

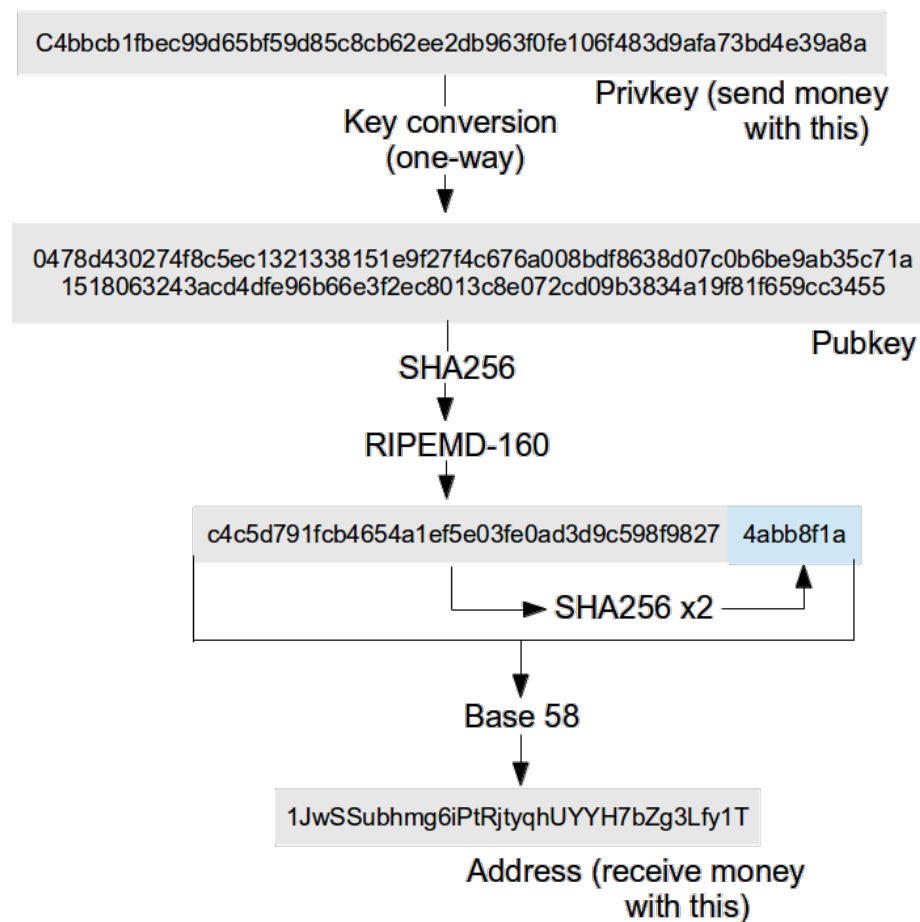
Riciclaggio e Anti riciclaggio nell'era del Bitcoin

