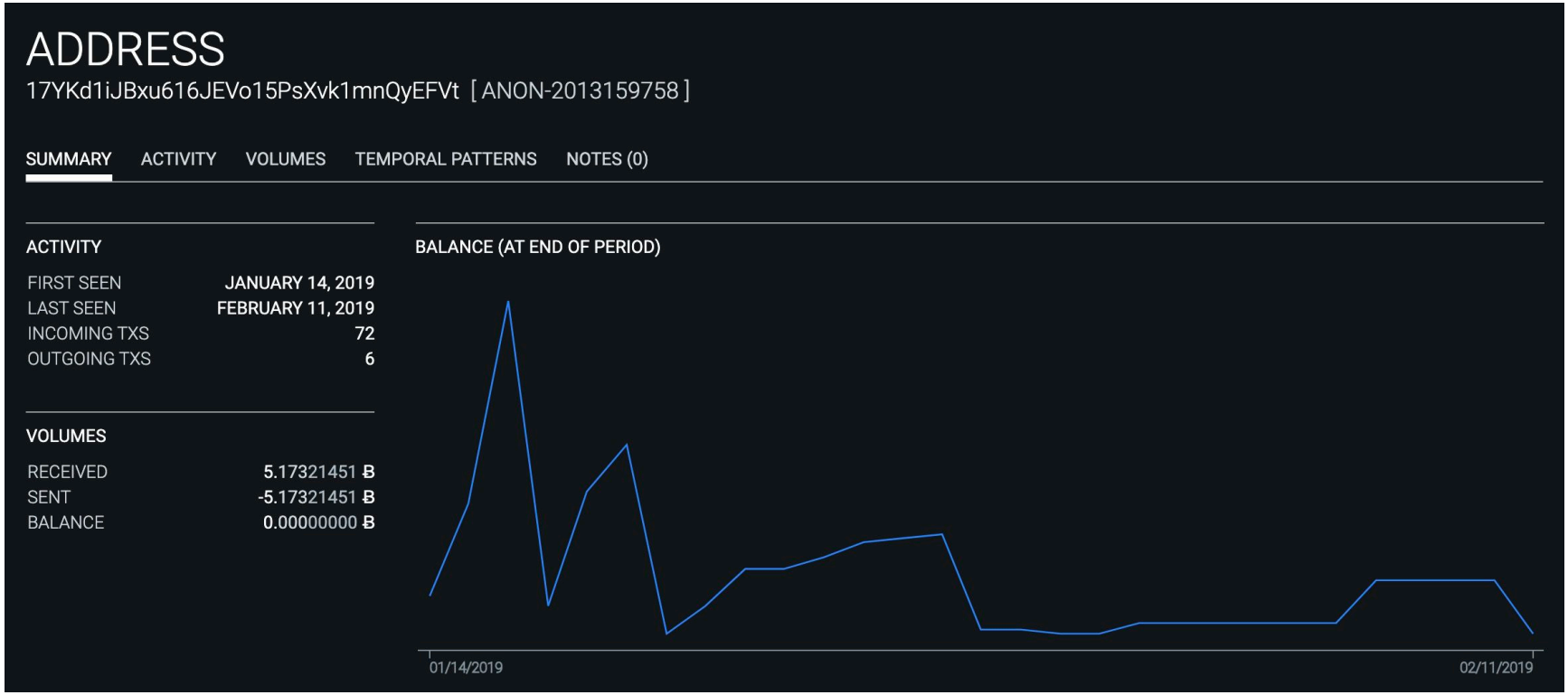
```
$ pwd
/home/btc/.bitcoin/blocks

$ ls -alh
total 105G
drwx------ 3 btc btcgroup  36K Jan 19 00:47 .
drwxr-xr-x 4 btc btcgroup 4.0K Jan 19 00:46 ..
-rw------- 1 btc btcgroup 128M Jan  4 00:59 blk00000.dat
-rw------- 1 btc btcgroup 128M Jan  4 01:00 blk00001.dat
-rw------- 1 btc btcgroup 128M Jan  4 01:00 blk00002.dat
-rw------- 1 btc btcgroup 128M Jan  4 01:00 blk00003.dat
-rw------- 1 btc btcgroup 128M Jan  4 01:01 blk00004.dat
```

