HACK IN BO
Spring 2016 Edition

Bitcoin Forensics

Aspetti tecnici e investigativi della criptomoneta

Paolo Dal Checco, *Consulente Informatico Forense*
Studio Associato Di.Fo.B

Chi sono

- PhD @UniTO nel gruppo di Sicurezza delle Reti e degli Elaboratori
- Professore a Contratto di Sicurezza Informatica @UniTO (SUISS)
- Consulente Informatico Forense (Perizie Informatiche) per Privati, Aziende, Avvocati, Procure, Tribunali, F.F.O.O.
- Tra i fondatori dell'Associazione DEFTA (www.deftlinux.net) e ONIF (www.onif.it)
- Direttivo Associazione IISFA, socio Tech & Law, Clusit
- paolo@dalchecco.it - @forensico - @studiodifob
- dalchecco.it, difob.it, bitcoinforensics.it, ransomware.it

Cosa dicono del Bitcoin ;-)

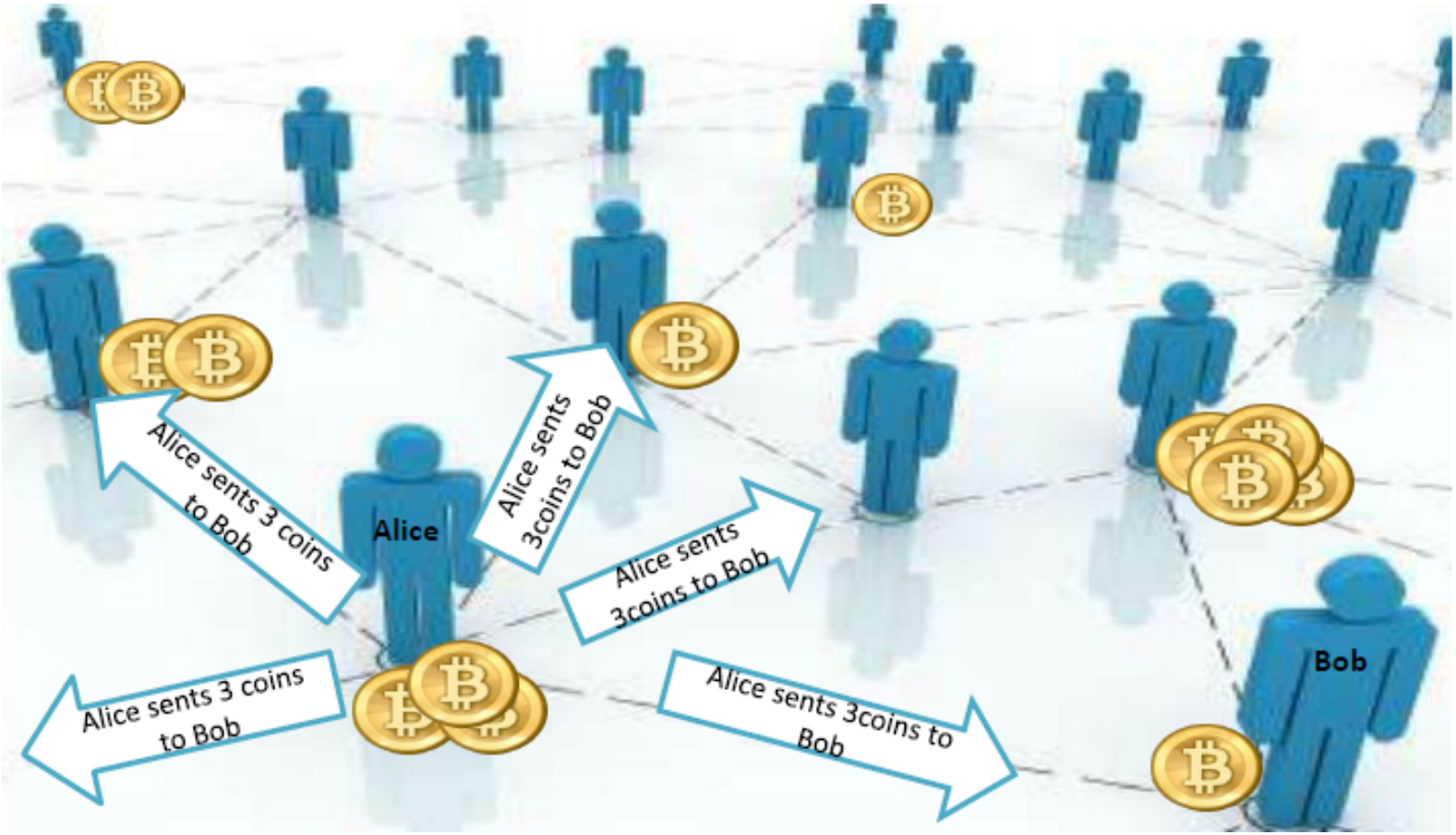
"una valuta elettronica la cui tracciabilità è criptata attraverso sequenze numeriche pressapoco intraducibili"

Cosa è il Bitcoin

- 'B' maiuscola, il protocollo, 'b' minuscola, l'unità di moneta
- Rete di pagamento digitale ideata nel 2009 da un anonimo "Satoshi Nakamoto", basata sulla sulla crittografia ("crittovaluta") e in particolare:
  - Algoritmo di firma digitale asimmetrica **ECDSA**
  - Algoritmi di hashing **SHA256** e **RIPEMD 160**

- Peer to peer, nessun ente centralizzato
- Limite di generazione BTC: 21 MLN raggiunto nel 2140
- Controvalore in valuta fiat stabilito dal mercato

Assenza di autorità centrale



Terminologia

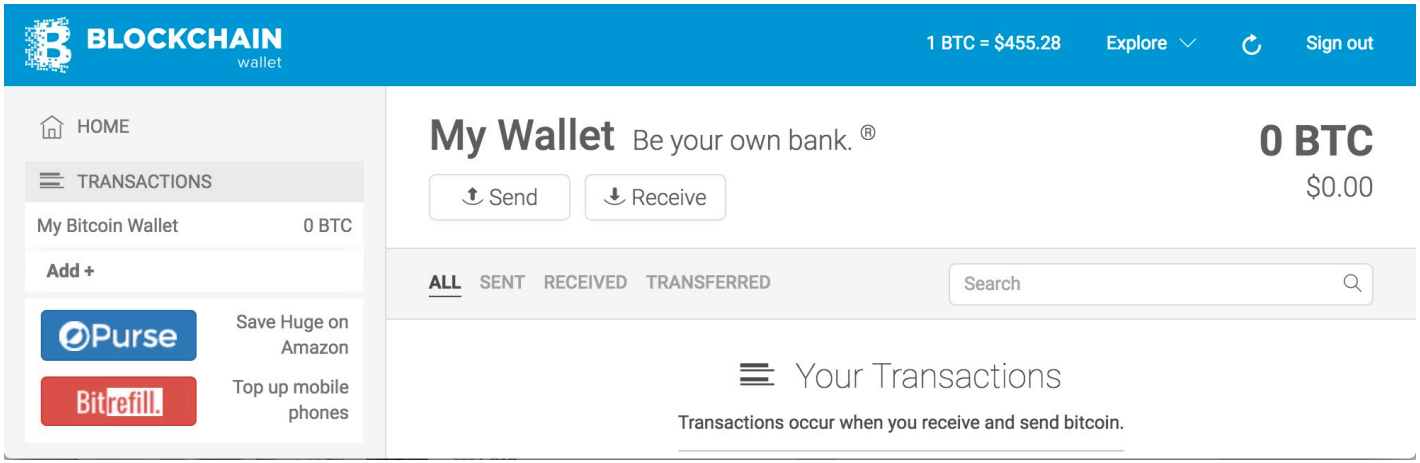
- **Chiave privata**: 256 bit, il codice da cui viene generato l'indirizzo, passando tramite la chiave pubblica generata da quella privata. Posso dimostrare di averla firmando un messaggio.
- **Chiave pubblica**: 512 bit, derivata dalla chiave privata tramite algoritmo a chiave pubblica/privata ECDSA 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.

Terminologia

Mobile Desktop Hardware Web

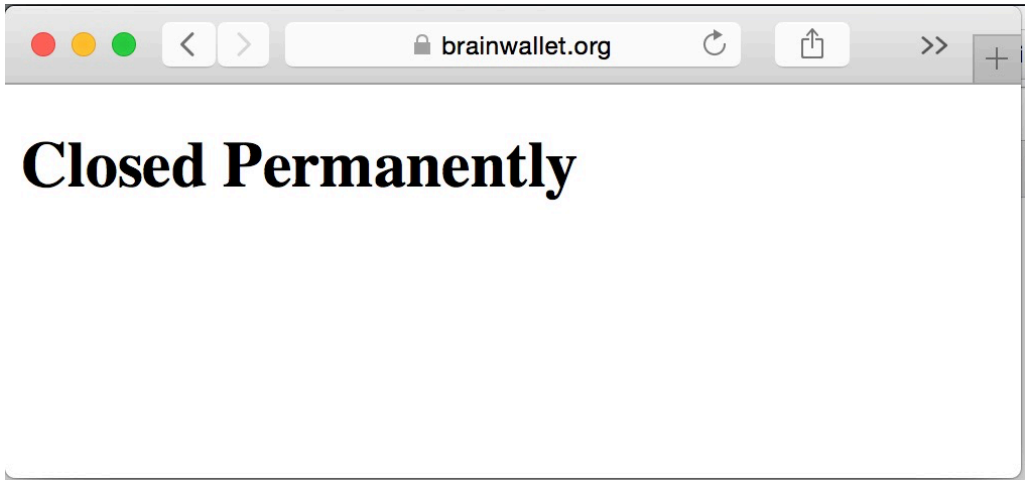
- **Wallet**: Il portafoglio che raccoglie i diversi indirizzi/address bitcoin, più facile da gestire rispetto a lavorare direttamente con indirizzi/transazioni

- Hot/Cold Wallet
- Wallet Deterministici



Attenzione ai Brainwallet

- https://en.bitcoin.it/wiki/Brainwallet
- http://brainwallet.org (https://brainwallet.github.io)

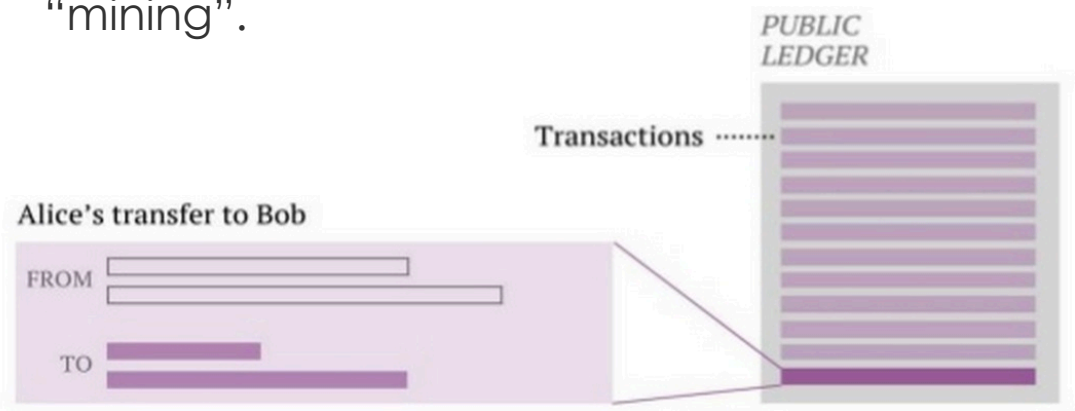


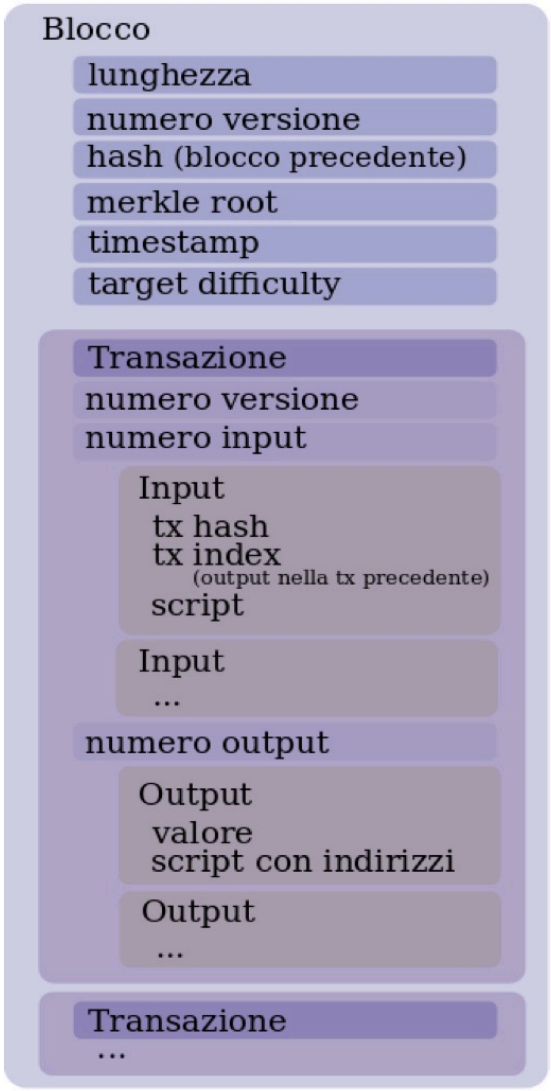
- Esiste ancora offlinebitcoins.com (USE AT YOUR OWN RISK)