Paolo Dal Checco, *Consulente Informatico Forense*

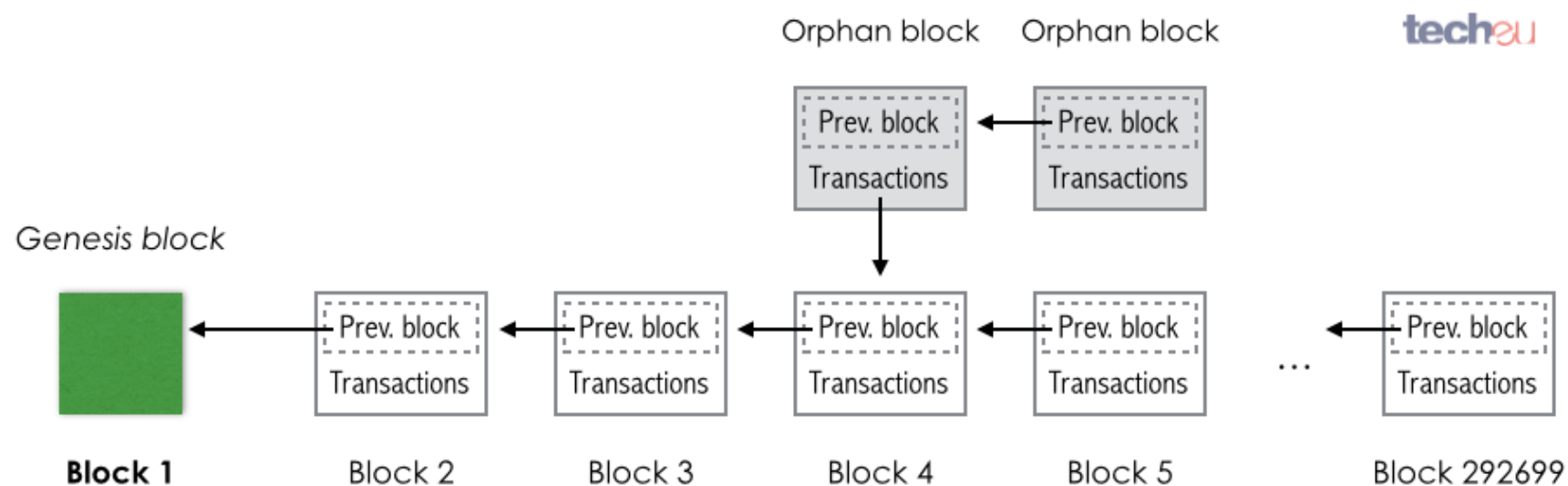
Cosa è il Bitcoin

- 'B' maiuscola, il protocollo, 'b' minuscola, l'unità di valuta
- Rete di pagamento digitale ideata nel 2009 da un anonimo "Satoshi Nakamoto", basata sulla crittografia ("crittovaluta")
 - Algoritmo di firma digitale asimmetrica **ECDSA**
 - Algoritmi di hashing **SHA256** e **RIPEMD 160**
- Peer to peer, nessun ente centralizzato che regola
- Controvalore in valuta fiat stabilito dal mercato
- La proprietà è garantita da chi possiede la chiave privata, che genera la pubblica da cui deriva un indirizzo
- Le transazioni sono pubbliche e inserite in una "blockchain" condivisa da tutti i partecipanti

Cosa è il Bitcoin



Cosa è il Bitcoin



Come ottenere bitcoin?



[Web](#) [News](#) [Videos](#) [Images](#) [Shopping](#) [More ▾](#) [Search tools](#)

About 338,000 results (0.34 seconds)

[Come iniziare - Bitcoin](#)
<https://bitcoin.org/it/come-iniziare> ▾ [Translate this page](#)
Puoi **ottenere bitcoin** accettandoli **come** pagamento per beni e servizi, oppure ... la tua esperienza per aiutare le imprese oneste ad **ottenere** maggiore visibilità.
[Scegli il tuo portafoglio](#) - [Da sapere](#) - [Come funziona Bitcoin?](#)

[Come ottenere Bitcoin | Salvatore Aranzulla](#)
www.aranzulla.it > ... > [Guadagnare su Internet](#) ▾ [Translate this page](#)
I **Bitcoin** vengono considerati **come** vere e proprie unità di conto e pertanto sono ...
Teoricamente è possibile **ottenere Bitcoin** facendo eseguire dei calcoli ...



[Come guadagnare Bitcoin | Salvatore Aranzulla](#)
www.aranzulla.it > ... > [Guadagnare su Internet](#) ▾ [Translate this page](#)
A questo punto ti starai sicuramente chiedendo **come** guadagnare **Bitcoin**, e io oggi sono qui per cercare di chiarirti un po' le idee in merito. Vediamo dunque ...

Come ottenere i bitcoin

- **www.coinbit.it** - Bitcoin in 5 minuti grazie ad un sistema completamente automatizzato. Bonifico, Postepay e Superflash.
- **postecoin.com** - Compra BitCoin con Postepay.
- **www.bitboat.net** - Il mercato numero uno in Italia, per comprare Bitcoin istantaneamente, in contanti.
- **postebit.it** - Compra bitcoin in contanti senza registrazione!
- **www.mars78.biz** - Compra BitCoin con Postepay, Superflash.
- **www.happycoins.com** - Compra BitCoin con Mybank, Sofort.
- **www.litebit.eu** - Compra BitCoin con Postepay, Sepa, Sofort.
- **localbitcoins.com** - Compra bitcoin online in Italy
- **howtobuybitcoins.info** - Come acquistare bitcoin in Italia.
- **bitdigital.it** – Acquista bitcoin

Come osservare le transazioni

- Installare client **locale** (bitcoin-core): scomodo
- Usare servizi **block explorer via web** come blockchain.info o blockexplorer.com
 - Indirizzo
 - Transazione
 - IP (attenzione, non è l'IP di chi ha eseguito la transazione)
 - Taint Analysis
 - Statistiche
 - Tag
- Esempio, indirizzo di Ross Ulbright (Dread Pirate Roberts) cui sono stati sequestrati 26.000 BTC

Come osservare le transazioni

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

Summary		Transactions	
Address	1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX ⓘ	No. Transactions	569
Hash 160	99bc78ba577a95a11f1a344d4d2ae55f2f857b98	Total Received	29,659.52104295 BTC
Tools	Taint Analysis - Related Tags - Unspent Outputs	Final Balance	0.71604295 BTC

Request Payment Donation Button



Transactions (Oldest First) Filter

Transaction ID	Fee	Size	Date
7b305c9b480028666d5aa4e2f938ff068db88d98d3efb6d6790eae23b6ea2a2e	0.00000229 BTC	225 bytes	2015-04-07 13:43:14
1PyKgvs6GTf2mJey77WW8yXNmPRWhHCLY ⓘ (0.01251105 BTC - Output) → Silkroad Seized Coins ⓘ - (Unspent) 0.0001 BTC 17J8A5vVtIgVCQc6ANPnQtj1a2tTTkdkbK ⓘ - (Spent) 0.01240876 BTC 0.0001 BTC			
59bc0e344f18a7d1ac9f877bbccd4b8ed09b9e20a7e4ea71e491e8a8805d0fd6	0.0001 BTC	372 bytes	2015-03-09 20:57:52
3D16k49WrdyVeED1766u4ZgMH63eZ8HzkG ⓘ (10.009 BTC - Output) → Silkroad Seized Coins ⓘ - (Unspent) 0.001 BTC 3CY3cYvXiRz2UYCh5gMxnf7o2kNynk5ygi ⓘ - (Spent) 10.0079 BTC 0.001 BTC			
ed978dc23454308b2321d396b5a1b8e37849a05042c6bed592c667b69c2cce57	0.0001 BTC	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

