

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

**Dalle Istituzioni
alla Blockchain**

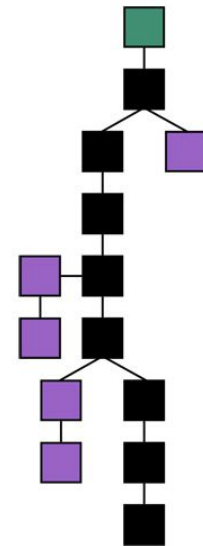
**Metodologie, procedure e limiti delle
indagini forensi e di Polizia Giudiziaria
su blockchain ed exchange**

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



- **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

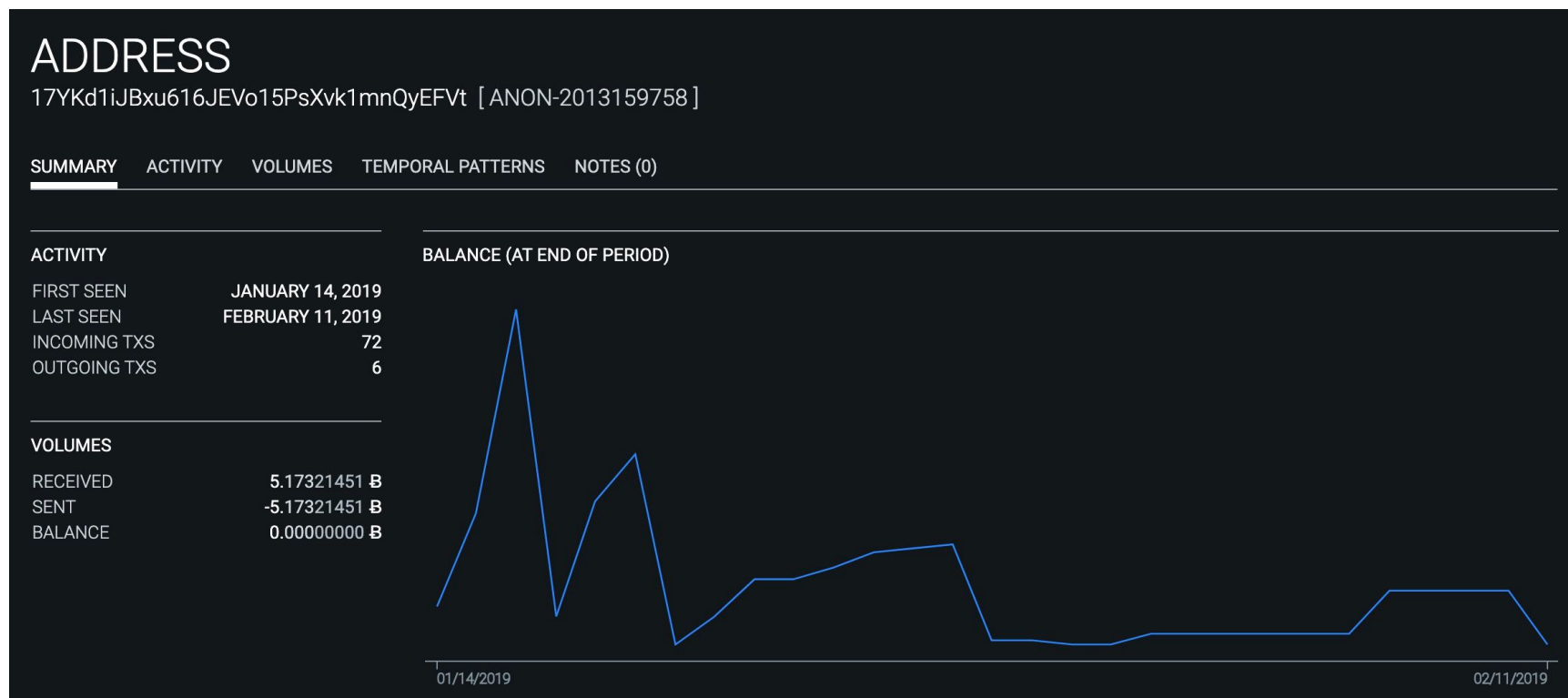


PMB:blocks Paolo\$ hexdump -C blk00000.dat | head -n 20

00000000	f9	be	b4	16	80	00	00	00	00	
00000010	00	00	00	00	00	00	00	00	00	
00000020	00	00	00	00	00	00	00	00	00	
00000030	7a	7b	00	00	00	00	00	00	00	;..
00000040	88	8a	00	00	00	00	00	00	00	..Q2:...K.^J)._I
00000050	ff	ff	00	00	00	00	00	00	00	+
00000060	00	00	00	00	00	00	00	00	00	
00000070	00	00	00	00	00	00	00	00	00	
00000080	ff	ff	00	00	00	00	00	00	00	
00000090	69	6d	00	00	00	00	00	00	00	..M.....EThe TI
000000a0	20	43	00	00	00	00	00	00	00	imes 03/Jan/2009
000000b0	72	69	00	00	00	00	00	00	00	Chancellor on bl
000000c0	61	69	00	00	00	00	00	00	00	rink of second bl
000000d0	ff	ff	00	00	00	00	00	00	00	ailout for banks