Bitcoin Forensics

BitcoinCore

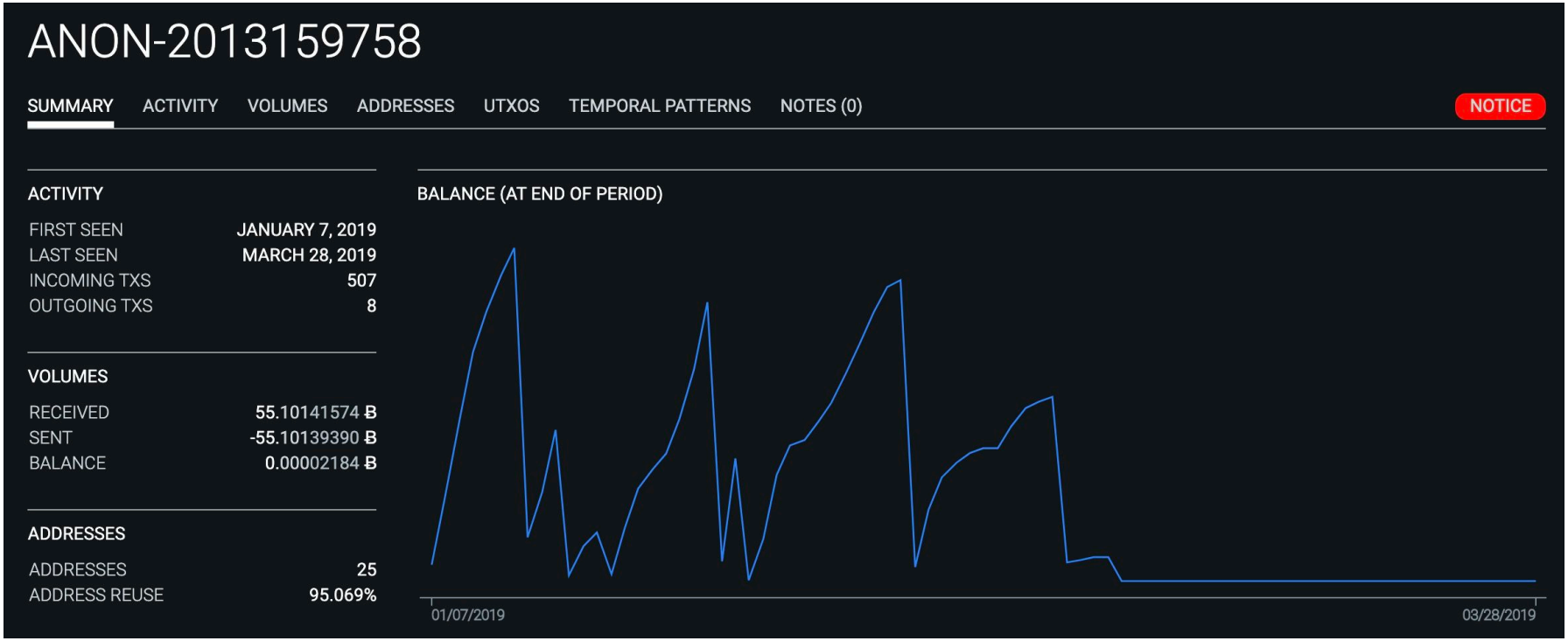
```
PMB:blocks Paolo$ hexdump -C blk00000.dat | head -n 20
00000000  f9 be b4 [illegible]                                 |................|
00000010  00 00 [illegible]                                   |................|
00000020  00 00 [illegible]                                   |............;...|
00000030  7a 7b [illegible]                                   |z{..z.,>gv.a....|
00000040  88 8a [illegible]                                   |..Q2:...K.^J)._I|
00000050  ff ff [illegible]                                   |......+|........|
00000060  00 00 [illegible]                                   |................|
00000070  00 00 [illegible]                                   |................|
00000080  ff ff [illegible]                                   |..M.......EThe T|
00000090  69 6d [illegible]                                   |imes 03/Jan/2009|
000000a0  20 43 [illegible]                                   | Chancellor on b|
000000b0  72 69 [illegible]                                   |rink of second b|
000000c0  61 69 [illegible]                                   |ailout for banks|
000000d0  ff ff [illegible]                                   |........*....CA.|
000000e0  67 8a [illegible]                                   |g....UH'.g..q0..|
000000f0  5c d6 [illegible]                                   |\..(.9..yb...a..|
00000100  49 f6 [illegible]                                   |I..?L.8..U......|
00000110  5c 38 4d [illegible]                                |\8M....W.Lp+k.._|
00000120  ac 00 00 00 00 f9 be b4  d9 d7 00 00 00 01 00 00    |................|
00000130  00 6f e2 8c 0a b6 f1 b3  72 c1 a6 a2 46 ae 63 f7    |.o......r...F.c.|
```

