ISACA®

Sistemi informativi: averne fiducia e trarne valore

Rome Chapter

Bitcoin: stato dell'arte, opportunità e rischi della criptomoneta

Dr. Paolo DAL CHECCO

Roma 26/04/2016

Agenda

- Presentazione relatore
- Il protocollo Bitcoin e la blockchain
- Anonimato, mixer, exchange e cash out
- Sicurezza e rischi del protocollo
- Bitcoin Forensics e indagini sulle criptomonete
- Le evoluzioni del sistema: Smart Contract e Public Notary
- Il futuro del Bitcoin
- Q&A
- Bibliografia & sitografia

Presentazione relatore

- **PhD in Informatica** @unito, gruppo Computer & Network Security
- **Professore a Contratto** di Sicurezza Informatica @unito/suiss
- **Consulente Informatico Forense** per Procure, Tribunali, Avvocati, Aziende e privati
- Co-titolare, insieme a Giuseppe Dezzani, dello Studio "**Digital Forensics Bureau**"
- Socio e membro del direttivo **IISFA**, socio **CLUSIT**, **Tech and Law**
- DEFT Developer tra i fondatori della **DEFT Association**
- Socio e tra i fondatori dell'**Osservatorio Nazionale d'Informatica Forense (ONIF)**
- Network, mobile, computer, cryptocurrency, audio, video forensics

Agenda

- Presentazione relatore
- Il protocollo Bitcoin e la blockchain
- Anonimato, mixer, exchange e cash out
- Sicurezza e rischi del protocollo
- Bitcoin Forensics e indagini sulle criptomonete
- Le evoluzioni del sistema: Smart Contract e Public Notary
- Il futuro del Bitcoin
- Q&A
- Bibliografia & sitografia

Le monete elettroniche

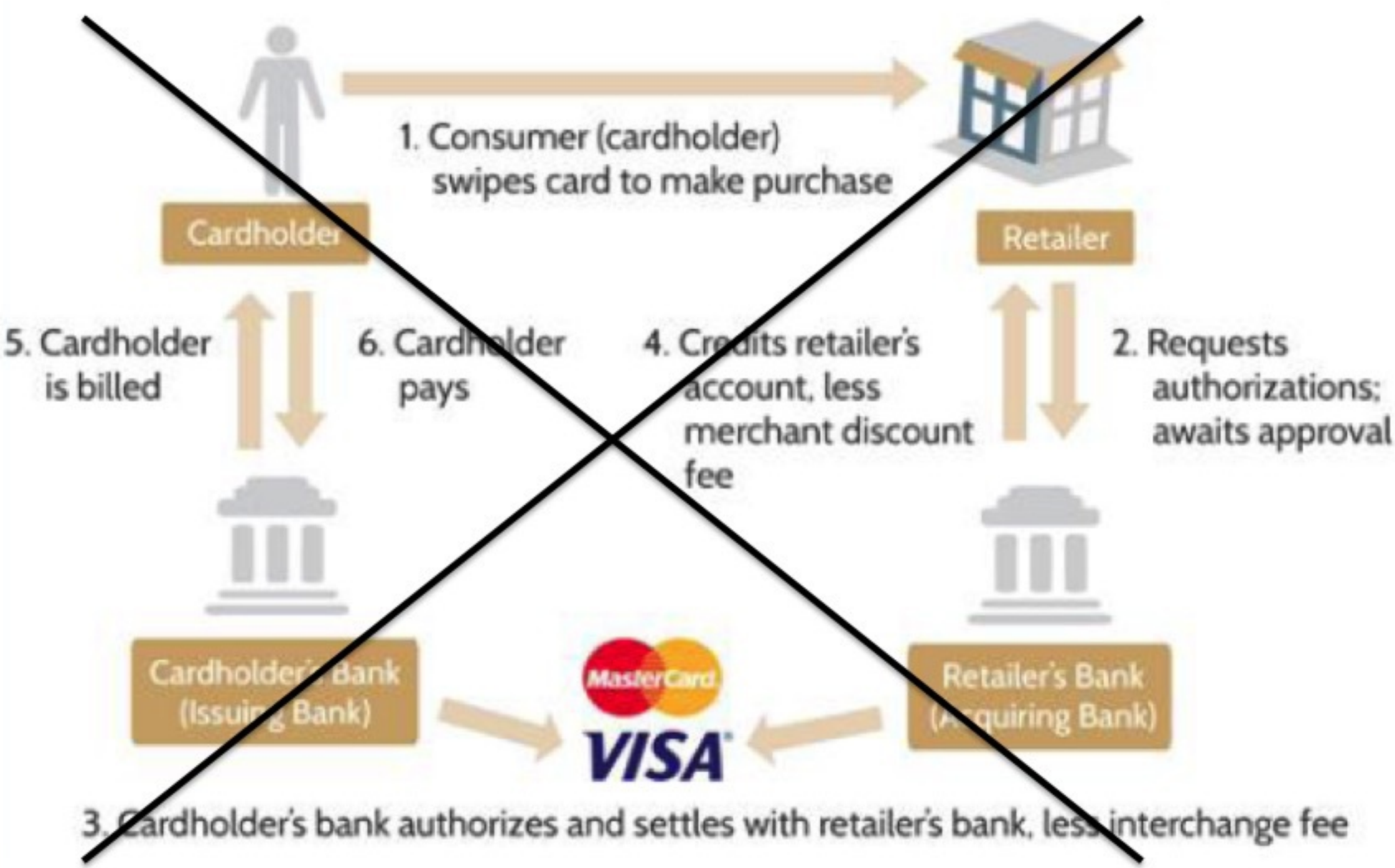
66 Coin, Asiacoin, Aidbit, Ascentcoin, BigBangCoin, Boolberry, BlackCoin, BellaCoin, BlueCoin, Blazecoin, Bitmoney, Dobbscoin, Borgcoin, GlobalBoost, GlobalBoost-Y, **Bitcoin**, BitLitS, Bunnycoin, CaiShen, Cannabiscoin, Bottlecaps, CAPTcoin, Cannacoin, Cloak, Compasscoin, Compucoin, CrackCoin, CoinShield, Cummingtonite, Dogecoin, DOGEBLACK, DogeCoinDark, Darkpeer, Darkcoin, DarkShibe, EmerCoin, FractalCoin, GlowCoin, Gnosis, Groupcoin, GunCoin, Hyperstake, Iconicx, Imperialcoin, IOcoin, Imperialcoin, Isracoin, Koolio, Kryptonite, KryptKoin, LATIUM, Electronic LIRA, Litecoin, Litecoindark, Latinum, Librexcoin, MiracleCoin, MozzShare, NeosCurrency, PureCoin, Quatloocoin, Rubycoin, RipoffCoin, RobotSexNickels, Shadowcoin, Shinycoin, Shibe, Sleakcoin, PotatoCoin, Squallcoin, Viacoin, VirtualminingCoin, Whistlecoin, GoldReserve, Monero, Stealthcoin, Servx coin, Guldencoin, Opalcoin, Old Shibe, Potcoin, Peoples, …

Oltre 500 criptovalute

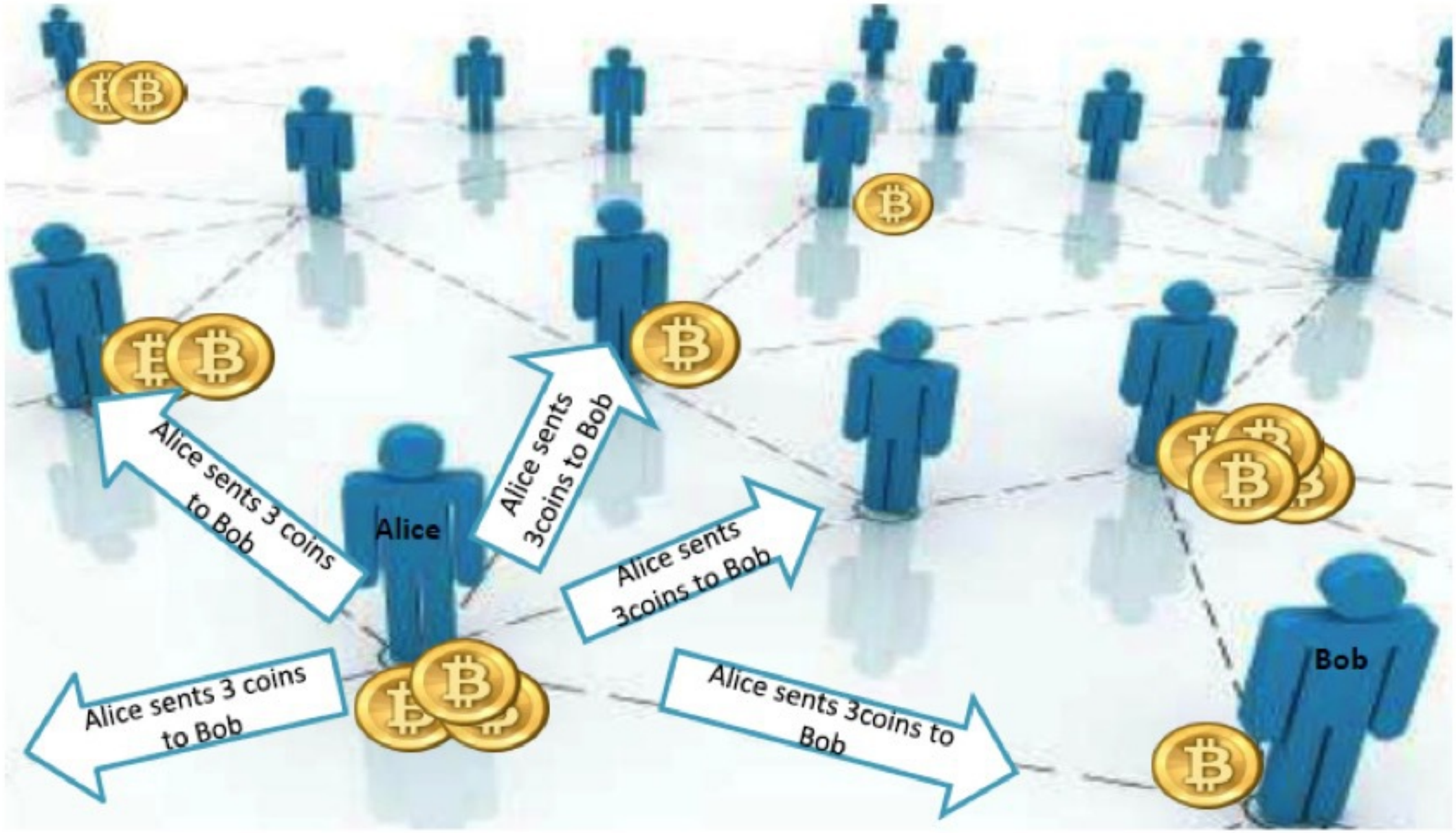
Cosa è il Bitcoin

- ‘B’ maiuscola, il protocollo, ‘b’ minuscola, l’unità di valuta
- Rete di pagamento digitale ideata nel 2009 da un anonimo “Satoshi Nakamoto”, basata sulla sulla crittografia (“crittovaluta”) e **open source**
  - Algoritmo di firma digitale asimmetrica **ECDSA**
  - Algoritmi di hashing **SHA256** e **RIPEMD 160**
- Peer to peer, nessun ente centralizzato
- Controvalore in valuta fiat stabilito dal mercato
- https://en.bitcoin.it/wiki/FAQ

Il “vecchio” sistema bancario



Assenza di autorità centrale



Terminologia: Chiave Privata Bitcoin

- Numero intero di 256 bit, **deve** essere casaule
- E' il codice da cui viene generata la chiave pubblica e quindi l'indirizzo Bitcoin
- Più facilmente archiviabile in formato WIF (Wallet Import Format)
- Posso dimostrare di averla firmando un messaggio
- E' uno dei punti più delicati di tutto il sistema, una chiave generata male (cattivo RNG) è vulnerabile e lo vedremo

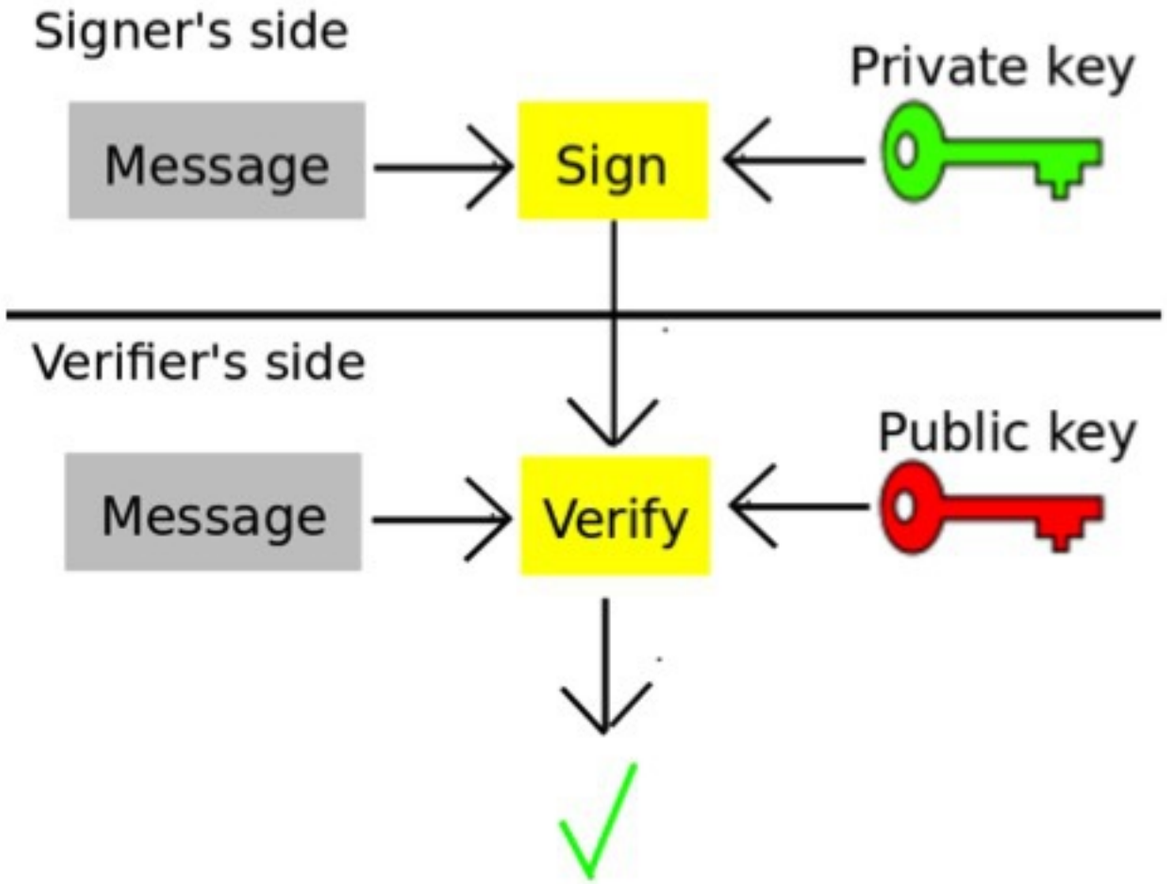
Private Key (Wallet Import Format)

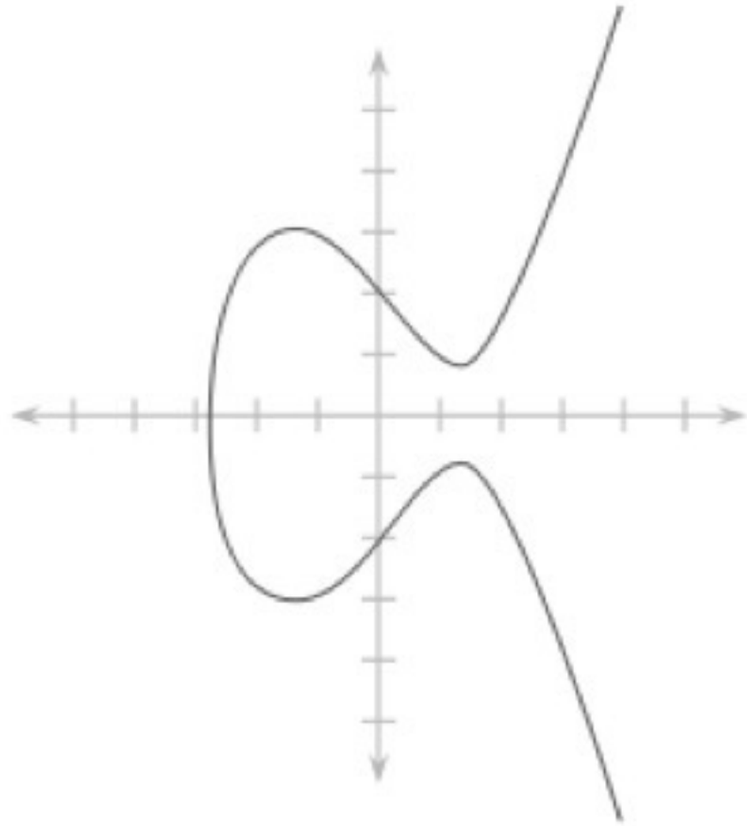
SECRET

`5KkrPXWACDU6JnRi6kuEokPr1rEFAF6pJdLQzExxSFwD5oicaVP`

Terminologia: Chiave Pubblica Bitcoin

- 512 bit, derivata dalla chiave privata tramite algoritmo a chiave pubblica/ privata ECDSA a Curve Ellittiche (secp256k1)
- con essa posso verificare un messaggio firmato con chiave privata
- È pubblica ma non compare nella blockchain fino a quando non l'indirizzo corrispondente non viene usato per trasferire bitcoin