000000e0	67	8a	00	00	00	00	00	00	00	*....CA.
000000f0	5c	d6	00	00	00	00	00	00	00	g....UH'.g..q0..
00000100	49	f6	00	00	00	00	00	00	00	\\..(9..yb...a..
00000110	5c	38	4a	00	00	00	00	00	00	I..?L.8..U.....
00000120	ac	00	00	00	00	f9	be	b4	d9	\\8M....W.Lp+k...
00000130	00	6f	e2	8c	0a	b6	f1	b3	72	r...F.c.

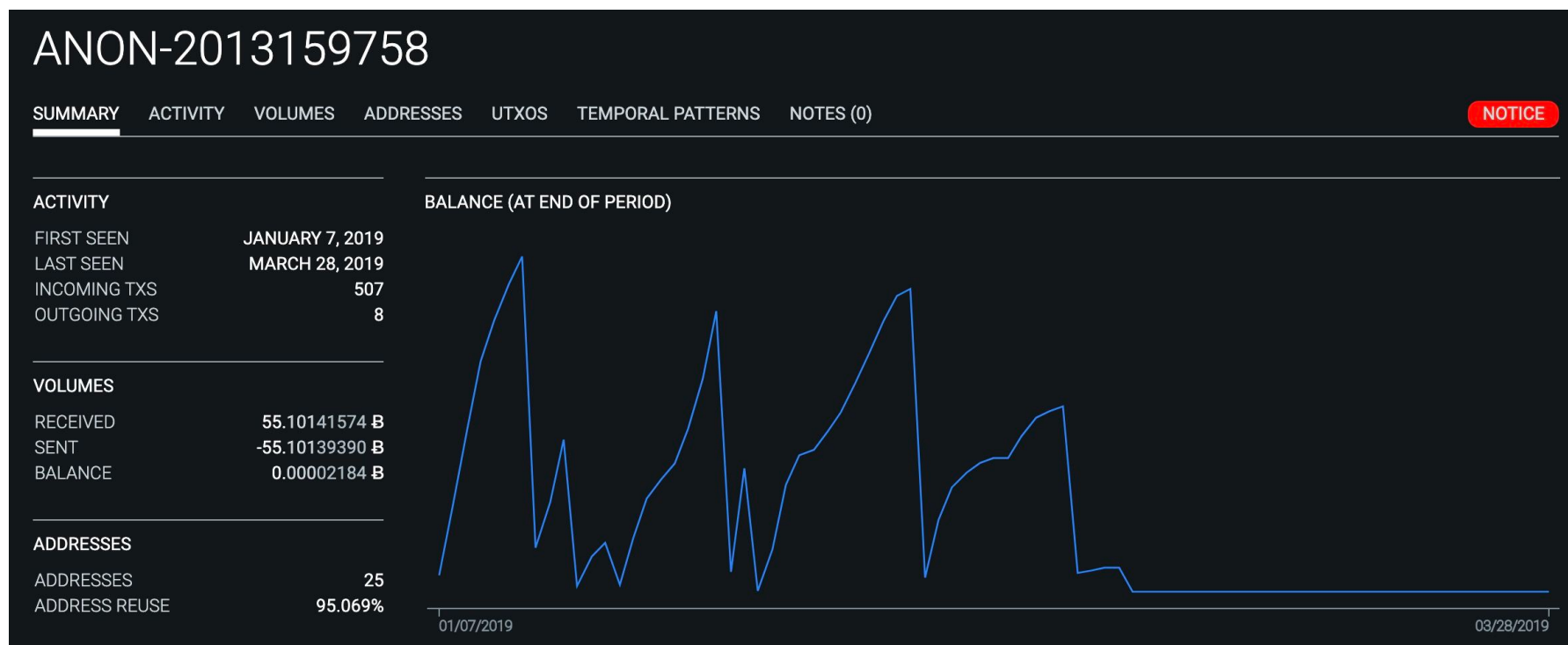
The image shows the front page of The Times newspaper from Saturday, January 3, 2009. The main headline is 'Eat Out from £5' with a sub-headline 'More than 900 great restaurants, including four Gordon Ramsay favourites from £15'. Below this is a large photograph of a soldier in a tank, with the headline 'Israel prepares to send tanks and troops into Gaza'. To the right of the tank photo is a small article about Michael Sheen, Frost, Nixon and me. Below the tank photo is a large headline 'Chancellor on brink of second bailout for banks'. To the right of this headline is a small article about Salman Rushdie. The newspaper is overlaid on a background of a hex dump of a Bitcoin block.