Strumenti online: blockchain explorers



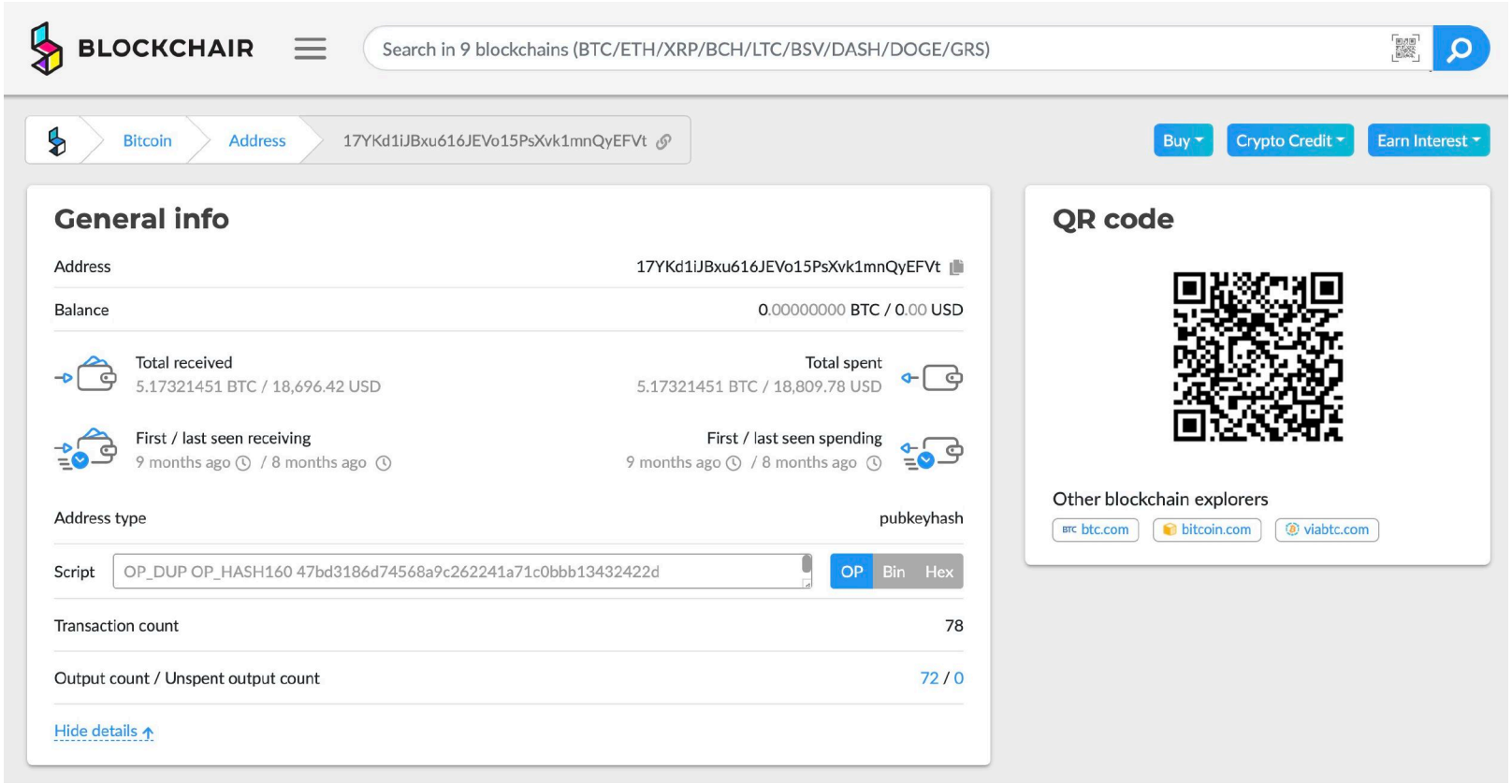
https://oxt.me

Strumenti online: blockchain explorers



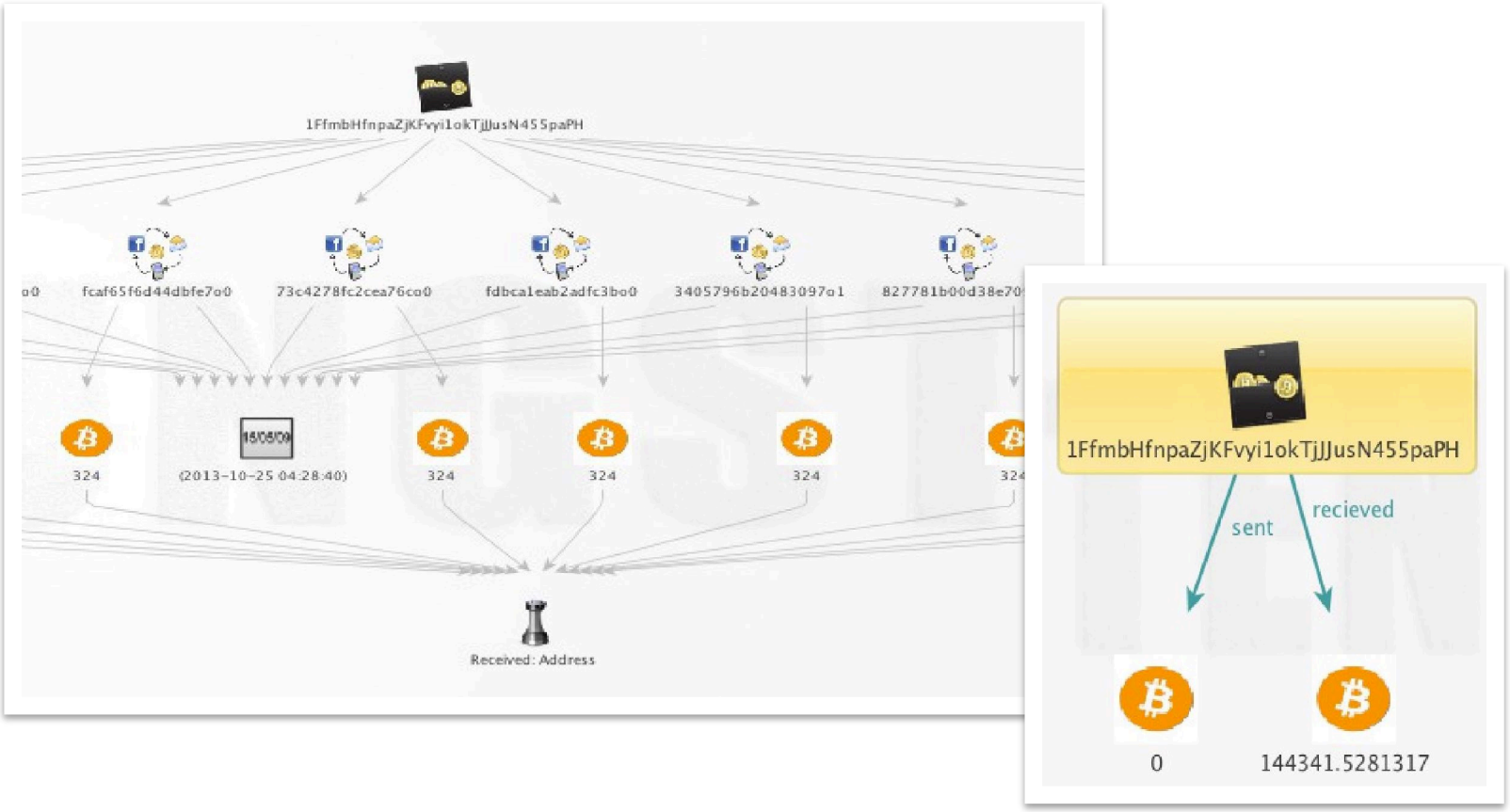
https://oxt.me

Strumenti online: blockchain explorers

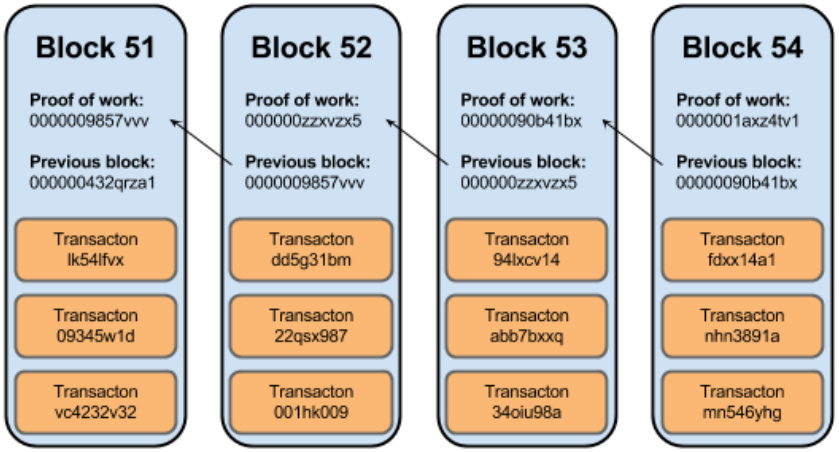


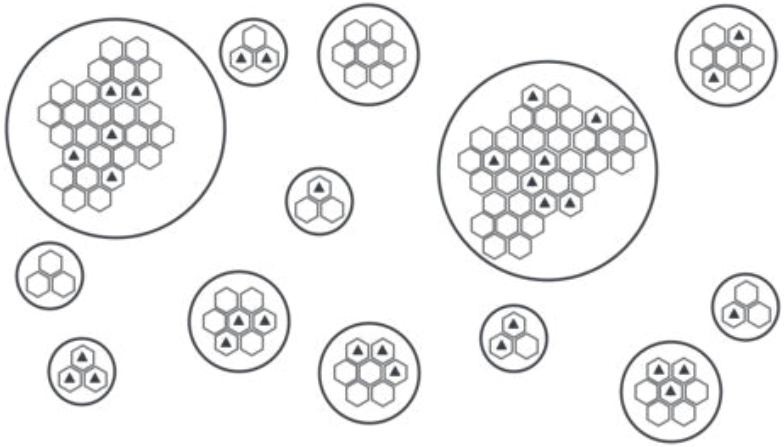
https://blockchair.com

Strumenti off/online: Maltego