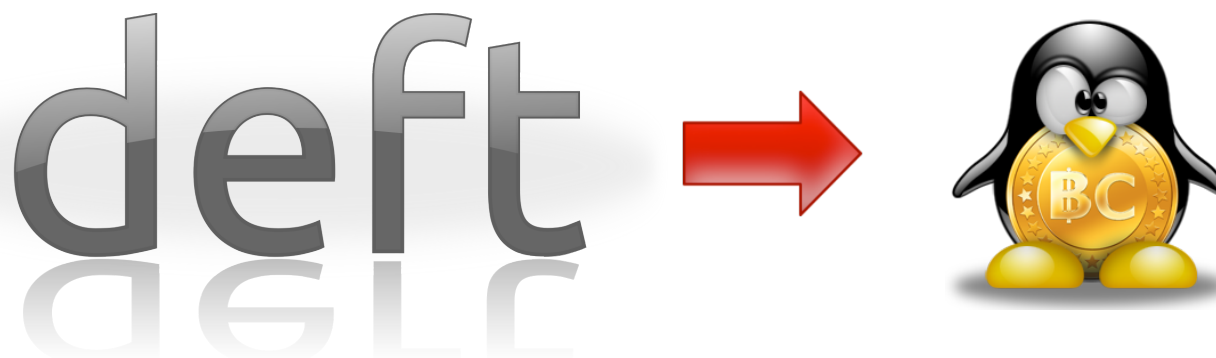
[View Tree Chart](#)

Network Propagation (Click to view)



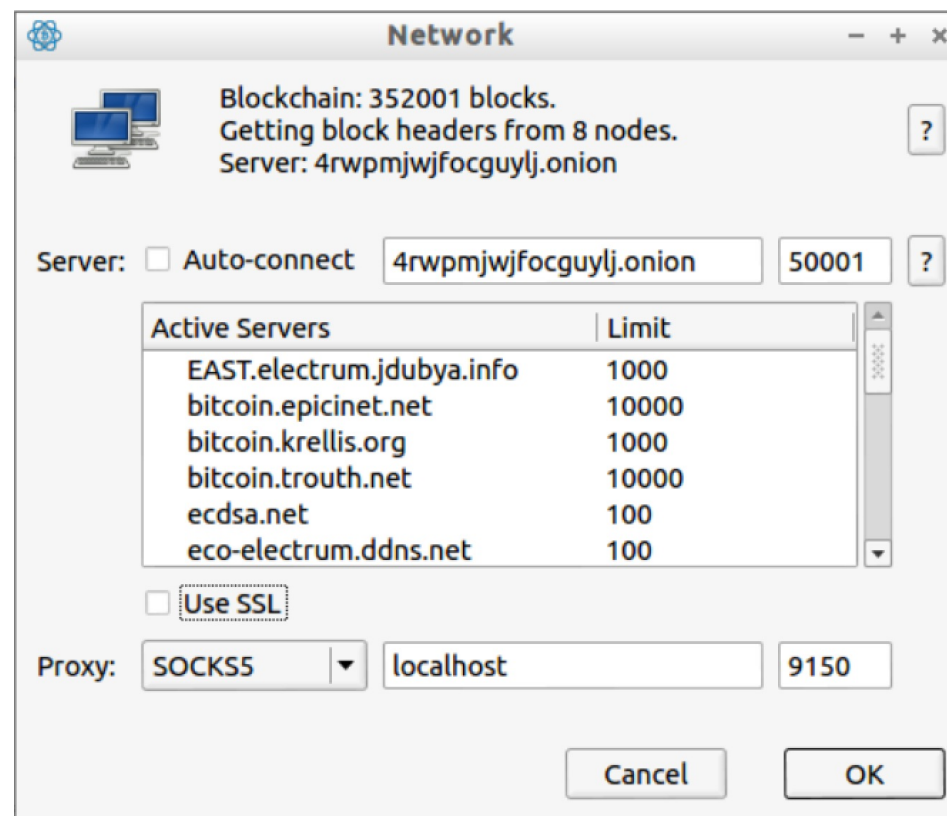
DEFTCoin ☺

- 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) 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)