Strumenti online: blockchain explorers



<https://oxt.me>

Strumenti online: blockchain explorers



<https://oxt.me>

Strumenti online: blockchain explorers

The screenshot shows the Blockchair website interface for a Bitcoin address. The top navigation bar includes the Blockchair logo, a search bar with the text "Search in 9 blockchains (BTC/ETH/XRP/BCH/LTC/BSV/DASH/DOGE/GRS)", and a QR code icon. Below the navigation bar, there are buttons for "Buy", "Crypto Credit", and "Earn Interest". The main content area is divided into two columns. The left column, titled "General info", displays the address "17YKd1iJBxu616JEVo15PsXvk1mnQyEFVt" and its balance "0.00000000 BTC / 0.00 USD". It also shows transaction statistics: "Total received" (5.17321451 BTC / 18,696.42 USD) and "Total spent" (5.17321451 BTC / 18,809.78 USD). The "First / last seen receiving" and "First / last seen spending" dates are both "9 months ago / 8 months ago". The "Address type" is "pubkeyhash". The "Script" field shows "OP_DUP OP_HASH160 47bd3186d74568a9c262241a71c0bbb13432422d" with tabs for "OP", "Bin", and "Hex". The "Transaction count" is 78, and the "Output count / Unspent output count" is 72 / 0. A "Hide details" link is at the bottom. The right column, titled "QR code", displays a QR code for the address. Below the QR code, there is a section for "Other blockchain explorers" with links to "btc btc.com", "bitcoin bitcoin.com", and "viabtc.com".

BLOCKCHAIR Search in 9 blockchains (BTC/ETH/XRP/BCH/LTC/BSV/DASH/DOGE/GRS)

Bitcoin Address 17YKd1iJBxu616JEVo15PsXvk1mnQyEFVt Buy Crypto Credit Earn Interest

General info

Address 17YKd1iJBxu616JEVo15PsXvk1mnQyEFVt

Balance 0.00000000 BTC / 0.00 USD

Total received 5.17321451 BTC / 18,696.42 USD Total spent 5.17321451 BTC / 18,809.78 USD

First / last seen receiving 9 months ago / 8 months ago First / last seen spending 9 months ago / 8 months ago

Address type pubkeyhash

Script OP_DUP OP_HASH160 47bd3186d74568a9c262241a71c0bbb13432422d OP Bin Hex

Transaction count 78

Output count / Unspent output count 72 / 0

[Hide details](#)

