Bitcoin e criptovalute

Milano, 12 novembre 2016

Chi Sono

Davide ‘Rebus’ Gabrini

Per chi lavoro non è un mistero.

Oltre a ciò:

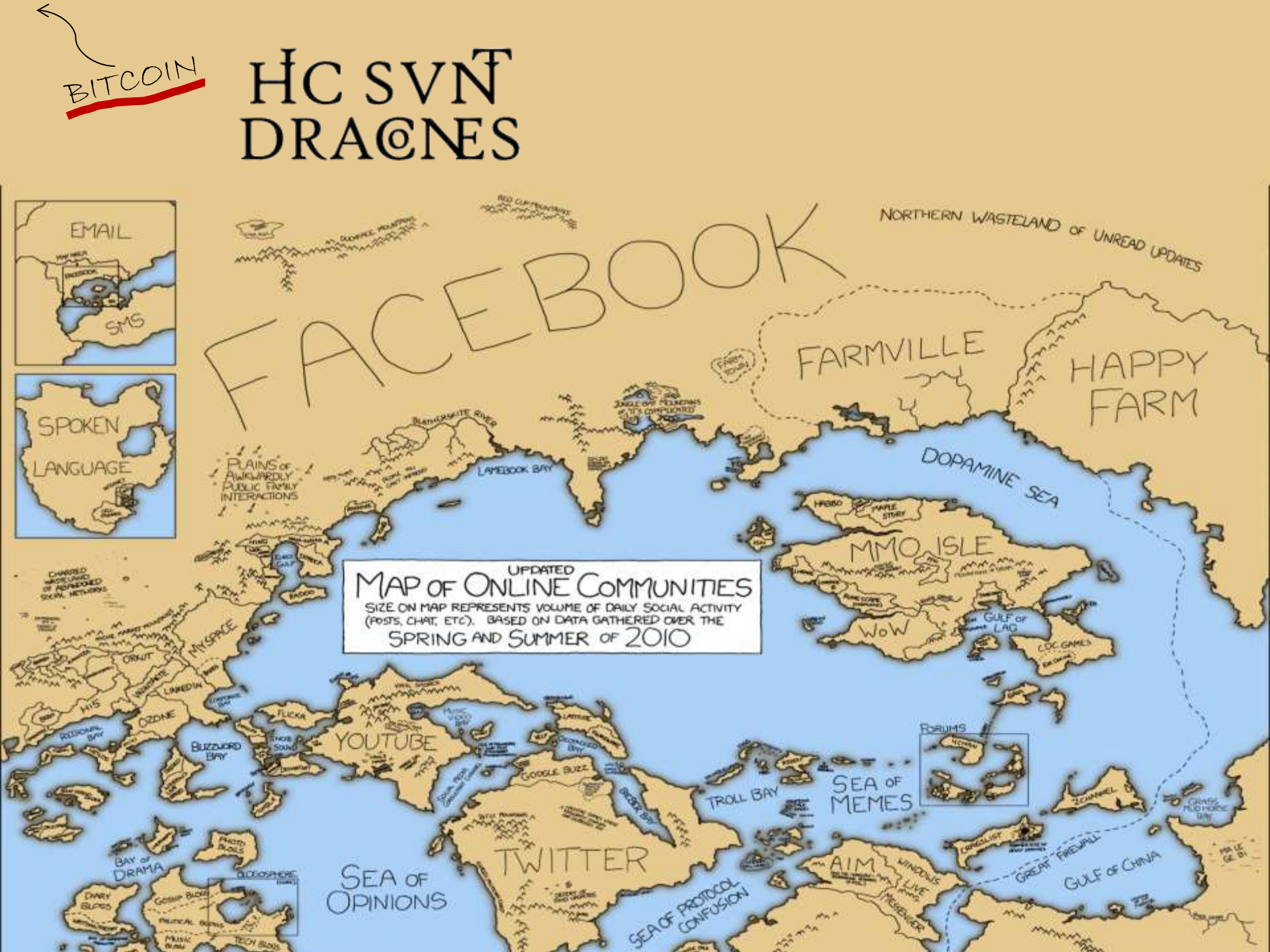
- Perito informatico
- Consulente tecnico e Perito forense
- Collaboratore UniPV
- Docente di sicurezza informatica e digital forensics per privati e P.A.
- Certificazioni CIFI, ACE, AME
- Socio Mensa, IISFA, DEFTA, Tech&Law fellow
- Socio fondatore Italian Gr.A.P.P.A.
- Presidente Nutria-LUG
- Sensei Zanshin Tech

Chi Sono

Franco Cimatti (HostFat)

- Perito informatico
- Da sempre appassionato di tecnologie p2p
- Seguo Bitcoin da circa maggio 2010
- Moderatore sez. ita. Bitcointalk.org
- Presidente assoc. Bitcoin Foundation Italia

- twitter hostfat
- hostfat gmail
- hostfat praticamente ovunque


BITCOIN
HC SVNT DRACONES
EMAIL
SMS
SPOKEN LANGUAGE
FACEBOOK
NORTHERN WASTELAND OF UNREAD UPDATES
FARMVILLE
HAPPY FARM
PLAINS OF AWKWARDLY PUBLIC FAMILY INTERACTIONS
LAMEBOOK BAY
DOPAMINE SEA
MMO ISLE
WoW
GULF OF LAG
UPDATED
MAP OF ONLINE COMMUNITIES
SIZE ON MAP REPRESENTS VOLUME OF DAILY SOCIAL ACTIVITY (POSTS, CHAT, ETC). BASED ON DATA GATHERED OVER THE SPRING AND SUMMER OF 2010
MYSPACE
ORKUT
LINKEDIN
HI5
OZONE
BUZZWORD BAY
YOUTUBE
FLICKR
GOOGLE BUZZ
TROLL BAY
SEA OF MEMES
FORUMS
TWITTER
SEA OF OPINIONS
BAY OF DRAMA
SEA OF PROTOCOL CONFUSION
AIM
GREAT FIREWALL
GULF OF CHINA

Introduzione

Cosa sono i bitcoin

- Moneta elettronica basata sulla crittografia (“crittovaluta”)
- Sistema pensato per Internet
  - Protocollo di scambio P2P tra sconosciuti garantito matematicamente
  - Nessuna autorità centrale
  - Tecnologie open source, sistema non vincolabile
- Veloce ed economico
  - Transazioni da qualsiasi conto a qualsiasi altro in media in 10 minuti
  - Nessun confine nazionale
  - Commissione indipendente dal valore della transazione
- Irreversibile e non falsificabile
- Pseudo-anonimo
  - I conti non hanno proprietà definita
  - È persino possibile eseguire versamenti su conti di nessuno
  - La proprietà è garantita da chi possiede la chiave privata

Cosa sono i bitcoin

- Controvalore in valuta fiat stabilito dal mercato
  - Controvalore altamente variabile
  - Assenza di regolamentazione su tracciabilità o plusvalore
  - Inflazione determinata a priori dall'algoritmo
  - Possono essere generati al massimo 21 milioni di BTC
  - BTC divisibili fino a 8 decimali:
    - cBTC = 0.01 BTC (centibitcoin)
    - mBTC = 0.001 BTC (millibitcoin)
    - µBTC = 0.000 001 BTC (microbitcoin)
    - Satoshi = 0.000 000 01 BTC
- Non esiste il bitcoin in sé, ma esistono le transazioni
- Transazioni memorizzate in un libro mastro pubblico: la blockchain

Terminologia

- **Chiave privata**: 256 bit, il punto di partenza per la generazione delle chiavi pubbliche e, di conseguenza, degli indirizzi. Se ne può dimostrare il possesso firmando un messaggio.
- **Chiave pubblica**: 512 bit, derivata dalla chiave privata. Può essere usata per verificare la firma di un messaggio.
- **Indirizzi bitcoin**: 160 bit, 27-34 caratteri alfanumerici. Gli indirizzi vengono derivati dalle chiavi pubbliche. Come un IBAN o un indirizzo e-mail, generabile autonomamente e senza limiti. Per bitcoin, inizia sempre per 1.

Bitcoin Address

SHARE

12St5js5pT18iMybf1TxghbAzLsH4yqYng

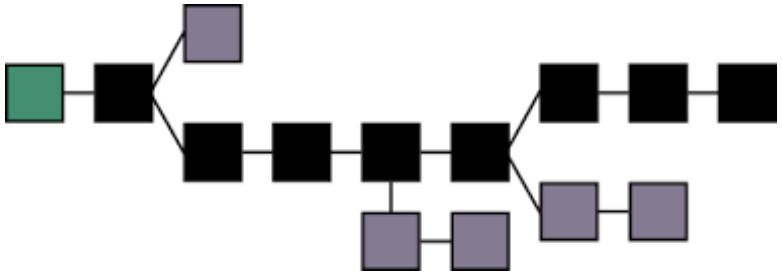
Private Key (Wallet Import Format)