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

WalletExplorer.com: smart Bitcoin block explorer

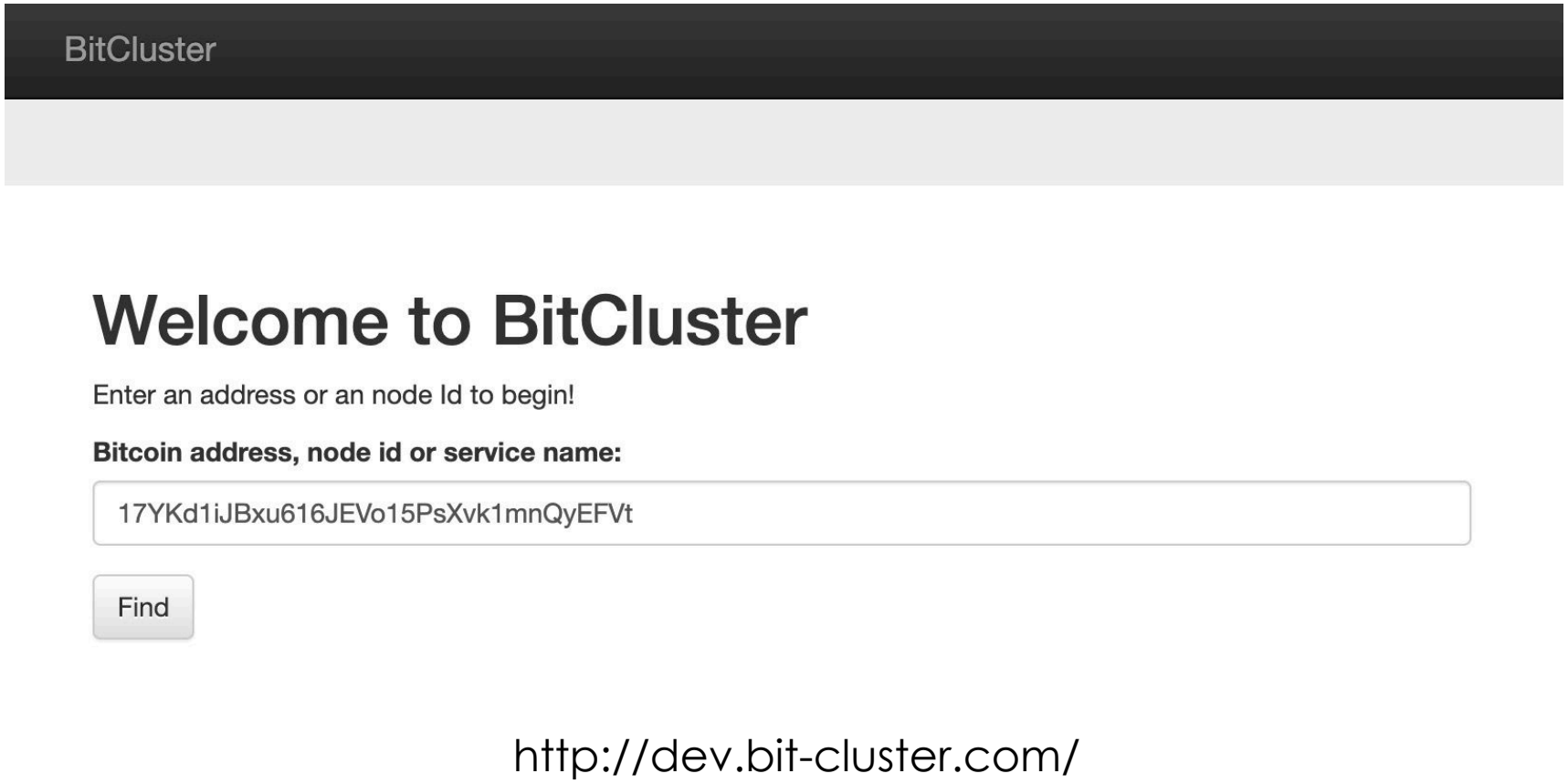
Wallet [00225e1533] (show transactions)

Page 1 / 1 (total addresses: 25)

address	balance	incoming txs	last used in block
1AuXbXYsB6HQLpiEhFr2EYp3DDioJDv46H	0.00001092	18	569229
1GF8J1XRaiX2oHM7SQo9VAFAtWZcRgMncg	0.00000546	12	564123
142e8SgyTLnkvwkDkNNon9jMtKY4UDvQqr	0.00000546	10	564123
145SmyE7DBEQExsnXZobojbQqr5UdgbCHh	0.	74	564123
17YKd1iJBxu616JEVo15PsXvk1mnQyEFVt	0.	72	562563
1G1qFoadiDxa7zTvppSMJhJi63tNUL3cy7	0.	70	560509
18Pt4B7Rz7Wf491FGQHPsfDeKRqnkyrMo6	0.	58	559366
1Jh1miFmhTmGQvn6Zejaqg85viD4k1vVjG	0.	47	564123
1JgjcCi7sWmr3L7YXKaTAW2qoQdKztcSeu	0.	34	564123
1GjZSJnpU4AfTS8vmre6rx7eQgeMUq8VYr	0.	25	560509
164NL2muDgdS83LpKWpwaky9Btdwanskb1	0.	14	564783