Terminologia

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

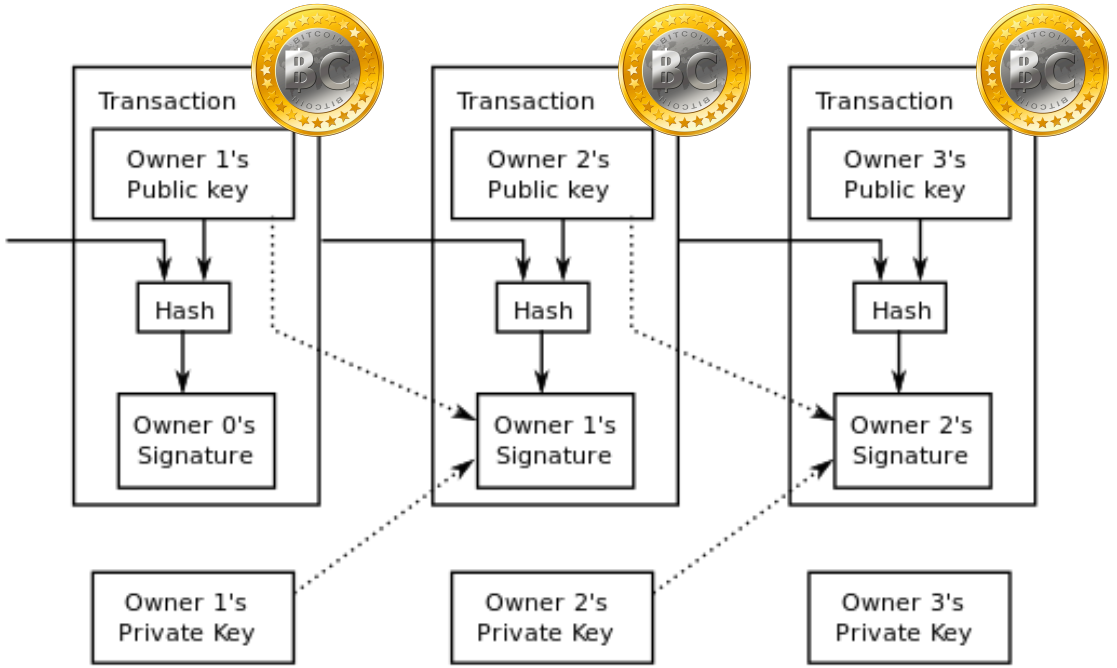
- **Blocco**: unità che compone la blockchain, contiene centinaia di transazioni verificate e "compattate" in un unico elemento che viene legato inscindibilmente tramite hash alla blockchain. Per essere attaccato alla Blockchain deve essere eseguito un opportuno calcolo sul blocco definito "mining".





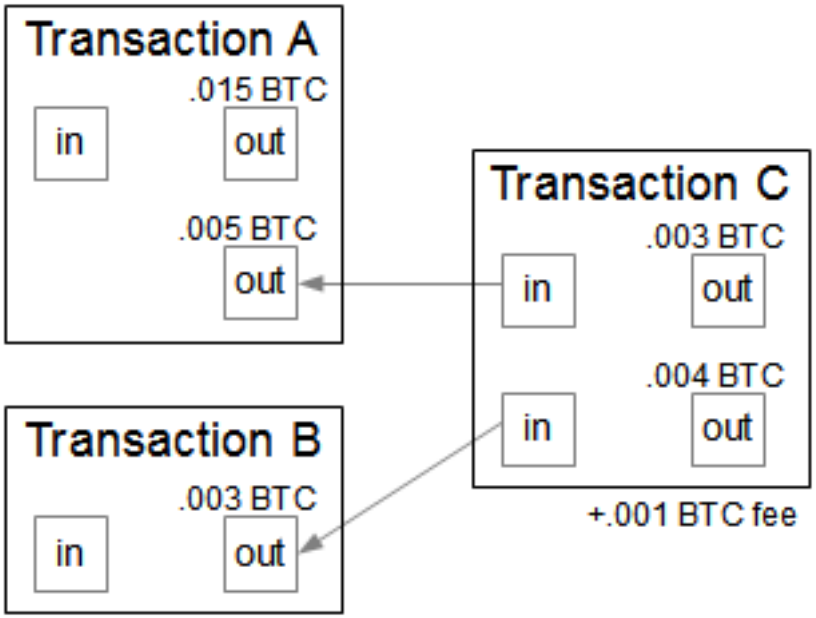
Terminologia

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



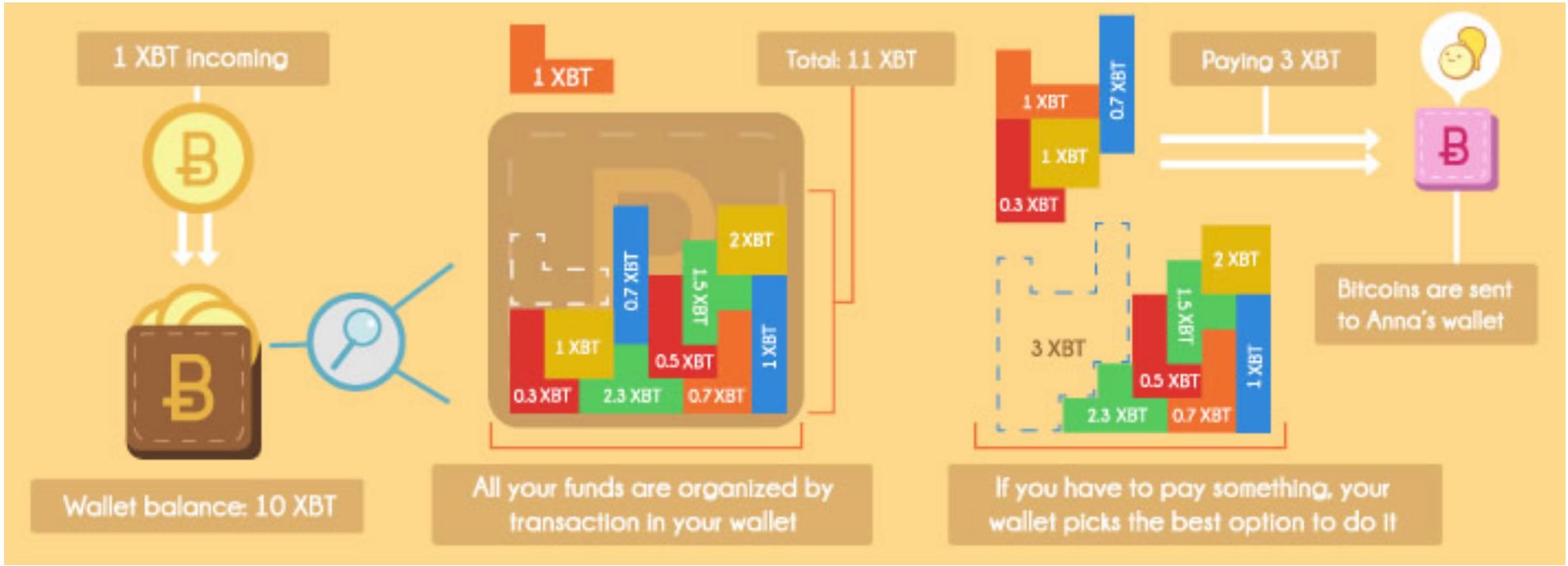
Transazioni

- Le transazioni possono avere più input e più output



http://www.righto.com/2014/02/bitcoins-hard-way-using-raw-bitcoin.html

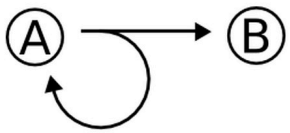
Transazioni e wallet



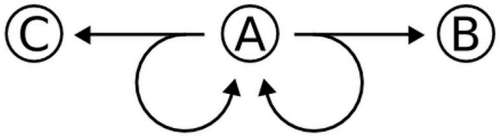
Src: bitcoinfees.com

Transazioni e change address

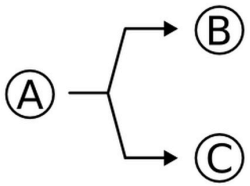
- Le transazioni UTXO vanno spese per intero → change address
- Sicurezza: una volta che un indirizzo è stato usato per versare bitcoin non dovrebbe più essere riciclato
- Privacy: non si sa a chi hai pagato ed è più complesso risalire al balance del tuo wallet
- Stesso change address
- Change address diverso



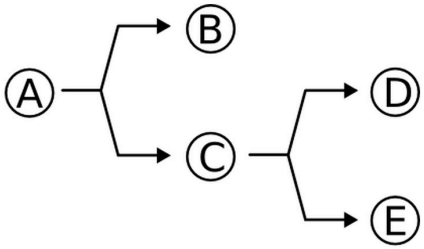
A paid B



A paid B **and** C



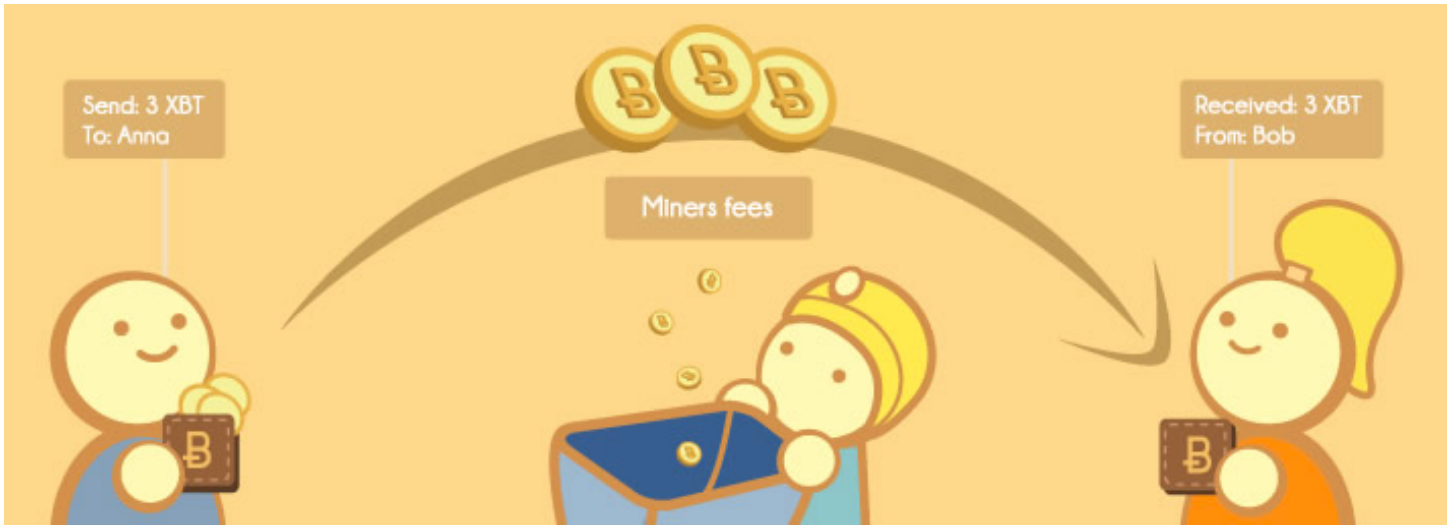
A paid (B **and/or** C)



A paid B **and/or** C;
C paid D **and/or** E

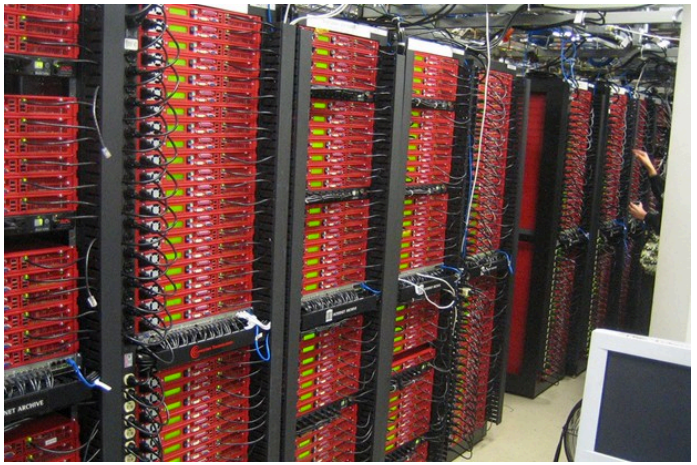
Fee

- Fee basate sulle priorità: pochi bitcoin o bitcoin troppo recenti (con pochi blocchi di anzianità) richiedono fee
- Fee basati sulla dimensione della tx:
  - 148 * number_of_inputs + 34 * number_of_outputs + 10