SECRET

5KkrPXWACDU6JnRi6kuEokPr1rEFAF6pJdLQzExxSFwD5oicaVP

Terminologia

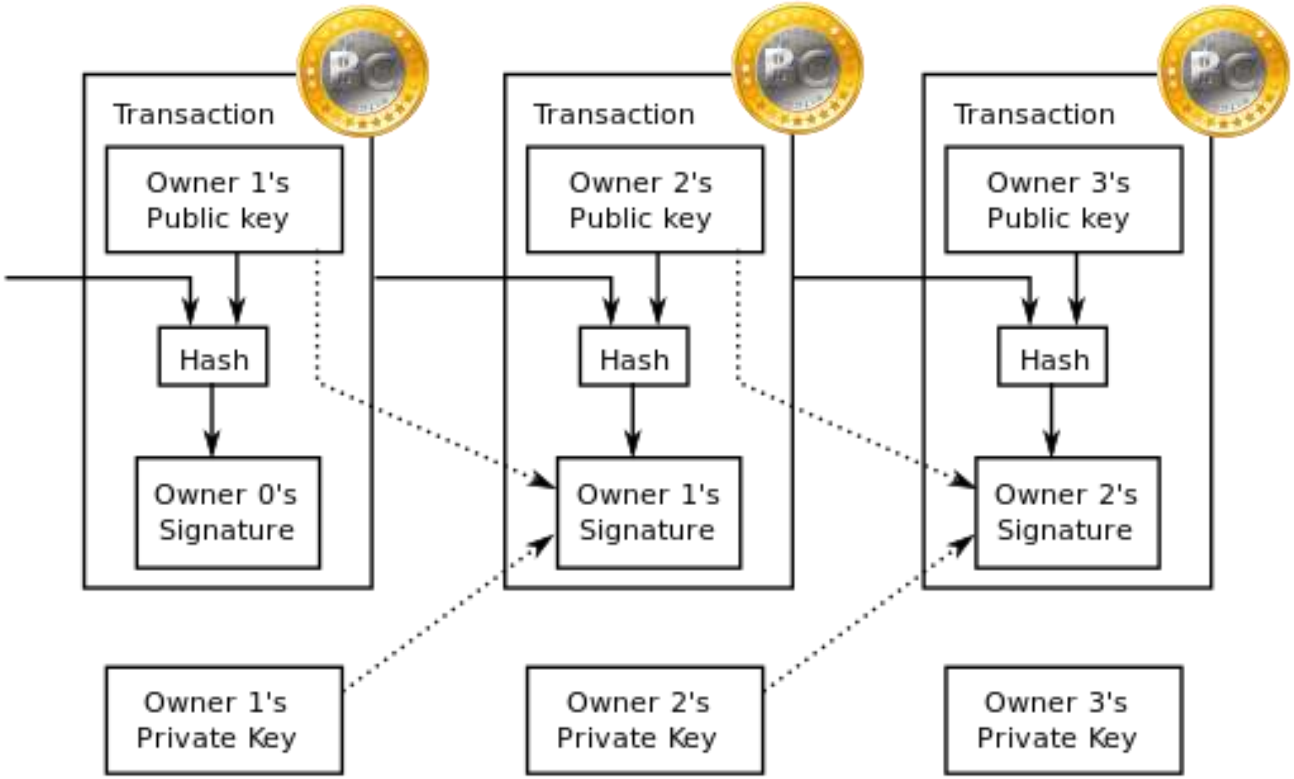
- **Blockchain**: il libro mastro delle transazioni. Pubblico, condiviso, decentralizzato, composto da blocchi la cui validità viene verificata matematicamente.



- **Blocco**: unità della blockchain. Contiene più transazioni, accorpate e validate dai miner, ed è legato matematicamente alla blockchain mediante hash.
- **Wallet**: Il portafoglio che raccoglie i diversi indirizzi bitcoin, può essere locale sul PC o un servizio web offerto da terzi. Generalmente è protetto da password. Può essere gerarchico deterministico.

Terminologia

- **Transazione**: passaggio irreversibile di una certa quantità di bitcoin da un indirizzo all'altro, che viene inserita in un blocco della blockchain e diventa quindi pubblica



Terminologia

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

How a ₿itcoin transaction works

Bob, an online merchant, decides to begin accepting bitcoins as payment. Alice, a buyer, has bitcoins and wants to purchase merchandise from Bob.

WALLETS AND ADDRESSES

Bob and Alice both have Bitcoin "wallets" on their computers.

Wallets are files that provide access to multiple Bitcoin addresses.

An address is a string of letters and numbers, such as 1HLiMwZEP kjEPeCh 43BeKJLJyb LCWrfDpN.

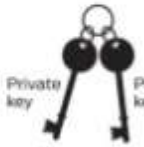
CREATING A NEW ADDRESS

Bob creates a new Bitcoin address for Alice to send her payment to.

Each address has its own balance of bitcoins.

SUBMITTING A PAYMENT

Alice tells her Bitcoin client that she'd like to transfer the purchase amount to Bob's address.



Public Key Cryptography 101

When Bob creates a new address, what he's really doing is generating a "cryptographic key pair," composed of a private key and a public key. If you sign a message with a private key (which only you know), it can be verified by using the matching public key (which is known to anyone). Bob's new Bitcoin address represents a unique public key, and the corresponding private key is stored in his wallet. The public key allows anyone to verify that a message signed with the private key is valid.

It's tempting to think of addresses as bank accounts, but they work a bit differently. Bitcoin users can create as many addresses as they wish and in fact are encouraged to create a new one for every new transaction to increase privacy. So long as no one knows which addresses are Alice's, her anonymity is protected.

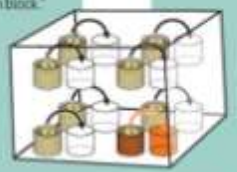
Alice's wallet holds the private key for each of her addresses. The Bitcoin client signs her transaction request with the private key of the address she's transferring bitcoins from.

Anyone on the network can now use the public key to verify that the transaction request is actually coming from the legitimate account owner.

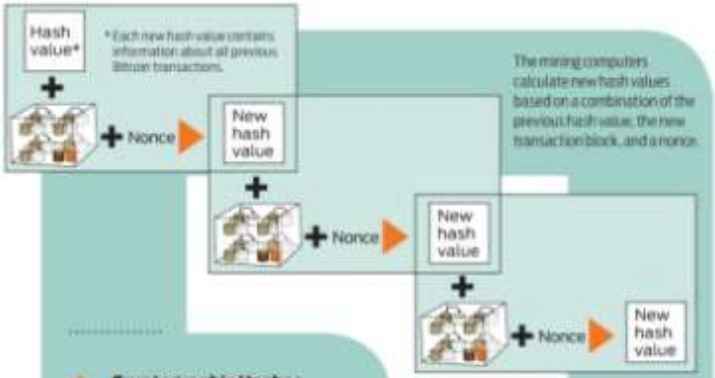
VERIFYING THE TRANSACTION

Gary, Garth, and Glenn are Bitcoin miners.

Their computers bundle the transactions of the past 10 minutes into a new "transaction block."



The miners' computers are set up to calculate cryptographic hash functions.



The mining computers calculate new hash values based on a combination of the previous hash value, the new transaction block, and a nonce.

Cryptographic Hashes

Cryptographic hash functions transform a collection of data into an alphanumeric string with a fixed length, called a hash value. Even tiny changes in the original data drastically change the resulting hash value. And it's essentially impossible to predict which initial data set will create a specific hash value.

Nonces

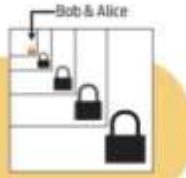
To create different hash values from the same data, Bitcoin uses "nonces." A nonce is just a random number that's added to data prior to hashing. Changing the nonce results in a wildly different hash value.

Creating hashes is computationally trivial, but the Bitcoin system requires that the new hash value have a particular form—specifically, it must start with a certain number of zeros.

The miners have no way to predict which nonce will produce a hash value with the required number of leading zeros. So they're forced to generate many hashes with different nonces until they happen upon one that works.

Each block includes a "coinbase" transaction that pays out 50 bitcoins to the winning miner—in this case, Gary. A new address is created in Gary's wallet with a balance of newly minted bitcoins.

TRANSACTION VERIFIED



As time goes on, Alice's transfer to Bob gets buried beneath other, more recent transactions. For anyone to modify the details, he would have to redo the work that Gary did—because any changes require a completely different winning nonce—and then redo the work of all the subsequent miners. Such a feat is nearly impossible.

All'inizio era il genesis block...

Block 0

Short link: http://blockexplorer.com/b/0

Hash: 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

Next block: 00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048

Time: 2009-01-03 18:15:05

Difficulty: 1 ("Bits": 1d00ffff)

Transactions: 1

Total BTC: 50

Size: 285 bytes

Merkle root: 4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

Nonce: 2083236893

Raw block

Transactions

Transaction	Fee	Size (kB)	From (amount)	To (amount)
4a5e1e4baa...	0	0.204	Generation: 50 + 0 total fees	1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa: 50

http://blockexplorer.com/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

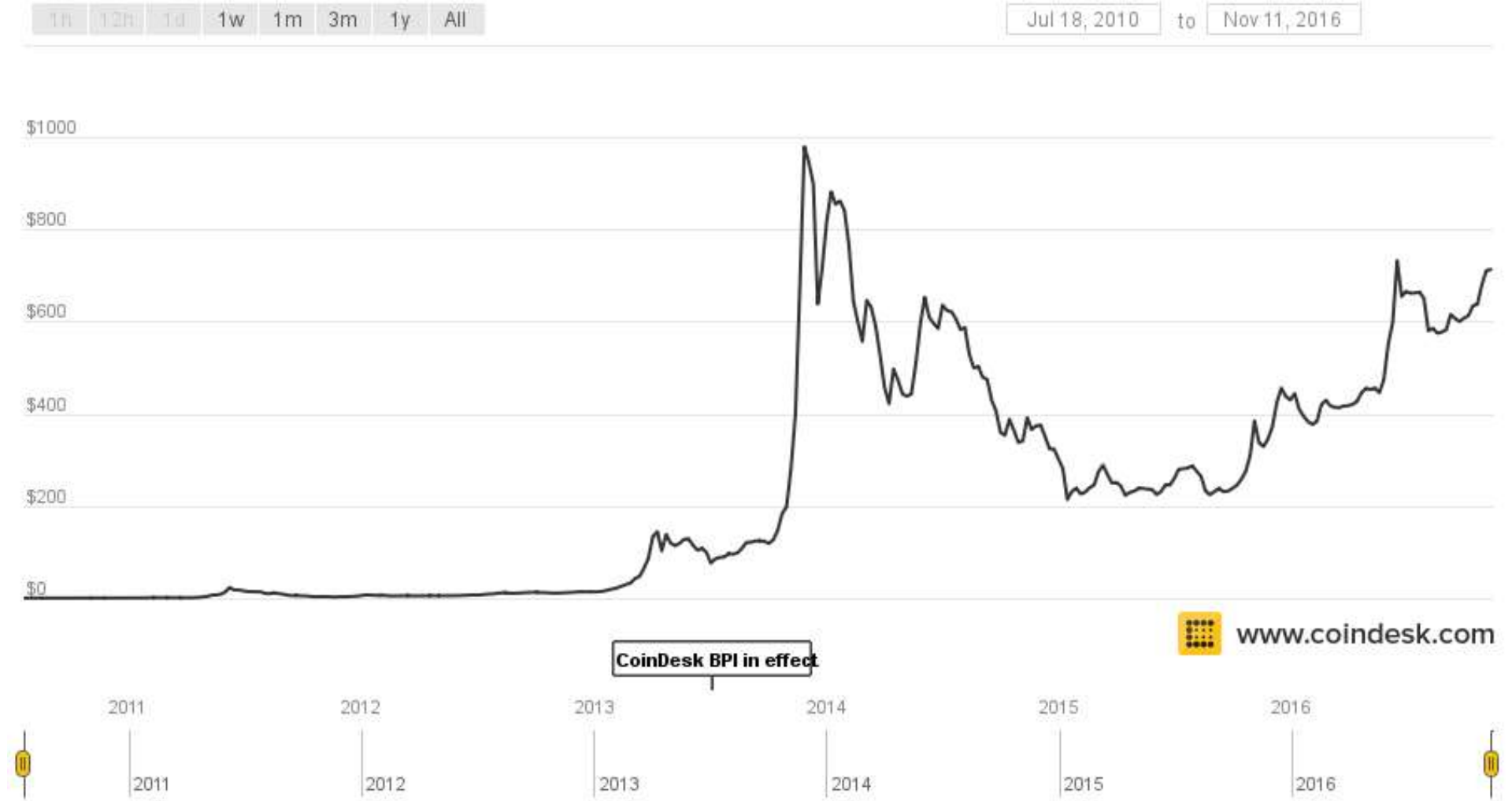
… e l'articolo di Satoshi Nakamoto (2008)