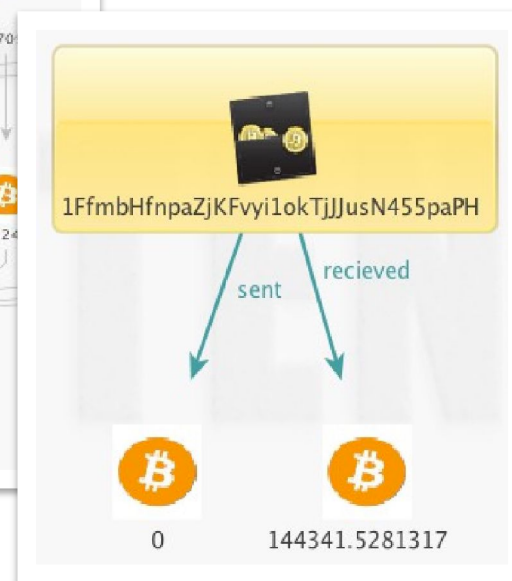
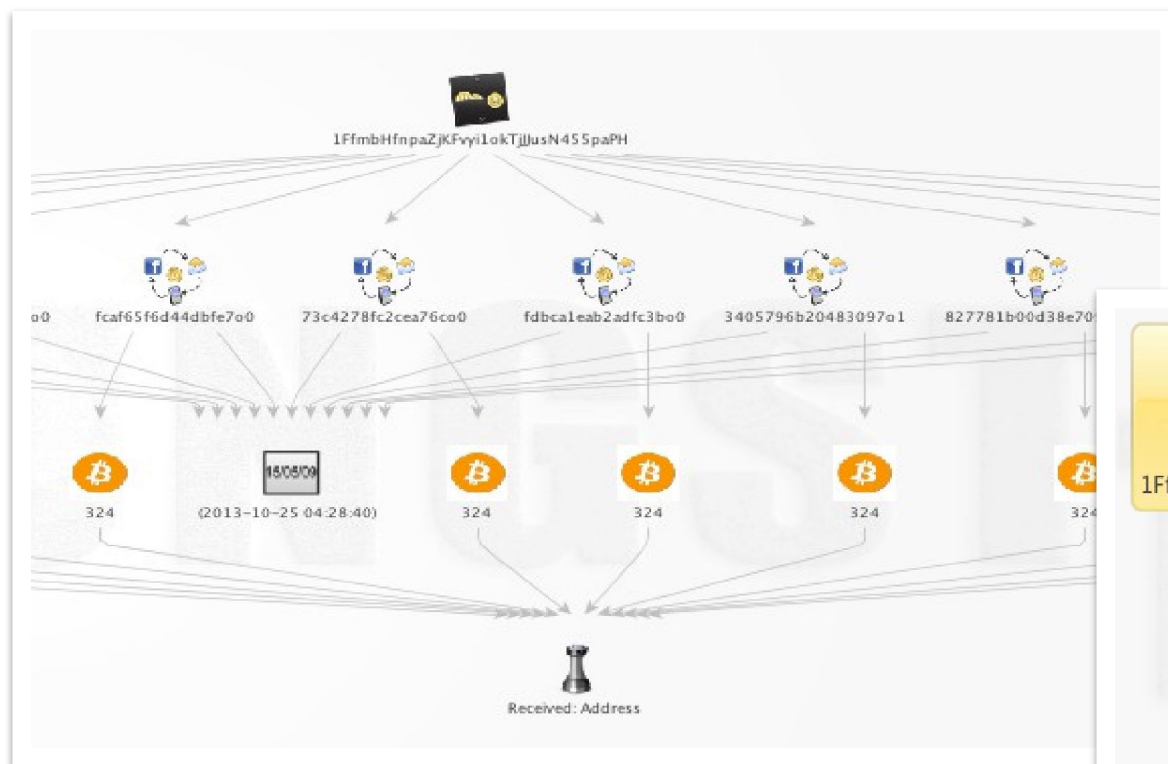
QR code

Other blockchain explorers

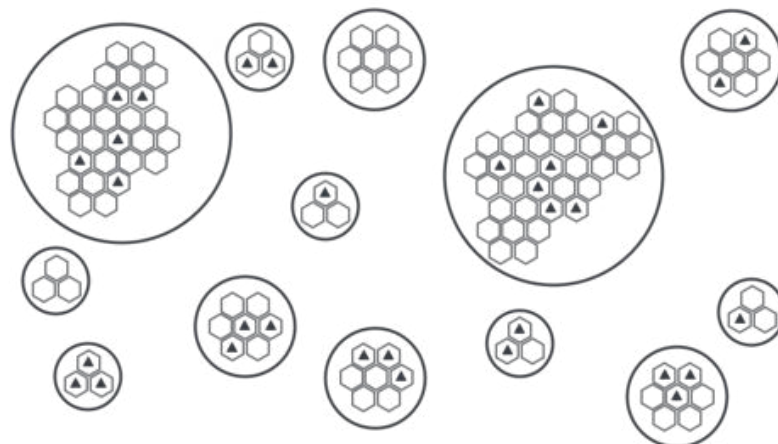
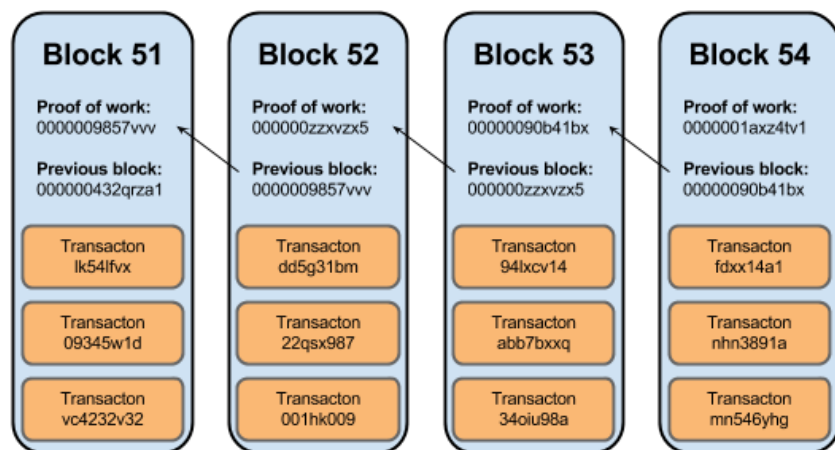
[btc btc.com](#) [bitcoin bitcoin.com](#) [viabtc.com](#)

<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 il 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
164NL2muDgdS83LpKWpwaky9Btdwansk1	0.	14	564783