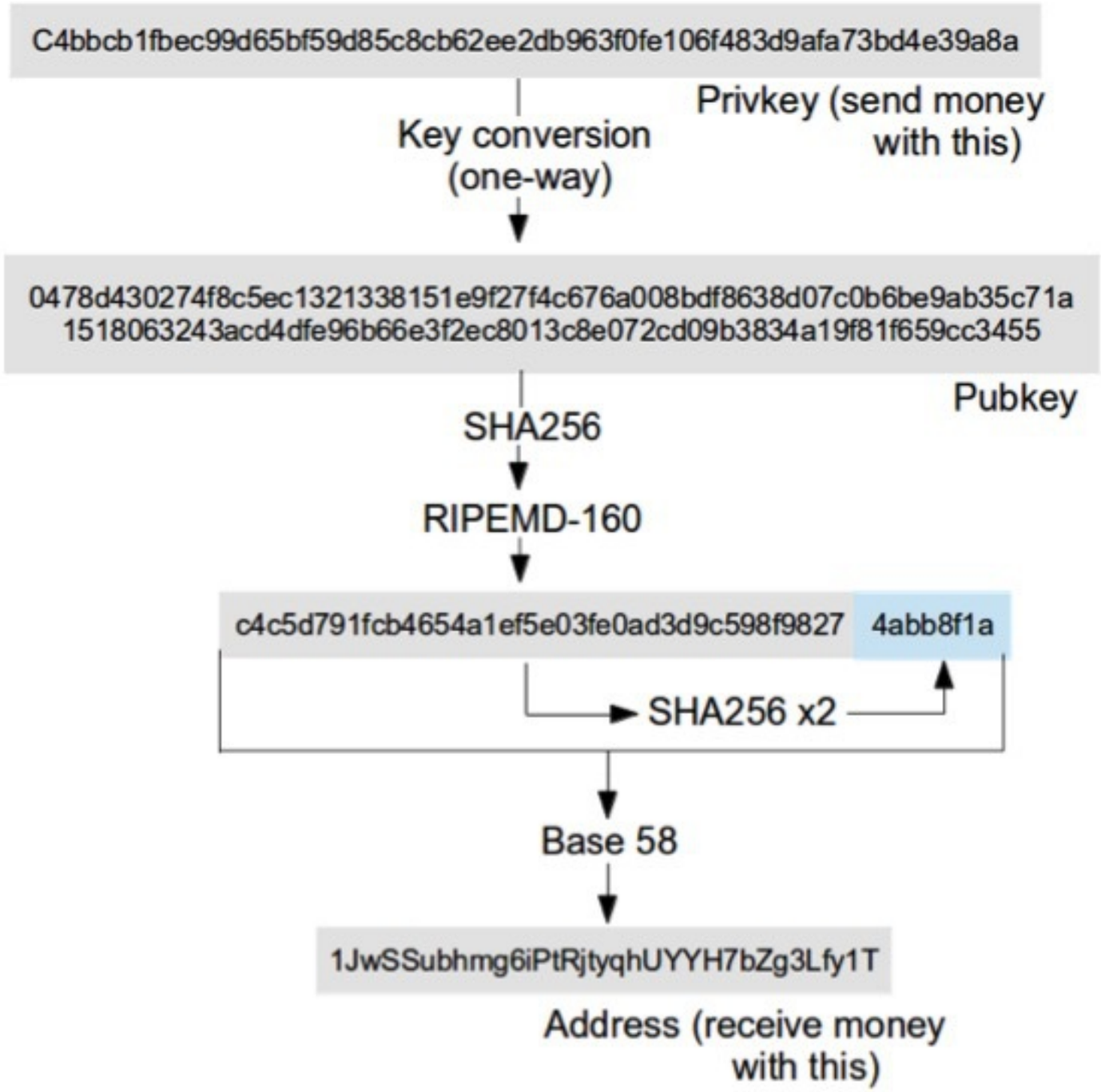




Terminologia: Indirizzi Bitcoin

- La chiave pubblica corrisponde a un indirizzo Bitcoin ma non viene usata per identificarlo
- Si usa un derivato da essa
- 160 bit, derivati da chiave pubblica mediante alcune operazioni che includono SHA256, RIPEMD-160 e Base58
- Risultato: 27-34 caratteri alfanumerici eccetto alcuni
- L'utilizzo dell'indirizzo (hash della chiave pubblica) invece della chiave pubblica riduce lo spazio d'attacco (2^{160} invece di 2^{256}) ma nel contempo previene eventuali problemi derivazione chiave pubblica → chiave privata

Da chiave privata a indirizzo Bitcoin



Un po’ di numeri…

address.hex:00b311d5766f9623408747554bcdec1d8dc05eeaf0

address.base58:13VhJywL2p5upGoXpU3RvECR7Heoq

address.base58check:1HKqKTMpBTZZ8H5zcqYEWYBaaWELrDEXeE

public-key-ripemd160.hex:b311d5766f9623408747554bcdec1d8dc05eeaf0

public-key-ripemd160.base58:3VhJywL2p5upGoXpU3RvECR7Heoq

public-key-ripemd160.base58check:HKqKTMpBTZZ8H5zcqYEWYBaaWELuen1WX

public-key-sha256.hex:c8d47a3b796bce36d80dd2e8622ce1bcc4eab1f4a78e8cd3e12b7db44d1c428a

public-key-sha256.base58:EWxTRzHpLN7GjXx6nwqDWJ6DSmrNTVYroZ2VdC7fg8Gq

public-key-sha256.base58check:2XSw67i599jF6FWxAApzSy2xBec9HrNCT7ZqWUo5dFhkqoDeQ3

public-key.hex:
045f81956d5826bad7d30daed2b5c8c98e72046c1ec8323da336445476183fb7ca54ba511b8b782bc5085962412e8b9879496e3b60bebee7c36987d1d5848b9a50

public-key.base58:PPBn9d92VkgAZeSLkWyyRSzZusyAaR79PQEjVGX2UoXqHxmgEmr1BvJBYtXXux6TrytQ7FtYqAV2h7TxuMN1sxH5

public-key.base58check:
3XTsV9raUUfajGdt6HibXREKMHXkZBQY6BLs9NSVGfE63GRFzKeBYQzCRVQzkkAQhnDkry1S6DdSXpmshbGuL73oiRr6Rs

private-key-wif.hex:809f86d081884c7d659a2feaa0c55ad015a3bf4f1b2b0b822cd15d6c15b0f00a08

private-key-wif.base58:fD8GVhUgAUmnrJPuyfqkUMDCk3RueN9bTskWv8nEsDWYF

private-key-wif.base58check:5K2YUVmWfxbmvsNxCsfvArXdGXm7d5DC9pn4yD75k2UaSYgkXTh

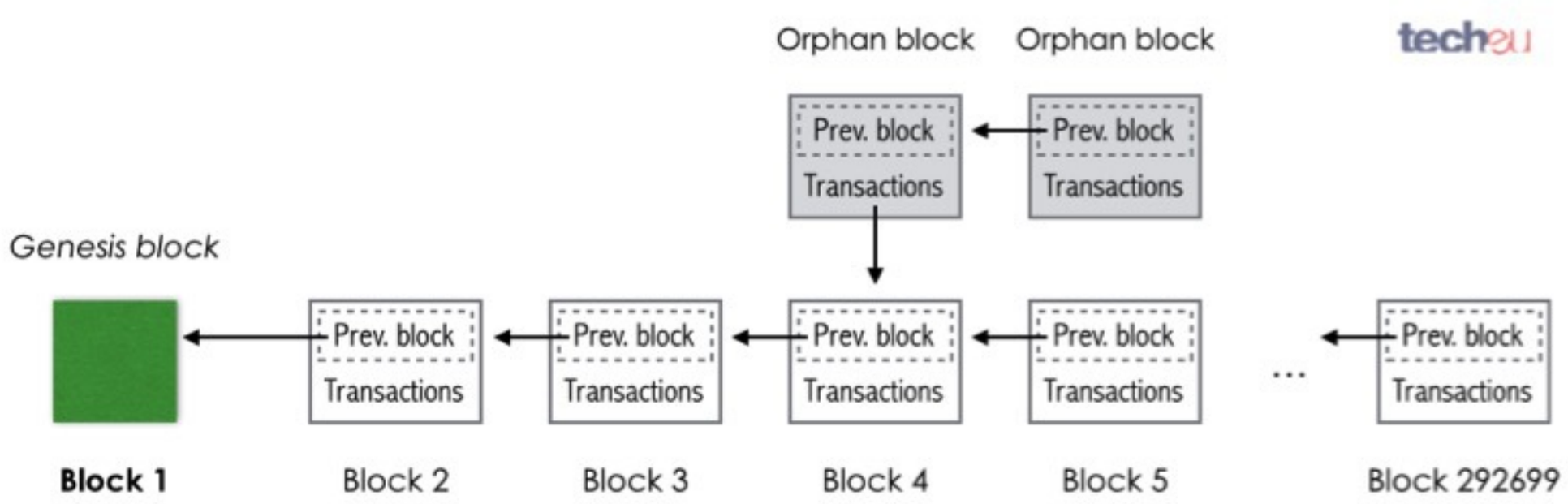
private-key.hex:9f86d081884c7d659a2feaa0c55ad015a3bf4f1b2b0b822cd15d6c15b0f00a08

private-key.base58: Bjj4AWTNrjQVHqgWbP2XaxXz4DYH1WZMyERHxsad7b2w

private-key.base58check:2DFtpKRbW2nfrzgAgE25onW3vwCQwM7S1iHk34LW9cwH1kzmHp

Terminologia: blockchain

- Il libro mastro delle transazioni, pubblico, condiviso, decentralizzato, viene composto autonomamente in base al concetto di “proof of work”
- Oltre 60 GB ad oggi, i client locali devono scaricarla tutta
- Scaricabile dalla rete peer attivando ad esempio il client Bitcoin-QT



Terminologia: wallet Bitcoin

- Il portafoglio che raccoglie i diversi indirizzi/address bitcoin, più facile da gestire rispetto a lavorare direttamente con gli indirizzi
- I wallet gestiscono in automatico chiavi private, indirizzi, change address, transazini con input multpli, sicurezza

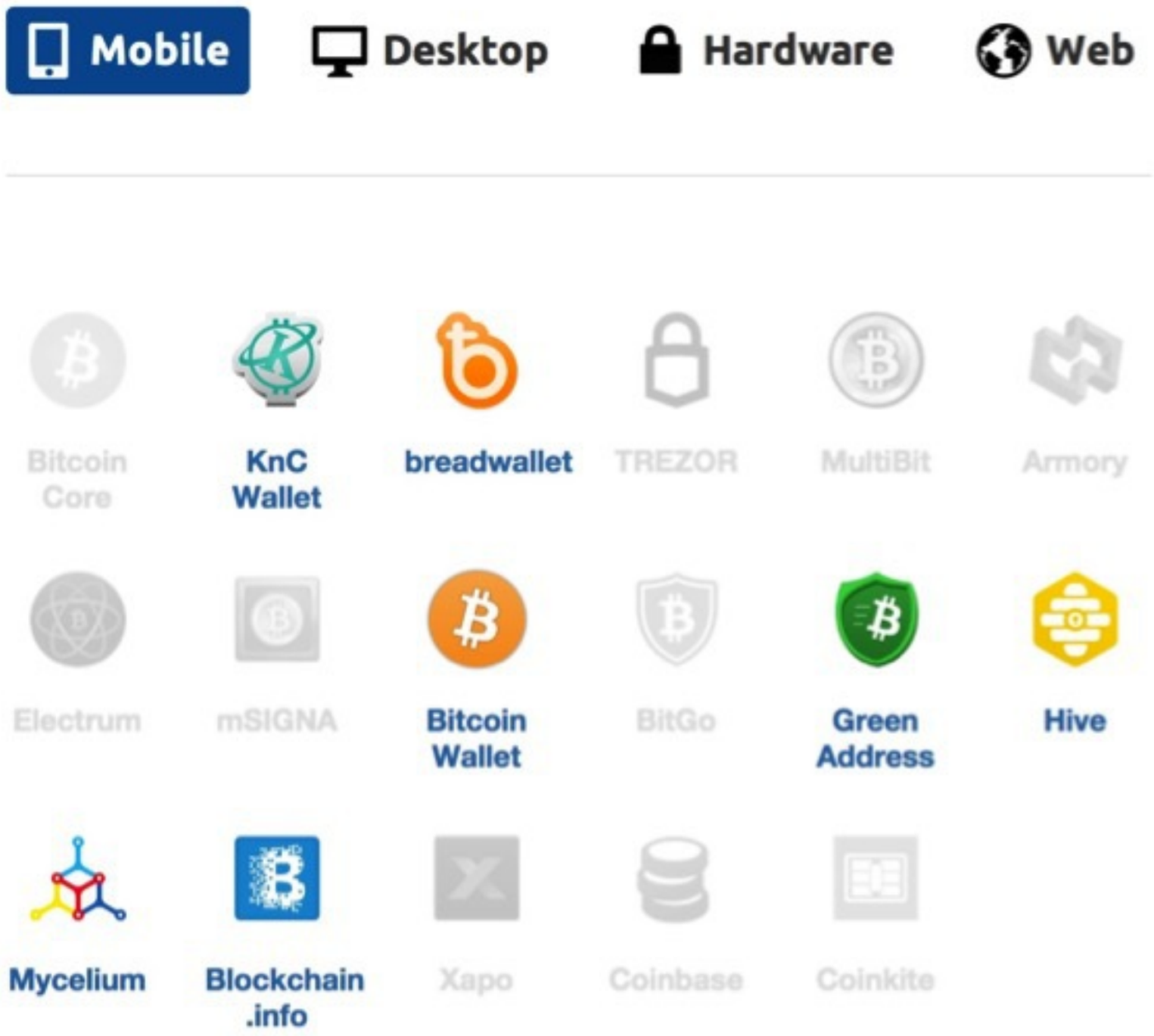
Terminologia: wallet deterministici

- Possibilità di derivare le nuove chiavi da un solo punto di partenza o seme ("seed") così da evitare l'archiviazione nel wallet delle chiavi private generate casualmente e permettere un **backup** più agevole
- Così agevole che con il sistema di memorizzazione "**mnemonic**" il wallet può essere tenuto "a memoria"