Bitcoin: A Peer-to-Peer Electronic Cash System

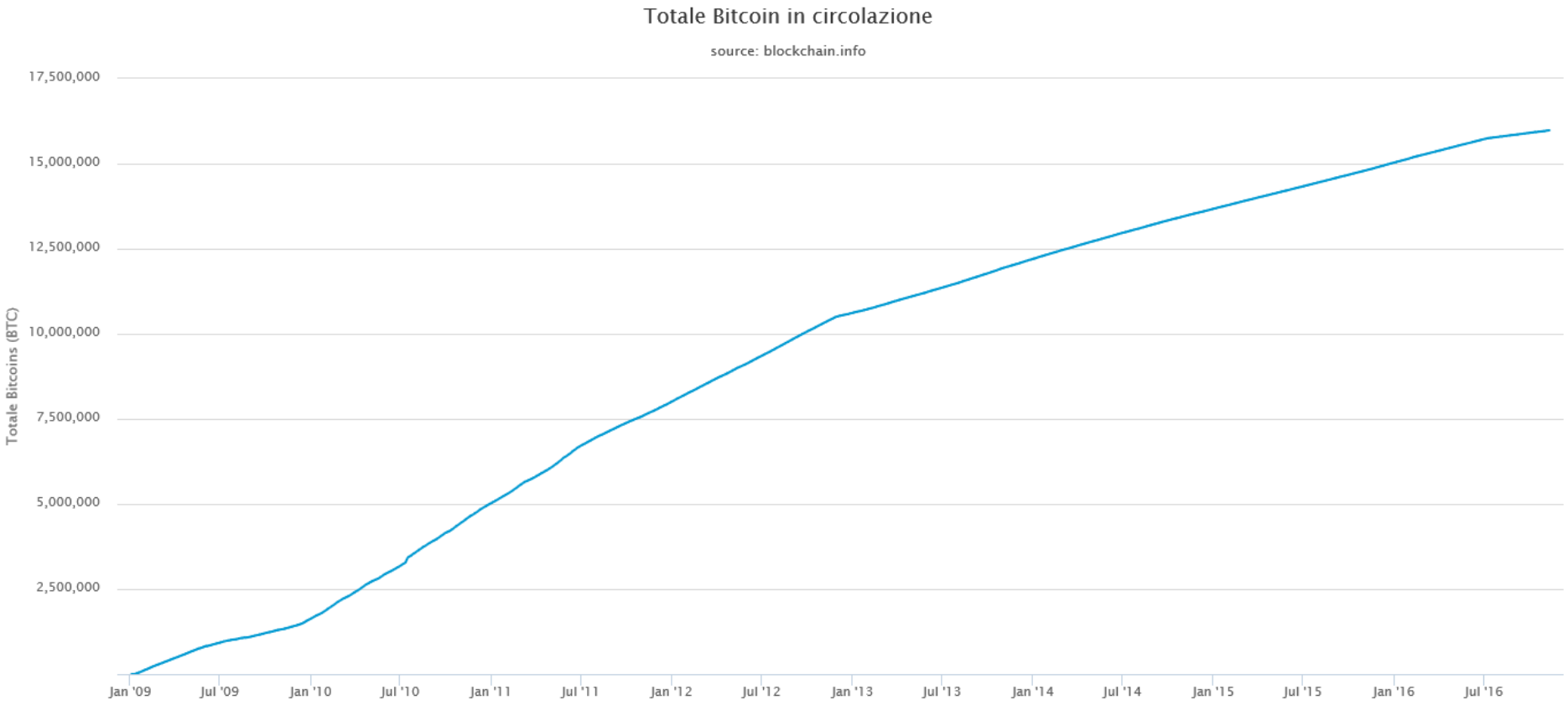
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

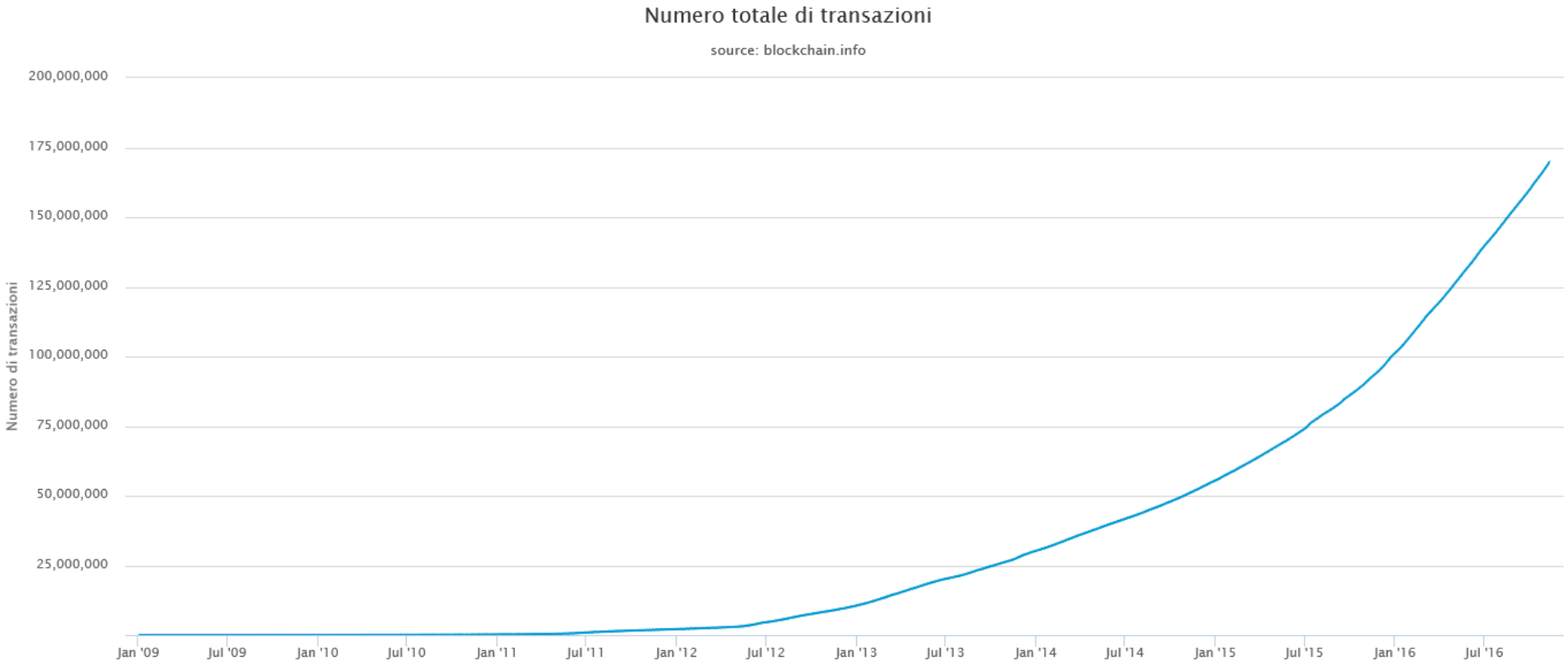
Quanto vale un bitcoin



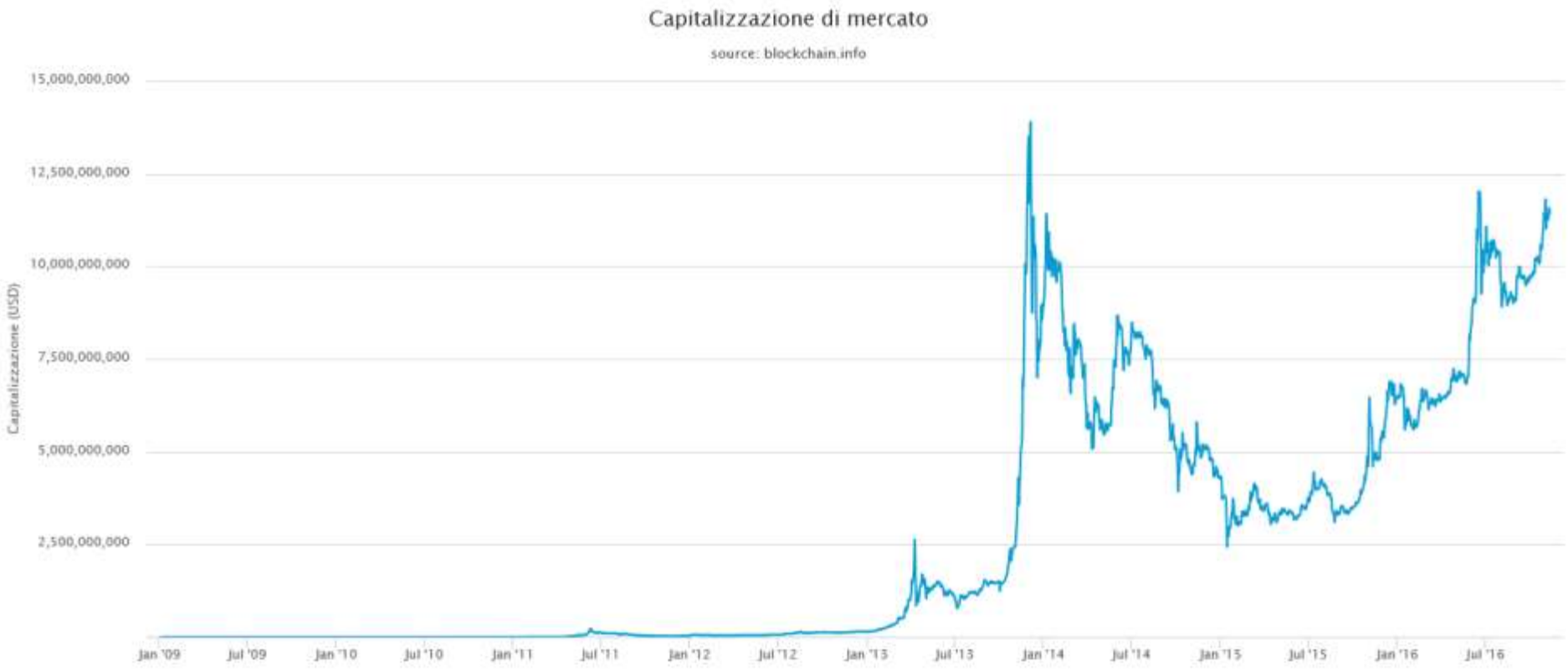
Oggi siamo a 16 milioni di bitcoin...