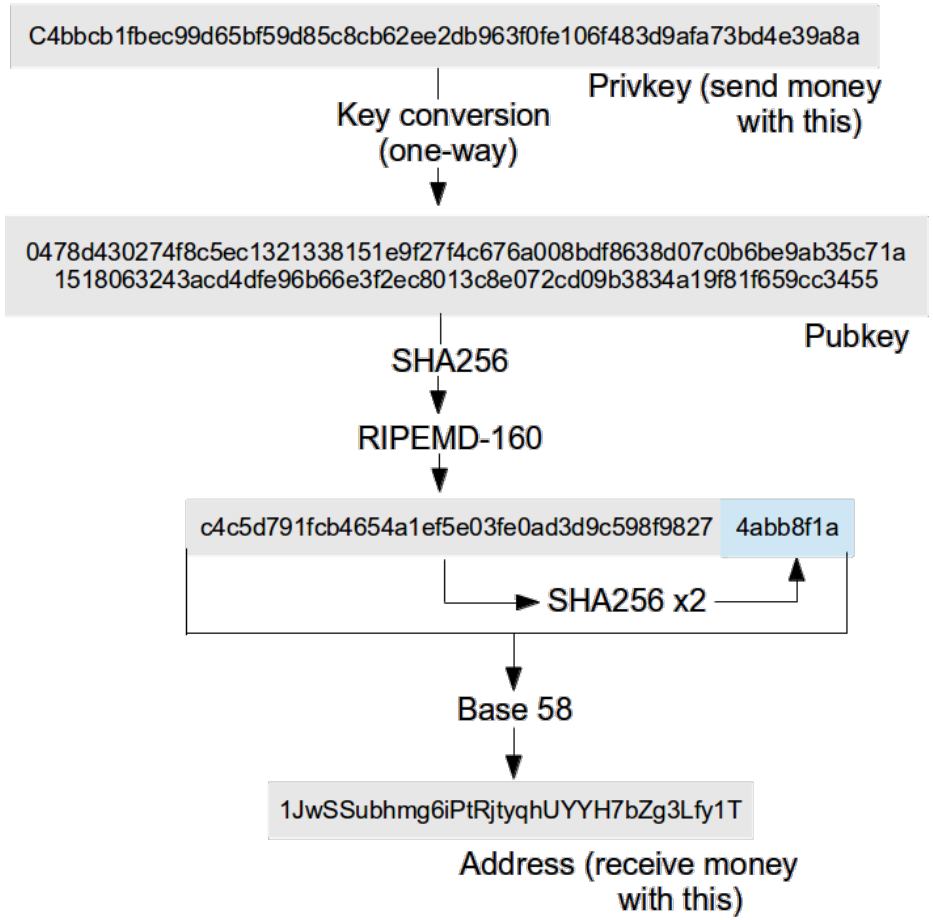


Terminologia

- **Minatori**: coloro che si offrono di raccogliere le transazioni che avvengono nel mondo in un blocco, verificarle e aggiungerle alla blockchain, il libro mastro, ottenendo una ricompensa per la chiusura del blocco e una commissione (volontaria) per ogni transazione inserita nel blocco

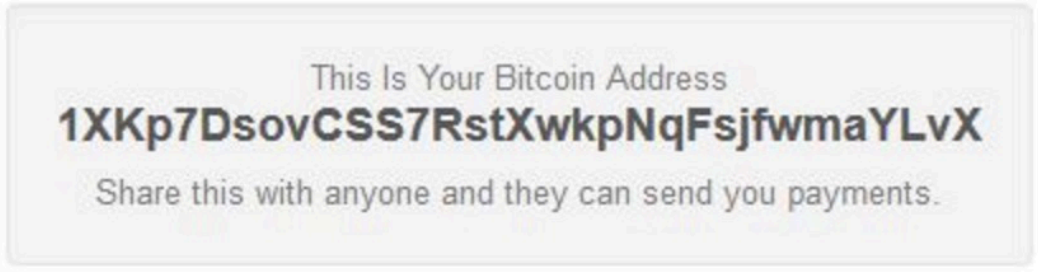


Da chiave privata a indirizzo Bitcoin



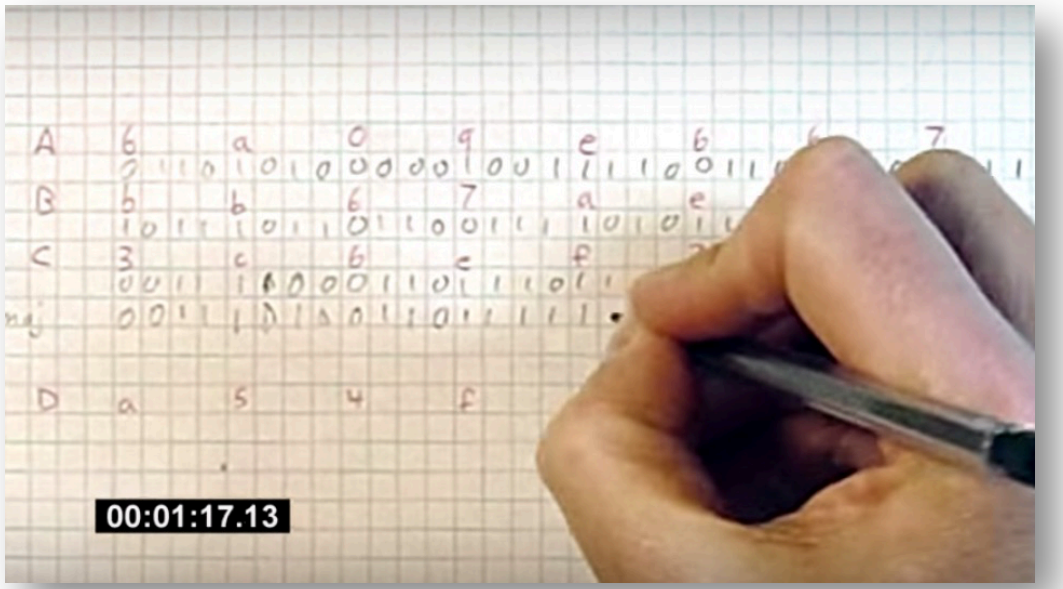
Formato degli indirizzi bitcoin

- 26-35 caratteri, "Base 58 check" encoded
- Inizia con 1 o 3 (per i multisig)
- Numeri e caratteri casuali eccetto lettrera 'o' maiuscola ("**O**"), lettera 'i' maiuscola ("**I**") lettera "elle" minuscola ("**l**") e il numero "zero" ("**0**") per evitare ambiguità
- **Regex**: ^[13][a-km-zA-HJ-NP-Z1-9]{25,34}$



Come generare indirizzi

- Se si usa un wallet, ci pensa lui
- Tool come bitcoin-tool, sx-tools
- Siti web (sconsigliato) o script da usare offline (Brainwallet, Bitaddress, ec…)
- A mano… (0.96 h/d)



http://www.righto.com/2014/09/mining-bitcoin-with-pencil-and-paper.html

Online o via js/script

bitaddress.org

Open Source JavaScript Client-Side Bitcoin Wallet Generator

Single Wallet | Paper Wallet | Bulk Wallet | Brain Wallet

Vanity Wallet | Split Wallet | Wallet Details

Generate New Address | Print

Bitcoin Address | **Private Key (Wallet Import Format)**

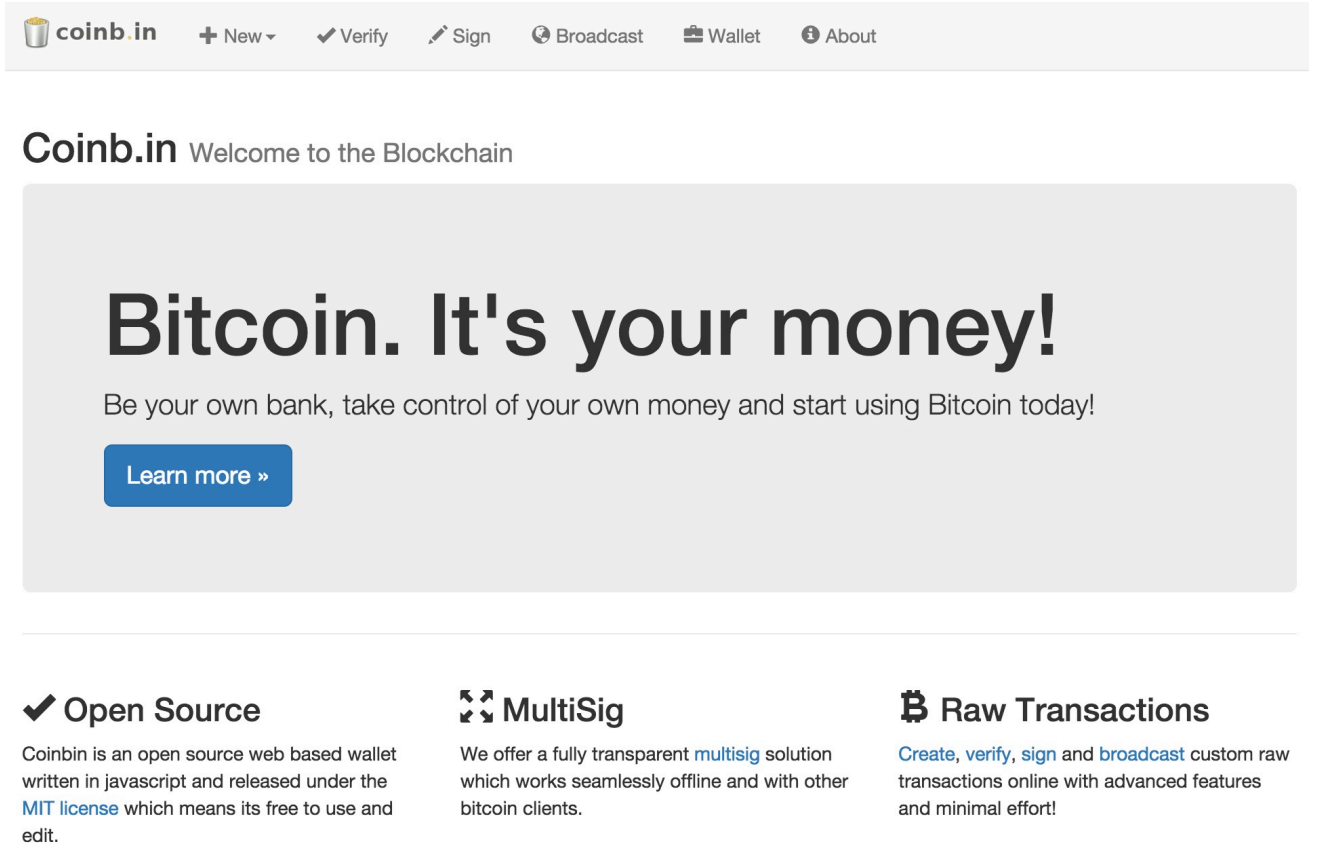
SHARE

17q8R5drRDfiYkPQ6tFVRMbsVe6P1E1ZsP

SECRET

5K2FA6vHkiV8Bk1mY9U91QjzaQeg4dCkH3h9S3B9LEdLyExLEtU

Online o via js/script



https://github.com/OutCast3k/coinbin → coinb.in

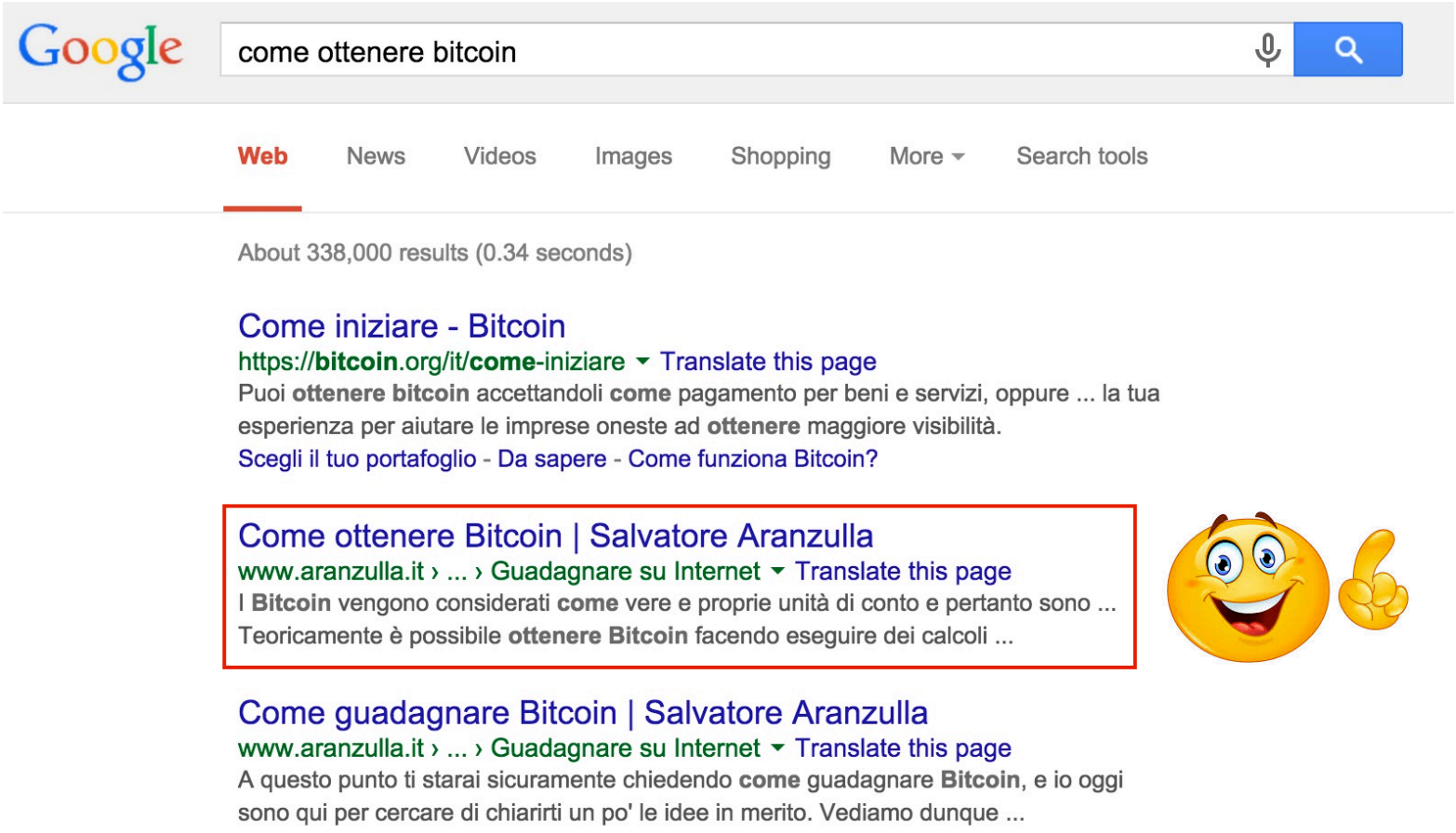
Vanity Addresses

- Indirizzi "personalizzati" che contengono una parte di testo scelto (1PAoLoLmzFVj8ALj6mfBsbifRoD4miY36v)