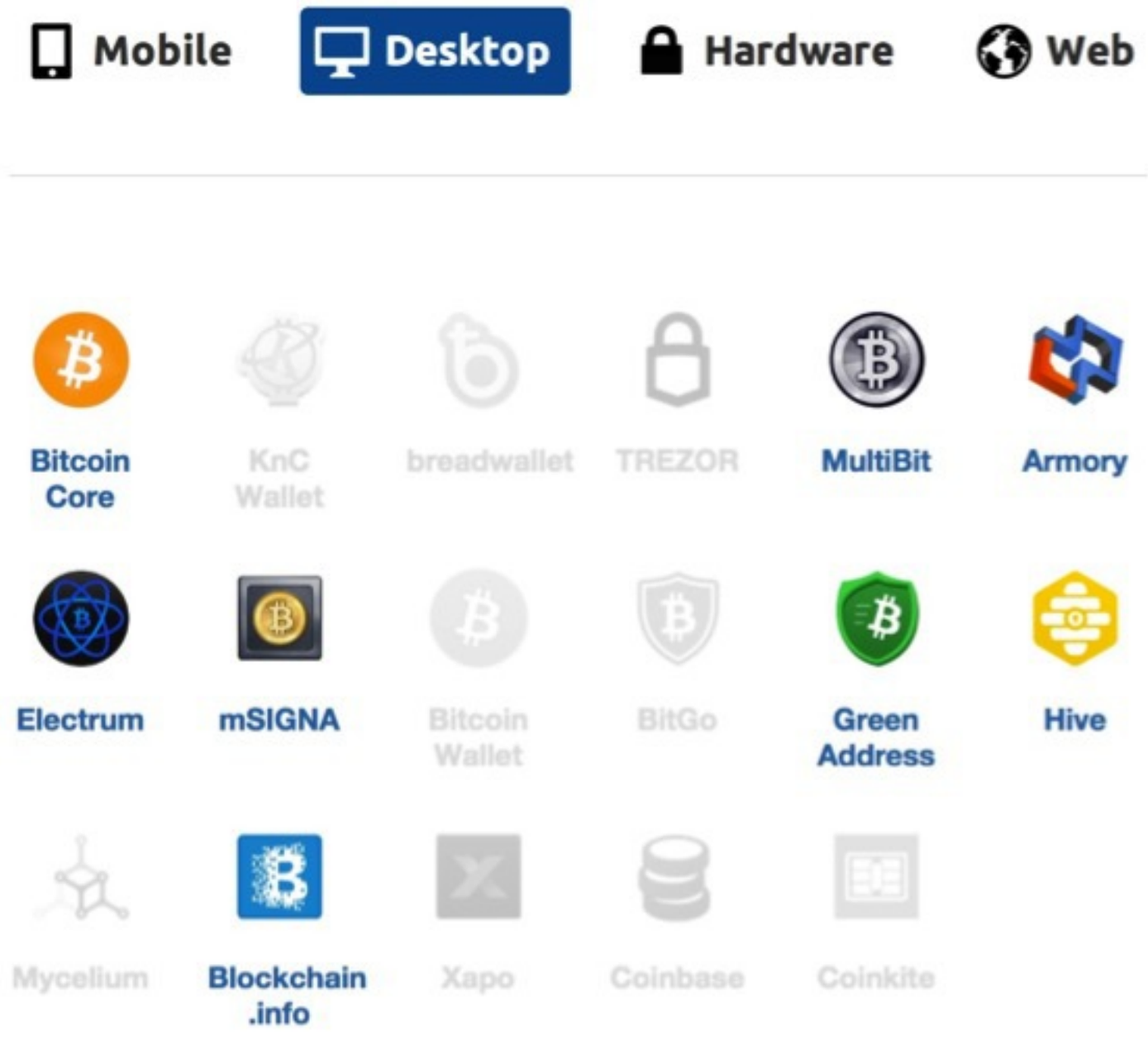
- Type1: deterministico
  - Caso più semplice, si parte da una stringa e si procede in modo lineare
  - Es: SHA256("stringa" + n)

- Type2: gerarchico deterministico
  - Standard BIP 0032
  - La generazione avviene ad albero, con rami e sotto rami, con la possibilità di utilizzare i rami in contesti diversi (pagamenti, ricezione fondi, etc…)
  - Anche le chiavi pubbliche possono essere generate in modo deterministico indipendentemente dalla conoscenza di quelle private

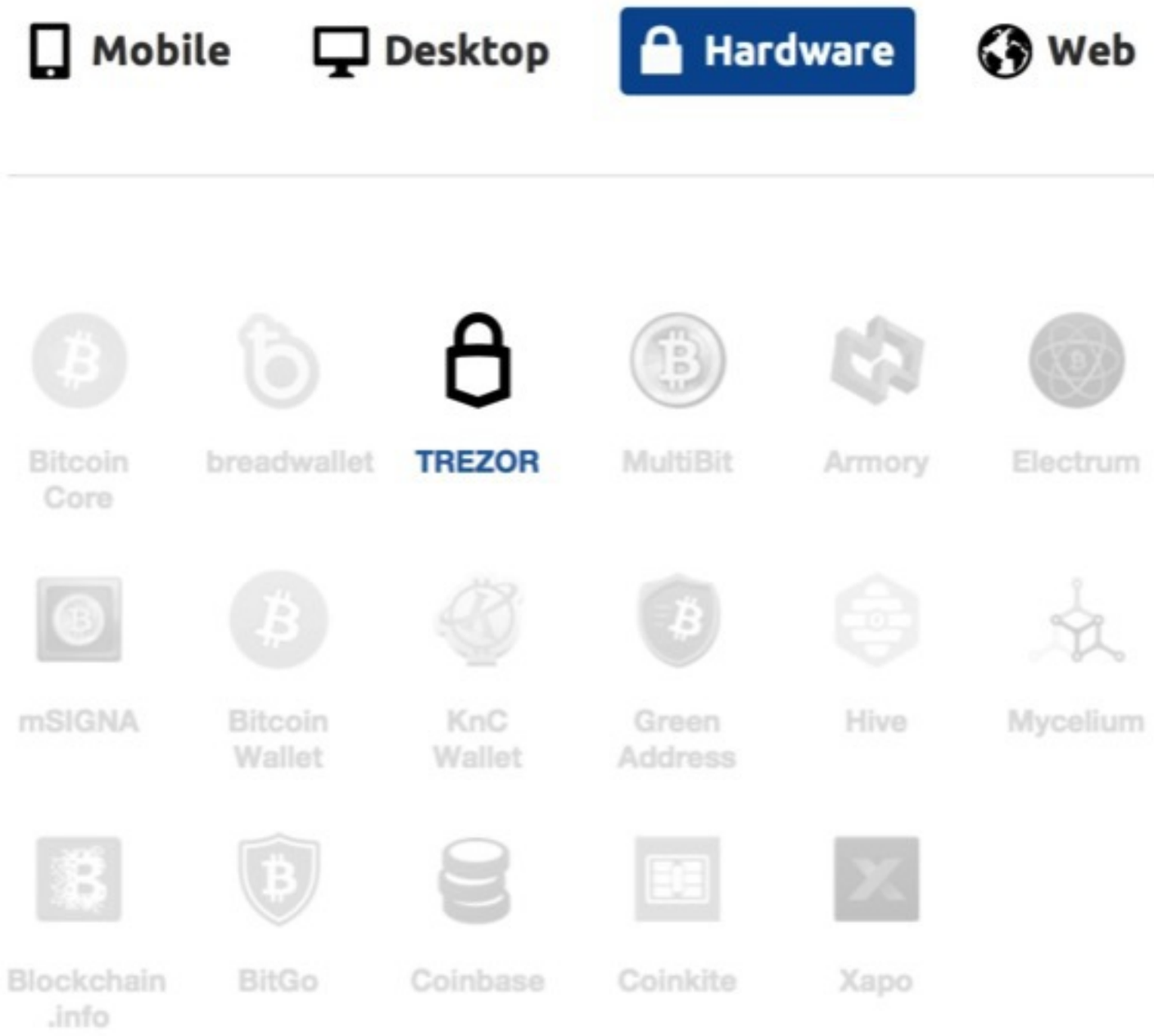
Tipi di wallet



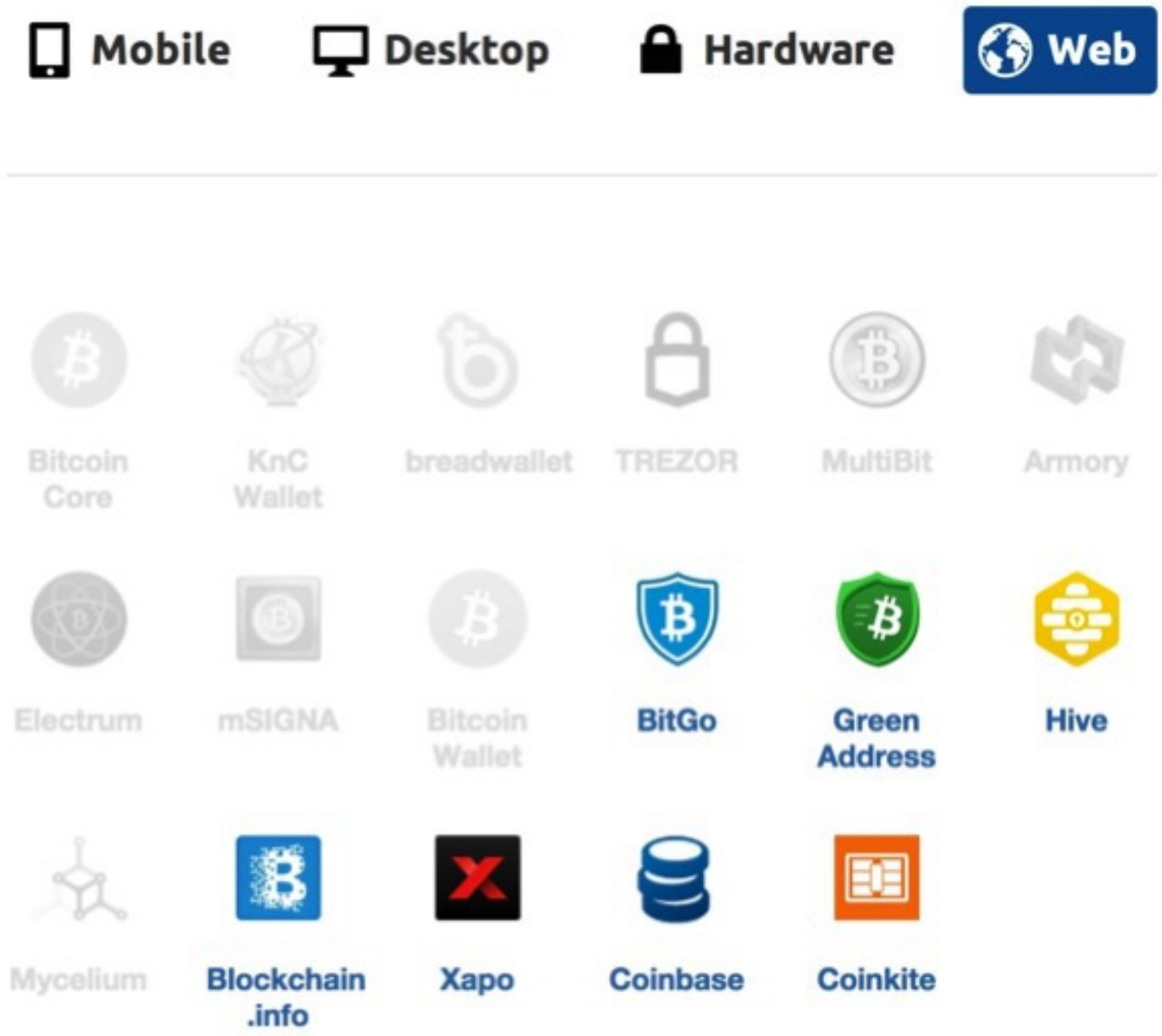
Tipi di wallet



Tipi di wallet



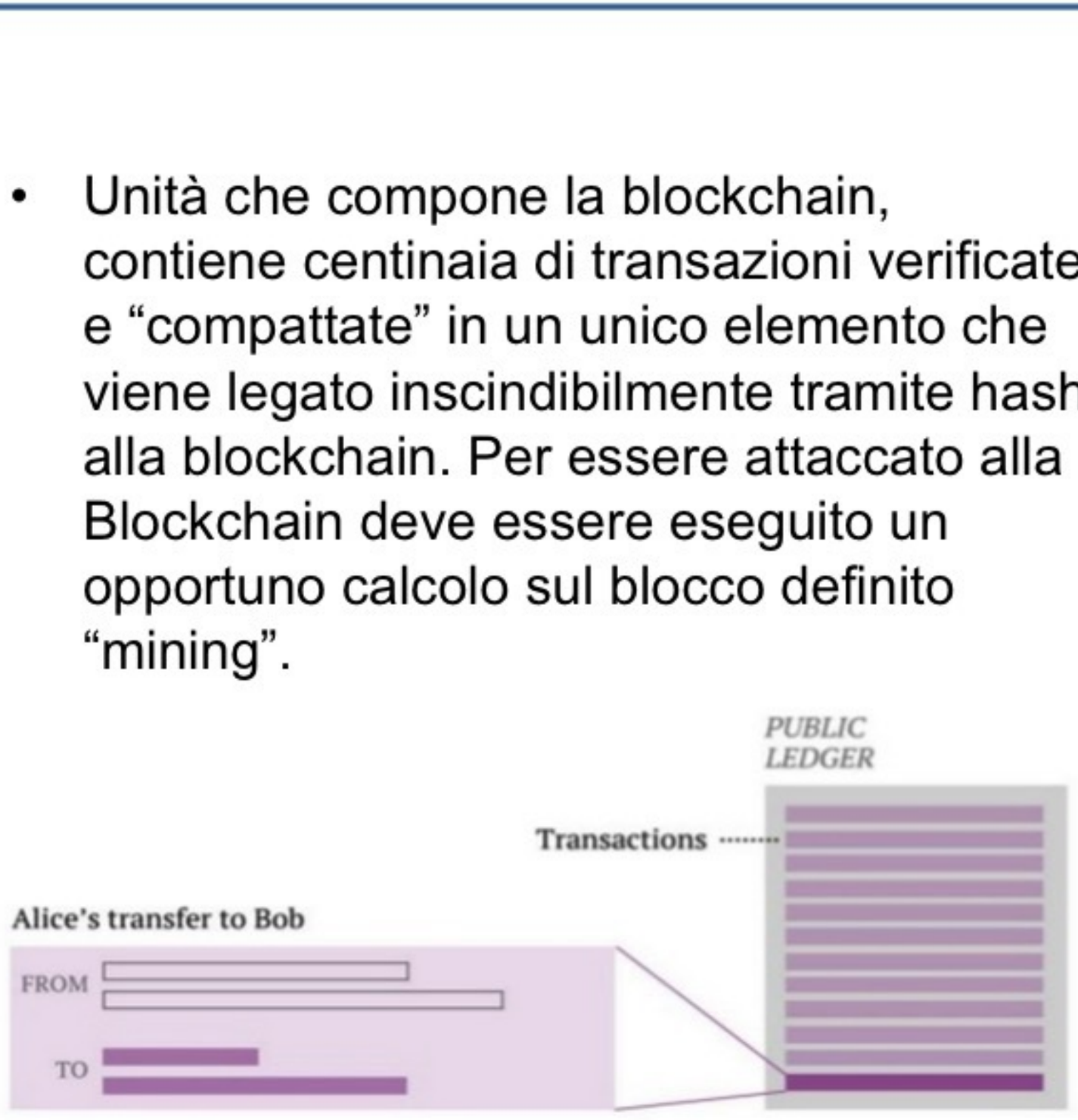
Tipi di wallet

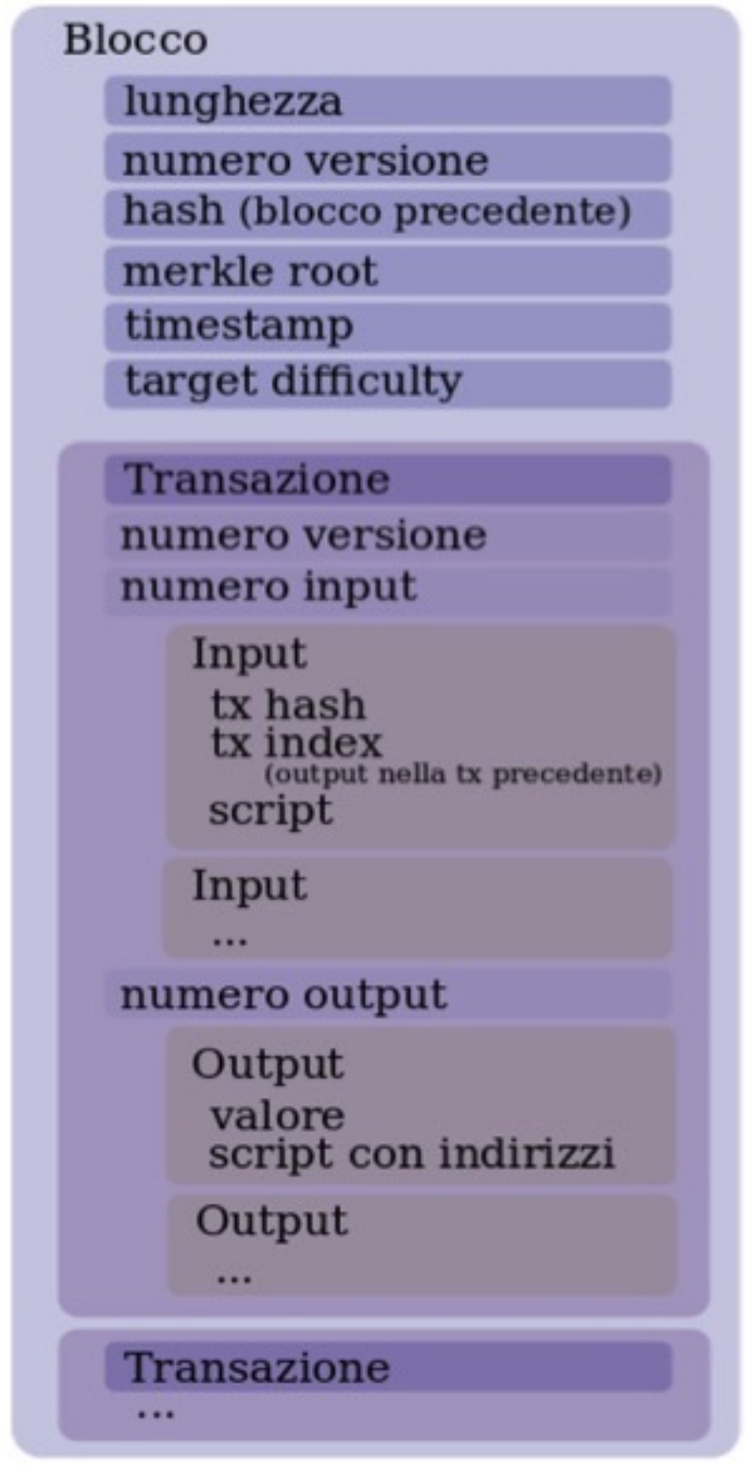


Tipi di wallet

Terminologia: blocco della blockchain

- 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: i bitcoin

- I bitcoin non esistono ;-)
- Possono esisterne (ma non esistono) al massimo 21 MLN (20,999,999.9769), e avverrà nel 2140
- Ciò che rende “tangibile” i bitcoin sono le transazioni che li contengono
- I bitcoin vengono generati durante il mining, un numero che viene dimezzato ogni 4 anni circa (210.000 blocchi), partendo da 50 BTC per blocco a partire dal 3 gennaio 2009