...e 170 milioni di transazioni



Il tutto vale al momento circa 11 miliardi di $



Tipi di wallet

Smartphone | Desktop | Hardware | Web


breadwallet


Bither


GreenBits


Coinomi


Coin.Space


Copay


Airbitz


Mycelium


Green Address


Simple Bitcoin


Bitcoin Wallet

Tipi di wallet

Smartphone | **Desktop** | Hardware | Web


Bitcoin Core


Bitcoin Knots


Armory


Electrum


mSIGNA


Bither

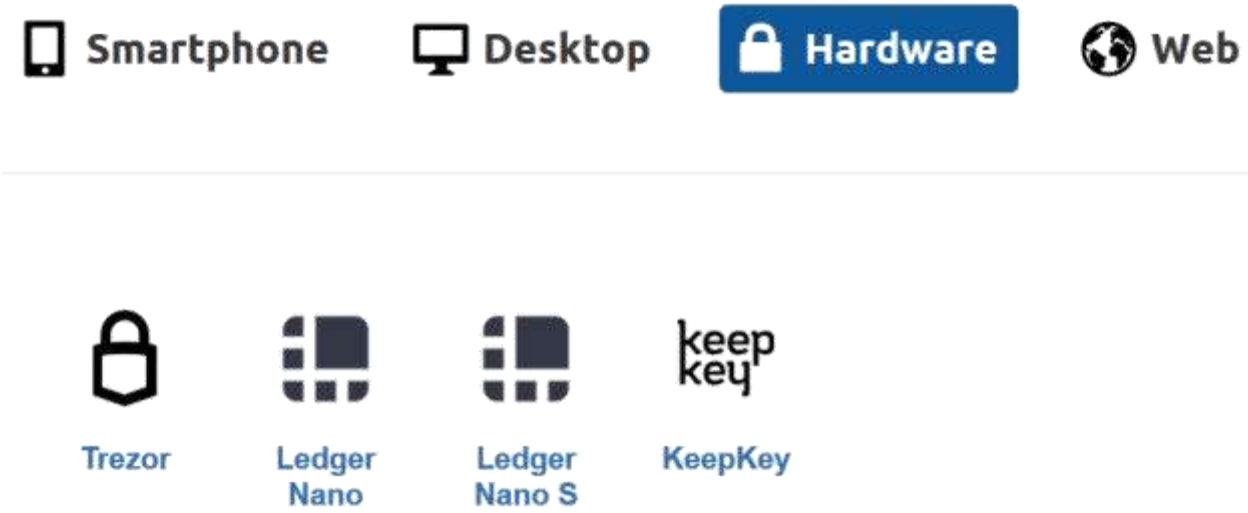

MultiBit HD


BitGo


Green Address


Copay

Tipi di wallet



Tipi di wallet

Smartphone Desktop Hardware Web


Green Address


Coin.Space


BitGo


Coinbase


Xapo

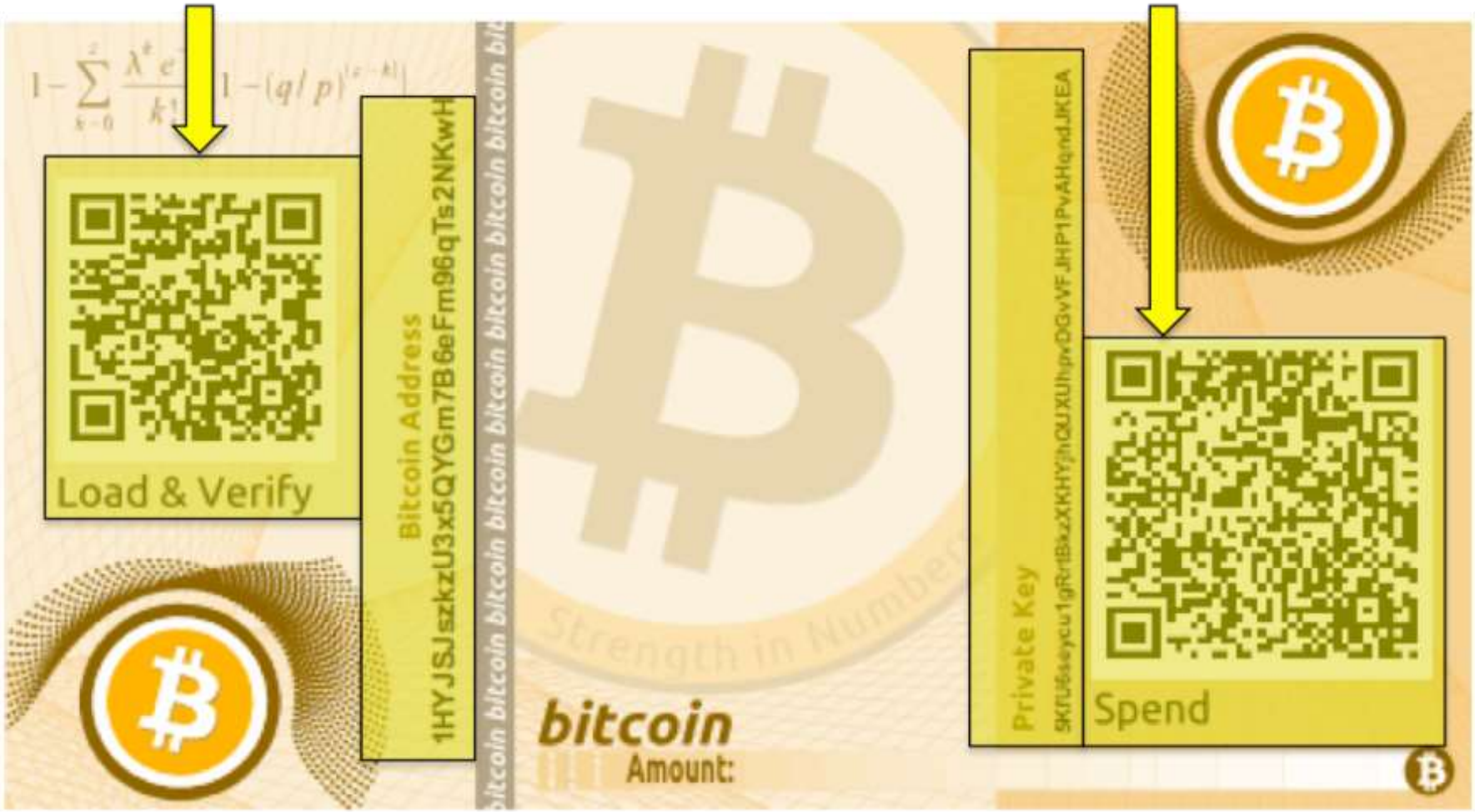

Coinapult


Circle

Paper wallet

Public Key:
Used to receive Bitcoins
Share this with anyone you wish

Private Key:
Used to spend Bitcoins
Never share this with anyone



Cold storage

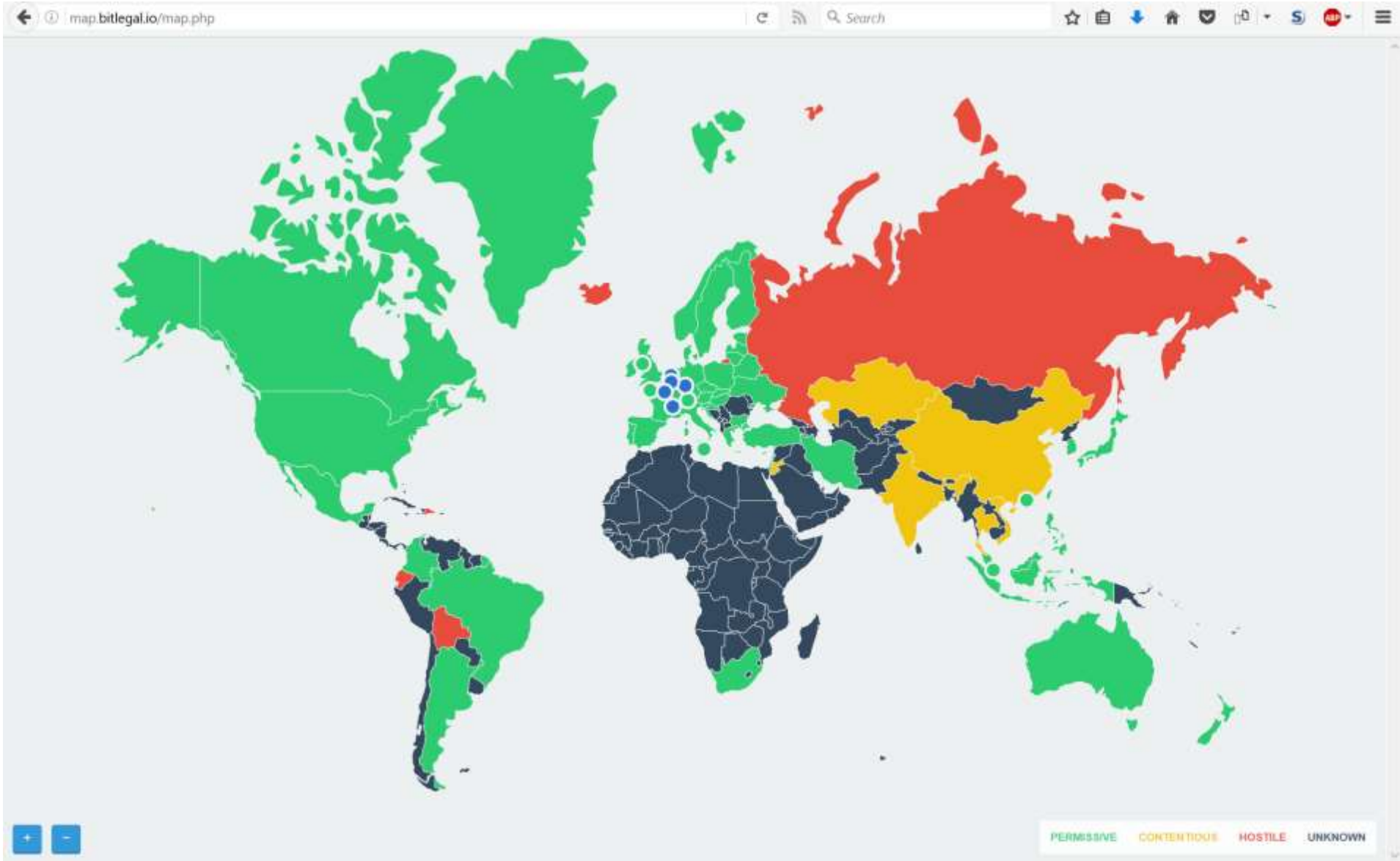
Dove si scambiano BTC <-> EURO

- Il valore è determinato dal mercato o dalla richiesta dell'exchanger
- Vi sono diversi servizi/siti online per lo scambio
  - Kraken,Therocktrading,Bitfinex,BTC-e etc…
- Costi e modalità diverse anche per il pagamento:
  - Bonifico, contanti (LocalBitCoins), Ricarica Superflash o Postepay (Bitboat, Postebit), Western Union, etc…
- Pochi servizi accettano carta di credito (Coinbase, Circle), quasi nessuno Paypal

Uso con carte prepagate/servizi pagamento

- Carte visa/mastercard
  - KYC1 – Nessuna o quasi verifica documenti. Limite annuo 2500 euro.
  - KYC2 – Verifica documenti. Limite annuo 10000/50000 euro.
  - NFC (poco diffuso ancora) – Sarà possibile pagare nei POS senza ricezione carta ad indirizzo fisico.
- Servizi di pagamento
  - Skrill
  - Paypal
  - Neteller

Come reagiscono i governi?



In Italia...

Bitlegal

Regulatory Details

Basic Rights		
Owning BTC	Yes	
Buying BTC	Yes	
BTC Transactions	Yes	
Mining BTC	Yes	
Taxation		
General Income - Exchanges	Likely	Italy assesses income tax on all types of gains