<https://www.walleexplorer.com>

Clustering

BitCluster

Welcome to BitCluster

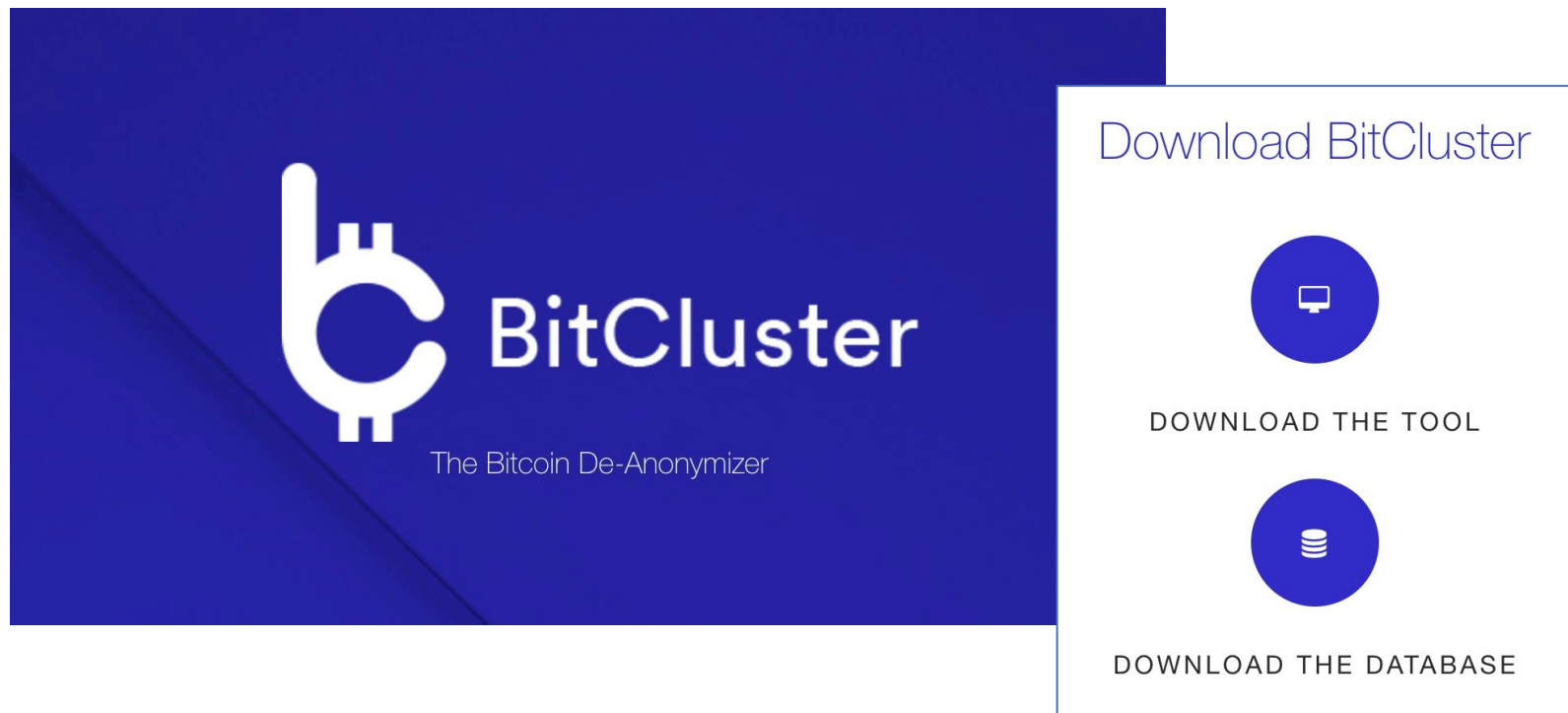
Enter an address or an node Id to begin!

Bitcoin address, node id or service name:

Find

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

Clustering



The image shows a promotional graphic for BitCluster. On the left, a dark blue rectangle contains a white Bitcoin symbol with a hand cursor pointing at it, followed by the text 'BitCluster' and 'The Bitcoin De-Anonymizer'. To the right, a white box with a blue border contains the text 'Download BitCluster' at the top. Below this, there are two circular icons: the first is a blue circle with a white computer monitor icon, and the second is a blue circle with a white database cylinder icon. Under the first icon is the text 'DOWNLOAD THE TOOL', and under the second is 'DOWNLOAD THE DATABASE'.