- `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`

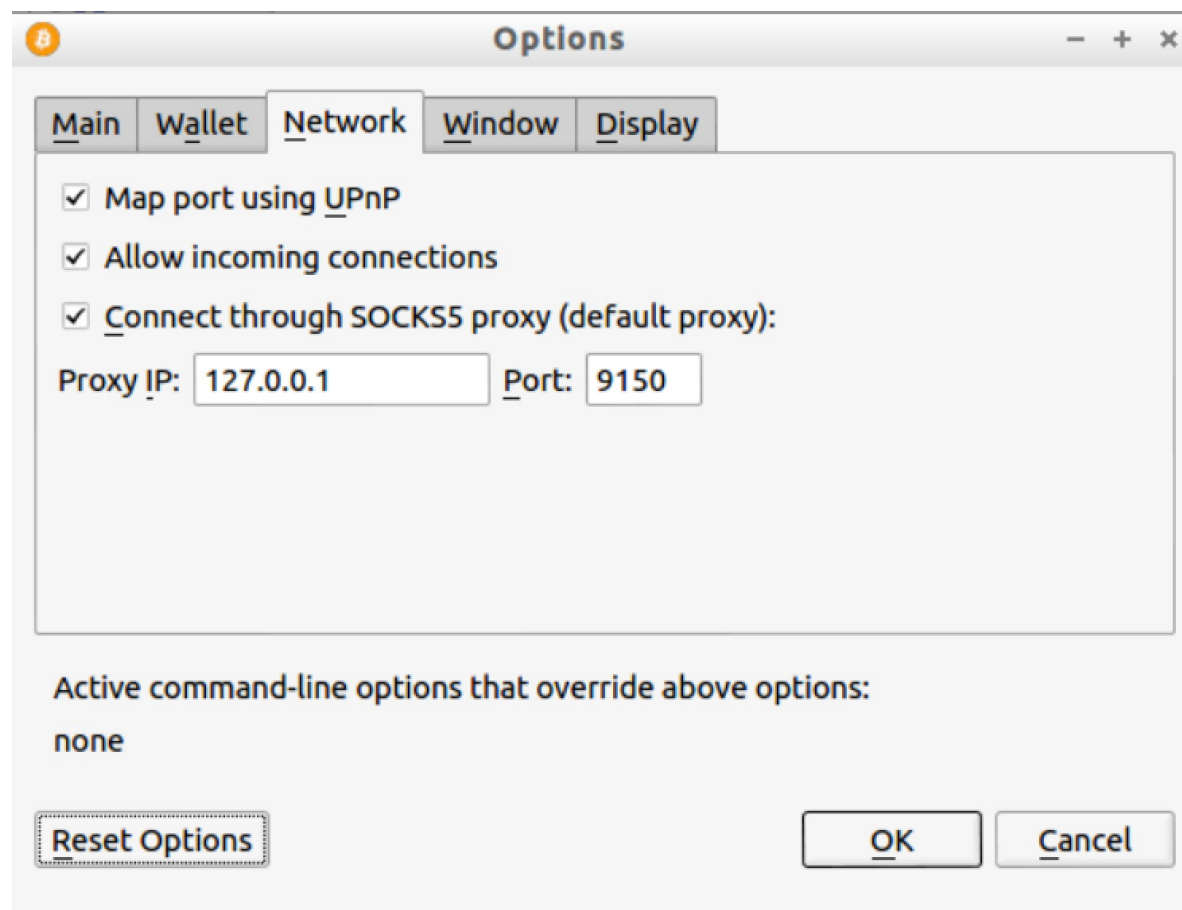


DEFTCoin: Bitcoin Core (+ Tor)

- `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**
 - github.com/gurnec/btcrecover
- **BTCScan**
 - <https://gist.github.com/chriswcohen/7e28c95ba7354a986c34/download>
- **KeyHunter**
 - <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
- <http://coinalytics.co/api/blockstem.html>

■ **Bitiodine**

- www.bitiodine.net

■ **Web Wallet**

DEFTCoin: 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 (!)



Come vengono ripuliti i bitcoin

How To Clean Your Coins

Step 1

**Deposit
Bitcoin**



Step 2

**Withdraw
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

Esperimenti sui Mixer/Tumbler

- Ho testato alcuni Mixer, con indirizzi qui offuscati
- In primis, ho testato se restituiscono i bitcoin...
- Quindi tramite **taint analysis** e **bitoidine**, ho verificato se lasciano tracce del “salto”



Esperimento con SatoshiDice

- Parto da quattro miei indirizzi:
 - 3bGacDLKPGMpjazaxz14gRrwrqEEzws1P
 - 3H2WXswWqXfPXa19DpiGYEZcdMkM5PqaTD
 - 3vBZoq4wQe34EVuwKZacmnuUMuU3MqeZXA
 - 3wQiW4914fdy253XS4MFaKeMiykpRhQSo
- Faccio generare deposit address a SatoshiDice e ottengo:
1aBme3pqrRSek1j9V132MXTBfropMycbRP
- Da lì eseguo 13 transazioni da circa 1 mBTC verso il deposit address **1DEFTAyfqK76woMv9U9o2rD4n3vWVCJLmy** e ottengo 13 indirizzi sorgenti diversi



Esperimento con SatoshiDice

- Certo un path comune o un taint tra gli indirizzi mittenti e il destinatario, con bitoidine e taint analysis

- 3bGacDLKPGMpjazaxz14gRrwrqEZEzws1P

2	3bGacDLKPGMpjazaxz14gRrwrqEZEzws1P	0.0014992355%	2
---	------------------------------------	---------------	---



- 3H2WXswWqXfPXa19DpiGYEZcdMkM5PaaTD

2	3H2WXswWqXfPXa19DpiGYEZcdMkM5PaaTD	0.2396184371%	2
---	------------------------------------	---------------	---



- 3vBZoq4wQe34EVuwKZacmnuUMuU3MqeZXA

	3vBZoq4wQe34EVuwKZacmnuUMuU3MqeZXA	0%	1
--	------------------------------------	----	---



- 3wQiW4914fdy253XS4MFaKeMiykpRhQSo

- NO TAIN



Esperimento con BitMixer

- <http://bitmixer.io>
(bitmixer2whesjgj.onion su Tor)
- Trasferisco fondi dal mio indirizzo
1QEjkMdqmDs5Ciefeccc9FGhUvfC8geiGf a
1FEUyk387UQGwypQSMWRPeXz5GPKKxE8z passando per il
deposit address Bitmixer 1Hn9gHszmR3uhTRJUacRFq28aa1Mo4s
- Taint analysis e bitiodine negative



No path found :(

There is no connection between the two addresses.