- bitcoinvanitygen.com (online)
- https://github.com/samr7/vanitygen (codice)

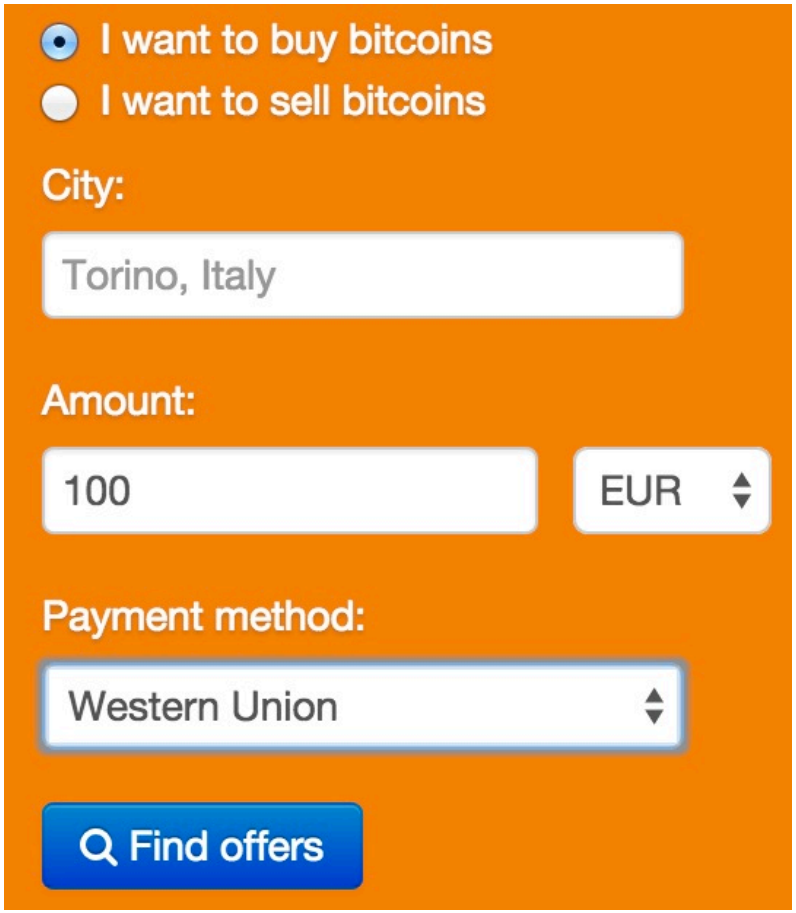
Paper Wallet

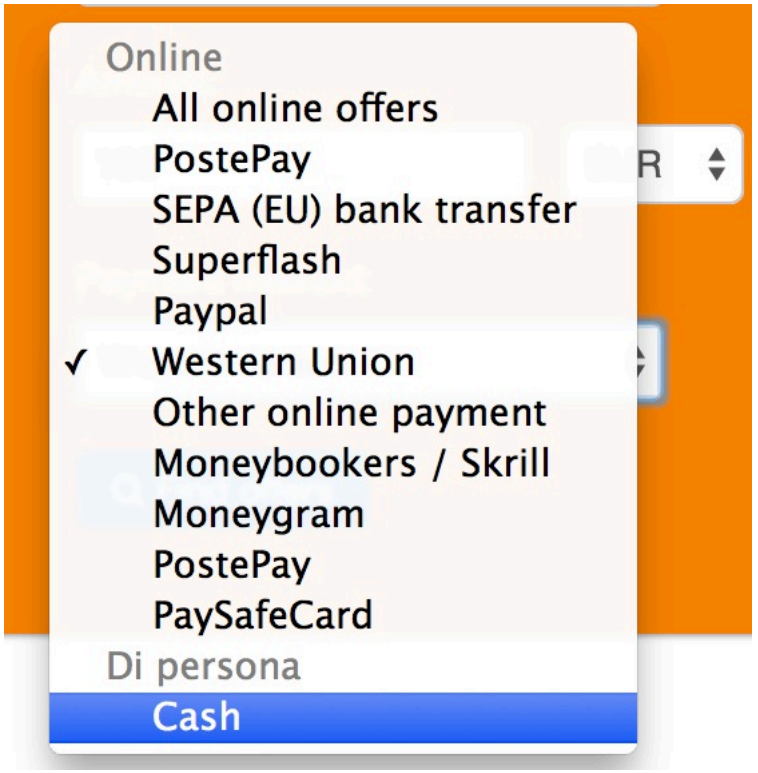
Come ottenere i bitcoin



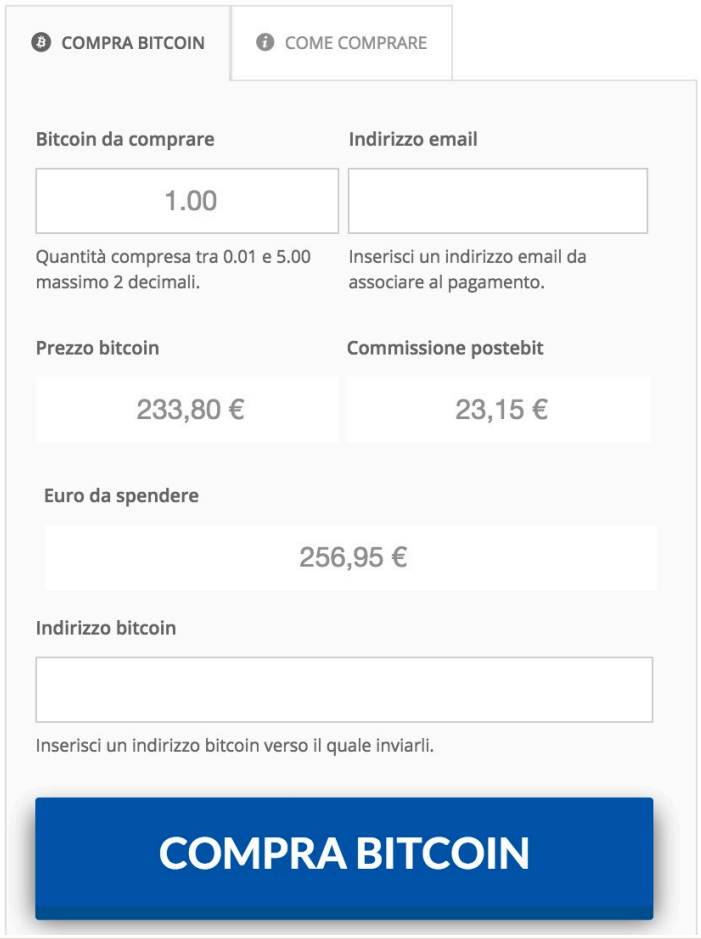
Come ottenere i bitcoin

LocalBitcoins.com





Come ottenere i bitcoin



DOVE PAGARE IN CONTANTI

Poste italiane PT · Sisal · BancaITB

DOVE PAGARE ONLINE

posteapp · postepay · BancoPosta

Come ottenere i bitcoin

TRADING LTD. THEROCK

Symbol	Description	Bid	Ask	Last value	Var %	Last trade
BTCEUR	Trade Bitcoins with EURO	€ 207.49	€ 210.27	€ 210.53	^ 0.24%	about a minute ago
BTCGBP	Trade Bitcoins with Pounds	£ 130.00	£ 258.87	£ 142.67	^ 0.00%	17 days ago
BTCUSD	Trade Bitcoins with USD	$ 238.50	$ 244.99	$ 244.99	^ 2.04%	32 minutes ago
BTCXRP	Trade Bitcoins with XRP	XRP 30,100.00	XRP 38,000.00	XRP 35.000,00	^ 0.00%	about 23 hours ago
EURDOG	Trade EUR with Dogecoins	DOGE 9,000.00	DOGE 10,500.00	DOGE 9,000.00	v -15.52%	3 minutes ago
EURXRP	Trade EURO with XRP	XRP 100.00	XRP 174.50	XRP 75,00	^ 0.00%	a day ago
LTCBTC	Trade Litecoins with Bitcoins	฿ 0.0059	฿ 0.0061	฿ 0.0059	v -3.28%	about an hour ago

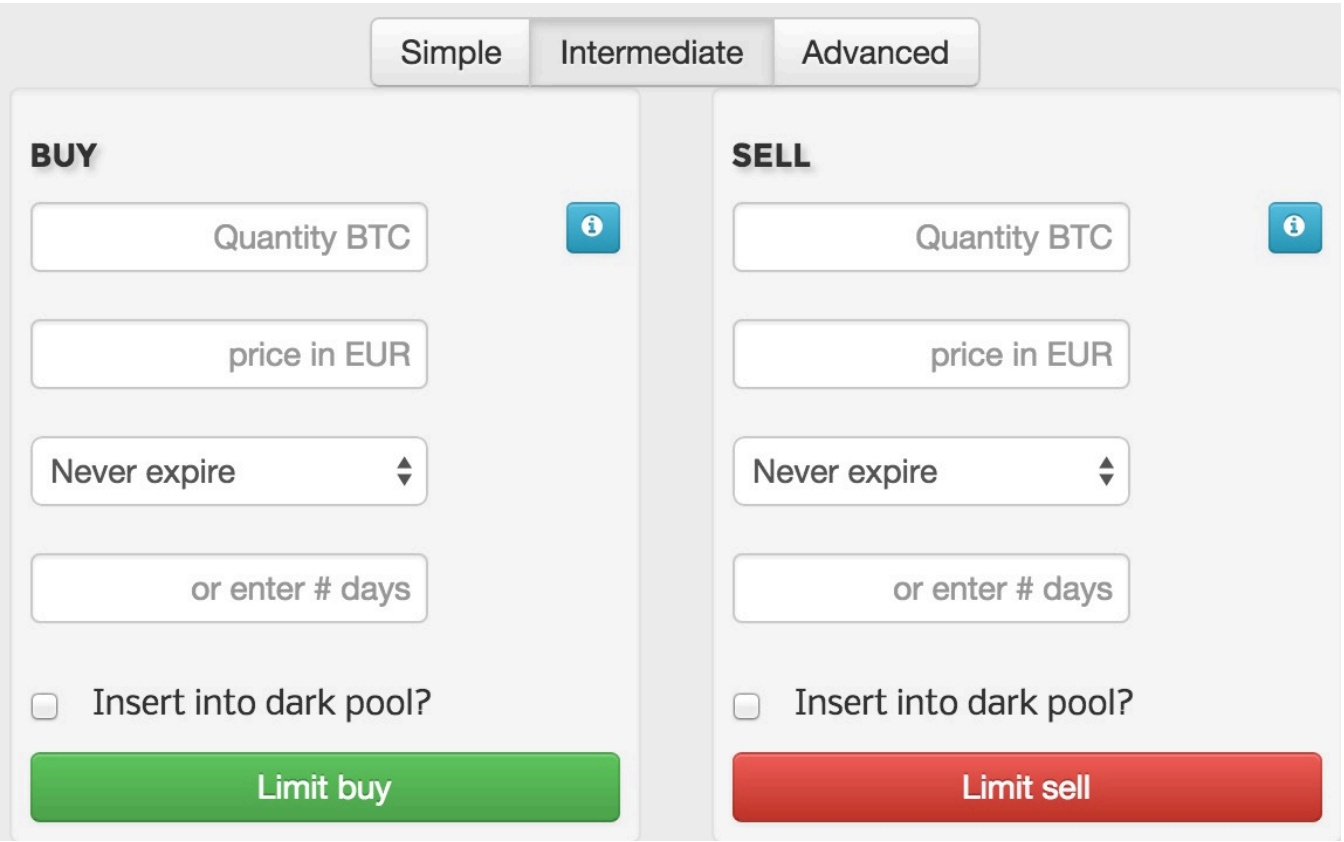
Bid (Buy)

quantity BTC	value EUR	depth EUR
0.06	207.49	12.45
0.11	207.48	35.27
0.36	207.32	109.91
0.20	207.31	151.37

Ask (Sell)