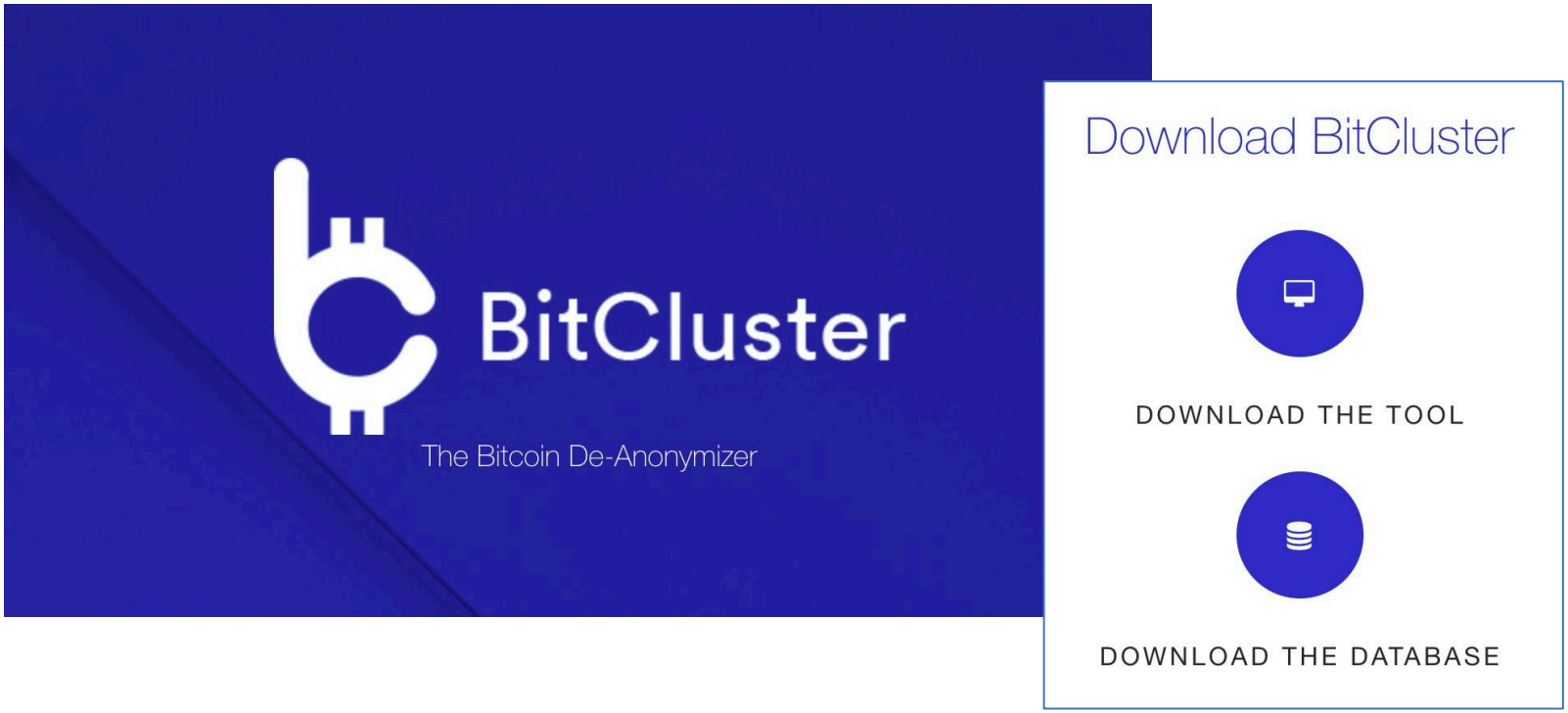
https://www.walletexplorer.com

Clustering



http://dev.bit-cluster.com/

Clustering



http://dev.bit-cluster.com/

Wallet SPV e leak

- I wallet SPV non scaricano l'intera blockchain, devono usare server
- I client SPV BIP37 utilizzano **filtri di bloom** per identificare e passare gli indirizzi del wallet ai server
  - Filtro di bloom: sistema per testare in modo efficiente se un elemento è parte di un insieme, con falsi positivi ma senza falsi negativi
- Se queste richieste vengono in qualche modo intercettate…
- Jonas Nick ha portato avanti parecchie ricerche sull'argomento, concludendo che un client SPV con pochi indirizzi Bitcoin (es. <20) rischia di lasciare facilmente identificare tutti gli indirizzi

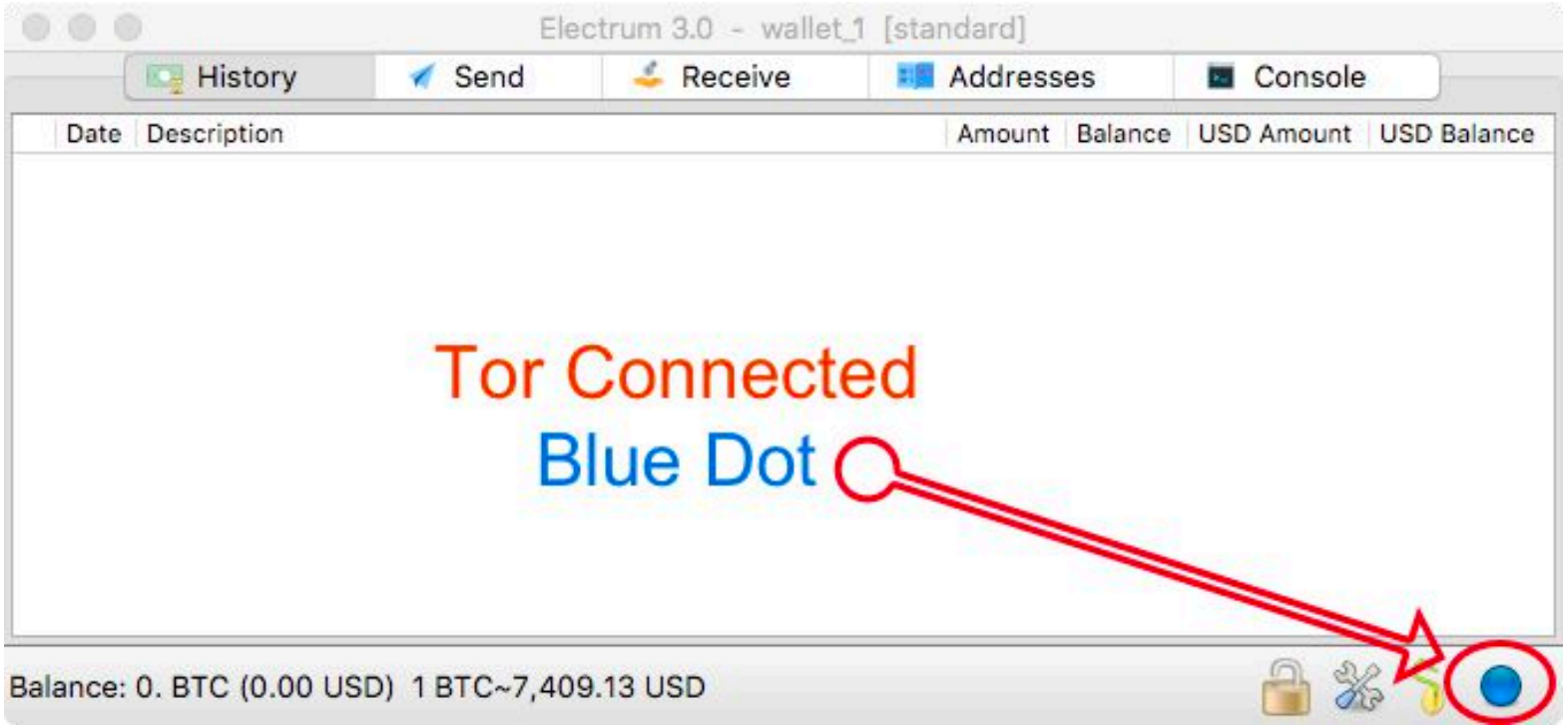
https://jonasnick.github.io/blog/2015/02/12/privacy-in-bitcoinj/