Download BitCluster

DOWNLOAD THE TOOL

DOWNLOAD THE DATABASE

<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

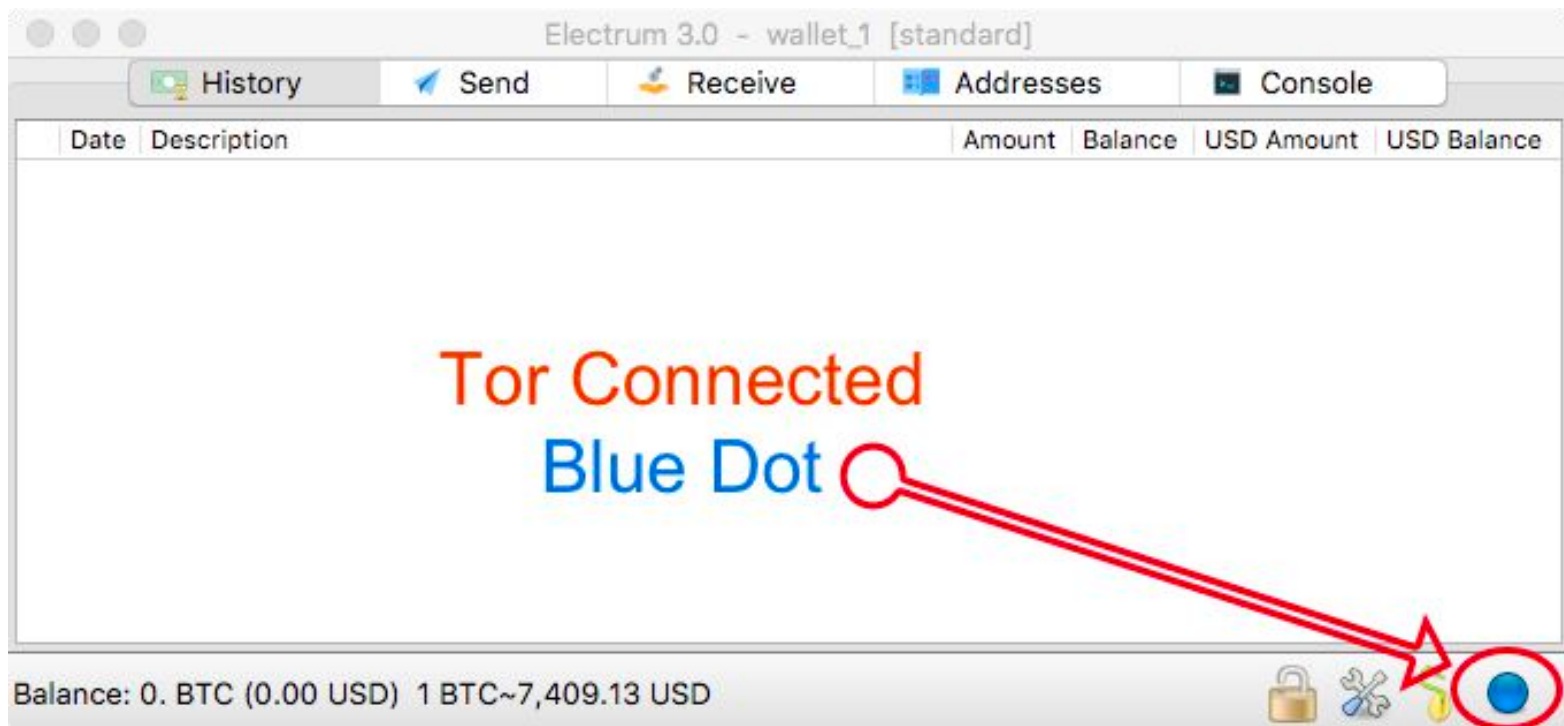


BITCOIN MIXER

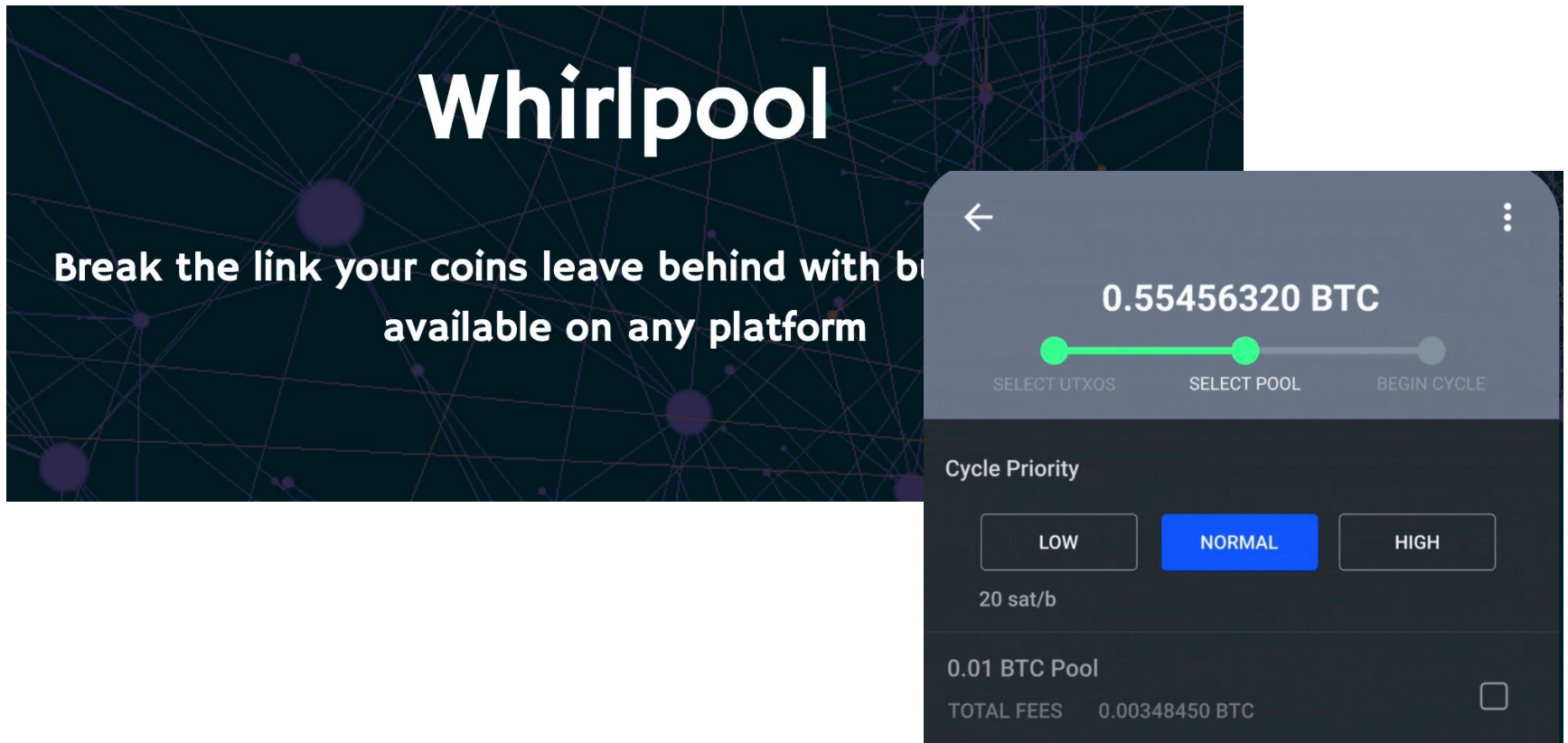
Bitcoin Mixer (Blender) is something that helps you to shuffle your bitcoins using our algorithms and to secure your identity.

Tor

- È sempre possibile operare dietro la rete Tor



CoinJoin



The image shows a mobile application interface for Whirlpool, a Bitcoin privacy tool. The background is a dark blue network graph. The word "Whirlpool" is written in large white letters. Below it, the text "Break the link your coins leave behind with b" and "available on any platform" is visible. Overlaid on the right is a dark grey control panel. At the top of the panel is a back arrow and a menu icon. Below them is the amount "0.55456320 BTC". A horizontal slider with two green dots is positioned below the amount. Under the slider are three labels: "SELECT UTXOS", "SELECT POOL", and "BEGIN CYCLE". Below the slider is a section titled "Cycle Priority" with three buttons: "LOW", "NORMAL" (which is highlighted in blue), and "HIGH". Below these buttons is the text "20 sat/b". At the bottom of the panel, it says "0.01 BTC Pool" and "TOTAL FEES 0.00348450 BTC". There is a small square icon in the bottom right corner of the panel.