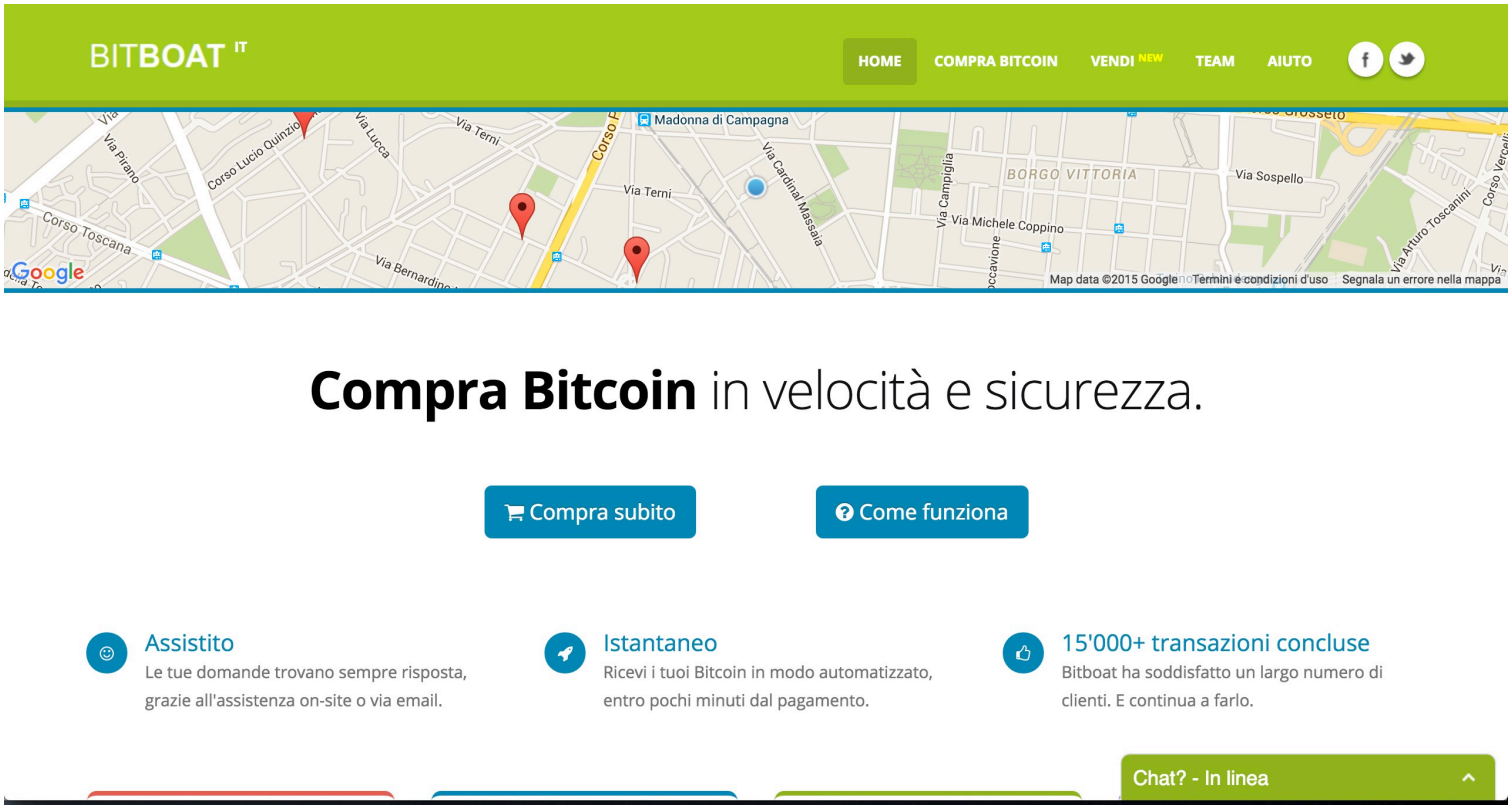
quantity BTC	value EUR	depth EUR
0.06	210.27	12.62
0.11	210.33	35.75
1.23	210.52	294.69
0.97	210.53	498.91

Come ottenere i bitcoin



Come ottenere i bitcoin

BITBOAT IT



Come ottenere i bitcoin

POLIZIA DI STATO

POLIZIA POSTALE E DELLE COMUNICAZIONI
COMPARTIMENTO FRIULI VENEZIA GIULIA
SEZIONE DI UDINE

SITO WEB SOTTOPOSTO A SEQUESTRO PREVENTIVO

(art. 321 c.p.p.)

TRIBUNALE DI TRIESTE

UFFICIO DEL GIUDICE PER LE INDAGINI PRELIMINARI

(nr. 2169/15 R.G.G.I.P. TRIESTE)

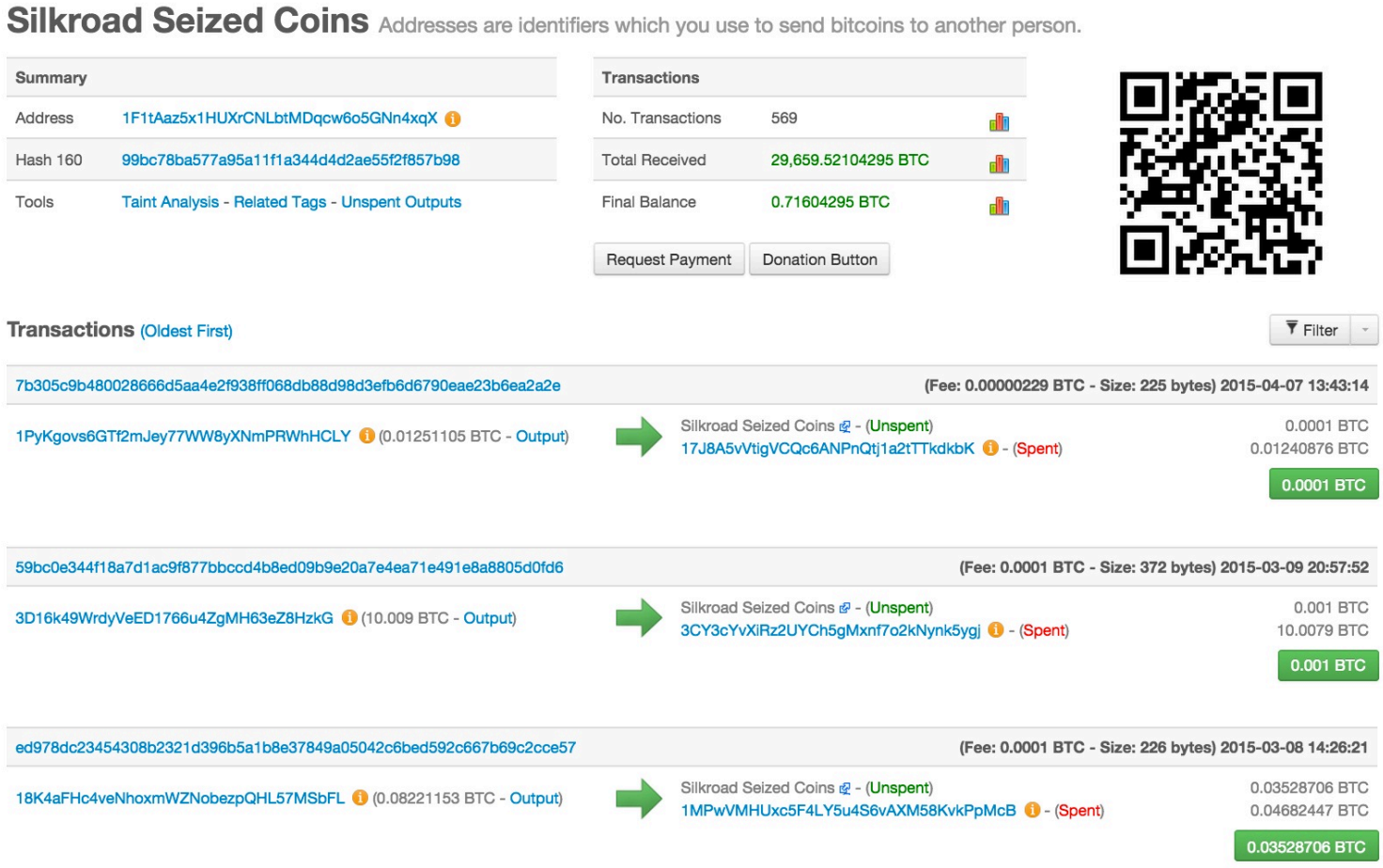
Bitcoin Forensics

- Deriva dalla Computer e Network Forensics
- Applicazione delle best practices di alle indagini sul mondo Bitcoin.
  - Elementi tradizionali (es. analisi di un PC su cui è stato installato un wallet)
  - Elementi innovativi (intelligence su transazioni presenti nella blockchain)
- Blockchain: la prova è pubblica, immutabile, precostituita, già "forense"

Strumenti: blockchain explorers

- Scelta tra online e offline/locale (con copia blockchain)
- NB: gli strumenti online di visualizzazione e analisi blockchain sono comodi ma informano il gestore circa le nostre ricerche
- Online: **blockexplorer.com**, **blockchain.info, blockr.io**
  - Blocchi (anche quelli doppi)
  - Transazioni (spese e non spese)
  - Indirizzi e transazioni (prima comparsa di un ADDR, saldo, etc…)
  - **Taint** Analysis
  - Statistiche
  - **Tag**
- Elenco di block explorer: https://docs.google.com/spreadsheets/d/1Ku9Nlo_TwhE_gLX3oDmRURbvc_iB_7j90MyfCG69zLw/edit?pli=1#gid=0

Come osservare le transazioni



Silkroad Seized Coins Addresses are identifiers which you use to send bitcoins to another person.

Summary	
Address	1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX
Hash 160	99bc78ba577a95a11f1a344d4d2ae55f2f857b98
Tools	Taint Analysis - Related Tags - Unspent Outputs

Transactions	
No. Transactions	569
Total Received	29,659.52104295 BTC
Final Balance	0.71604295 BTC

Request Payment | Donation Button

Transactions (Oldest First) — Filter

7b305c9b480028666d5aa4e2f938ff068db88d98d3efb6d6790eae23b6ea2a2e — (Fee: 0.00000229 BTC - Size: 225 bytes) 2015-04-07 13:43:14

1PyKgovs6GTf2mJey77WW8yXNmPRWhHCLY (0.01251105 BTC - Output) → Silkroad Seized Coins - (Unspent) 0.0001 BTC
17J8A5vVtigVCQc6ANPnQtj1a2tTTkdkbK - (Spent) 0.01240876 BTC
0.0001 BTC

59bc0e344f18a7d1ac9f877bbccd4b8ed09b9e20a7e4ea71e491e8a8805d0fd6 — (Fee: 0.0001 BTC - Size: 372 bytes) 2015-03-09 20:57:52

3D16k49WrdyVeED1766u4ZgMH63eZ8HzkG (10.009 BTC - Output) → Silkroad Seized Coins - (Unspent) 0.001 BTC
3CY3cYvXiRz2UYCh5gMxnf7o2kNynk5ygj - (Spent) 10.0079 BTC
0.001 BTC

ed978dc23454308b2321d396b5a1b8e37849a05042c6bed592c667b69c2cce57 — (Fee: 0.0001 BTC - Size: 226 bytes) 2015-03-08 14:26:21

18K4aFHc4veNhoxmWZNobezpQHL57MSbFL (0.08221153 BTC - Output) → Silkroad Seized Coins - (Unspent) 0.03528706 BTC
1MPwVMHUxc5F4LY5u4S6vAXM58KvkPpMcB - (Spent) 0.04682447 BTC
0.03528706 BTC

Come osservare le transazioni

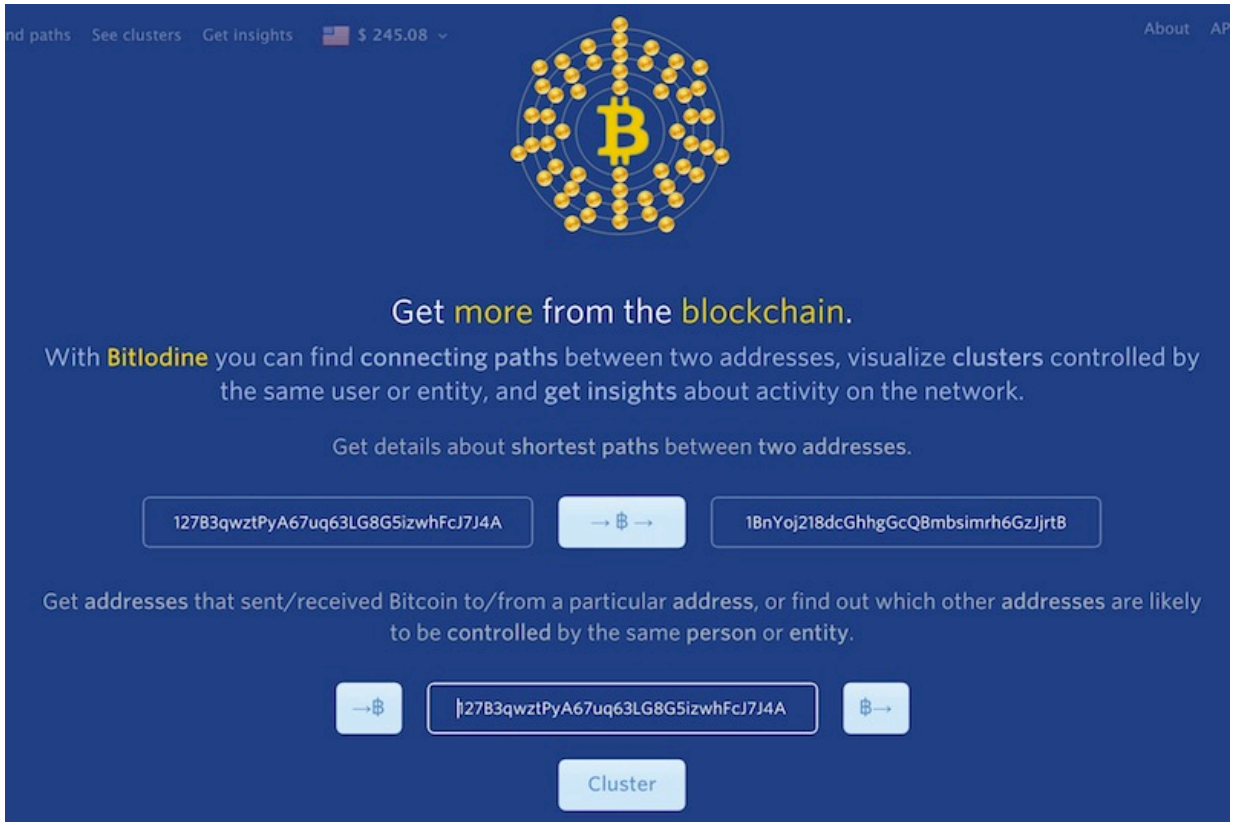
- Attenzione a non riporre fiducia nell'IP indicato nella transazione su Blockchain.info