Mixing

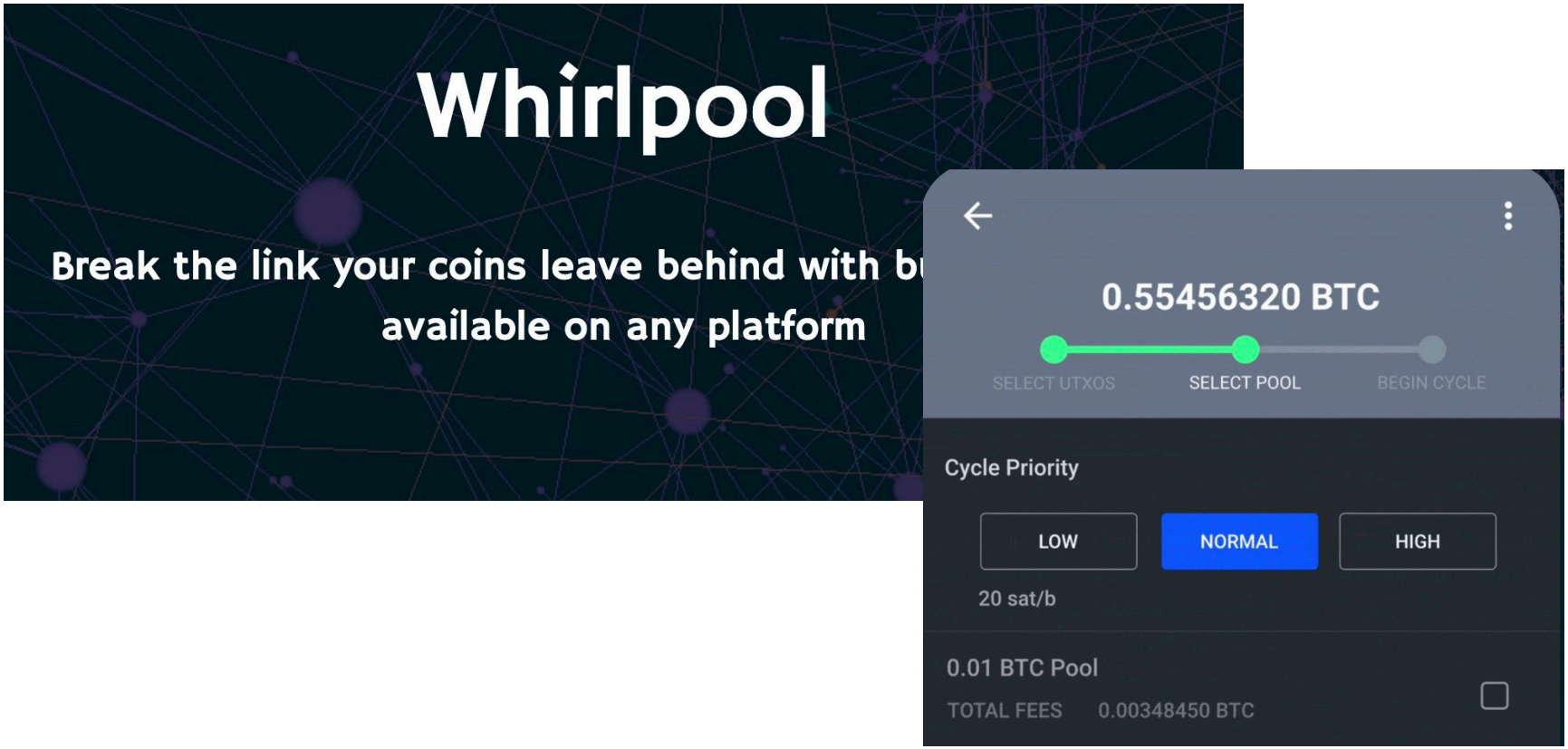
- Sempre più frequente utilizzo dei Mixer o Tumbler