Esperimento con Bitcoin Fog



- www.bitcoinfog.com (foggeddriztrcar2.onion su Tor)
- Trasferisco fondi dal mio indirizzo
1Mdc7jHvdnsSSuJoTDdYTpLkxCjeU6fhtA a
1ANVcxswtQ48Sf32CfyjMbatJzLyg4361g passando per il deposit
address Bitcoin Fog 1BGowvbGnmnhWpF178CLWSS4998K4Hdsrk
- Taint analysis e bitiodine negative 👍 👍

No path found :(

There is no connection between the two addresses.

Esperimento con CoinJoin



- www.blockchain.info (blockchainbdgpzk.onion)
- Trasferisco fondi dal mio indirizzo
1dfgRye9C338WmgVq4L985Eyf87cbvcqPA a
133cdg1ZMFG6bAsD5uRZ19bkJP97nok12r4 utilizzando il
trasferimento CoinJoin di Blockchain.info con “normal privacy”

- Bitiodine negativo 

No path found :(

There is no connection between the two addresses.

- Ma... Received (Origin) Taint Analysis di 13wQ... POSITIVA! 



0.0036054111%

Esperimento con OnionWallet

- ow24et3tetp6tvmk.onion



- Trasferisco fondi dal mio indirizzo
18Qs1edswdFfeeVXvbrhH2cc34221t2ACd al wallet OnionWallet
e da lì... no riesco a farli uscire verso il mio indirizzo
1adbe4pGpkmv4Nw796VMUBaxcVdrVbzW2esH!
- Ho perso i (milli)bitcoin, la funzione SEND è difettosa.... 
- Tanto per tentare, ho messo altri mBTC sul wallet, casomai ci fosse stato un limite per i versamenti.
- Ho perso anche quelli (ma li vedo sul wallet)... 