Terminologia: transazioni bitcoin

- passaggio irreversibile di una certa quantità di bitcoin da un indirizzo all'altro, che viene trasmessa dal client alla rete, inserita nella blockchain e diventa pubblica
- in realtà non passa da un indirizzo all'altro, ma dall'output di una transazione precedente a un indirizzo bitcoin dove la transazione rimarrà attestata
- le transazioni vanno spese per intero da qui la necessità di utilizzare **change address**)
- Irreversibili (attenzione a non inserire un indirizzo non proprio o comunque di cui non è nota chiave privata)
- Ricevere bitcoin su un indirizzo non richiede consenso

Terminologia: transazioni bitcoin

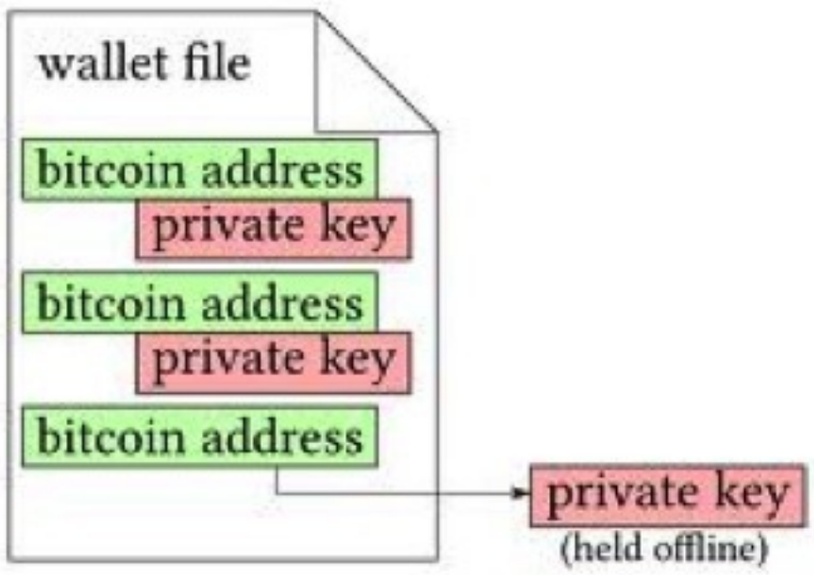
- Una transazione contiene:

1. Input
   - **txID** della transazione che identifica la provenienza della somma che si intende trasferire
   - **Index** all'interno del txID per indicare l'input da spendere (possono esserci numerosi input in una tx)
   - **scriptSig**, firma che certifica l'autenticità dell'input (cioè si dimostra che la transazione di input è nostra)

2. Output
   1. **Valore** in satoshi (0.00000001 BTC) della transazione
   2. Indirizzo bitcoin cui accreditare o script di sblocco

Terminologia: transazioni bitcoin offline

- Optimum per quanto riguarda la sicurezza
- Le chiavi private stanno su PC (o HW) offline
- Si prepara la transazione su, si firma offline, si inoltra
- Alcuni client migliori di altri per gestire offline tx (es. Armory)



Terminologia: transazioni bitcoin

Transaction 7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18

INPUTS From		OUTPUTS To		
From (previous transactions Joe has received):				
Joe	0.1005 BTC	Output #0 Alice's Address	0.1000 BTC	(spent)
		Transaction Fees:	0.0005 BTC	

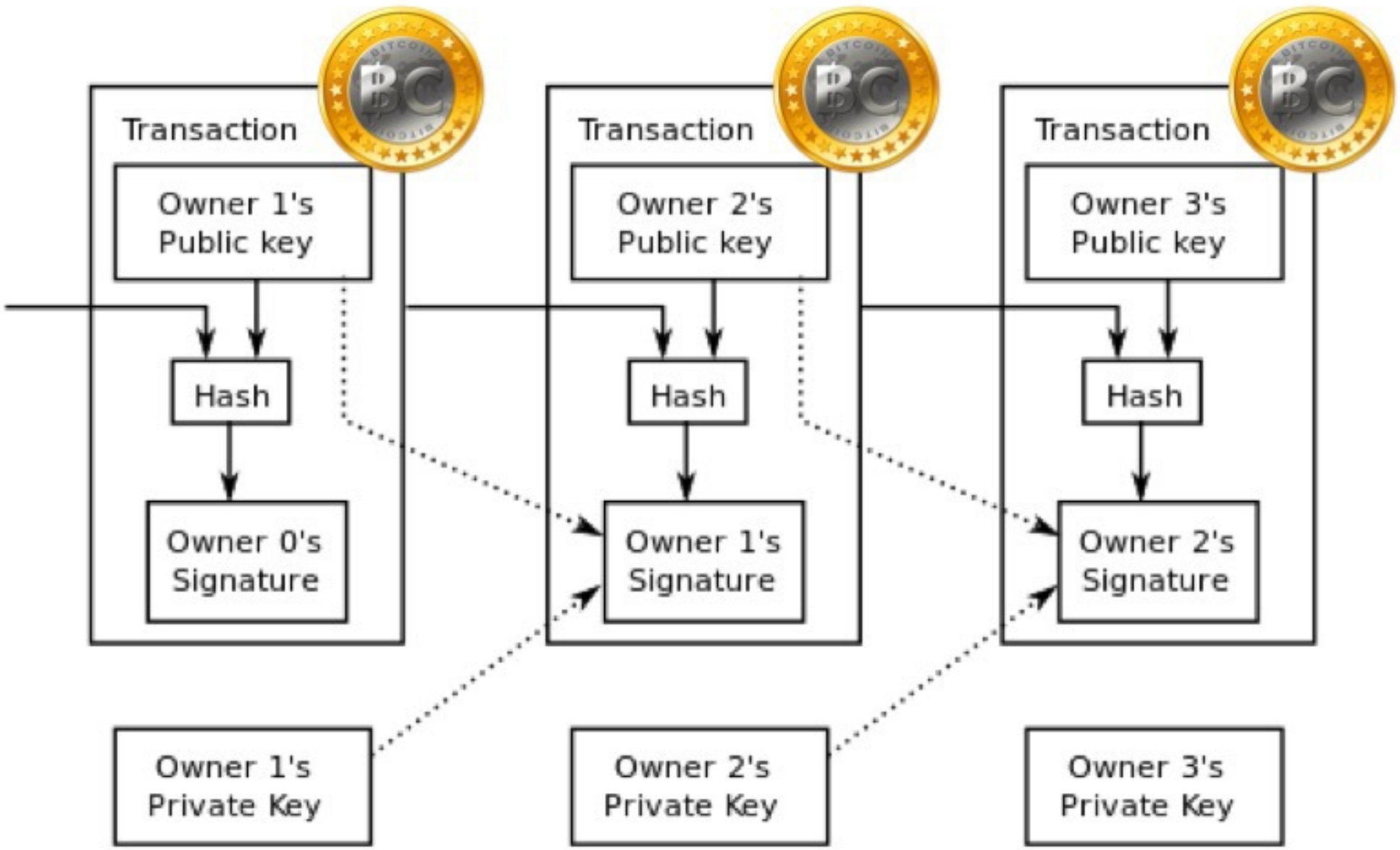
Transaction 0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2

INPUTS From		OUTPUTS To		
7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18 : 0				
Alice	0.1000 BTC	Output #0 Bob's Address	0.0150 BTC	(spent)
		Output #1 Alice's Address (change)	0.0845 BTC	(unspent)
		Transaction Fees:	0.0005 BTC	

Transaction 2bbac8bb3a57a2363407ac8c16a67015ed2e88a4388af58cf90299e0744d3de4

INPUTS From		OUTPUTS To		
0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2 : 0				
Bob	0.0150 BTC	Output #0 Gopesh's Address	0.0100 BTC	(unspent)
		Output #1 Bob"s Address (change)	0.0845 BTC	(unspent)
		Transaction Fees:	0.0005 BTC	

Terminologia: transazioni bitcoin



Terminologia: mining

- 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 (transaction fee) per ogni transazione inserita nel blocco

Terminologia: mining e transaction fees

- Incentivo per i miners
- Non ci sono minimi o massimi, lo standard si evolve
- Non dipendono dalle cifre trasferite ma dalla dimensione in Byte che occupa la transazione
- Oggi: 0.0001 BTC ogni Kb di transazione
- Attenzione che se preparate una transazione a mano e non specificate ogni TXOUT, tutto il resto va in fee

Terminologia: mining e reward

Block	Reward Era	BTC/block	Year	Start BTC	BTC Added	End BTC	BTC Increase	End BTC % of Limit
0	1	50.00000000	2009.007	0.00000000	10500000.00000000	10500000.00000000	infinite	50.00000006%
210000	2	25.00000000	2013.000	10500000.00000000	5250000.00000000	15750000.00000000	50.00000000%	75.00000008%
420000	3	12.50000000	2016.993	15750000.00000000	2625000.00000000	18375000.00000000	16.66666667%	87.50000010%
630000	4	6.25000000	2020.986	18375000.00000000	1312500.00000000	19687500.00000000	7.14285714%	93.75000010%
840000	5	3.12500000	2024.978	19687500.00000000	656250.00000000	20343750.00000000	3.33333333%	96.87500011%
1050000	6	1.56250000	2028.971	20343750.00000000	328125.00000000	20671875.00000000	1.61290323%	98.43750011%
1260000	7	0.78125000	2032.964	20671875.00000000	164062.50000000	20835937.50000000	0.79365079%	99.21875011%
1470000	8	0.39062500	2036.956	20835937.50000000	82031.25000000	20917968.75000000	0.39370079%	99.60937511%
1680000	9	0.19531250	2040.949	20917968.75000000	41015.62500000	20958984.37500000	0.19607843%	99.80468761%

...

6510000	32	0.00000002	2132.781	20999999.97060000	0.00420000	20999999.97480000	0.00000002%	99.99999999%
6720000	33	0.00000001	2136.774	20999999.97480000	0.00210000	20999999.97690000	0.00000001%	100.00000000%
6930000	34	0.00000000	2140.767	20999999.97690000	0.00000000	20999999.97690000	0.00000000%	100.00000000%

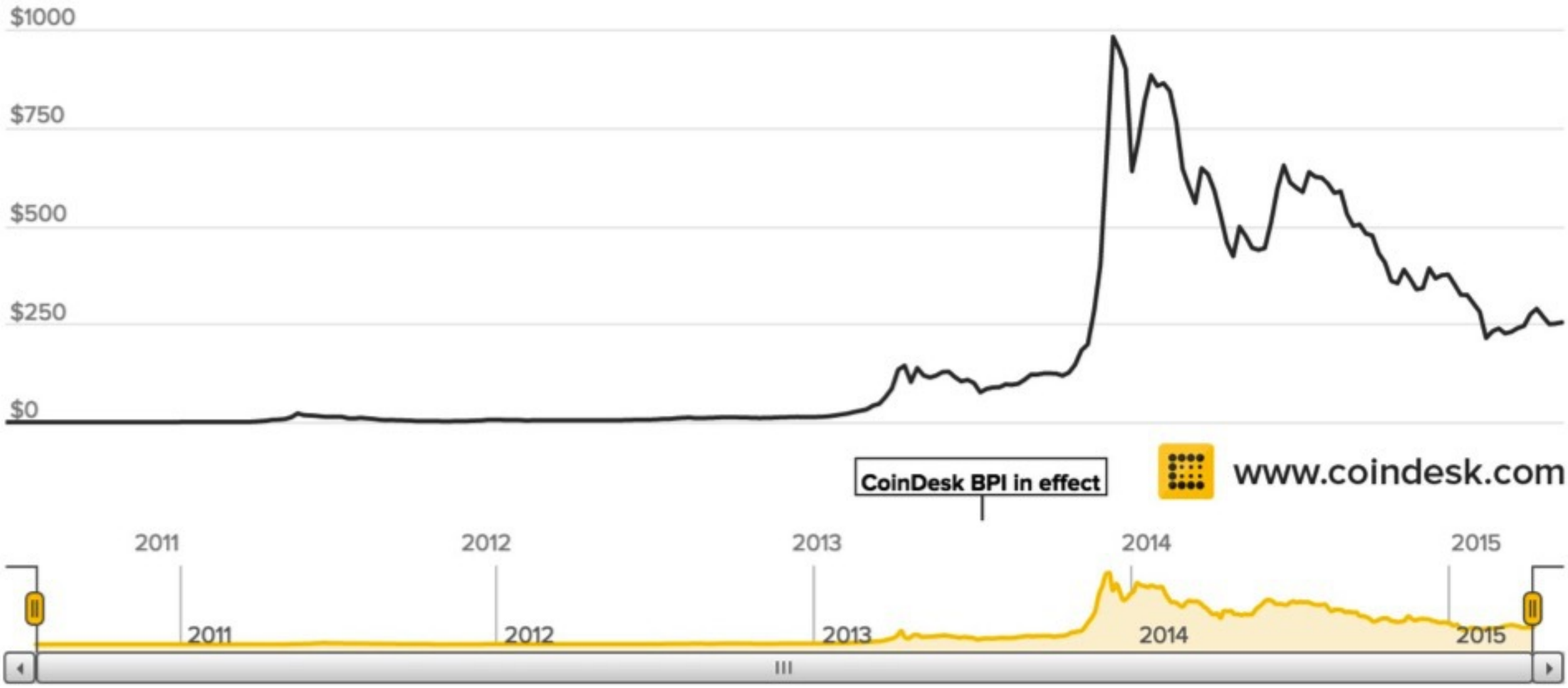
https://en.bitcoin.it/wiki/Controlled_supply

Bitcoin units

Unit	Abbreviation	Decimal (BTC)	Alternate names	Info
Algorithmic Max	-	20,999,999.9769[1]	-	Current Max Possible: 20999839.77085749[2]
megaBitcoin	MBTC	1,000,000	-	Rarely used in context
kiloBitcoin	kBTC	1,000	-	Rarely used in context
Original Block Reward	-	50	block	Until block 210000[3]
Current Block Reward	-	25	block	As of block 210000[4]
decaBitcoin	daBTC	10	-	Rarely used in context
Bitcoin	BTC	1	coin	Base unit (100 million satoshis)
deciBitcoin	dBTC	0.1	-	Rarely used in context
centiBitcoin	cBTC	0.01	bitcent	Frequently used until the November 2013 bubble
milliBitcoin	mBTC	0.001	millibit, millicoin, millie	Thousandth of a Bitcoin, frequently used subdivision
microBitcoin	µBTC	0.000001	bit	Millionth of a Bitcoin, frequently used subdivision
Finney[5]	-	0.0000001	Finney	10 millionth, 1e-7
satoshi	-	0.00000001	*none*	100 millionth, 1e-8, currently the smallest possible unit

https://en.bitcoin.it/wiki/Units

Quanto “vale” un bitcoin



Caratteristiche salienti

- **Veloce** (10-60 min)
- **Economico** (costo transazione indipendente da somma)
- Pseudo-**anonimo** ma pubblico, le transazioni Bitcoin sono tracciabili
- Nessuna **autorità centrale**
- Irreversibile e **non falsificabile**
- Impossibile (difficile) da **confiscare**
- Pensato per **Internet**, funziona ovunque, richiede connessione
- **Inflazione** determinata a priori
- E' più facile (farsi**) rubare bitcoin** o perderli rispetto alla valuta fiat
- **Controvalore** altamente variabile
- Poca chiarezza e controllo su **plusvalore**