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

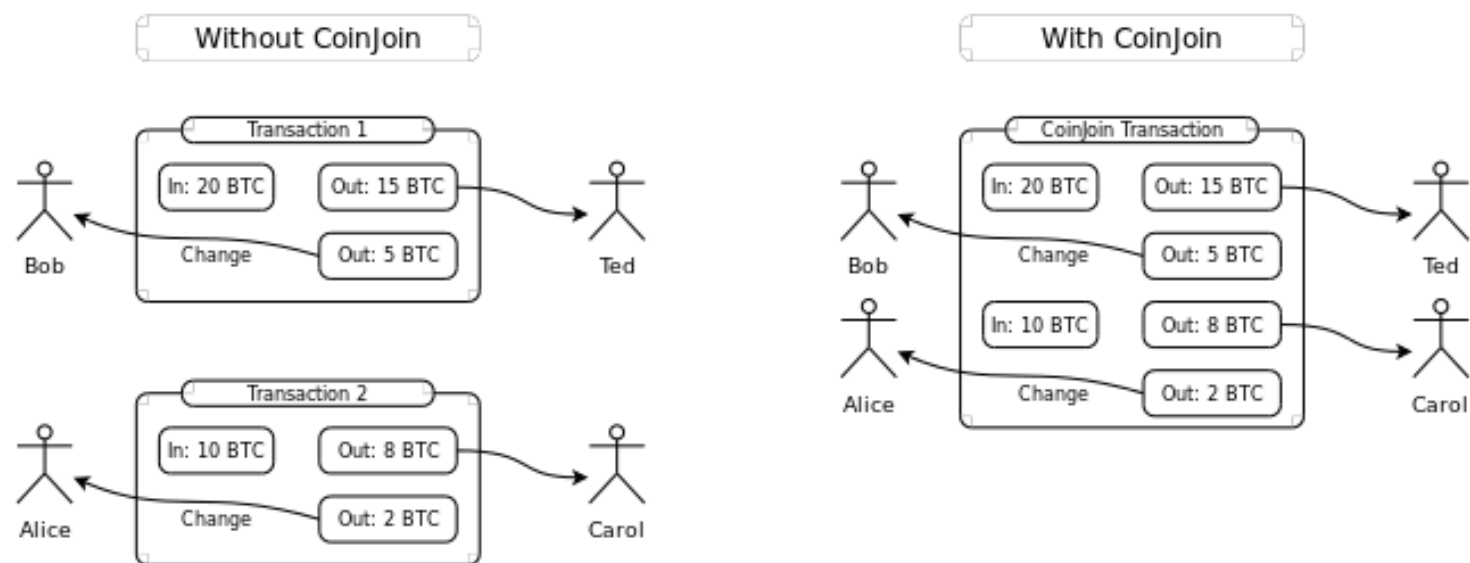
20 sat/b

0.01 BTC Pool

TOTAL FEES 0.00348450 BTC

Demixing

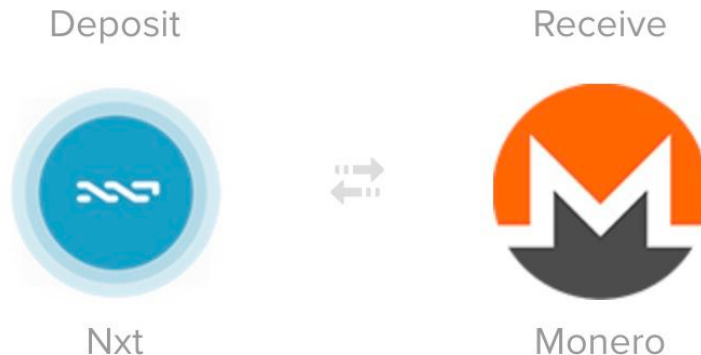
- Alcuni mixer (es. CoinJoin, etc... non parliamo ora dei Tumbler) utilizzano dei pattern/protocolli che possono permettere una ricostruzione parziale dell'ordine delle transazioni e identificare il legame tra entrata e uscita



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 creare dei pattern pattern per identificare i punti di uscita (ex. Wallet Wannacry verso Monero)

Choose Which Assets to Trade



Strumenti commerciali d'intelligence

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

- | | | | | |
|---|-------------|-------------|------------|----|
| 1 | 09T17:29:37 | 9+02:00,5d | 5 | |
| 1 | 2,1.3 | -15T17:23:4 | 78+02:00,8 | 35 |
| 1 | m,1.4 | -15T09:27:1 | 43+02:00,4 | 3e |
| 1 | k,1.4 | -15T14:37:5 | 80+02:00,3 | f3 |
| 1 | d,1.5 | 15T18:39:41 | 3+02:00,26 | 9 |
| 1 | 7,1.4 | -16T17:57:5 | 23+02:00,5 | 35 |
| 1 | H,1.3 | -17T09:48:0 | 08+02:00,6 | 39 |
| 1 | y,1.5 | -17T11:33:1 | 12+02:00,4 | 3e |
| 1 | R,1.4 | -17T15:39:4 | 92+02:00,f | 3d |
| 1 | 6,1.3 | -17T17:29:1 | 90+02:00,3 | 49 |
| 1 | m,1.3 | -20T11:15:3 | 58+02:00,c | 3d |
| 1 | 2,1.4 | -22T12:08:0 | 53+02:00,1 | 57 |
| 1 | y,1.6 | -25T17:21:5 | 88+02:00,0 | 35 |

- Metodologie, procedure e limiti delle indagini forensi e di PG su blockchain ed exchange – Paolo Dal Checco*

Paolo Dal Checco

Web: www.dalchecco.it

Mail: paolo@dalchecco.it