General Income - Commerce	Likely	
General Income - Mining	Unknown	
VAT - Exchanges	Likely	Value Added Tax applies to the importation of goods into Italy, and the transfer of goods/ rendering of services related to business operations; if bitcoins are classified as either goods or services, VAT will likely apply to sales/transfers
VAT - Commerce	Likely	Regardless of classification, purchases of goods and services with bitcoins will likely be subject to VAT
VAT - Mining	Unknown	
Capital Gains - Exchanges	Unclear	Italy does not have a separate capital gains tax for businesses, but individuals may be subject to preferred capital gains rates on the disposal of certain assets - so classification will be key
Capital Gains - Mining	Unknown	

Mixer

- Centralizzati (rischio di controparte)
  - Bitcoin inviati in pochi indirizzi, controllati dal servizio, contenenti grosse quantità di bitcoin. Ritirati poi in quantità diverse, in tempi diversi
  - Bitcoin inviati in tanti indirizzi, forniti a random o meno, sempre controllati dal servizio. Le transazioni in uscita vengono poi fatte da altri indirizzi, usati in precedenza da altri utenti, rompendo il legame con la transazione iniziale.
- Joinmarket (sicuro)
  - Uso di tecnica CoinJoin
  - Incentivo partecipazione di capitali esterni

Altre criptovalute

- Litecoin, Dogecoin ecc.
  - Velocità di conferma differente
  - Inflazione infinita
- Dash, Monero, Zerocoin, Zcash
  - Maggiore privacy nelle transazioni
- Steem
  - Ricavo partecipazione social
- Ripple
  - Sistemi di intermediazione bancaria e gestione asset

Evoluzioni

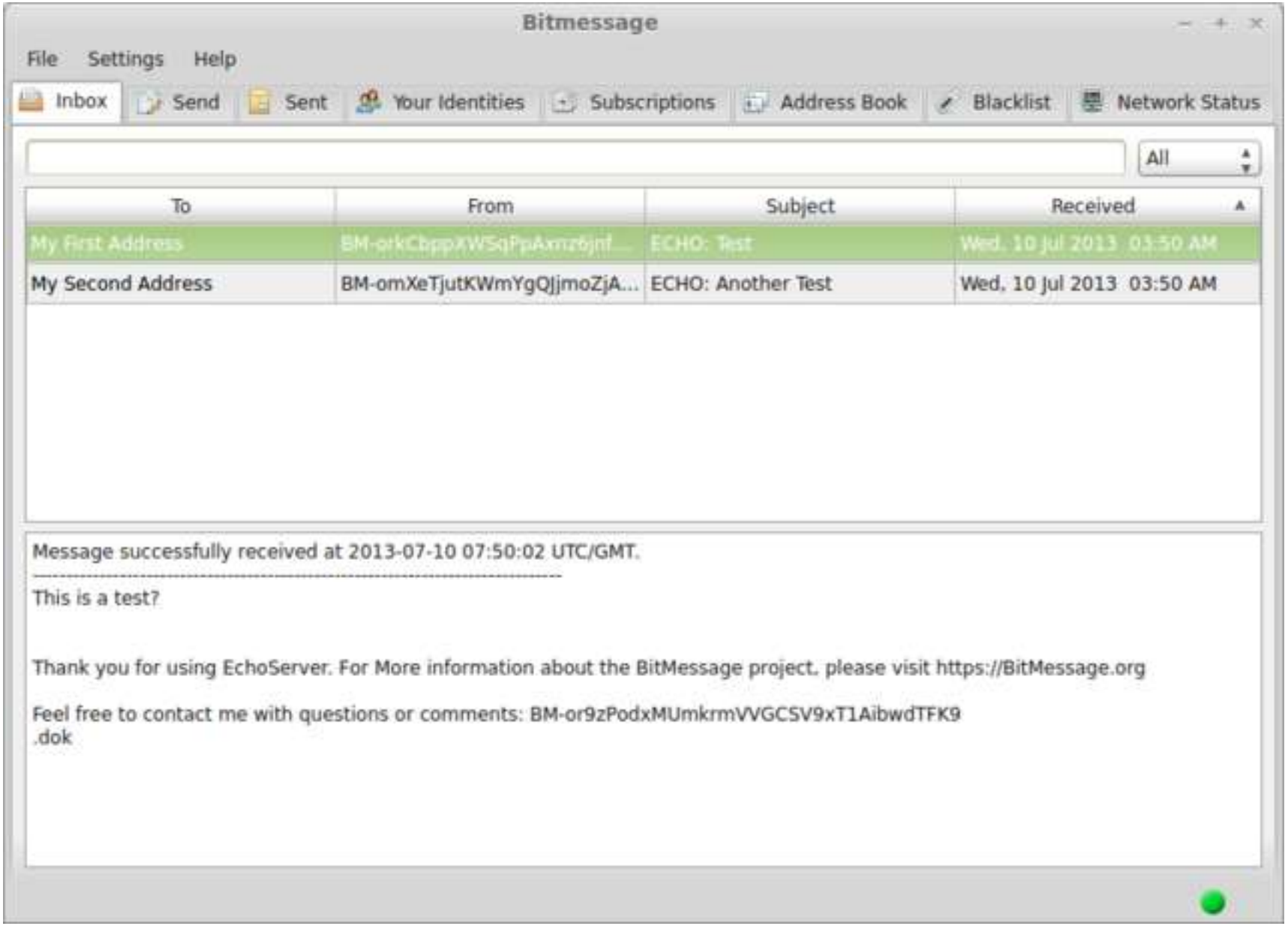
Usi alternativi

- Scambio messaggi
  - BitMessage
- Contratti complessi
  - Ethereum
- Firme digitali
- Marcature temporali
- Trasferimento diritti d'autore
  - MyPowers
- Cloud storage decentralizzato
  - Storj
- Identità digitale, autorizzazioni, autenticazioni, e-voting…