Tor

- È sempre possibile operare dietro la rete Tor

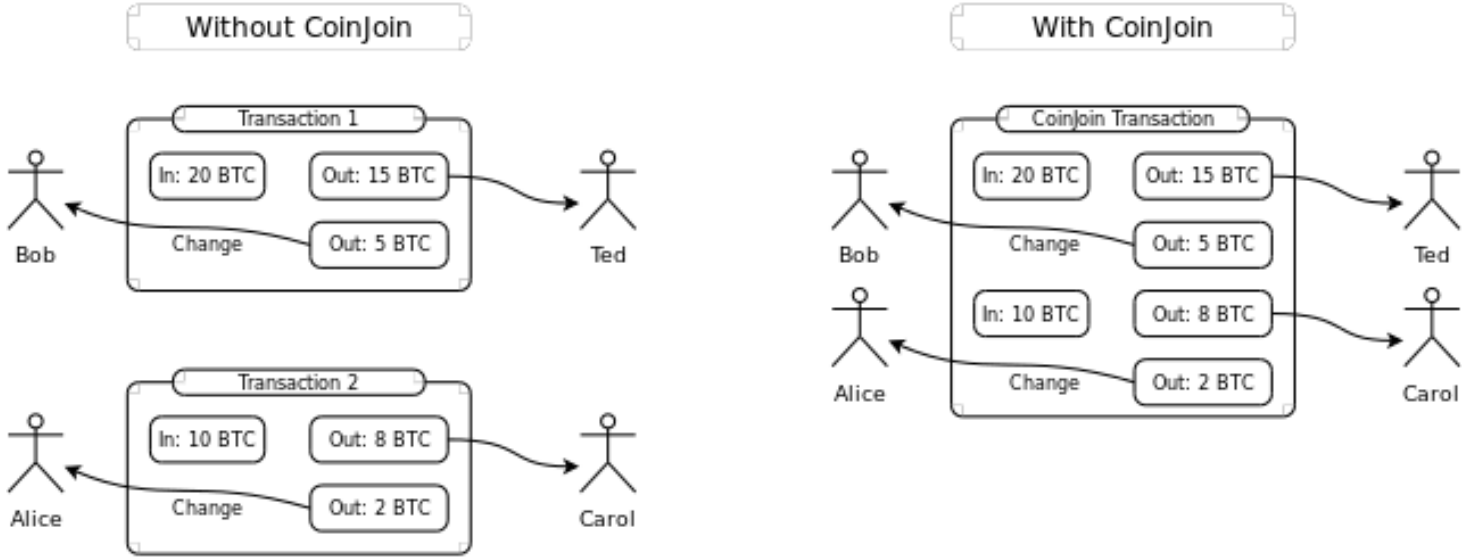


CoinJoin


Whirlpool
Break the link your coins leave behind with b
available on any platform
0.55456320 BTC
SELECT UTXOS
SELECT POOL
BEGIN CYCLE
Cycle Priority
LOW
NORMAL
HIGH
20 sat/b
0.01 BTC Pool
TOTAL FEES 0.00348450 BTC

Demixing

- Alcuni mixer (es. CoinJoin, etc… non parliamo ora dei Tumbler) utilizzano dei pattern/protocolli che possono permettere una ricostruzione parziale dell'ordine delle transazioni e identificare il legame tra entrata e uscita



Currency exchangers

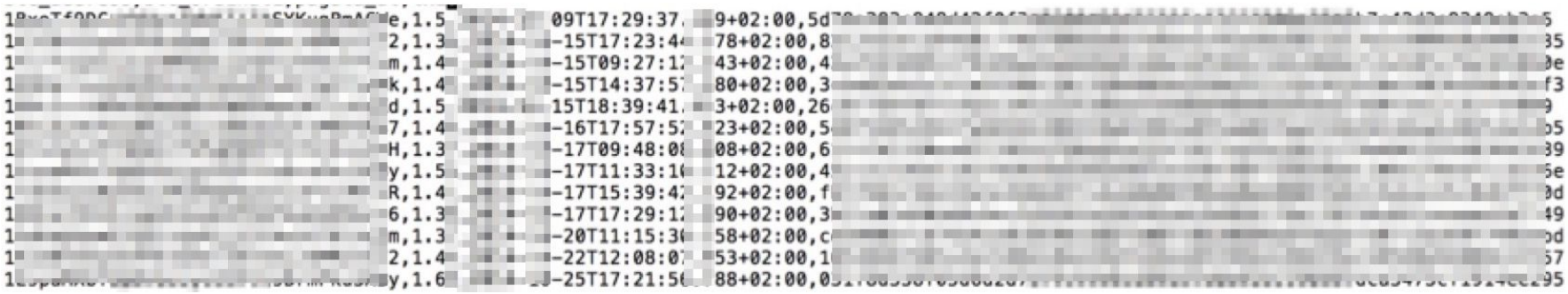
- Ci sono siti che forniscono servizio di cambio da una criptomoneta a un'altra, senza passare per moneta FIAT, spesso senza registrazione
- Questi siti possono utilizzare delle tracce che permettono di crare dei pattern pattern per identificare i punti di uscita (ex. Wallet Wannacry verso Monero)

Strumenti commerciali d'intelligence

- ~~Neutrino PFlow (neutrino.nu)~~ 
- Elliptic (elliptic.co) 
- Chainalyis (chainalysis.com) 
- Blockseer (blockseer.com) 
- Scorechain (scorechain.com) 
- Skry (skry.tech) 
- Blockchaingroup (blockchaingroup.io) 
- Sabr (sabr.io) 

Gli exchange come endpoint

- Gli exchange hanno l'elenco delle transazioni EUR-> BTC e viceversa, importanti per le investigazioni sul Bitcoin



- Gli exchange hanno anche spesso email, Postepay, Carta di credito, IBAN di chi ha eseguito il versamento, oltre indirizzo IP, cellulare e KYC
- Possiamo seguire la blockchain in avanti e indietro, tenendo conto degli ovvi limiti delle transazioni con multipli IN e OUT e dei change address

Paolo Dal Checco

Web: www.dalchecco.it

Mail: paolo@dalchecco.it