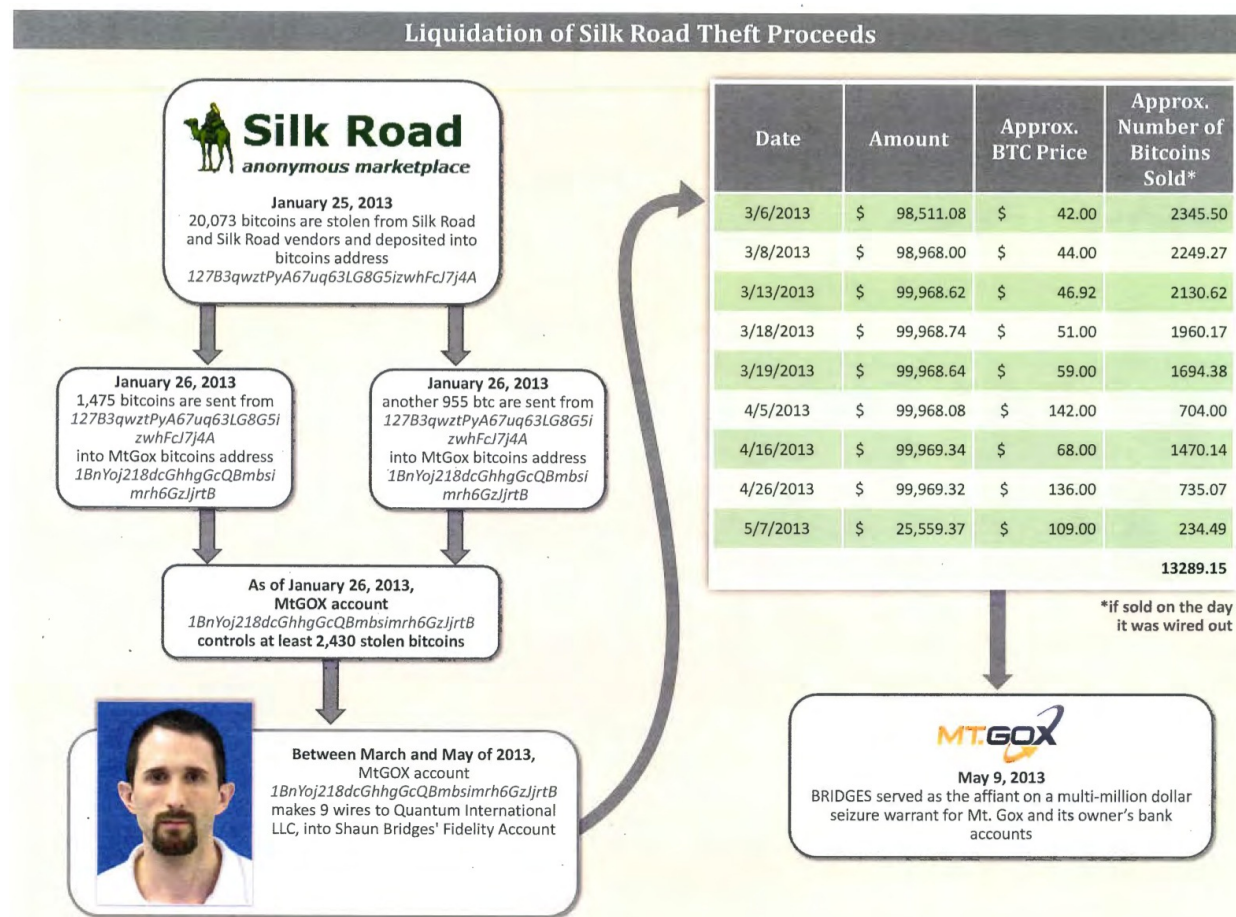
Esperimento con BitLaundry

- app.bitlaundry.com (no Onion Server, posso cmq usare Tor)
- Trasferisco fondi dal mio indirizzo
1wsDGdZJ2eErQHavxMMtujKz9q6Z2acDfy sul temporaneo di
Bitlaundry 1sedwh3r4GtXQGmsE2B9hwvBRwmYbqjTAU e poi da
lì il giorno dopo lui versa sul mio
19thHSoirgwxxc2fgaASWdT7dDnDs28Hdm
- La taint analysis è negativa, così come bitiodine:  
non c'è alcun collegamento tra i due indirizzi.