BitMessage

- È un sistema che permette di mandare e ricevere messaggi usando un protocollo peer-to-peer, decentralizzato, trustless, autenticato, cifrato.
- Gli utenti non devono scambiarsi alcun dato eccetto un indirizzo (di circa 36 caratteri) per garantire la sicurezza.
- Non è necessario avere concetti di chiavi pubbliche o private per usare il sistema.
- È progettato per mascherare dati a chi non è coinvolto nella comunicazione, che rimangono riservati a mittente e destinatario
- pyBitMessage

pyBitmessage



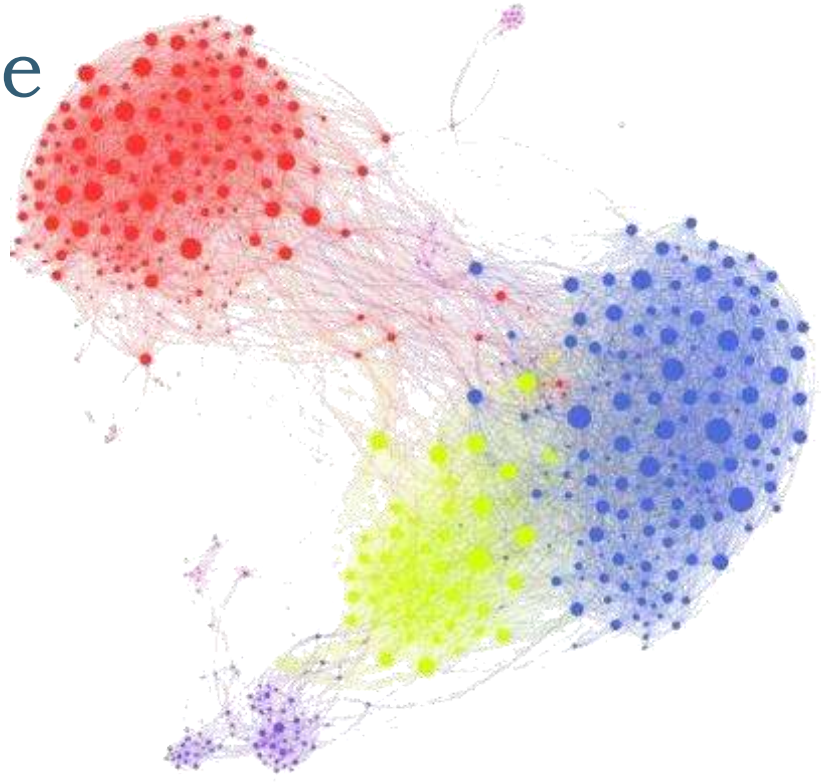
Indagini

Coinvolgimento in attività criminali

- Ransomware
- Dark market
  - Beni
    - Droga, armi, documenti falsi, refurtiva, pedoporno…
    - Carte di credito, account, leak…
  - Servizi
    - Furti di dati
    - DDoS ed estorsioni
    - Altre nefandezze
- Assasination market (solo teorizzato per ora)
  - Jim Bell 1995-96 essay

Entità

- Per entità si intende un insieme di indirizzi riconducibili allo stesso possessore.
- Miliardi di indirizzi diversi →
Migliaia di entità con più di 10 BTC
- Raggruppare indirizzi in entità
è il passaggio fondamentale
per il tracciamento



Deanonimizzazione

- Chi sta dietro le transazioni “anonime”?
- La storia delle transazioni (blockchain) è pubblica, gli indirizzi (assimilabili a IBAN o indirizzi email) sono pubblici e raggruppabili in entità.
- Le entità sono pseudonime, è utile associare l'entità alla persona/organizzazione:
  - Usando dati o eventi noti (es. indirizzi, importi, lasso temporale).
  - Da dispositivi informatici (es. sequestri).

Strumenti online

- blockexplorer.com, blockchain.info
- blockr.info, chain.so, walletexplorer.com, blockseer.com…
  - Browsing di blocchi e transazioni
  - Statistiche (prima comparsa di un indirizzo, saldo, ecc.)
  - Taint Analysis (stima della relazione tra due indirizzi)
- Skry.tech (ex Coinalytics.co)
  - Blockchain Explorer, Jarvis -> Skry Platform
  - Intelligence real-time, pattern recognition, modelli predittivi e altre buzz-feature ;-)

Blockchain explorer

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

1PyKgovs6GTt2mJey77WW8yXNmPRWhHCLY (0.01251105 BTC - Output) → Silkroad Seized Coins - (Unspent) 0.0001 BTC
17J8A5vVtigVCQc6ANPnQtj1a2tTTkdkbK - (Spent) 0.01240876 BTC
0.0001 BTC

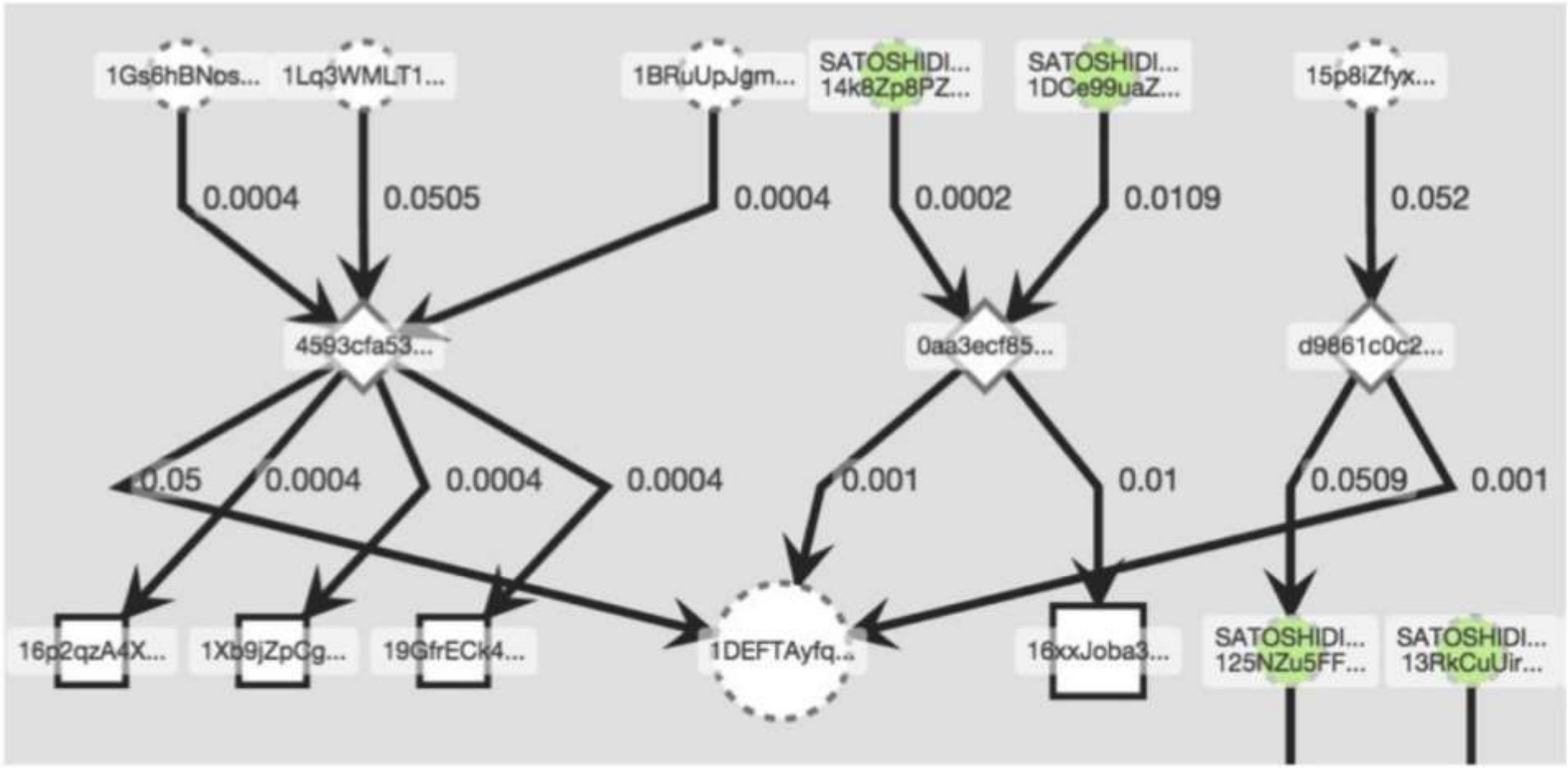
59bc0e344f18a7d1ac9f877bbccd4b8ed09b9e20a7e4ea71e491e8a8805d0fd6 — (Fee: 0.0001 BTC - Size: 372 bytes) 2015-03-09 20:57:52

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

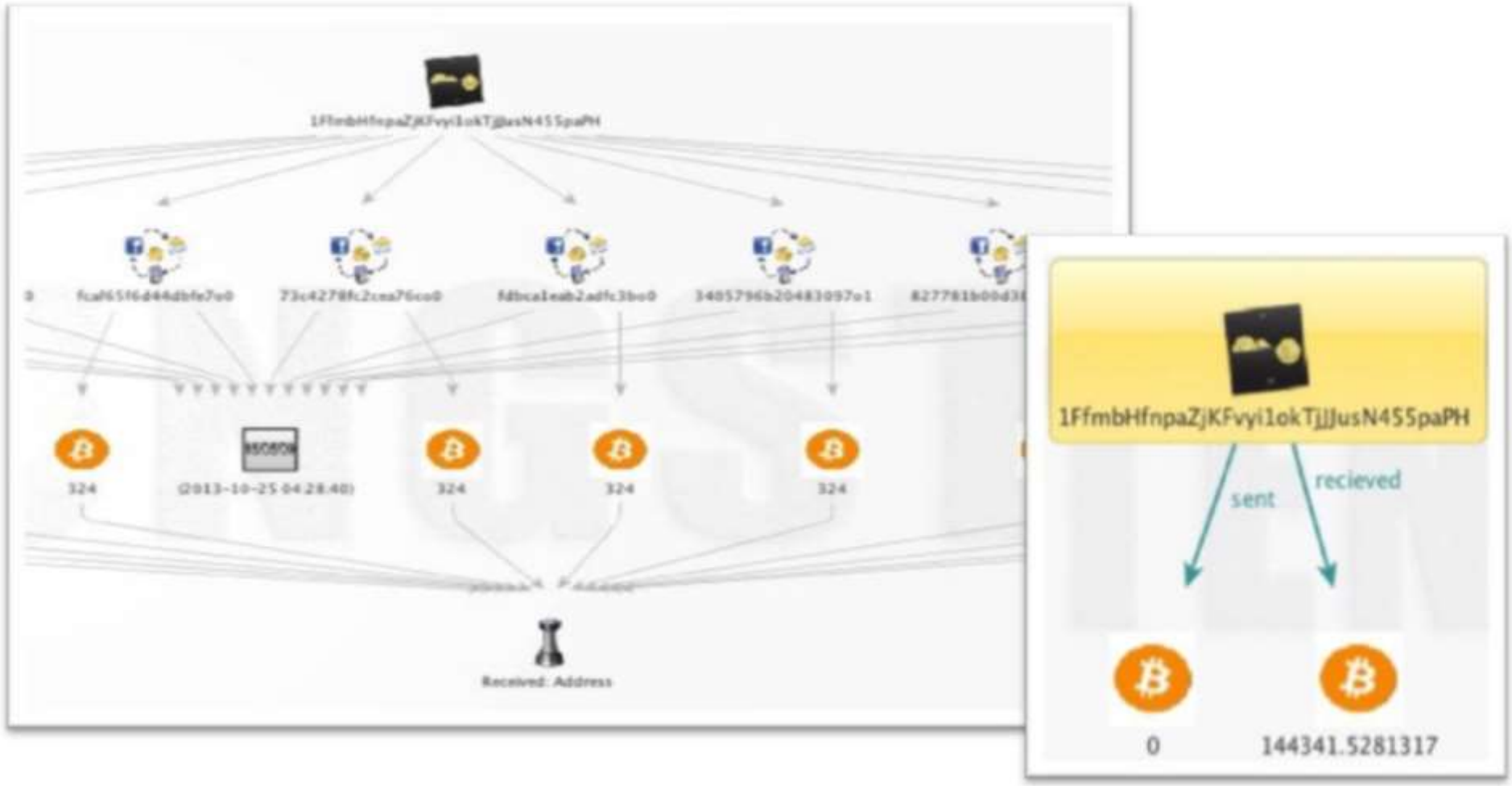
18K4aFHc4veNhoxmWZNobezpQHL57MSbFL (0.08221153 BTC - Output) → Silkroad Seized Coins - (Unspent) 0.03528706 BTC
1MPwVMHUxc5F4LY5u4S6vAXM58KvkPpMcB - (Spent) 0.04682447 BTC
0.03528706 BTC

blockseer.com



Maltego (online/offline)