Relayed by IP	24.165.94.91 (whois)
Visualize	View Tree Chart

Network Propagation (Click to view)

Strumenti: Bitcoin forensics

- Bitiodine
  - Spagnuolo, Maggi, Zanero
  - Crawl di siti di scambio bitcoin per raccogliere indirizzi
  - Raggruppa indirizzi in wallet
  - Analisi del percorso di collegamento tra indirizzi



Strumenti: Bitcoin Disk Forensics

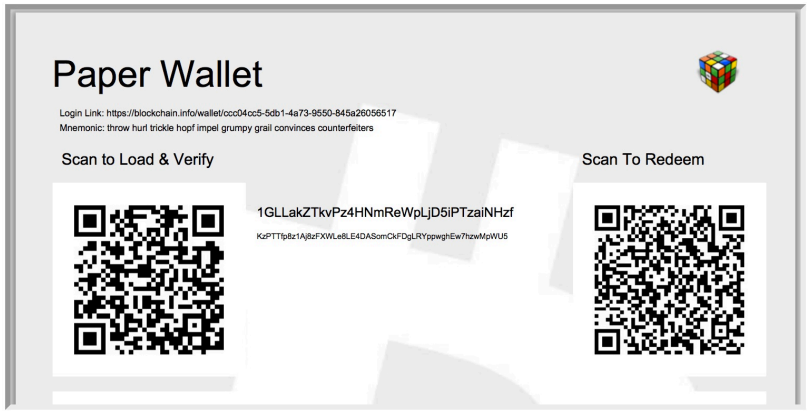
- Magnet Forensics (indirizzi, chiavi, transazioni, wallet, etc…)
  - http://www.magnetforensics.com
- KeyHunter (chiavi private)
  - https://github.com/pierce403/keyhunter
- BTScan (indirizzi, chiavi private, chiavi pubbliche)
  - https://gist.github.com/chriswcohen/7e28c95ba7354a986c34/download
- BTC Recover (brute force di wallet)
  - github.com/gurnec/btcrecover

Artefatti per bitcoin forensics

- File di log dei client
  - IP locale (!)
  - Transazioni
  - Etc…

```
2015-04-15 07:03:17 receive version message: /Satoshi:0.10.0/: ver
sion 70002, blocks=352195, us=77.118.15.18:63642, peer=2
2015-04-15 07:03:17 Added time data, samples 3, offset -1 (+0 minu
tes)
2015-04-15 07:03:24 receive version message: /Satoshi:0.10.0/: ver
sion 70002, blocks=352195, us=77.118.15.18:33944, peer=3
2015-04-15 07:03:24 Added time data, samples 4, offset +0 (+0 minu
tes)
```

- Cache del browser
  - Web wallet history
  - Paper wallet (!)

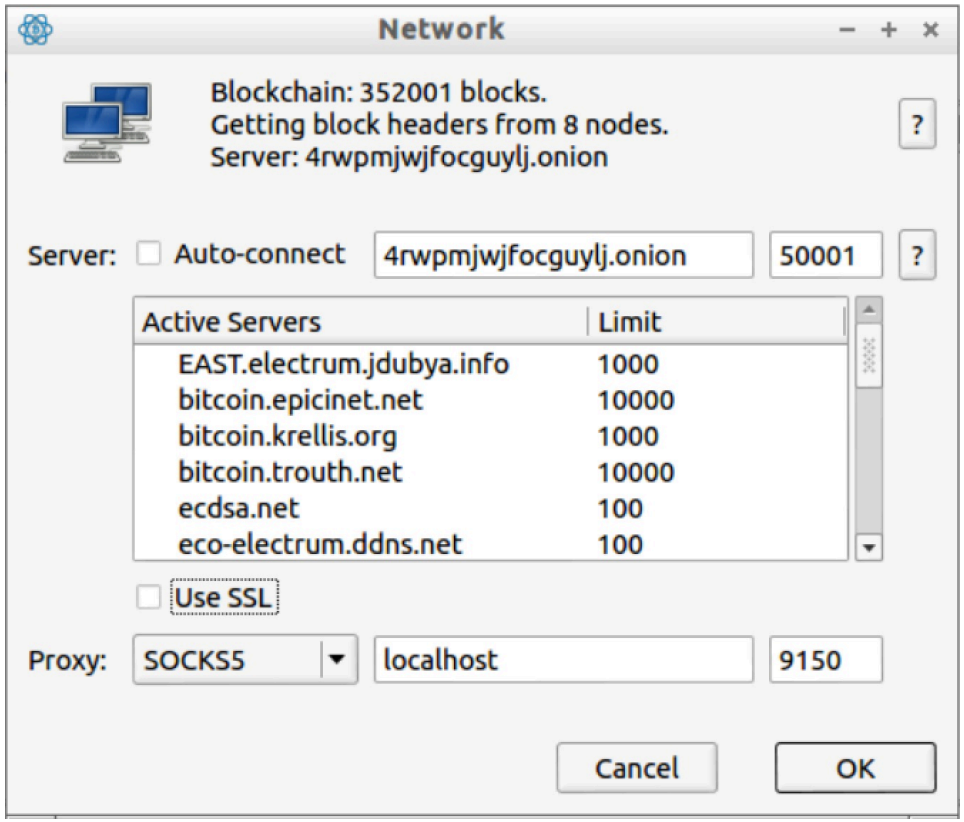


DEFTCoin ☺

- Ci sono già diverse distro (alcune un po' obsolete) dedicate al Bitcoin (CoinOS, Electrum Live CD, Paper-BTC, Live Miner, BTC Vault, BitBuntu, Bitkey, etc…)
- Perché non crearsi una stazione di lavoro (live o installed) per Bitcoicon Forensics e Intelligenge con… **DEFT**?
- Ovviamente potremo concentrarci sui tool più utili, usando Tor Browser preinstallato (che offre socks5 sulla 9150 invece che la 9050)

DEFTCoin: Electrum (+ Tor)

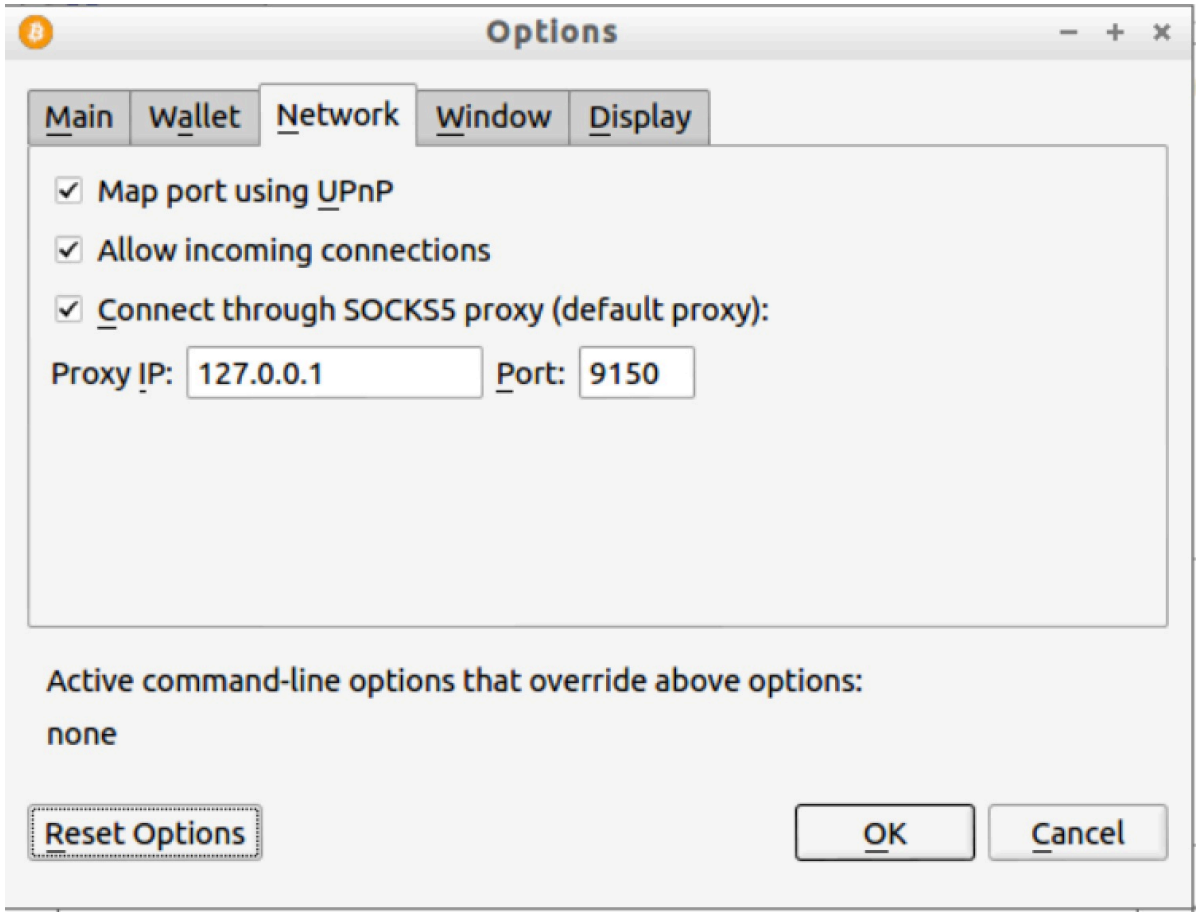
- Possibilità di usare Bitcoin su rete anonima Tor
- wget https://download.electrum.org/Electrum-2.0.4.tar.gz
- decomprimere tgz e poi nel folder "***python electrum***"
- Per usare Tor, avvio Tor Browser e setto proprietà Network via cmdline o GUI
  - ./electrum -s 56ckl5obj37gypcu.onion:50001:t -p socks5:localhost:9150 --verbose



DEFTCoin: Bitcoin Core (+ Tor)

- Anche Bitcoin-Core può essere utilizzato su rete anonima Tor
- wget https://bitcoin.org/bin/bitcoin-core-0.10.0/bitcoin-0.10.0-win32.zip
- vi /root/.bitcoind/bitcoin.conf
  - rpcuser= deftuser
  - rpcpassword=deftpassword
  - txindex=1 (facoltativo)
- ./bitcoin-qt
  - Oppure ./bitcoind –daemon e poi ./bitcoin-cli stop per uscire
- Consigliato utilizzare blockchain pre-scaricata (da torrent o meglio ancora da un altro client)
- Per usare Tor, avvio Tor Browser
  - ./bitcoin-qt -proxy 127.0.0.1:9150 –onlynet=tor
  - ./bitcoin-qt -proxy 127.0.0.1:9150 –onion=hiddenservice.onion:port
    - https://en.bitcoin.it/wiki/Fallback_Nodes

DEFTCoin: Bitcoin Core (+ Tor)



DEFTCoin: tool per bitcoin forensics

- **BX libBitcoin Explorer (ex SX Tools)**
  - github.com/libbitcoin/libbitcoin-explorer
- **Bitcoin-Tools**
  - github.com/gavinandresen/bitcointools
- **BTC Recover (brute force di wallet)**
  - github.com/gurnec/btcrecover
- **BTCScan (indrizzi, chiavi private, wallet, etc…)**
  - https://gist.github.com/chriswcohen/7e28c95ba7354a986c34/download
- **KeyHunter (chiavi private)**
  - https://github.com/pierce403/keyhunter
- **Bitcoin Sneak Peak**
  - Chrome Extension
- **Bulk Extractor (si possono personalizzare le regexp…)**
  - github.com/simsong/bulk_extractor (ma c'è già)