Dove si scambiano BTC <-> EURO

- Il valore è determinato dal mercato
- Vi sono/erano diversi servizi/siti online per lo scambio
  - Bitboat, Postebit, Coinbit, LocalBitCoins, etc…
- Costi e modalità diverse anche per il pagamento:
  - Bonifico, contanti, Ricarica Superflash o Postepay, Paysafe Card, Western Union, etc…
- Non è in genere accettata carta di credito o Paypal

Come ottenere i bitcoin

Google

come ottenere bitcoin

Web News Videos Images Shopping More Search tools

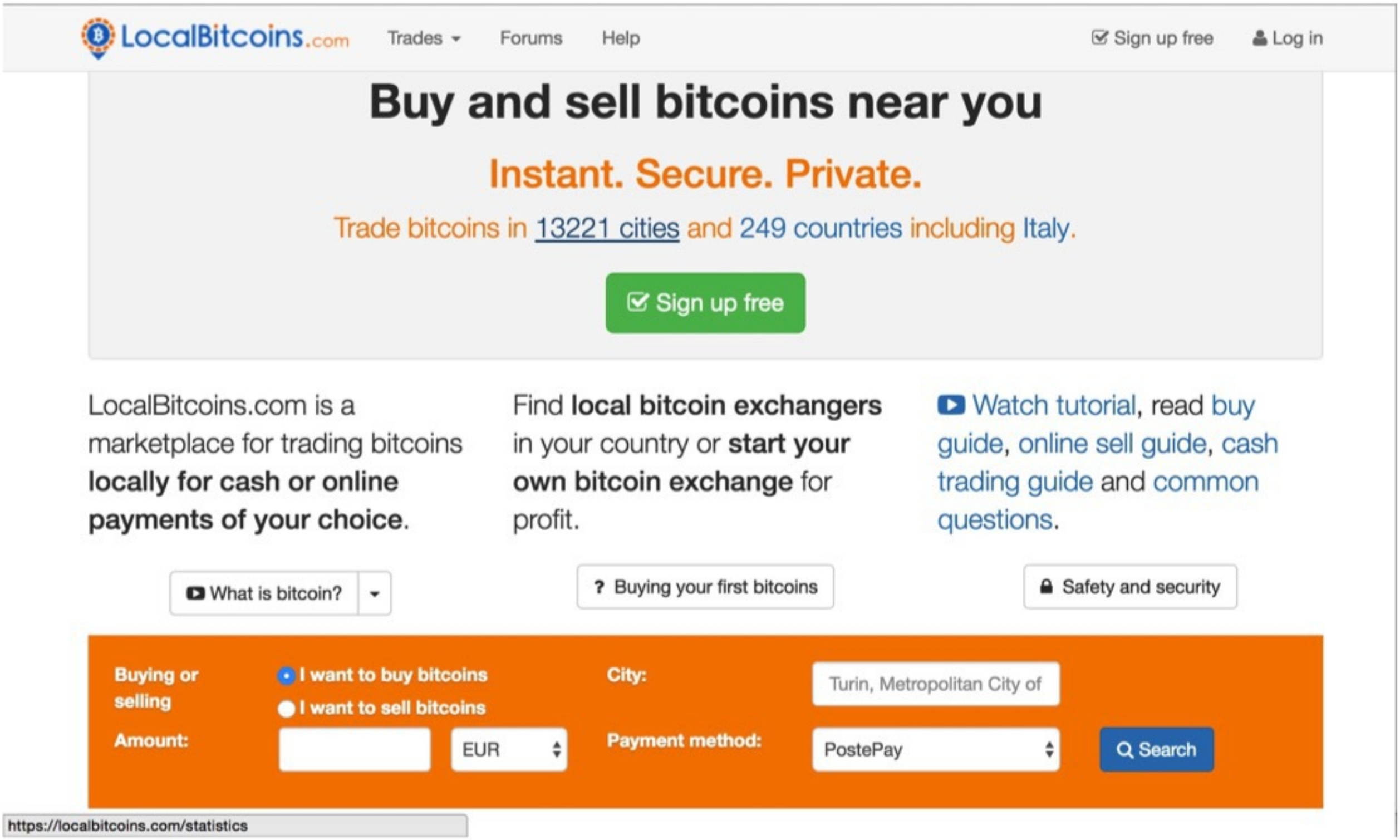
About 338,000 results (0.34 seconds)

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



Come ottenere i bitcoin

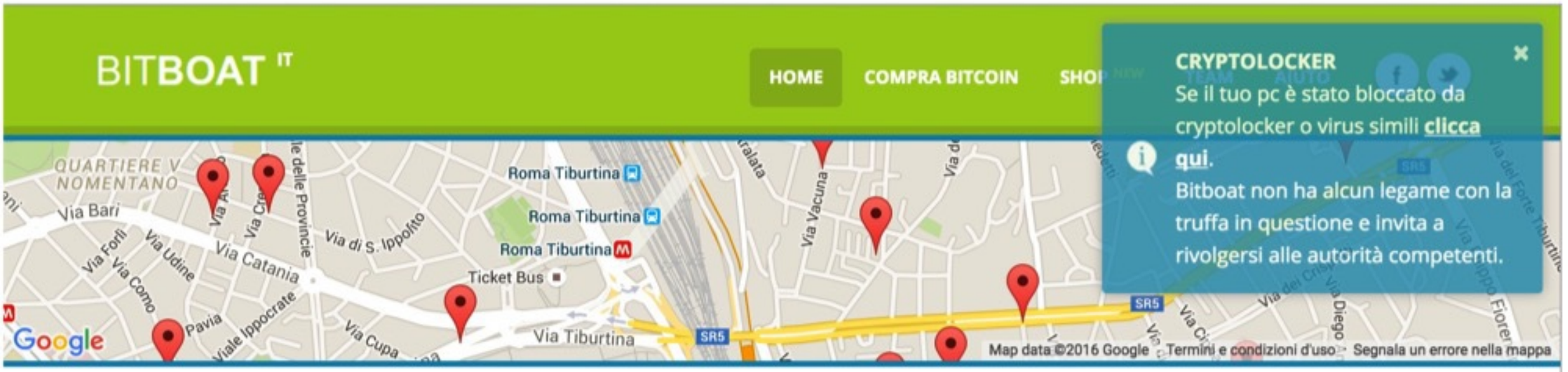
LocalBitcoins.com Trades Forums Help Sign up free Log in

Buying or selling: (•) I want to buy bitcoins ( ) I want to sell bitcoins
Amount: 100 EUR
City: Turin, Metropolitan City of
Payment method: Cash
Search

Results for buying bitcoins with cash near Turin, Metropolitan City of Turin, Italy

Seller	Distance	Location	Price/BTC	Limits	
mike222 (100+; 100%)	0 km	Turin, Metropolitan City of Turin, Italy	410.66 EUR	10 - 50 EUR	Buy
btcfast (1000+; 100%)	0 km	Turin, Metropolitan City of Turin, Italy	421.75 EUR	At least 300 EUR	Buy
colinas (1000+; 100%)	0 km	Turin, Italy	422.98 EUR	500 - 10000 EUR	Buy
sonic1991 (100+; 100%)	0 km	Turin, Italy	433.08 EUR	50 - 300 EUR	Buy
Pitchotto (21; 100%)	1.6 km	Turin, Italy	457.59 EUR	400 - 10000 EUR	Buy

Come ottenere i bitcoin



Compra Bitcoin in velocità e sicurezza.

Compra subito

Come funziona

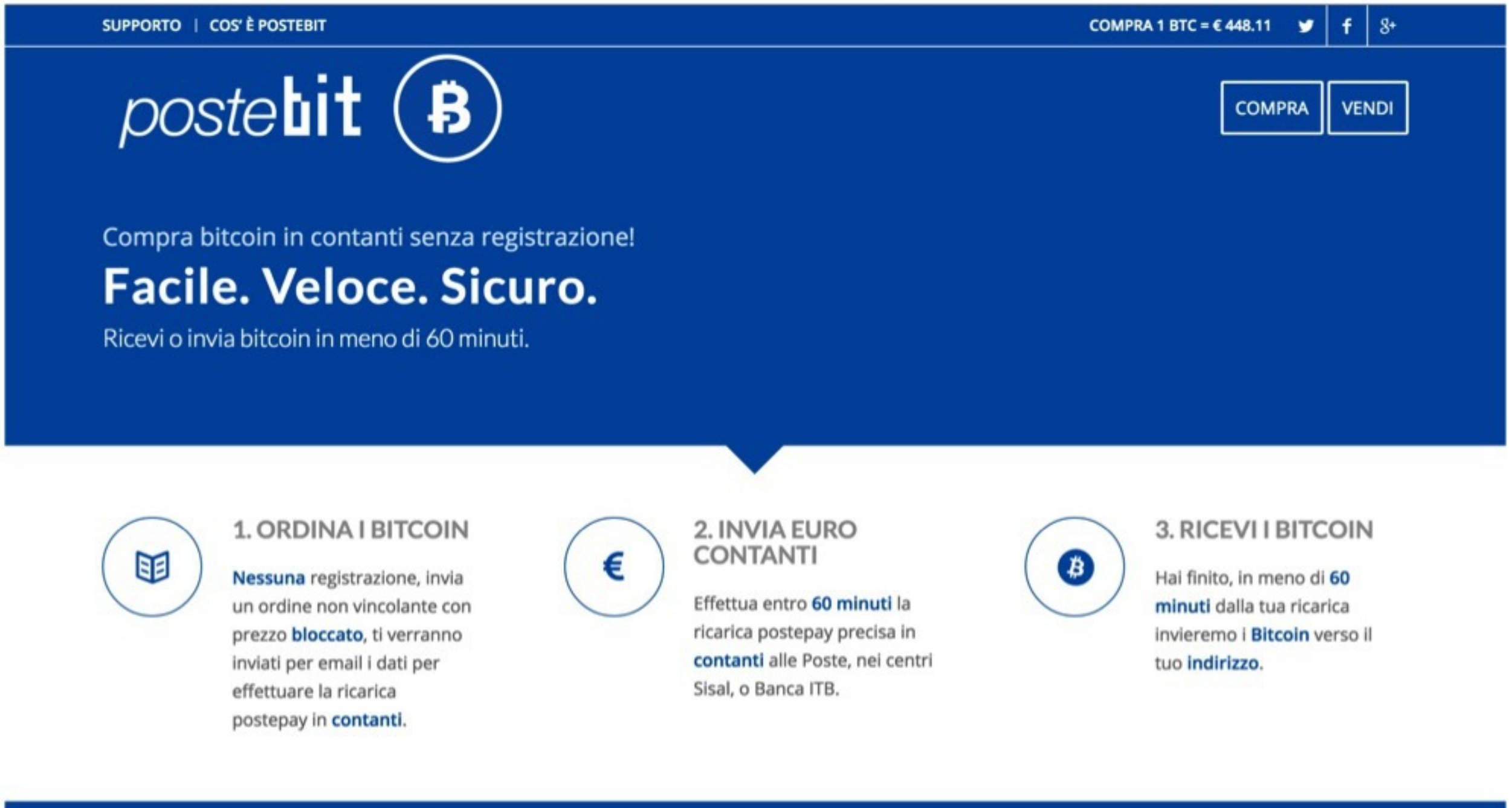
Assistito
Le tue domande trovano sempre risposta,
grazie all'assistenza on-site o via

Istantaneo
Ricevi i tuoi Bitcoin in modo automatizzato, entro pochi minuti dal pagamento.

25'000+ transazioni concluse

Chat? - Offline

Come ottenere i bitcoin



Come ottenere i bitcoin

Come ottenere i bitcoin

Flash Bitcoin

Ciao! Sei pronto a comprare un po' di **Bitcoin** ?

Compila i seguenti campi e clicca sul tasto "procedi".

Indirizzo bitcoin

Indirizzo Email

Numero bitcoin

0,010

Totale

2,13 Aggiornare

Ricarica SuperFlash Ricarica PostePay

Ricarica SuperFlash con carta di credito allo sportello

procedi

Come ottenere i bitcoin

BitDigital.it

Compra Bitcoin | Stato Ordini

Compra Bitcoin

= 249.59€

Indirizzo Bitcoin

inserisci il tuo indirizzo btc

Email

inserisci la tua email

Bitcoin da acquistare

0,2

Importo da spendere

49.92

Metodo di Pagamento

- **Superflash**
- **PostePay**

ACQUISTA BITCOIN

COME ACQUISTARE

Semplice Veloce Sicuro

Compila correttamente il modulo d'acquisto qui a sinistra e controlla l'email. Ricevuta l'email dentro c'è il tuo **link di conferma**. Cliccando confermi l'ordine. Una volta confermato riceverai un'altra email con gli **estremi per il pagamento** da effettuare entro **un'ora di tempo**. In assenza di conferma, l'ordine sara' **automaticamente annullato**. Riceverai i bitcoin direttamente nel tuo **wallet** entro pochi minuti. Inoltre puoi seguire la transazione in tempo reale nella nostra homepage per visualizzare informazioni dettagliate su **Blockchain**.

Perchè affidarsi a noi?

Miglior Prezzo

Abbiamo i **prezzi piu' bassi** per l'acquisto di Bitcoin

Velocità

Ricevi Bitcoin **entro 5 minuti** dalla verifica dell'avvenuto pagamento.

Facilità D'acquisto

Puoi acquistare Bitcoin effettuando una ricarica sulla nostra carta **PostePay - SuperFlash** in qualunque ufficio postale o tabaccheria convenzionata ITB.

Affidabilità

Il nostro sistema è del tutto affidabile perchè **completamente automatizzato**: dall'avvenuta verifica di pagamento fino alla transazione dei Bitcoin acquistati.

Sicurezza

Sarà nostra cura prendere ogni **precauzione** affinchè la transazione si concluda senza imprevisti.

Assistenza

Se hai dubbi o domande: consulta la sezione AIUTO oppure inviaci una richiesta di supporto, risponderemo in breve tempo.

postepay

Compra Bitcoin ricaricando la nostra carta Postepay negli uffici

INTESA SANPAOLO SUPERFLASH

Compra Bitcoin ricaricando la nostra carta Superflash in contanti

Come ottenere i bitcoin

BitDigital.it

ULTIME TRANSAZIONI

0.37 BTC	1HNVa1qvZpkzZQH7zJbyYyjxU1FkP5hnnn	€ 90
0.49 BTC	14aWSzdTH27L35X5G1THBmQRiVoqtGiExv	€ 119.15
0.4 BTC	1E43oKFp1inojtn3FV3MUiYVKpEtMRoZnd	€ 99.3
0.46 BTC	14UmgSbbQGK2mVVHbaprwG8wqRbNTuN8pw	€ 114.73
0.36 BTC	15hcpHSwFEQu4i7\	

Clicca sull'indirizzo del tuo wallet

Dopo aver comprato i tuoi bitcoin clicca sull'indirizzo del tuo wallet qui a lato per visualizzare le informazioni dettagliate sulla transazione su Blockchain

Come ottenere i bitcoin

BitDigital.it

ULTIME TRANSAZIONI

0.37 BTC → 1HNVa1qvZpkzZQH7zJbyYyjxU1FkP5hnnn € 90

Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary		Transactions	
Address	1HNVa1qvZpkzZQH7zJbyYyjxU1FkP5hnnn	No. Transactions	3
Tools	Taint Analysis - Related Tags - Unspent Outputs	Total Received	0.99 BTC
		Final Balance	0.37 BTC

Request Payment | Donation Button

Transactions (Oldest First) Filter

f1c8a9068b019f0243fa584e68e1a37a0c160bf4d2f230a9d64c2dbab61446b0			2015-04-04 12:35:40
38Ju3WeXbhpS9Ak3K7ShgwW4KgzBtHcu1z	→	1HNVa1qvZpkzZQH7zJbyYyjxU1FkP5hnnn	0.37 BTC
			0.37 BTC

https://blockchain.info/address/1HNVa1qvZpkzZQH7zJbyYyjxU1FkP5hnnn

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	Ł 0.0059	Ł 0.0061	Ł 0.0059	v -3.39%	about an hour ago

Bid (Buy)