- github.com/bostonlink/bitcoin-explorer



Strumenti offline

- Bitcoin Core
- Insight github.com/bitpay/insight-ui
- BTCpLex github.com/tsileo/btcplex
- Bitcoin-ABE github.com/bitcoin-abe/bitcoin-abe
- Statoshi jlopp.github.io/statoshi
- libbitcoin-explorer github.com/libbitcoin/libbitcoin-explorer
- Bitcoin-tools github.com/gavinandresen/bitcointools
- Bitcoin Sneak Peek (Chrome ext)
- **Bitiodine** (online e offline)

Analisi artefatti locali

- IEF
- Bulk extractor
- KeyHunter
- BTScan
- BTC recover
- Log del client (IP locale, transazioni…)
- Browser history (wallet online, paper wallet…)
- Bruteforce wallet
- RAM dump e analisi

Sequestro e confisca

Sequestro di denaro (P.G.)

- Come ci si comporta coi soldi?
  - Sequestro fisico
  - Deposito giudiziario
- E coi soldi stranieri?
- E coi soldi virtuali?

Come trattare le crittovalute?

- Sono denaro?
  - «Le valute virtuali non sono emesse da banche centrali o da autorità pubbliche, non costituiscono moneta legale né sono assimilabili alla moneta elettronica» (Banca d'Italia, 30 gennaio 2015)
- Sono dati e li trattiamo per tali?
- È un bene indifferenziato?

Aspetti giuridici da approfondire

- Manca normativa specifica in materia di criptovalute
- Alcuni stati hanno normato singoli aspetti marginali
  - in Spagna i casinò online in bitcoin sono soggetti alla legge sul gioco;
  - In Italia i trader non sono considerati cambiavalute e quindi non sono soggetti agli adempimenti antiriciclaggio
- Art. 648 bis c.p.: «fuori dai casi di concorso nel reato, chi sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto doloso, ovvero compie altre operazioni in relazione ad essi, in modo da ostacolare l'identificazione della loro provenienza delittuosa.»
- Oggetto materiale del reato comprende anche i beni immateriali riconducibili a un'essenza economico-finanziaria (fonte CoinLex - Studio Capaccioli).
- Le criptovalute sono in questo senso beni, o comunque "altre utilità", e hanno comunque "essenza economico-finanziaria".

Sequestro

1. Togliere il bene dalla disponibilità dell'indagato
2. Porlo a disposizione dell'Autorità Giudiziaria

- Inibire accesso al wallet (p.e. sequestrando il dispositivo fisico che lo memorizza) **non basta**
  - Non garantisce la disponibilità all'A.G.
  - Non garantisce che non esistano altre copie del wallet o delle chiavi segrete
    - Soprattutto se si consente copia alla difesa…
  - Ne consegue che cambiare la password di cifratura di un esemplare del wallet non assicura nulla.

Finalità del sequestro

- Probatorio
  - Acquisire potenziali fonti di prova
  - Ha più senso verso i wallet
  - Il resto lo fa la blockchain
- Preventivo
  - Impedisce la prosecuzione del reato
  - Impedisce di goderne i frutti
  - Ha più senso sui bitcoin
- Conservativo
  - Mantiene il bene disponibile nel tempo
  - Ha più senso sui bitcoin
  - Ha ancora più senso la conversione…

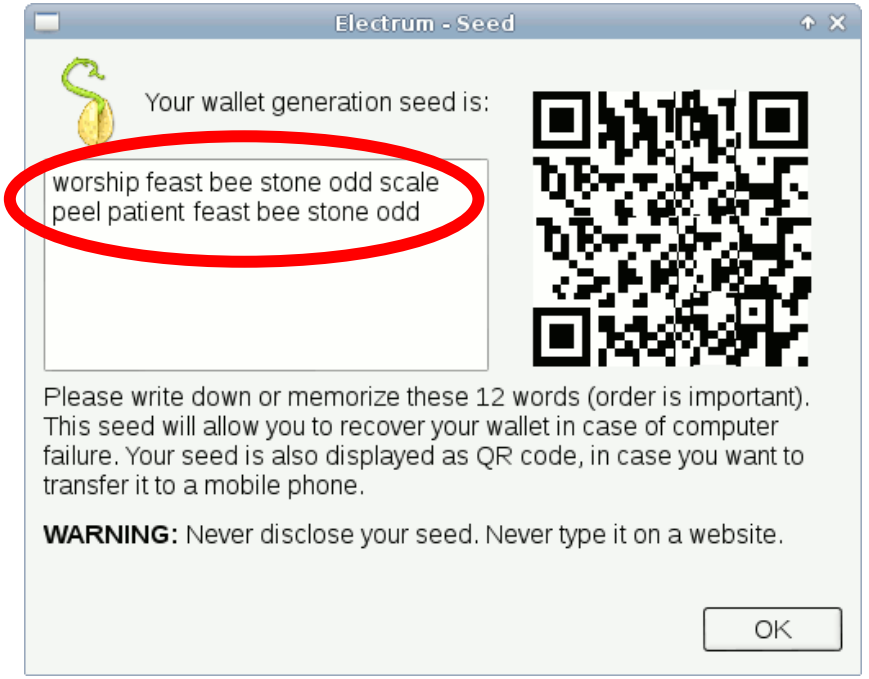
Tipi di wallet

- Locale
  - Smartphone, PC, hardware, cold storage…
  - Deterministico, Gerarchico (HD), Armory
  - Accesso via password o seed
- Remoto
  - Interfacce di accesso
  - Metodi di autenticazione
  - Opzioni di backup/export
- Multisig
  - Operando su un solo soggetto si ottiene il blocco dei Bitcoin (sempre se non esistono altre copie…), ma non se ne ottiene la disponibilità.

Accesso ai Bitcoin

Chi possiede i Bitcoin? Chi ne può disporre, ovvero chi ha le relative chiavi segrete

- Accesso al wallet
- Accesso a backup/esportazioni
- Conoscenza password/root key/seed
  - Collaborazione diretta
  - Via diplomatica
  - Spyware/keylogger
  - Brute force
  - Blitz
  - Memory dump?
  - Good old post-it ☺

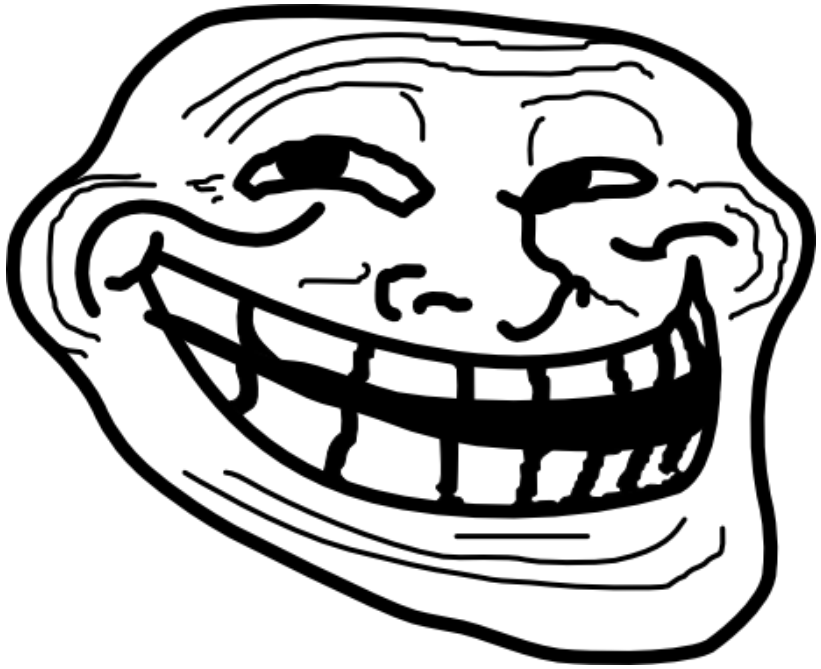


Social engineering

Se non puoi prenderteli, fatteli mandare ☺

Metodi alternativi

- Sequestro per equivalente
  - Applicazioni limitate a taluni reati, per lo più di natura tributaria
  - Misura residuale
  - Non a discrezione della P.G.
- Giudiziale custodia