DEFTCoin: risorse per bitcoin forensics

- **Block Explorer**
  - blockr.io, blockchain.info, blockexplorer.com
- **Bitcoin Intelligence**
  - coinalytics.co/tools/tracker.html
  - coinalytics.co/tools/explorer.html
  - coinalytics.co/api/blockstem.html
  - www.walletexplorer.com
- **Bitiodine**
  - www.bitiodine.net
- **Web Wallet**

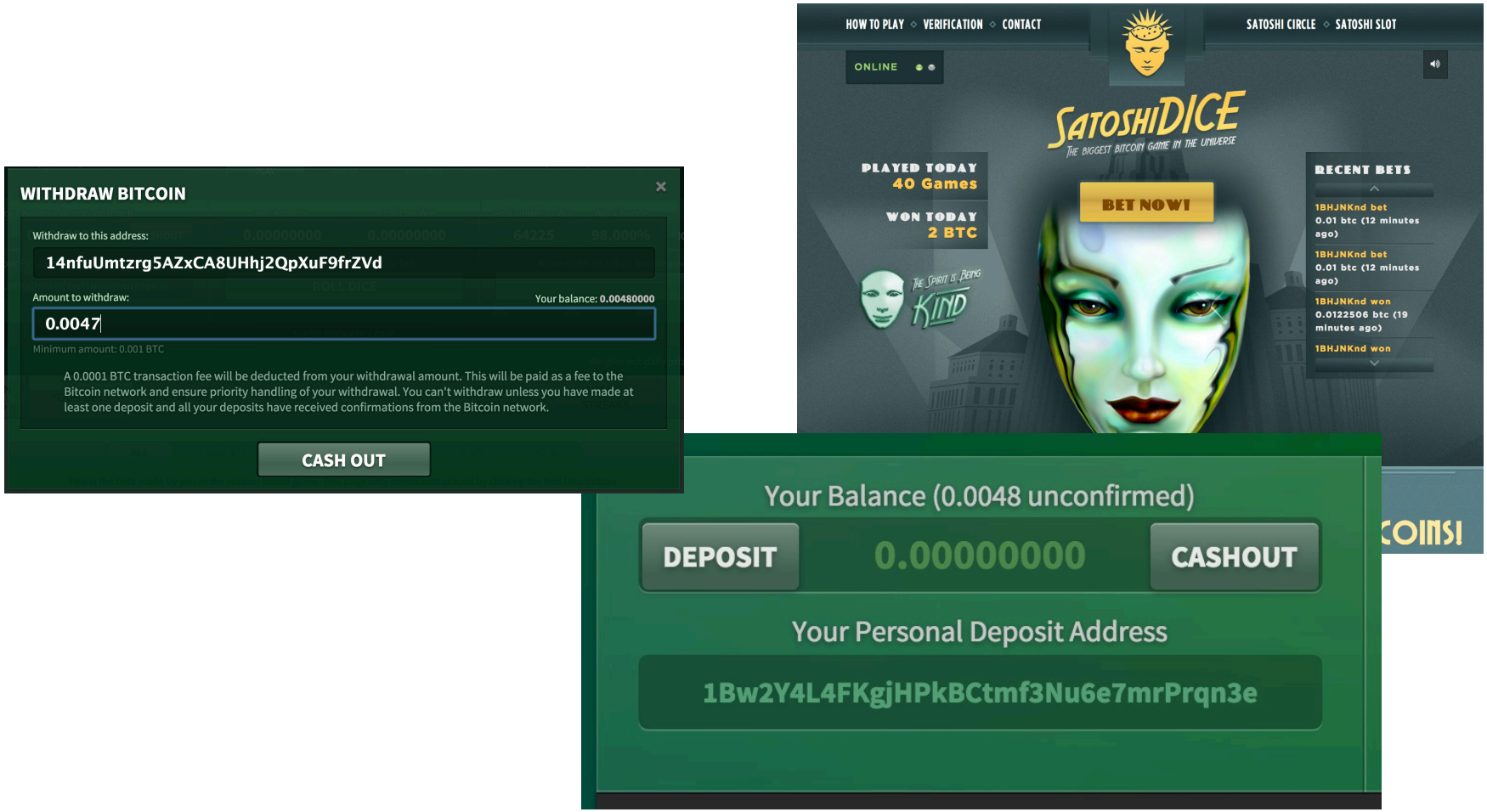
Anonimato dei wallet e delle transazioni

- Esistono mixer appositi di terze parti
  - Si paga commissione, c'è il rischio di essere derubati
- Utilizzo di wallet online degli exchange tradizionali
  - Coinjoin/SharedCoin, CoinSwap
  - Talvolta pongono limiti su quantità massima di BTC "ripulibili"
- Le transazioni sono pubbliche e così anche gli indirizzi
- E' possibile incrociare i dati della blockchain
- Il punto debole sono gli endpoint:
  - Dove entra moneta fiat per diventare bitcoin (vale anche per il mining anche se non entra moneta fiat)
  - Dove da Bitcoin si ritorna a moneta fiat