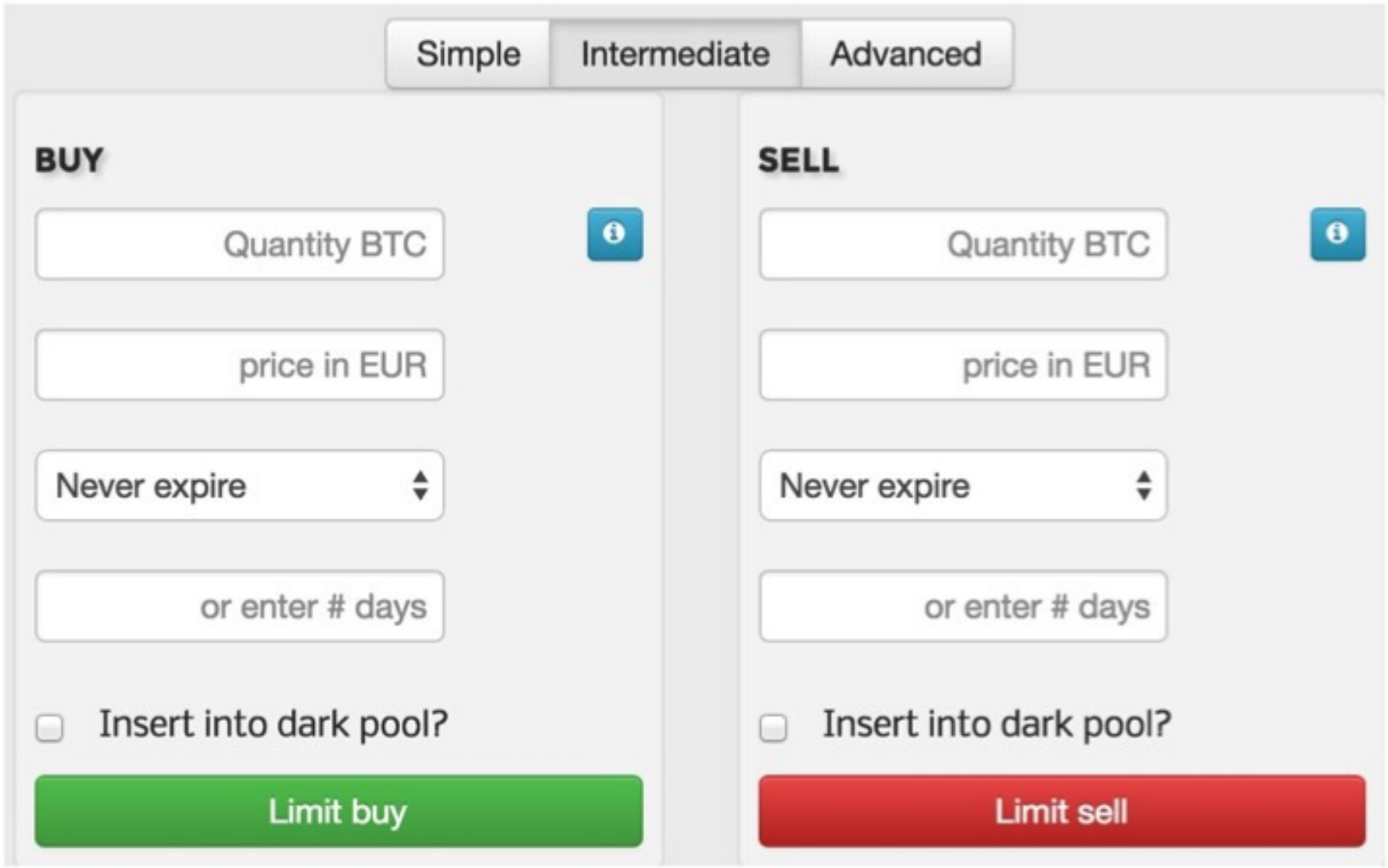
quantity BTC	value EUR	depth EUR
0.06	207.49	12.45
0.11	207.48	35.27
0.36	207.32	109.91
0.20	207.31	151.37

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

https://blockchain.info/address/1HNVa1qvZpkzZQH7zJbyYyjxU1FkP5hnnn

Come ottenere i bitcoin



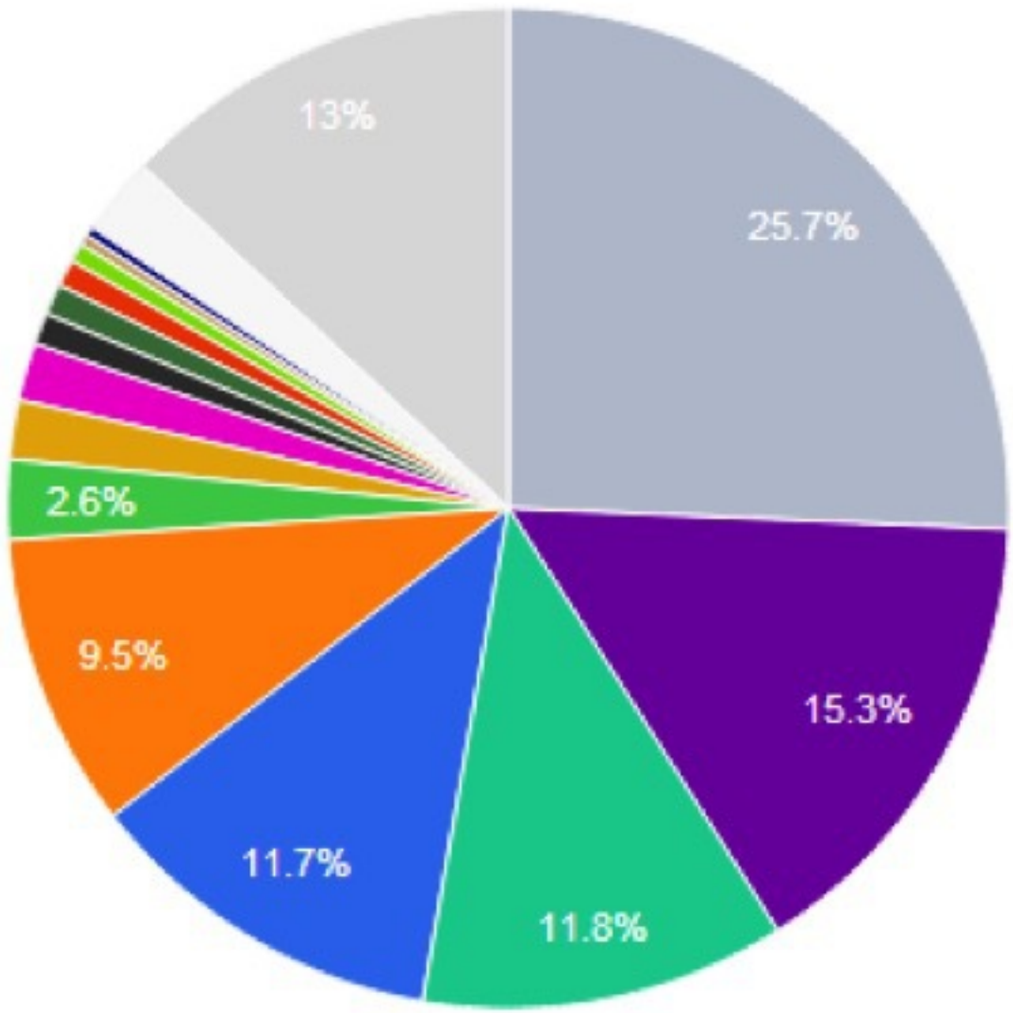
https://blockchain.info/address/1HNVa1qvZpkzZQH7zJbyYyjxU1FkP5hnnn

Come generare bitcoin

- Mining
- Il lavoro viene ripagato solo se si mina il blocco “vincente”, altrimenti è lavoro inutile
- Impossibile minare da soli ormai, ci vuole un pool

Come generare bitcoin

Hash Rate Distribution



WeMineLTC	26,106.5 MH/s
Coinotron	15,546.1 MH/s
Give Me Coins	11,983.4 MH/s
LiteGuardian	11,927.4 MH/s
LitecoinPool.org	9,681.5 MH/s
LTCRabbit.com	2,618.5 MH/s
Hypernova	1,943.9 MH/s
P2Pool	1,879.8 MH/s
Pool-X.eu	1,041.8 MH/s
HashFaster	1,017.0 MH/s
Show all pools...	
Unknown	13,264.0 MH/s
Total	101,704.5 MH/s

Aspetti giuridici del Bitcoin

- I bitcoin sono legali o illegali?
- E' legale possederle, vendere o acquistare bitcoin?
- Cosa si deve pagare se si vendono bitcoin?
- Le plusvalenze come vanno normate?
- I bitcoin sono utilizzati per riciclare?

Normativa

- Mi rifaccio all'ottima analisi di **Stefano Capaccioli** (www.coinlex.it), fornendo alcuni spunti approfondibili tramite il suo libro uscito a giugno 2015, riportato in bibliografia
- La normativa è ancora in divenire, in alcuni stati più avanti rispetto ad altri
- Al momento stiamo assistendo a episodi "particolari", paesi dove i Bitcoin sono banditi, altri che li riconoscono, in altri ancora la Giustizia non sa esattamente come reagire a episodi nei quali i bitcoin sono coinvolti nel bene o nel male…

Criptovaluta (definizione)

- 1. RAPPRESENTAZIONE DIGITALE DI VALORE: Rappresentazione di una quantità non emessa da autorità (centrale o pubblica), non necessariamente collegata a moneta a corso legale che può essere usata come mezzo di scambio o trasferita, immagazzinata o commercializzata elettronicamente.
- 2. DECENTRALIZZATA: sistema basato sull'assenza di un emittente, di un amministratore ovvero di un gruppo di controllo e su filosofia "open source".
- 3. PEER-TO-PEER: Rete informatica che non possiede nodi gerarchizzati sotto forma di client o server fissi, ma un numero di nodi equivalenti che possono fungere sia da client che da serveE verso gli altri nodi della rete ed ognuno in grado di avviare ovvero completare una transazione.
- 4. BLOCKCHAIN: registro distribuito incrementale delle transazioni, liberamente accessibile e basato sul consenso decentralizzato.
- 5. ALGORITMO OPEN SOURCE: Programma informatico aperto e pubblico che contiene un numero determinato e finito di istruzioni per la realizzazione del sistema.

Normativa

Le criptovalute **possono** essere «*considerate*»:

- **Moneta**: ma non è fiat, rappresentativa o merce
- **Valuta estera**: manca però definizione di valuta
- **Beni Immateriali**: art. 810 del CC, «*sono beni le cose che possono formare oggetto di diritti*»
- **Commodity**: materia prima, ma manca materialità
- **Security (titolo)**: MIFID Direttiva 2004/39/CE
- **Diritti di Baratto (Barter Rights)**: non si concilia con mining, l'attività di investimento o di pagamento
- **Sistema di pagamento:** riferimento, PSD (Payment Services Directive) 64/2007/CE recepita mediante D. Lgs. 27 gennaio 2010 n. 11

Normativa

Le criptovalute **non** possono essere «*considerate*»:

- **Titoli di credito**: non incorporano il diritto ad una specifica prestazione e comunque non incorporano un credito pecuniario;
- **Titoli rappresentativi di merce**: non è identificata né la merce né il servizio né sono connesse a rapporti contrattuali
- **Titoli di legittimazione**: non è identificabile la prestazione
- **Partecipazioni o quote**: non essendovi alcun emittente di cui con il possesso delle criptovalute si possa far parte né diritti da esercitare.
- **Monete**, non avendo il corso legale in alcun paese
- **Strumento finanziario**: non essendovi alcun contratto diretto al trasferimento della moneta (reale)

Normativa (Italia)

- "*In Italia l'acquisto, l'utilizzo e l'accettazione in pagamento delle valute virtuali debbono allo stato ritenersi attività lecite; le parti sono libere di obbligarsi a corrispondere somme anche non espresse in valute aventi corso legale*"
- BANCA D'ITALIA, Avvertenza sull'utilizzo delle cosiddette "valute virtuali", 30.01.2015
  - http://www.bancaditalia.it/compiti/vigilanza/avvisi-pub/avvertenza-valute-virtuali/AVVERTENZA_VALUTE_VIRTUALI.pdf
  - https://www.bancaditalia.it/pubblicazioni/bollettino-vigilanza/2015-01/20150130_II15.pdf

Legalità del Bitcoin per paese

Country	Legal?	Notes
Australia	Yes[10]	
Bangladesh	No[3]	
Belgium	Yes[11]	
Bolivia	No[4]	Banco Central de Bolivia, the central bank of Bolivia, issued a resolution banning bitcoin in 2014.[12]
Brazil	Yes[13]	Bitcoin is regulated under a 2013 law that discusses both mobile payment systems and electronic currencies.[13]
Canada	Yes[14]	Bitcoin is regulated under anti-money laundering and counter-terrorist financing laws in Canada.[15]
China (PRC)	Restricted[16]	Financial institutions cannot use or involve themselves with bitcoins.[16]
Colombia	Yes[17]	
Croatia	Yes[18]	
Czech Republic	Yes[19]	
Cyprus	Yes[20]	
Denmark	Yes[21]	
Ecuador	No[5]	

https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country

Legalità del Bitcoin per paese

France	Yes[22]	
Germany	Yes[23]	
Hong Kong	Yes[24]	
Iceland	Restricted[25]	According to a 2014 opinion from the Central Bank of Iceland "there is no authorization to purchase foreign currency from financial institutions in Iceland or to transfer foreign currency across borders on the basis of transactions with virtual currency. For this reason alone, transactions with virtual currency are subject to restrictions in Iceland."[25] This does not stop[26] businesses in Iceland from mining bitcoins.[27]
Indonesia	No[*disputed – discuss*]	In January, 2014, the Indonesian monetary authority called bitcoin "illegal and unsupported"[28] prompting media to report that "Indonesia has become the latest country... to ban the use of the Bitcoin virtual currency"[9] and "Bank Indonesia declares Bitcoin as illegal currency".[29]
Israel	Yes[30]	
Italy	Yes[31]	
Japan	Yes[32]	
Jordan	Yes	The government of Jordan has issued a warning discouraging the use of bitcoin and other similar systems.[33]

https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country

Legalità del Bitcoin per paese

Kyrgyzstan	No[6]	In a July, 2014, statement the Kyrgyz monetary authority made clear that "the use of 'virtual currency', bitcoins, in particular, as a means of payment in the Kyrgyz Republic will be a violation of the law of our state."[6]
Lebanon	Yes	The government of Lebanon has issued a warning discouraging the use of bitcoin and other similar systems.[33]
New Zealand	Yes[34]	
Norway	Yes[35]	
Poland	Yes[36]	
Russia	No[7]	As of January 2015, a bill explicitly banning bitcoins does not exist in Russia,[37] although it appears a *de facto* ban is in place. CNBC reported that bitcoin was illegal in Russia in December, 2014,[38] and various Russian authorities and organizations have spoken out or taken actions against bitcoin. In early 2015, Russia's media regulator blocked several bitcoin-related websites,[37] in 2015 a Russian state-owned media outlet reported that "The [Russian] Central Bank... said that bitcoin usage was illegal under Russian federal law,"[37] and in February 2014, the Russian Prosecutor General's Office was quoted as saying, "Cyber currencies... including the most well-known, bitcoin, are money substitutes and cannot be used by individuals or legal entities."[39]

https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country

Legalità del Bitcoin per paese

Singapore	Yes[40]	
Slovenia	Yes[41]	
South Korea	Yes[42]	While not illegal in the country, Korean authorities will prosecute illegal activity involving bitcoin[43] and have indicted at least one individual for purchasing drugs with bitcoin.[44]
Spain	Yes[45]	
Switzerland	Yes[46]	Bitcoin businesses in Switzerland are subject to anti-money laundering regulations and in some instances may need to obtain a banking license.[46]
Sweden	Yes[47]	
Taiwan	Restricted[7]	bitcoin ATMs banned[7]
Thailand	No[48]	Bank of Thailand declared bitcoin illegal in 2013, but some bitcoin companies have been able to obtain business licenses.[49] One startup denied a business license was reportedly told that "buying and selling bitcoins, using bitcoins to buy or sell goods and services, and transferring bitcoins in and out of Thailand were all currently illegal."[48]
Turkey	Yes[50]	
United Kingdom	Yes[51]	
United States	Yes	
Vietnam	No[8]	As of 2014, trading in bitcoin is illegal in this country according to a statement released by the State Bank of Vietnam in February, 2014.[52][53]

https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country

Principali documenti emessi

1. Francia: Sentenza del Tribunale di Creteil e Corte di Appello di Parigi
2. FBI *Report on bitcoin*.
3. BCE *Virtual Currency Schemes*
4. FINCEN – USA
5. Sentenza USA: SEC VS SHAVERS
6. European Bank Authority
7. GERMANIA – BAFIN
8. Sentenza Civile in Olanda del Tribunale di OVERJISSEL
9. Report al Parlamento Svizzero.
10. FAFT – GAFI.
11. Rapporto OCSE.
12. Rapporto del Senato Francese
13. Canada – Bill C-31
14. Casi giudiziari pendenti in USA (Processo Silk Road)

IVA sulle transazioni Bitcoin?