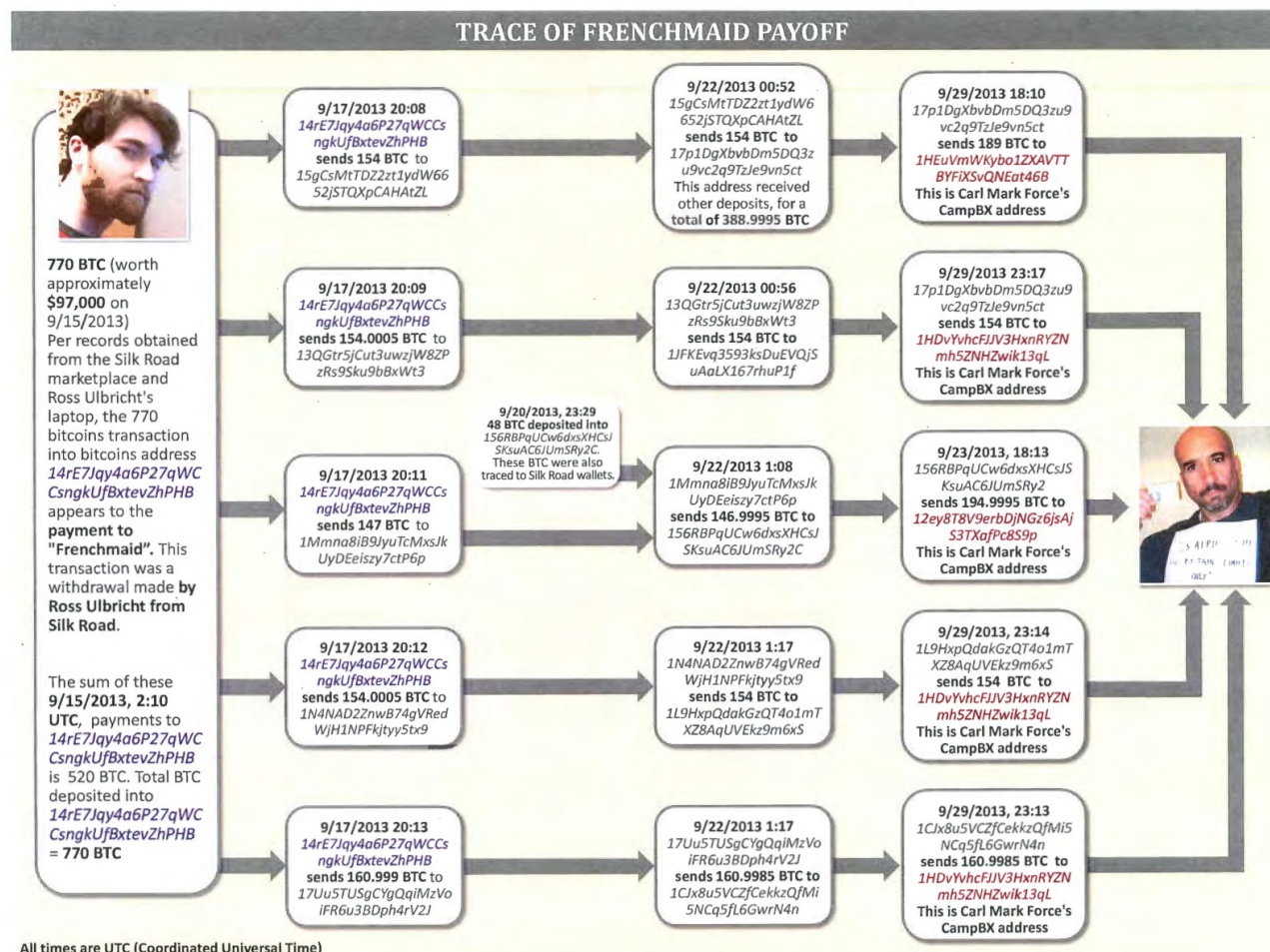
No path found :(

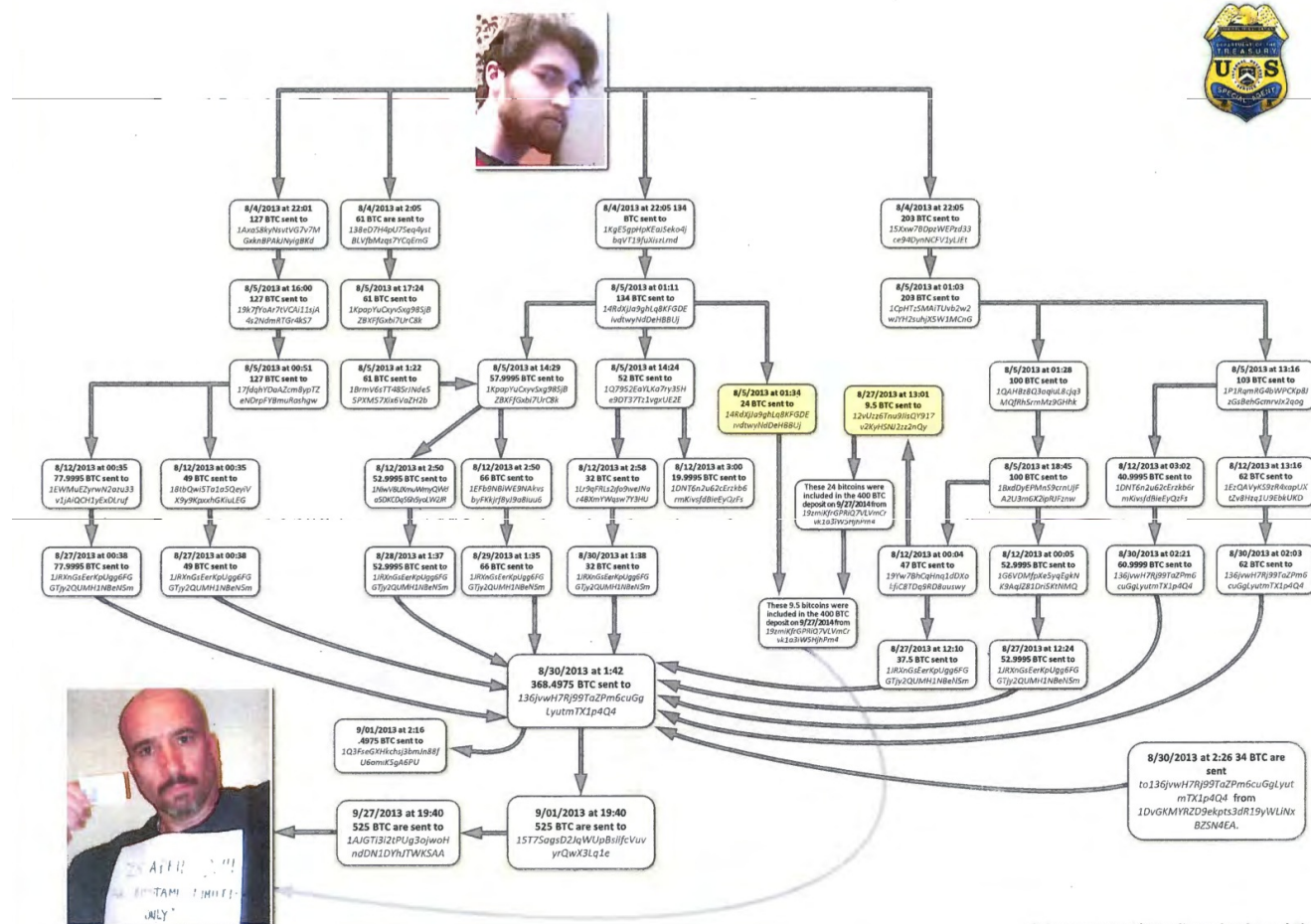
There is no connection between the two addresses.

Case Study 1: riciclaggio



Case Study 1: riciclaggio





All times are UTC (Coordinated Universal Time)

Case Study 2: monitoraggio

PERIZIA DI STIMA

Per il conferimento di beni o servizi in natura

di nr. 45 bitcoin

ex 2465 c.c.

per il conferimento nella società

ORACLIZE S.r.l.



- La prima Srl con Capitale Sociale Interamente Versato in BTC
- Interessante dal punto di vista contabile/giuridico... ancora di più dal punto di vista della trasparenza: **ogni movimento contabile del Capitale Sociale sarà pubblicamente visibile!**

Case Study 2: monitoraggio

- Bitcoin acquistati su Bitcoin.de (venditore Bitcoin Deutschland AG, Herford Germany)
- Acquisto di 45 BTC (circa 10.500 €) su indirizzo 1CXGwYxPo7SANCjuJNC3f16MZN2NjhKvxA
- Prova di appartenenza della relativa chiave privata
- Da lì trasferiti su **17Pmk7rGGXKopNfF8boxyBxyKowEB2tocP** e fermi tutt'ora

756ca57287aadcb2d332b45e27035a41d52aa802757f0e1210482208a39297c6

(Fee: 0 BTC - Size: 339 bytes) 2015-03-24 11:44:06

1CXGwYxPo7SANCjuJNC3f16MZN2NjhKvxA ⓘ (40 BTC - Output)

1CXGwYxPo7SANCjuJNC3f16MZN2NjhKvxA ⓘ (5 BTC - Output)