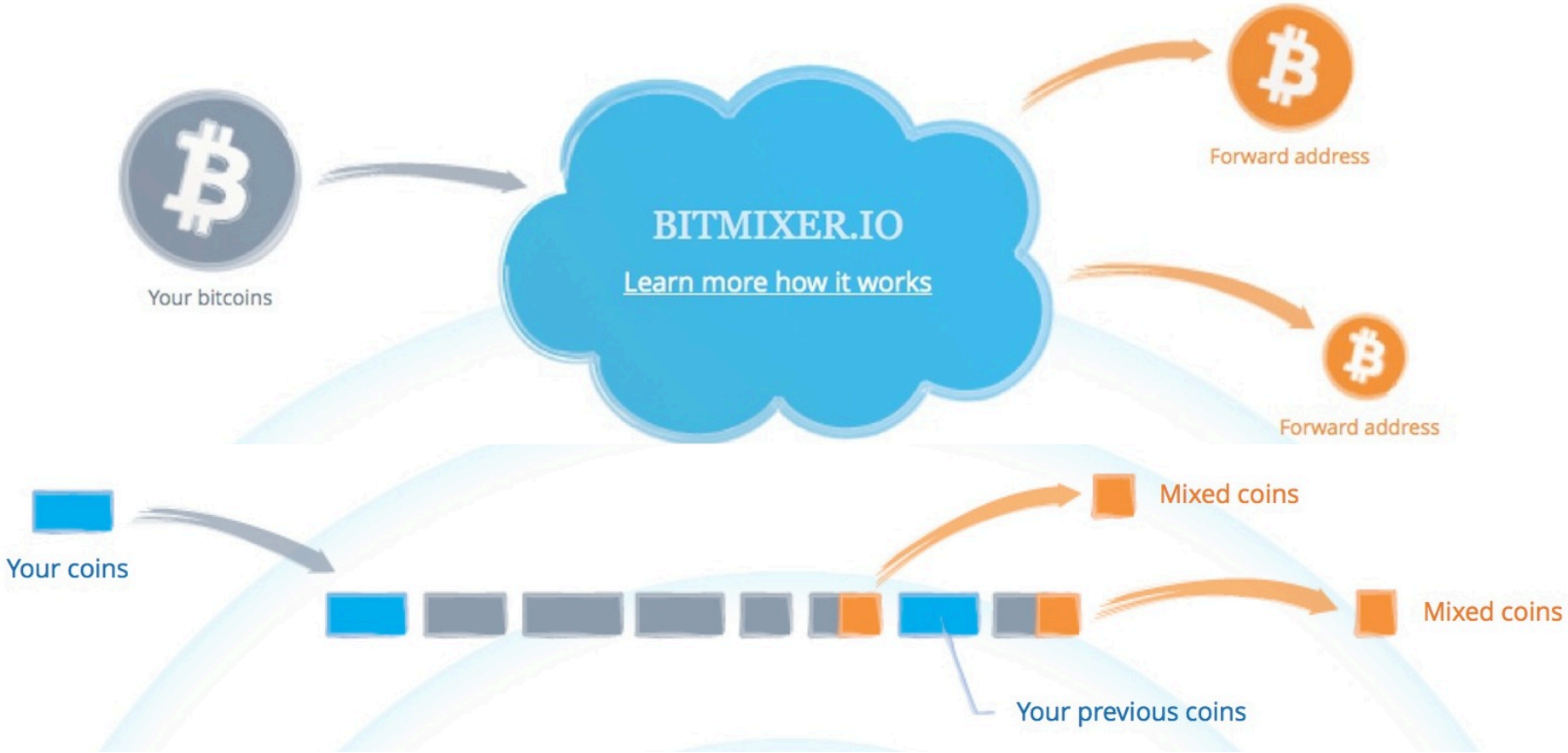
Come vengono "ripuliti" i bitcoin

- 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

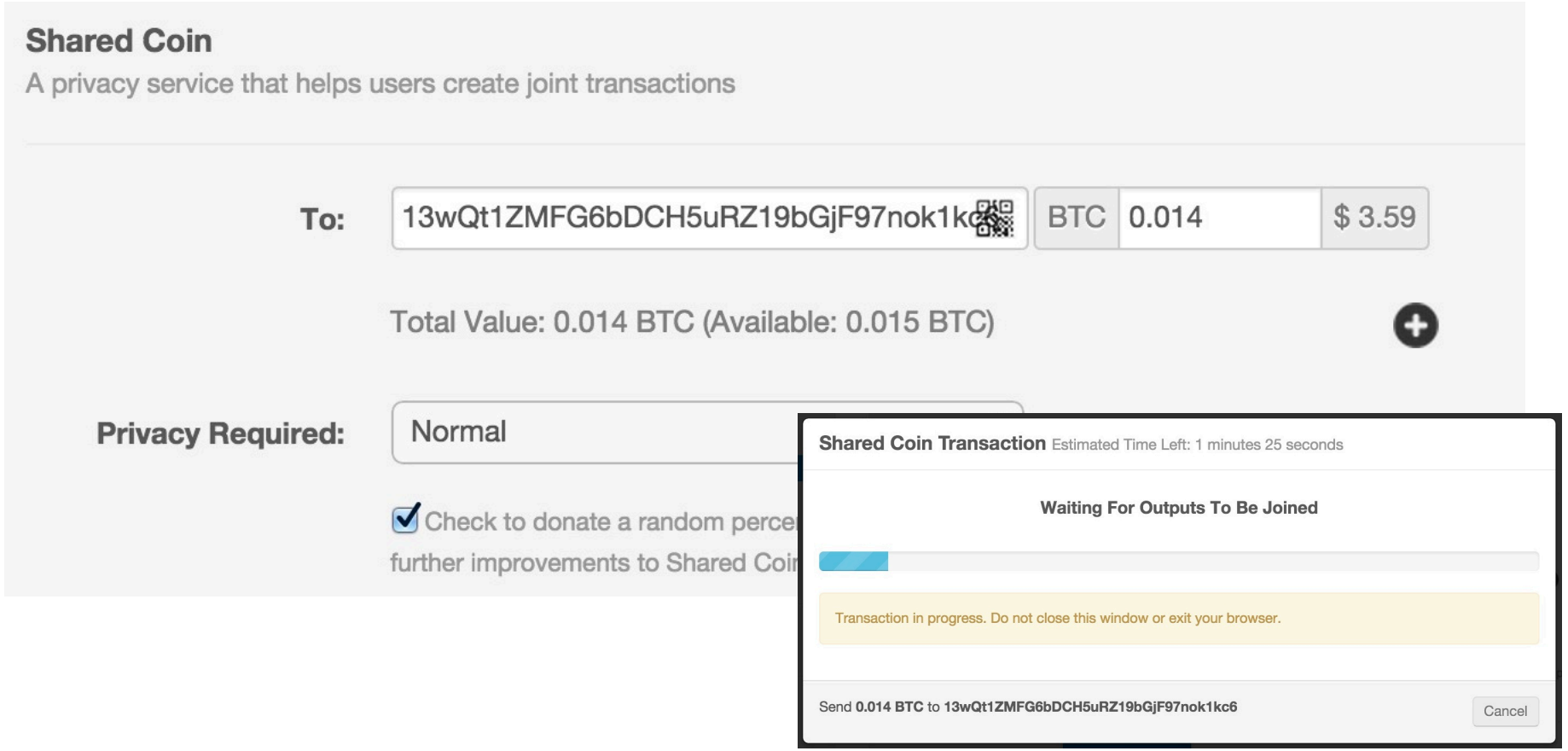
Come vengono "ripuliti" i bitcoin



Come vengono "ripuliti" i bitcoin



Come vengono "ripuliti" i bitcoin



Come vengono "ripuliti" i bitcoin

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

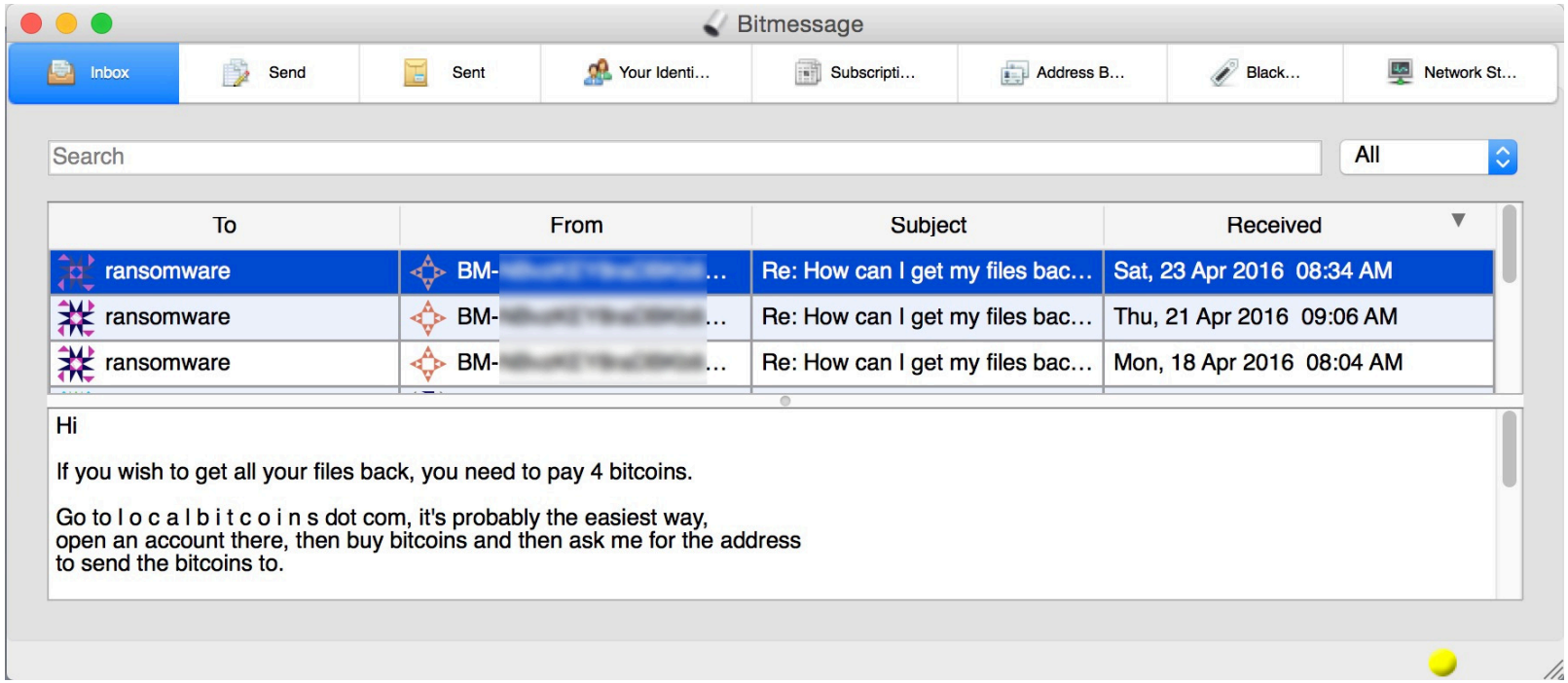
4 Conferme | € 2.74

Oltre le transazioni

- Il Bitcoin e i sistemi basati sulla Blockchain permettono di fare molte più cose delle semplici transazioni
- Da un certo punto di vista, estremizzando potrebbero anche essere viste come "effetto collaterale" di altre funzionalità acanzate, come:
  - Smart Contracts
  - Marche Temporali
  - Domain Registration
  - Colored Coins
  - Messaging

Bitmessage

- Chat sicure e private tramite un meccanismo simile al Bitcoin
- Purtroppo l'utilizzo che ne viene fatto non è sempre buono



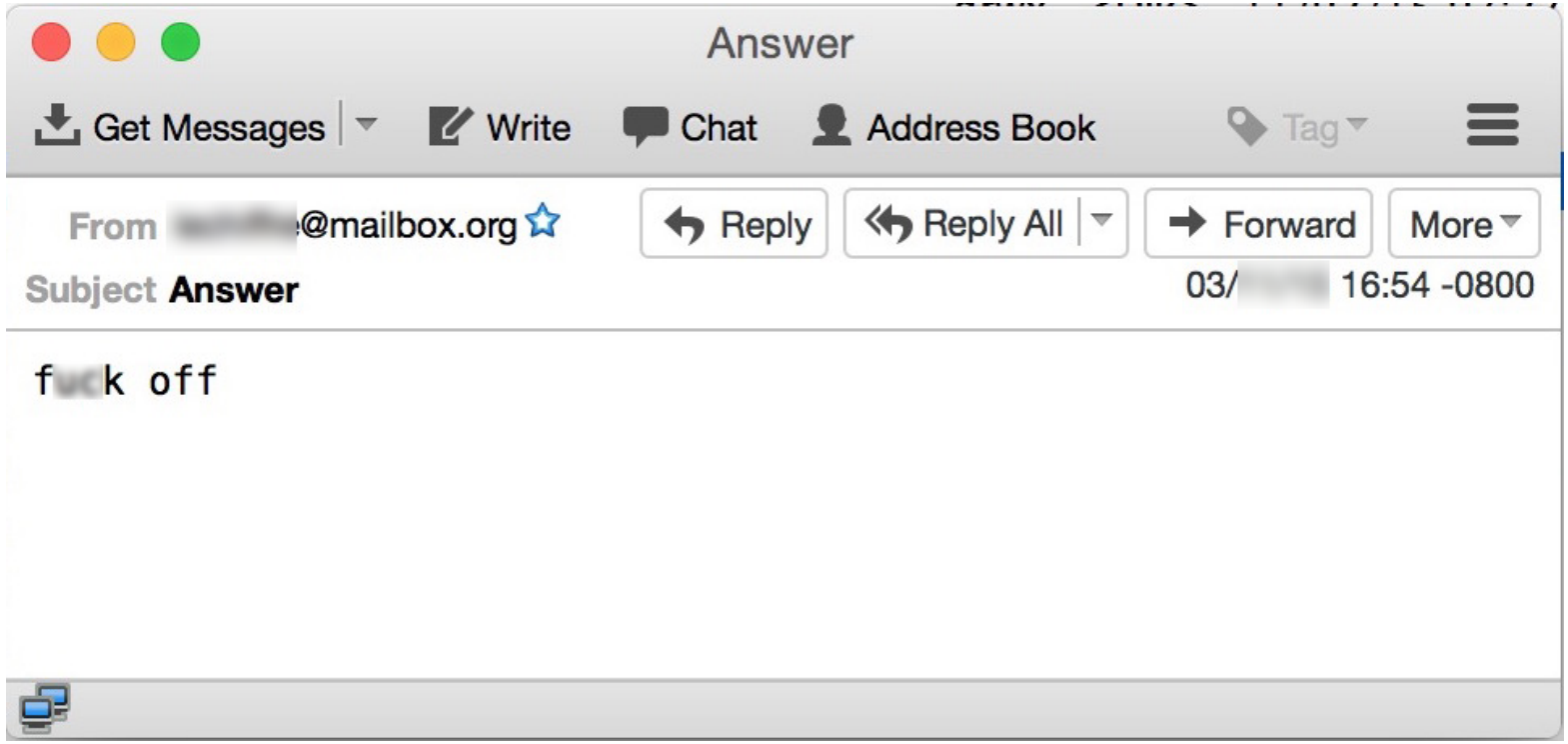
Bitmessage

- Il fatto che i criminali comunichino comunque può portare dei vantaggi…

04. [redacted] 13:14:39	[redacted]	Russian Federation/Komsomolsk-na-amure	Chrome	Windows 7
04. [redacted] 12:33:53	[redacted]	Russian Federation/Irkutsk	Chrome	Windows 10
04. [redacted] 12:24:10	[redacted]	Anonymous Proxy	Firefox	Windows 7
04. [redacted] 11:39:30	[redacted]	United States/Mountain View	Chrome	Android
04. [redacted] 10:53:44	[redacted]	Russian Federation/Rostov-on-don	Chrome	Windows 7
04. [redacted] 10:49:53	[redacted]	Belarus/Minsk	Chrome	Windows 7
04. [redacted] 10:18:04	[redacted]	Russian Federation/Rostov-on-don	Chrome	Windows 7
04. [redacted] 10:16:01	[redacted]	Anonymous Proxy	Firefox	Windows 8.1
04. [redacted] 09:37:32	[redacted]	Russian Federation/Omsk	Chrome	Windows 8.1
04. [redacted] 08:47:35	[redacted]	Russian Federation/Tver	Chrome	Windows 8.1

Bitmessage

- .. ovviamente quando capiscono di essere stati tracciati non la prendono bene. ☺



Messaggi nella blockchain

- www.eternitywall.it
- blockchain-pen.mkvd.net

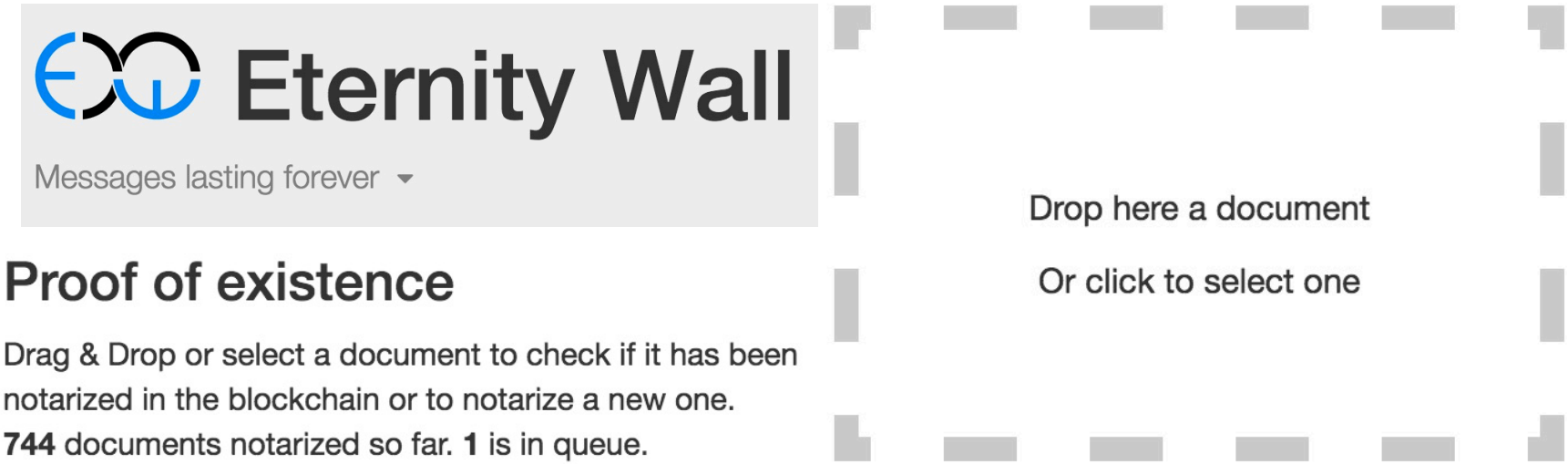
October 18, 2015 9:28 PM

Fate attenzione a questo utente Facebook:
http://j.mp/fbuserprofile

(4)

Blockchain per marche temporali

- http://www.proofofexistence.com
- http://eternitywall.it/notarize



Oltre le transazioni economiche…

- Il meccanismo della BlockChain può essere utilizzato per innumerevoli fini: smart contracts, marche temporali, scambio dati e… **registrazione di domini web**
- Siamo abituati a Whois, register, DNS, sequestro, confisca, etc… ma con I domini .bit tutto potrebbe cambiare (un po' come con i BTC)
- Namecoin: usare la blockchain per attribuire domini
- La proprietà è garantita dalla chiave privata
- Il registro è pubblico e distribuito
- Client "Namecoin" oppure via web (es. getdotbit.com)
- Per i browser: www.freespeechme.org (scarica la namechain…)

Oltre le transazioni economiche…

- Costi irrisori di registrazione e aggiornamento:
- Ad oggi 1 NMC = 0.0011 BTC = 0.37 EUR
  - Registrazione: 0.2 NMC
  - Aggiornamento o rinnovo: 0.005
- Ogni sei mesi è necessario rinnovare oppure il dominio si libera
- Blockchain via web: namecha.in o namecoin.webbtc.com
  - Nomi di dominio: http://namecha.in/d/domain
- Utilizzati anche per fornire indirizzi "umani" a onion service di Tor
  - es. blackmarket.bit → dsiewrkwerosdf.onion

Cybersquatting su Namecoin

Name d/difob (difob.bit)

Summary

Status	Active
Expires after block	302840 (17145 blocks to go)
Last update	2016-01-10 15:30:58 (block 266840)
Registered since	2016-01-10 15:30:58 (block 266840)
First registration	2015-05-10 04:23:41 (block 230043)

Current value

Bitmessage address: BM-2cWE[illegible]z5sMa

Cybersquatting su Namecoin

- Comunicano tramite BitMessage
- Fanno uno "sconto sostanziale" per il recupero del dominio se si dimostra di aver contribuito allo sviluppo del protocollo…

namecoin	BM-NB…	Re: Namecoin domain	Tue, 08 Mar 2016 11:51 PM
namecoin	BM-NB…	Re: Namecoin domain	Mon, 07 Mar 2016 10:12 AM
namecoin	BM-NB…	Re: Namecoin domain	Sun, 06 Mar 2016 10:03 AM

> Is icloud.bit for sale?
>
Yes, it is.
d/icloud costs 40.0 NMC. If you can prove you owned the name before, or you can prove you contributed to the Namecoin development in some way then you'll get a substantial discount.

Grazie

Email/Twitter

paolo@dalchecco.it / @forensico

Web

www.dalchecco.it / www.difob.it
www.bitcoinforensics.it / www.ransomware.it