- **Svezia**: Ruling appellato – Corte di Giustizia ECJ C-264/14
- **Regno Unito**: Chiarimento provvisorio – esenzione IVA
- **Estonia**: Chiarimento - imponibile IVA
- **Polonia**: Interpelli - imponibile IVA
- **Germania**: esclusa da IVA
- **Belgio**: interpello – esente IVA
- **Francia**: rapporto – supporterà esenzione IVA
- **Finlandia**: Ruling – esenzione IVA
- **Spagna**: Ruling – esenzione IVA
- **Italia**: *Interpello presentato da Capaccioli*

Comunque a fini IVA per tutti è SERVIZIO

Plusvalenze sulle rendite da Bitcoin?

- TUIR (Testo Unico delle Imposte sui Redditi) 917/1986
- Accettazione bitcoin in cambio beni e servizi – valore normale beni e servizi qualora imponibili (es. Prestazione occasionale)
- Plusvalenze da gestione bitcoin:
  - **Redditi Diversi** (o redditi da capitale) se i redditi derivano da un evento incerto (art. 67 t.u.i.r.). – titoli non rappresentativi di merce
  - art. 67 t.u.i.r. – c-ter: "*le plusvalenze, diverse da quelle di cui alle lettere c) e c-bis), realizzate mediante* ***cessione a titolo oneroso ovvero rimborso di titoli non rappresentativi di merci****, di certificati di massa, di valute estere, oggetto di cessione a termine o rivenienti da depositi o conti correnti, di metalli preziosi, semprechè siano allo stato grezzo o monetato, e di quote di partecipazione ad organismi d'investimento collettivo. Agli effetti dell'applicazione della presente lettera si considera cessione a titolo oneroso anche il prelievo delle valute estere dal deposito o conto corrente;*"

Riflessioni

Può essere usato
- *Per comprare droga e armi*
- *Per riciclare*
- *Per finanziare Terrorismo*

Caratteristiche
Anonimo
Non tracciabile
Senza valore intrinseco
Può essere prodotto senza costi

Caratteristiche
Pseudonimo
Tracciabile
Valore derivante da domanda /offerta
Costa Produrlo

bitcoin

COINLEX.

Agenda

- Presentazione relatore
- Il protocollo Bitcoin e la blockchain
- Anonimato, mixer, exchange e cash out
- Sicurezza e rischi del protocollo
- Bitcoin Forensics e indagini sulle criptomonete
- Le evoluzioni del sistema: Smart Contract e Public Notary
- Il futuro del Bitcoin
- Q&A
- Bibliografia & sitografia

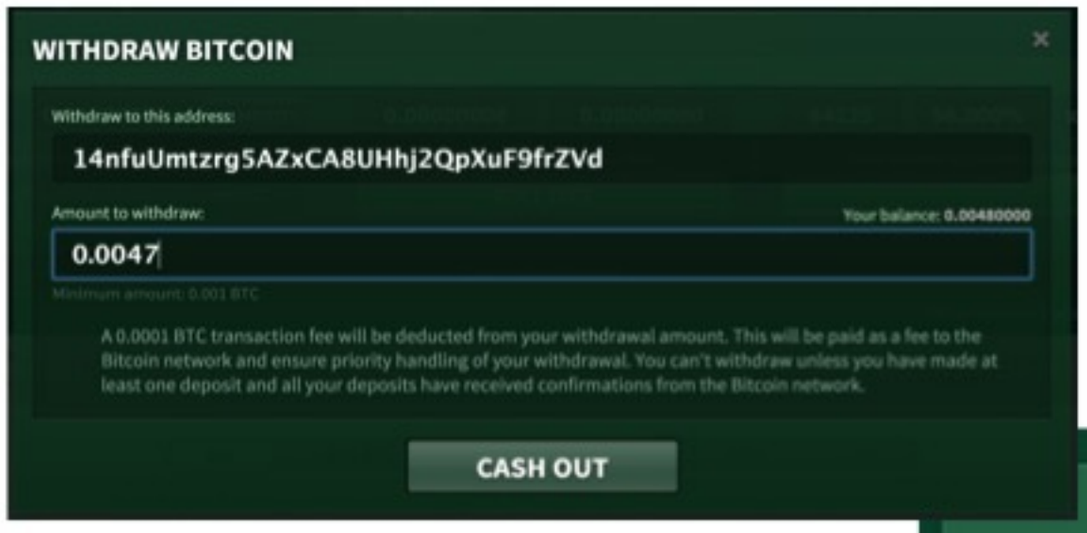
Anonimato

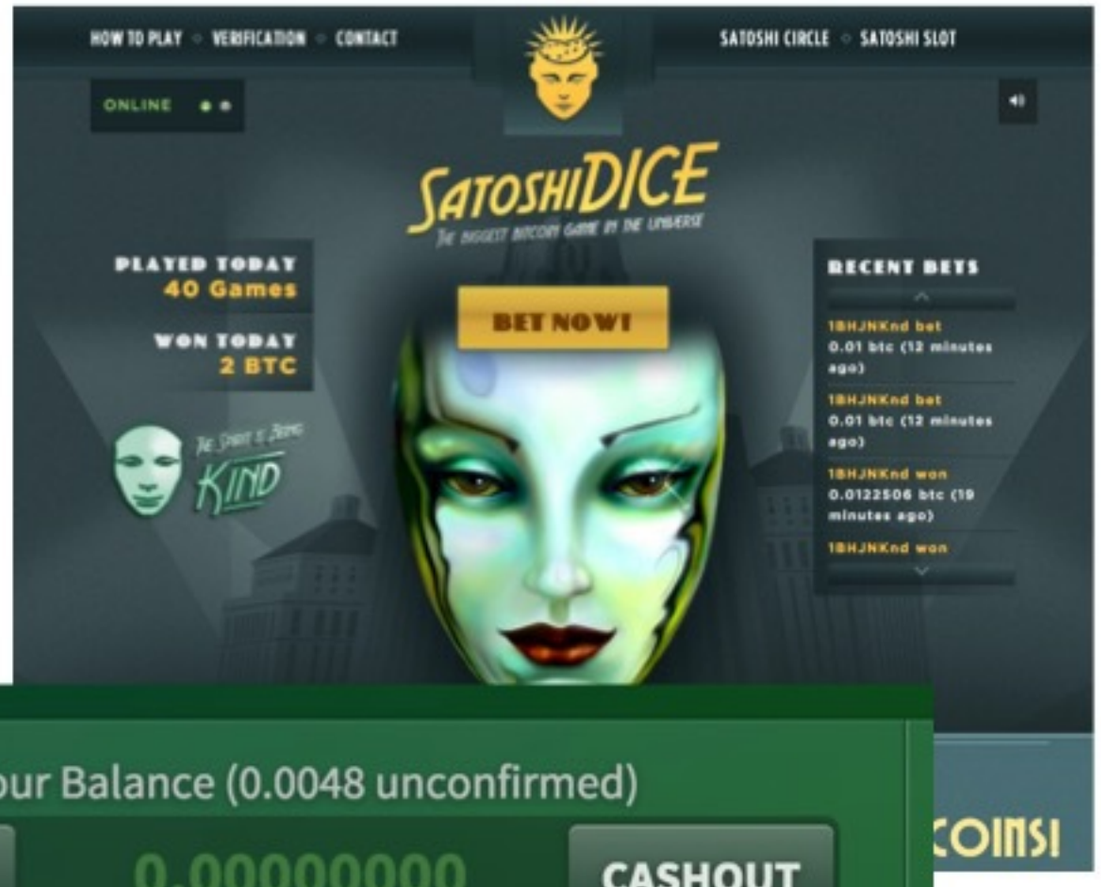
- Il Bitcoin non è “anonimo”, ma “pseudonimo”
- Non esiste registro che lega indirizzo a proprietario
- Le transazioni non mantengono (in genere) traccia di IP (non confondere il “relay IP”)
- Si può fare intelligence sugli end-point, cioè quando la moneta FIAT viene scambiata in BTC e viceversa

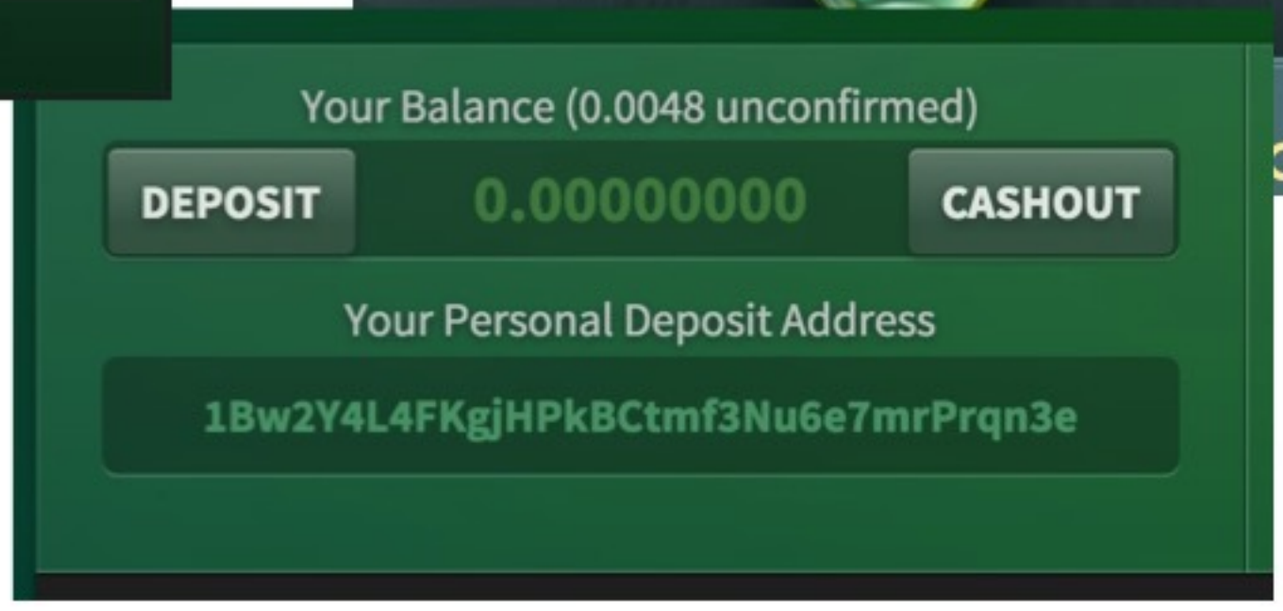
Come vengono “ripuliti” i bitcoin

- 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

Shared Coin

A privacy service that helps users create joint transactions

To: 13wQt1ZMFG6bDCH5uRZ19bGjF97nok1kc6 | BTC | 0.014 | $ 3.59

Total Value: 0.014 BTC (Available: 0.015 BTC)

Privacy Required: Normal

Check to donate a random percer

further improvements to Shared Coin

Shared Coin Transaction Estimated Time Left: 1 minutes 25 seconds

Waiting For Outputs To Be Joined

Transaction in progress. Do not close this window or exit your browser.

Send **0.014 BTC** to **13wQt1ZMFG6bDCH5uRZ19bGjF97nok1kc6** Cancel

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

Agenda

- Presentazione relatore
- Il protocollo Bitcoin e la blockchain
- Anonimato, mixer, exchange e cash out
- Sicurezza e rischi del protocollo
- Bitcoin Forensics e indagini sulle criptomonete
- Le evoluzioni del sistema: Smart Contract e Public Notary
- Il futuro del Bitcoin
- Q&A
- Bibliografia & sitografia

Sicurezza e Rischi del Protocollo

- Diverse criticità:
  - Metodo di generazione della chiave privata
    - Buon RNG, attenzione ai brainwallet
  - Conservazione del wallet
    - Protezione con password
  - Conservazione delle chiavi private
    - Wallet gerarchico deterministico
  - Wallet online e sicurezza delle chiavi
    - Backup? Esportazione chiavi?
    - N-Lock Time
  - Cambio password del wallet
    - Inutile se esiste un backup con la pwd precedente
  - Backup
    - Perso il wallet o le chiavi, persi i bitcoin

Sicurezza e Rischi del Protocollo

- Diverse criticità:
  - Indirizzi protetti da una sola chiave
    - Multisig
  - Trojan che acquisiscono copia dei wallet
  - Trojan che modificano gli indirizzi XBT in clipboard

Agenda

- Presentazione relatore
- Il protocollo Bitcoin e la blockchain
- Anonimato, mixer, exchange e cash out
- Sicurezza e rischi del protocollo
- Bitcoin Forensics e indagini sulle criptomonete
- Le evoluzioni del sistema: Smart Contract e Public Notary
- Il futuro del Bitcoin
- Q&A
- Bibliografia & sitografia

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** e **blockchain.info**
  - Blocchi (anche quelli doppi)
  - Transazioni (spese e non spese)
  - Indirizzi e transazioni (prima comparsa di un ADDR, saldo, etc…)
  - Taint Analysis
  - Statistiche
  - **Tag**

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

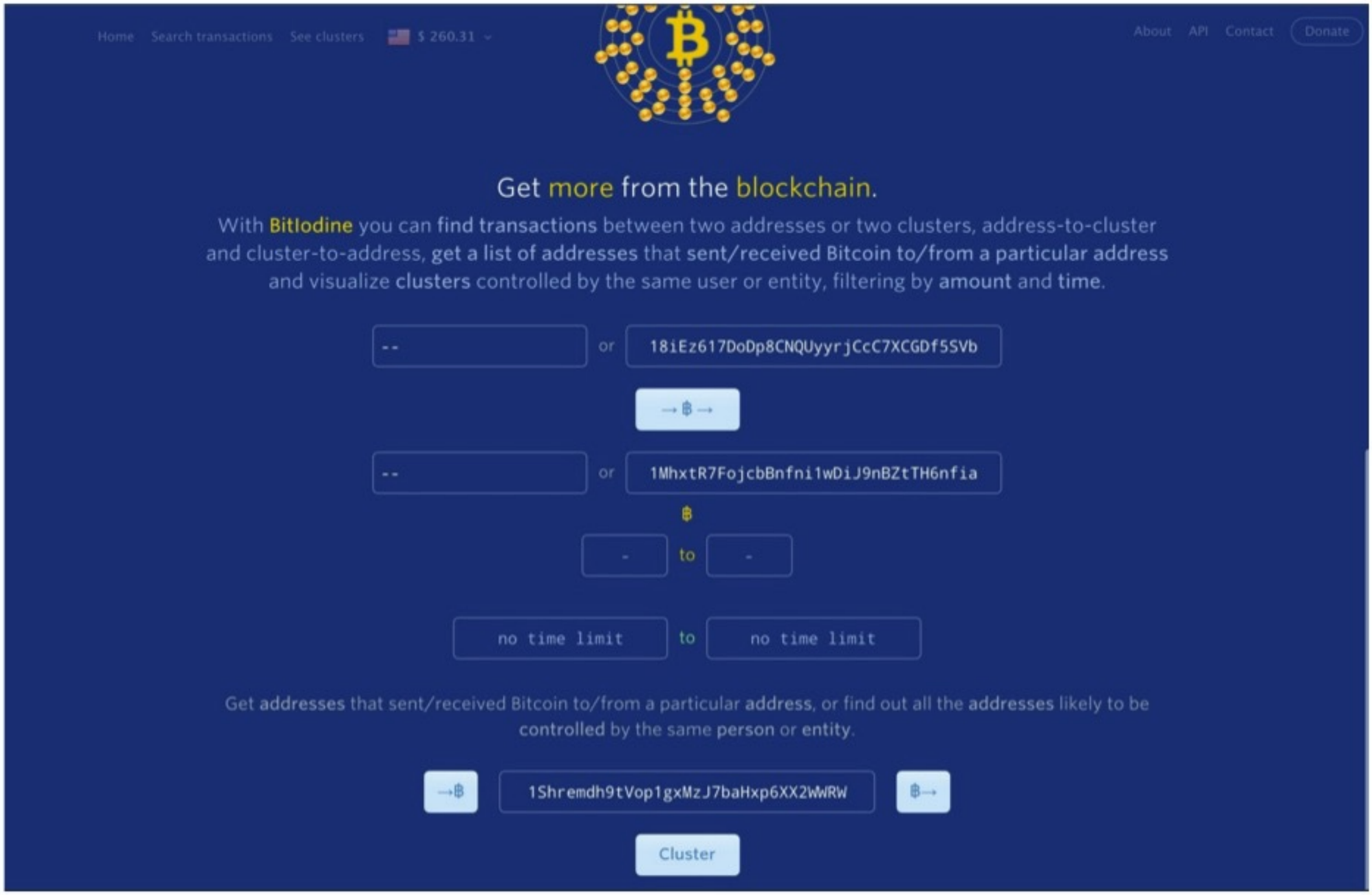
Relayed by IP	24.165.94.91 (whois)	BLOCKCHAIN info
Visualize	View Tree Chart	