17Pmk7rGGXKopNfF8boxyBxyKowEB2tocP

ⓘ - (Unspent)

45 BTC

45 BTC

Case Study 2: monitoraggio

- Possiamo monitorare l'indirizzo e sapere in diretta quando e come verranno spesi! 😊
- Convertiamo l'indirizzo su blockchain in RSS
- <http://blockexplorer.com/rssa/17Pmk7rGGXKopNfF8boxyBxyKowEB2tocP.xml>
- Attiviamo un servizio di monitor orario gratuito della pagina/feed RSS (es. www.followthatpage.com)
- Riceveremo un alert gratuito via mail non appena verranno ricevuti o spesi BTC (tenere conto che chiunque può versare BTC su quell'indirizzo anche all'insaputa del proprietario)
- **Fa riflettere pensare che se le tasse si pagassero in BTC potremmo vedere come vengono utilizzate... 😊**

Case Study 2: monitoraggio



- FollowThatPage free:
 - 20 daily runs
 - 1 hourly run
- Alternative:
 - feed2mail.com
 - watchthatpage.com
 - changedetection.com
 - changedetect.com
 - followthatpage.com
 - onwebchange.com
 - changedetection

New page details

Page address

☐ Ignore numbers

☒ Report additions

☒ Report removals

Lines of context

Select here how many lines of context you want to see in the reports around the lines of text that have changed. Allowed values: 0 to 30000. If you specify 1 or more, all added and removed text is shown.

Description

You can enter a description of the page, to be used in the subject headers of the emails we send you. If empty, we use the page address (URL).

Report errors ☐ Report all errors, including server connection failures

☒ Report HTTP errors (like "page not found")

☐ Don't report errors

Frequency ☐ Check daily (max 20 pages)

☒ Check hourly (max 1 page)

With a [Pro account](#), you can check pages every 10 minutes!

Case Study 2: monitoraggio

- Ad ogni entrata/uscita di BTC relativa all'indirizzo monitorato ricevo una mail, con i dettagli della nuova transazione

Changes in 'http://blockexplorer.com/rssa/1GQ6CxYZiYWP[REDACTED]VyW48MU9PfXr.xml'	• Follow That Page	• 07/04/15 01:47
Changes in 'http://blockexplorer.com/rssa/1GQ6CxYZiYWP[REDACTED]VyW48MU9PfXr.xml'	• Follow That Page	• 06/04/15 11:57
Changes in 'http://blockexplorer.com/rssa/1GQ6CxYZiYWP[REDACTED]VyW48MU9PfXr.xml'	• Follow That Page	• 04/04/15 19:46
Changes in 'http://blockexplorer.com/rssa/1GQ6CxYZiYWP[REDACTED]VyW48MU9PfXr.xml'	• Follow That Page	• 03/04/15 17:46
Changes in 'http://blockexplorer.com/rssa/1GQ6CxYZiYWP[REDACTED]VyW48MU9PfXr.xml'	• Follow That Page	• 03/04/15 14:46
Following 'http://blockexplorer.com/rssa/1GQ6CxYZiYWP[REDACTED]VyW48MU9PfXr.xml'	• Follow That Page	• 03/04/15 13:46

- Molto più comodo rispetto a monitorare in locale, ancora non ci sono strumenti validi per farlo
- Alternative locali:
 - Bitcoin-core (bitcoin-cli) – solo info su address locali, per avere info su transazioni di altri abilitare “txinfo=1” in bitcoin.conf
 - Bitcoin ABE
 - Insight

Case Study 2: monitoraggio

- Altri indirizzi interessanti da monitorare:
 - 1FeexV6bAHb8ybZjqQMjJrcCrHGW9sb6uF: 79,957 BTC dal 2011
 - 12ib7dApVFvg82TXKycWBNpN8kFyiAN1dr: 31,000 BTC dal 2010
 - 12tkqA9xSoowkzoERHMWNKsTey55YEBqkv: 28,150 BTC dal 2010
 - 16cou7Ht6WjTzuFyDBnht9hmvXytg6XdVT: 53,000 BTC con una spesa nel 2012
 - 1HQ3Go3ggs8pFnXuHVHRytPCq5fGG8HbhxBitcoin: 69,471 BTC dal 2013

Case Study 3: furto

- Provare a versare un mBTC su questi indirizzi, dopo aver verificato su Blockchain che non sono mai stati utilizzati... ☺
 - **1A79FTMhX7vu1AMhFhvTNeZaaBD4CMbqoj**
(chiave privata 5KR997pmcHZRx1gtadKiRYCfgrdnrcBwYgsYtc8DkUNcknjdH)
 - **16p75ACof9eWEvXhW6c2WbCaZi87WA9ZLh**
(chiave privata 5KZaymxsoFk7pi6gqqsMiYECwUAeDWheZwugKArcGCtU1Zke8xC)
- Li ho generati io, ho quindi la chiave privata (che riporto sopra) ma non li ho messi in wallet né ho mai pubblicato le chiavi
- Se succede qualcosa ai mBTC che depositate, *follow the money...* ☺

Grazie

Email/Twitter

paolo@dalchecco.it / @forensico

Web

www.dalchecco.it / www.bitcoinforensics.it

Donazioni per DEFT Association

1DEFTAyfqK76woMv9U9o2rD4n3vWVCJLmy