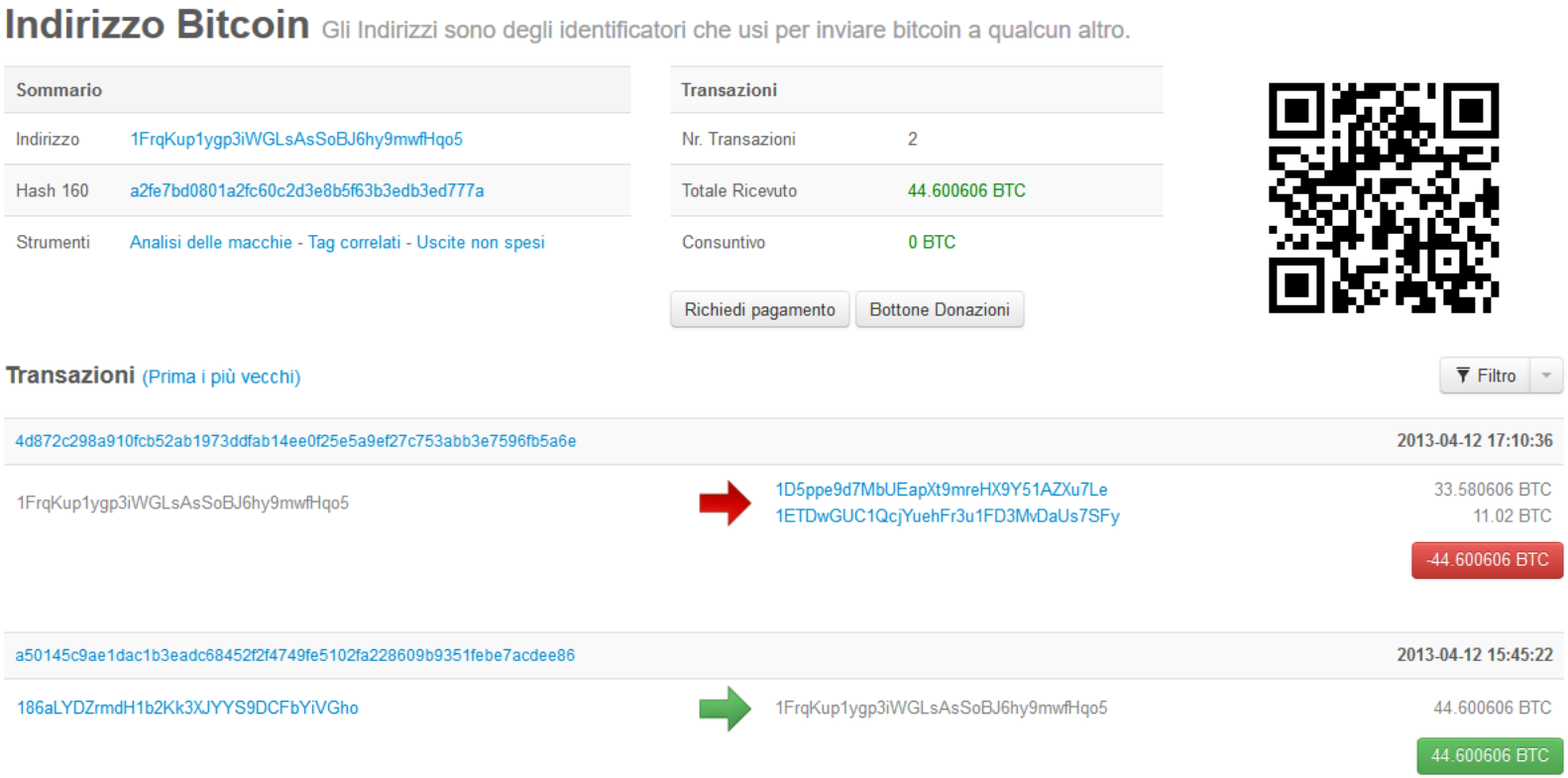


Confisca

- Confisca per equivalente (art. 240 c.p.)
- Conversione in valuta
- Asta giudiziaria
- Assegnazione alla P.G. per attività di contrasto
- Distruzione?

Il primo sequestro noto di Bitcoin

- 12 aprile 2013 ad opera della Drug Enforcement Administration (DEA)
- A carico di Eric Daniel Hughes
- 11.02 BTC ottenuti mediante attività undercover



Indirizzo Bitcoin Gli Indirizzi sono degli identificatori che usi per inviare bitcoin a qualcun altro.

Sommario	
Indirizzo	1FrqKup1ygp3iWGLsAsSoBJ6hy9mwfHqo5
Hash 160	a2fe7bd0801a2fc60c2d3e8b5f63b3edb3ed777a
Strumenti	Analisi delle macchie - Tag correlati - Uscite non spesi

Transazioni	
Nr. Transazioni	2
Totale Ricevuto	44.600606 BTC
Consuntivo	0 BTC

Richiedi pagamento | Bottone Donazioni

Transazioni (Prima i più vecchi) — Filtro

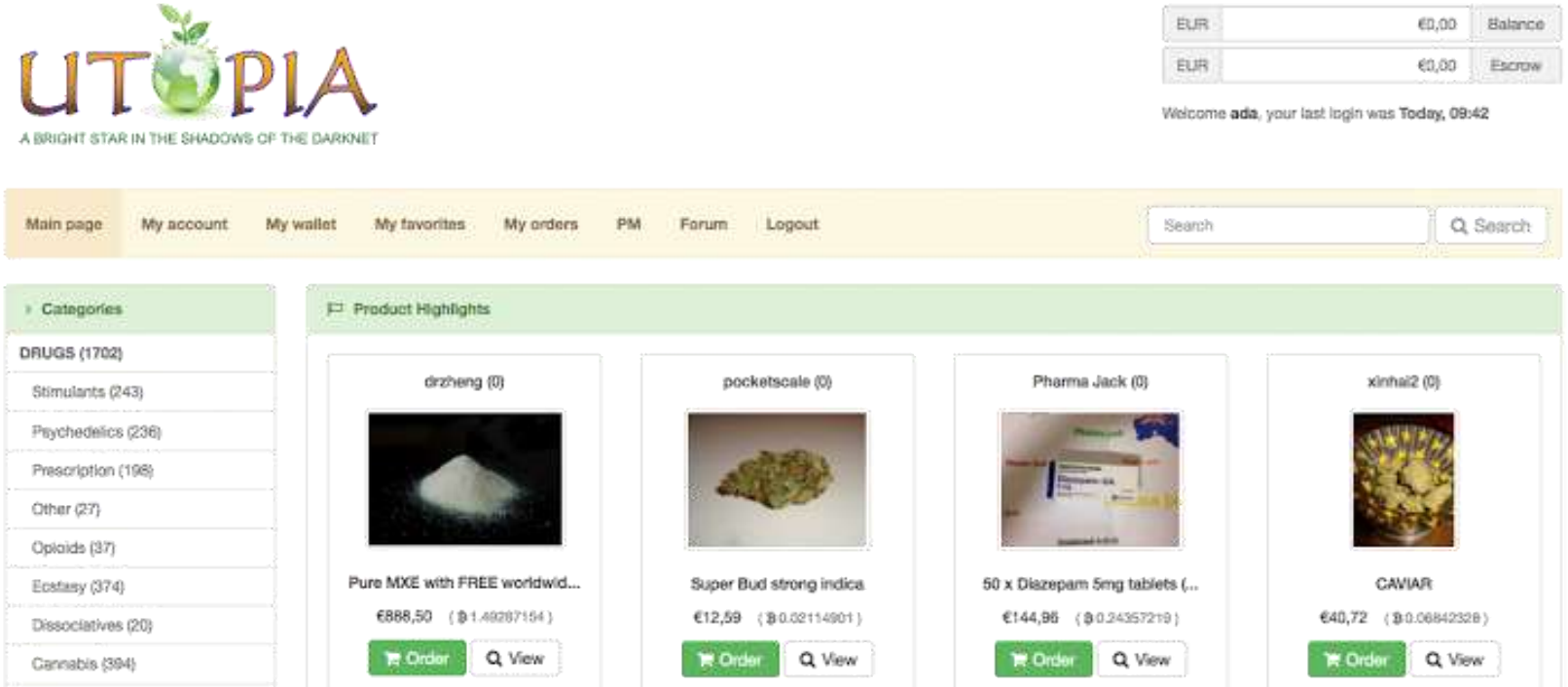
4d872c298a910fcb52ab1973ddfab14ee0f25e5a9ef27c753abb3e7596fb5a6e			2013-04-12 17:10:36
1FrqKup1ygp3iWGLsAsSoBJ6hy9mwfHqo5	→	1D5ppe9d7MbUEapXt9mreHX9Y51AZXu7Le 1ETDwGUC1QcjYuehFr3u1FD3MvDaUs7SFy	33.580606 BTC 11.02 BTC
			-44.600606 BTC
a50145c9ae1dac1b3eadc68452f2f4749fe5102fa228609b9351febe7acdee86			2013-04-12 15:45:22
186aLYDZrmdH1b2Kk3XJYYS9DCFbYiVGho	→	1FrqKup1ygp3iWGLsAsSoBJ6hy9mwfHqo5	44.600606 BTC
			44.600606 BTC

Silk Road

- 2 ottobre 2013, sempre DEA
- A carico di Ross William Ulbricht
- Accesso ai Bitcoin ottenuto mediante blitz alla Glen Park library
- Sequestrati e in seguito confiscati 144.000 BTC
- Disposta asta giudiziaria in diverse tranche

Operazione Commodore

- 11 febbraio 2014, da parte della polizia olandese
- A carico di 5 persone accusate di gestire il dark market Utopia (in 9 giorni, 13.000 item in vendita)
- Attività sotto copertura
- Sequestrati 900 BTC durante le perquisizioni domiciliari



Operazione Babylon

- 31 luglio 2015 dal Servizio Polizia Postale
- A carico di «un 41enne campano»
- Attività sotto copertura
- *Sequestro* di 14.000 wallet degli utenti
- Sequestro dei Bitcoin dell'indagato durante la perquisizione domiciliare

Consigli operativi

- I Bitcoin **vanno trasferiti**, è l'unico modo certo
  - Creazione di un indirizzo in ricezione
  - Disposizione di pagamento
  - Verbalizzazione delle operazioni
  - Catena di custodia rafforzata dalla blockchain
- Ma non basta: come assicurare la disponibilità esclusiva all'Autorità Giudiziaria?
  - Trasferimento su cold storage
  - Distruzione sicura delle chiavi digitali
  - Trattazione del reperto fisico come da procedura penale
  - Trasferimento del wallet cifrato su supporto digitale durevole
  - Deposito separato di wallet e password
  - Distruzione sicura di ogni altra copia (generazione mediante live CD?)

Credits

Vi hanno intrattenuto

Davide Rebus Gabrini
Franco hostfat Cimatti

grazie agli importanti e consistenti contributi di
Paolo Dal Checco
Raffaele Marco Concas
Matteo e Pietro Brunati

facebook.com/gabrini  facebook.com/franco.cimatti

twitter.com/therebus  twitter.com/hostfat

it.linkedin.com/in/rebus  it.linkedin.com/in/hostfat

Queste e altre cazzate su **http://www.tipiloschi.net**