Network Propagation (Click to view)

Tool per Bitcoin Forensics: Bitlodine

- Spagnuolo, Maggi, Zanero
- Permette di identificare:
  - Transazioni tra due indirizzi o due cluster, da indirizzo a cluster, da cluster a indirizzo
  - Lista di indirizzi che hanno inviato/ricevuto Bitcoin verso/da un particolare indirizzo
  - Visualizzare cluster controllati dallo stesso utente o entità (filtrando per importo e periodo)
- Utilizza una copia della blockchain, fa crawl di siti di scambio bitcoin, clusterizza indirizzi in wallet, analizza change address o txin multiple che vanno in un txout

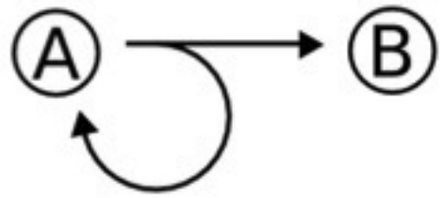
Tool per Bitcoin Forensics: Bitlodine



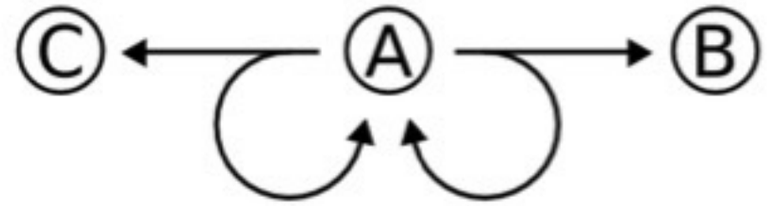
Bitcoin forensics e change address

- Sicurezza: una volta che un indirizzo è stato usato per versare bitcoin non dovrebbe più essere riciclato (anche per questioni matematiche)
- Privacy: non si sa a chi hai pagato ed è più complesso risalire al balance del tuo wallet

- Stesso change address

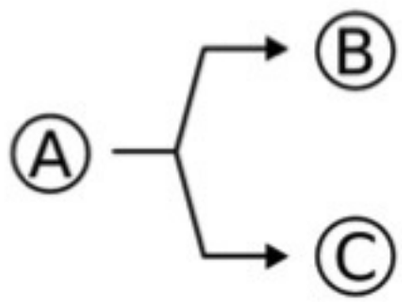


A paid B

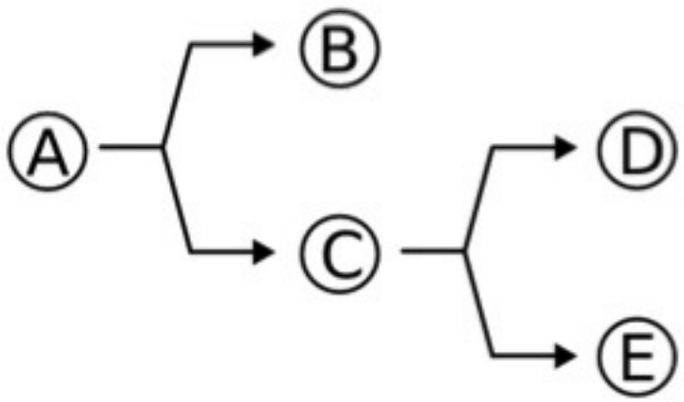


A paid B **and** C

- Change address diverso



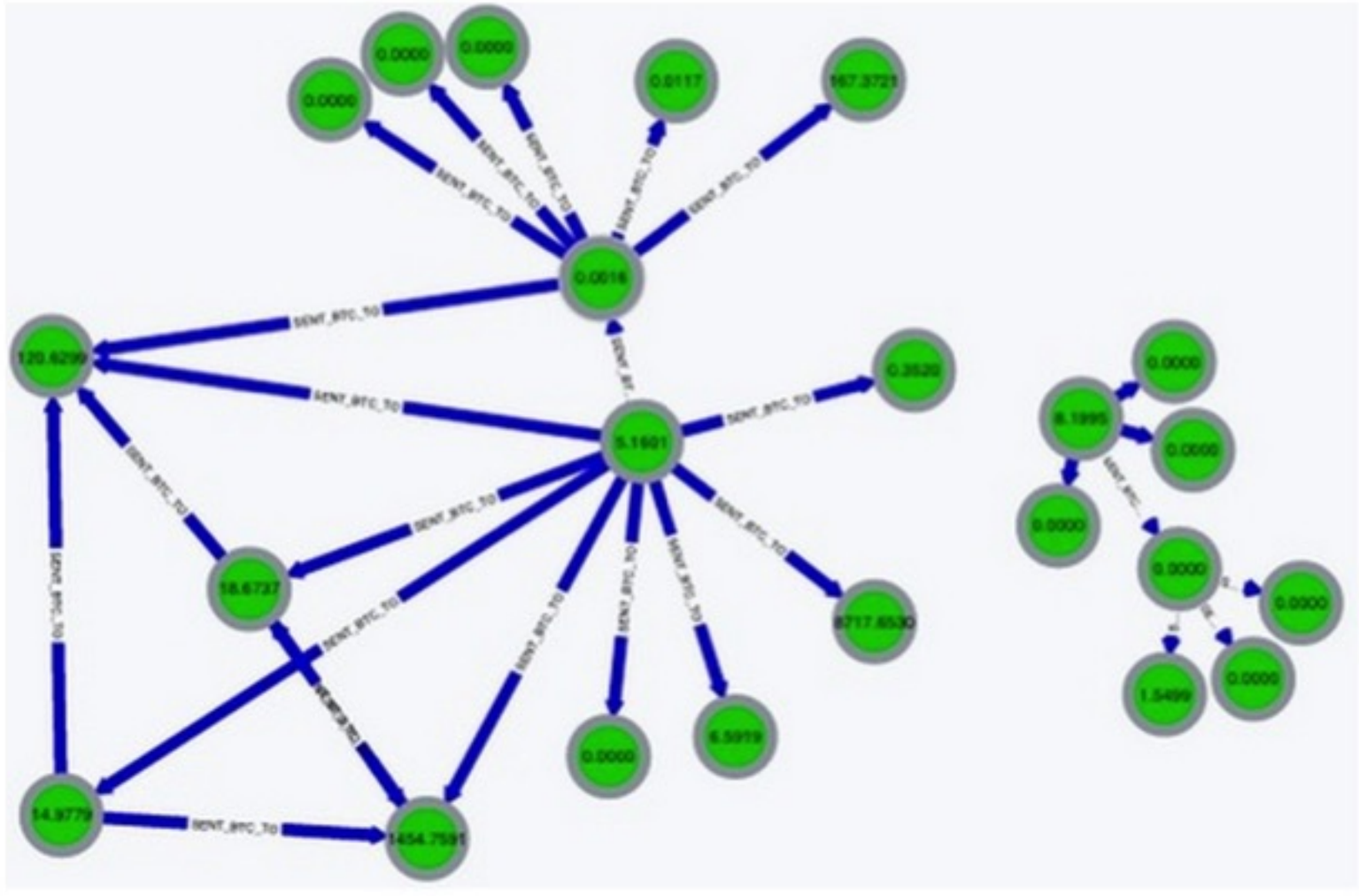
A paid (B **and/or** C)



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

Strumenti: Bitcoin forensics (network)

- Blockr.io
- Blockchain.info
  - taint analysis
- Blockexplorer
- Coinalytics
  - Tracker
  - explorer



Strumenti: Bitcoin forensics (disk)

- 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 (!)

Agenda

- Presentazione relatore
- Il protocollo Bitcoin e la blockchain
- Anonimato, mixer, exchange e cash out
- Sicurezza e rischi del protocollo
- Bitcoin Forensics e indagini sulle criptomonete
- Le evoluzioni del sistema: Smart Contract e Public Notary
- Il futuro del Bitcoin
- Q&A
- Bibliografia & sitografia

Smart Contract

- Il Bitcoin non serve solo come rete di pagamenti
- Possibilità di “programmare” dei contratti intelligenti
- Es. Oraclize, assicurazione sui viaggi
- Evoluzione del Bitcoin verso gli Smart Contract: ETH
- Gestione di asset reali con il Bitcoin: colored coin (es. biglietti del cinema, coupon, noleggio auto)

Public Notary

- La Blockchain è un registro pubblico e immutabile
- Può contenere dati che attestano l'esistenza di altri
  - Hash di documenti
  - Contratti
- Eternity Wall
- Proof of Existence
- CryptoPublicNotary

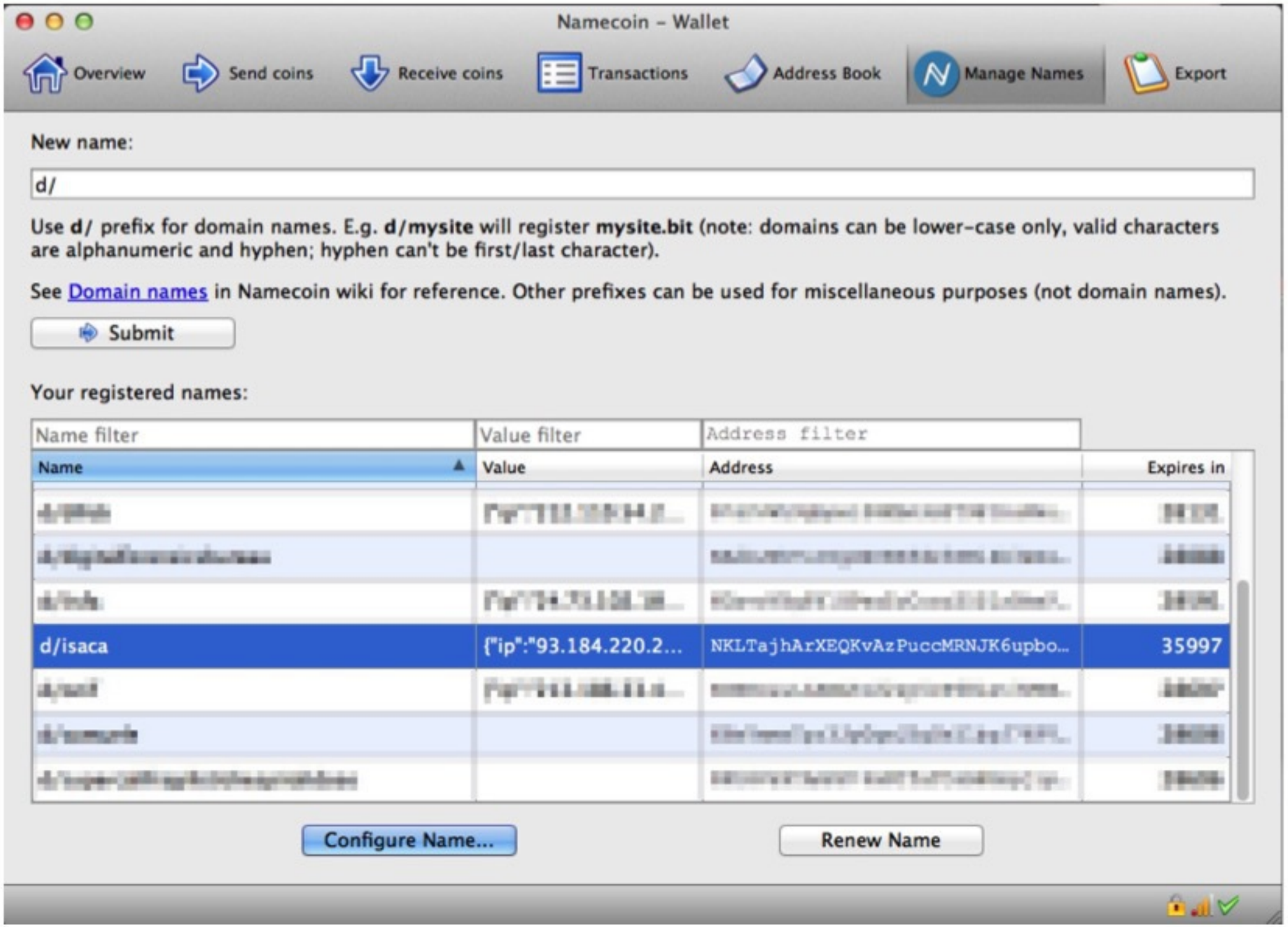
Oltre le transazioni economiche…

- 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 = 0.21 EUR
  - Registrazione: 0.2 NMC (meno di centesimo di €)
  - 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

Oltre le transazioni economiche…



Oltre le transazioni economiche…

Name d/isaca (isaca.bit)

Summary

Status	Active
Expires after block	273952 (35997 blocks to go)
Last update	2015-07-05 21:38:56 (block 237952)
Registered since	2015-07-05 21:38:56 (block 237952)

Current value


```
{
    "ip": "93.184.220.25",
    "translate": "isaca.org.",
    "bitmessage": "Trust in, and value from, information system
s",
    "name": "ISACA",
    "map": {
        "*": {
            "ip": "93.184.220.25"
        }
    }
}
```


Operations

Date/time	Block	Transaction	Operation	Value
2015-07-05 21:38:56	237952	0fcb12d3d7...	OP_NAME_FIRSTUPDATE	{"ip":"93.184.220.25","map":{"*":{"ip":"93.184.220.25"}},"translate":"isaca.org.", "name":"ISACA", "bitmessage":"Trust in, and value from, information systems"}
2015-07-05 19:50:22	237939	3940a210e6...	OP_NAME_NEW	7a0b3d45cf5d4b289240b1e9c0269db634862d76

http://namecha.in/name/d/isaca

Agenda

- Presentazione relatore
- Il protocollo Bitcoin e la blockchain
- Anonimato, mixer, exchange e cash out
- Sicurezza e rischi del protocollo
- Bitcoin Forensics e indagini sulle criptomonete
- Le evoluzioni del sistema: Smart Contract e Public Notary
- Il futuro del Bitcoin
- Q&A
- Bibliografia & sitografia

99BITCOINS
We Translate Bitcoin into Plain English

Seleziona lingua Powered by Google Traduttore

BLOG | GET YOUR FIRST BITCOIN | HOW TO BUY BITCOINS | BITCOIN MINING | TOOLS & RESOURCES

YOU ARE AT: Home » Bitcoin Obituaries: Following Bitcoin While it Dies and Goes Up in Price

Bitcoin Obituaries

Bitcoin has died 101 times

Obituary Stats | Submit Obituary

‘Bitcoin is dead,’ says prominent fintech exec

Daniel Roberts
Daniel Roberts
April 19, 2016

Taavet Hinrikus, CEO of TransferWise, discusses how his company is going after the world's largest financial institutions, one small transaction at a time.

Exactly three months ago, a well-known bitcoin developer, Mike Hearn, wrote a post on Medium that rocked the community of people who believe in the future of the digital currency and its technology. Bitcoin, he wrote, has failed. “It has failed because the community has failed… Worse still, the network is on the brink of technical collapse.” The post led to screaming headlines about the end of bitcoin.

Agenda

- Presentazione relatore
- Il protocollo Bitcoin e la blockchain
- Anonimato, mixer, exchange e cash out
- Sicurezza e rischi del protocollo
- Bitcoin Forensics e indagini sulle criptomonete
- Le evoluzioni del sistema: Smart Contract e Public Notary
- Il futuro del Bitcoin
- Q&A
- Bibliografia & sitografia

Agenda

- Presentazione relatore
- Il protocollo Bitcoin e la blockchain
- Anonimato, mixer, exchange e cash out
- Sicurezza e rischi del protocollo
- Bitcoin Forensics e indagini sulle criptomonete
- Le evoluzioni del sistema: Smart Contract e Public Notary
- Il futuro del Bitcoin
- Q&A
- Bibliografia & sitografia

Bibliografia & Sitografia

- *“Mastering Bitcoin, unlocking digital crypto-currencies”*, Andreas M. Antonopoulos, 12/2014, O-REILLY
- "*Criptovalute e bitcoin: un'analisi giuridica*", 2015, Pagine XVI - 288, Giuffré, http://www.giuffre.it/it-IT/products/24193164.html
- “*Investire Bitcoin*”, Stefano Pepe, Dario Flaccovio Editore
- “*Bitcoin: tra moneta virtuale e commodity finanziaria*”
  - Perugini, Maioli, SSRN 2526207
- *“Bitlodine: Extracting Intelligence from the Bitcoin Network*”, thesis of Michele Spagniuolo
- http://it.bitcoin.it/
- http://www.bitcoinforensics.it

Contatti

Email/Twitter

paolo@dalchecco.it / @forensico

Web

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