Bitcoin Overview

Gabriele Palozzi

Bitcoin - Idea

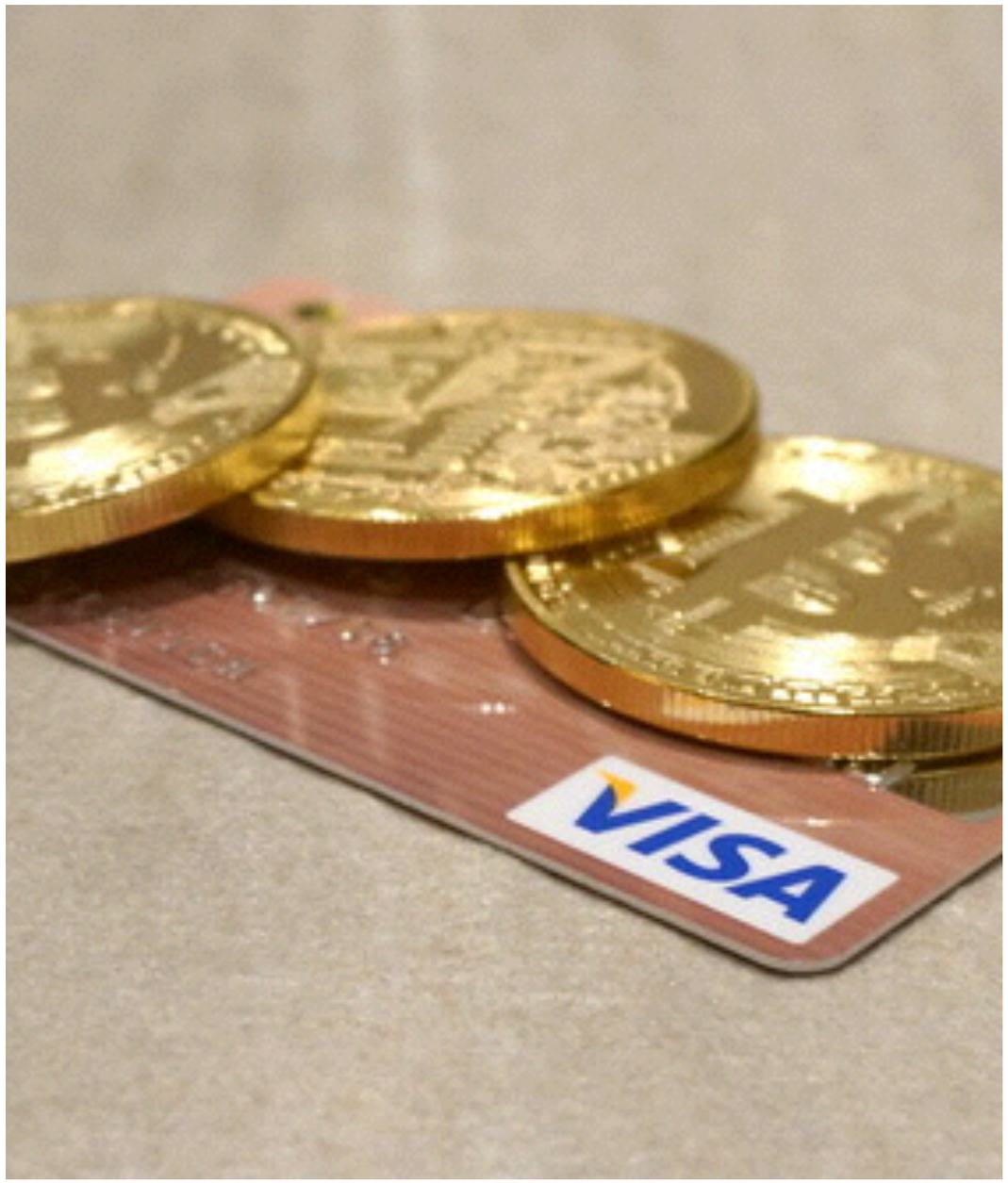
- 21 milioni di monete

  (raggiungibili nel 2140)

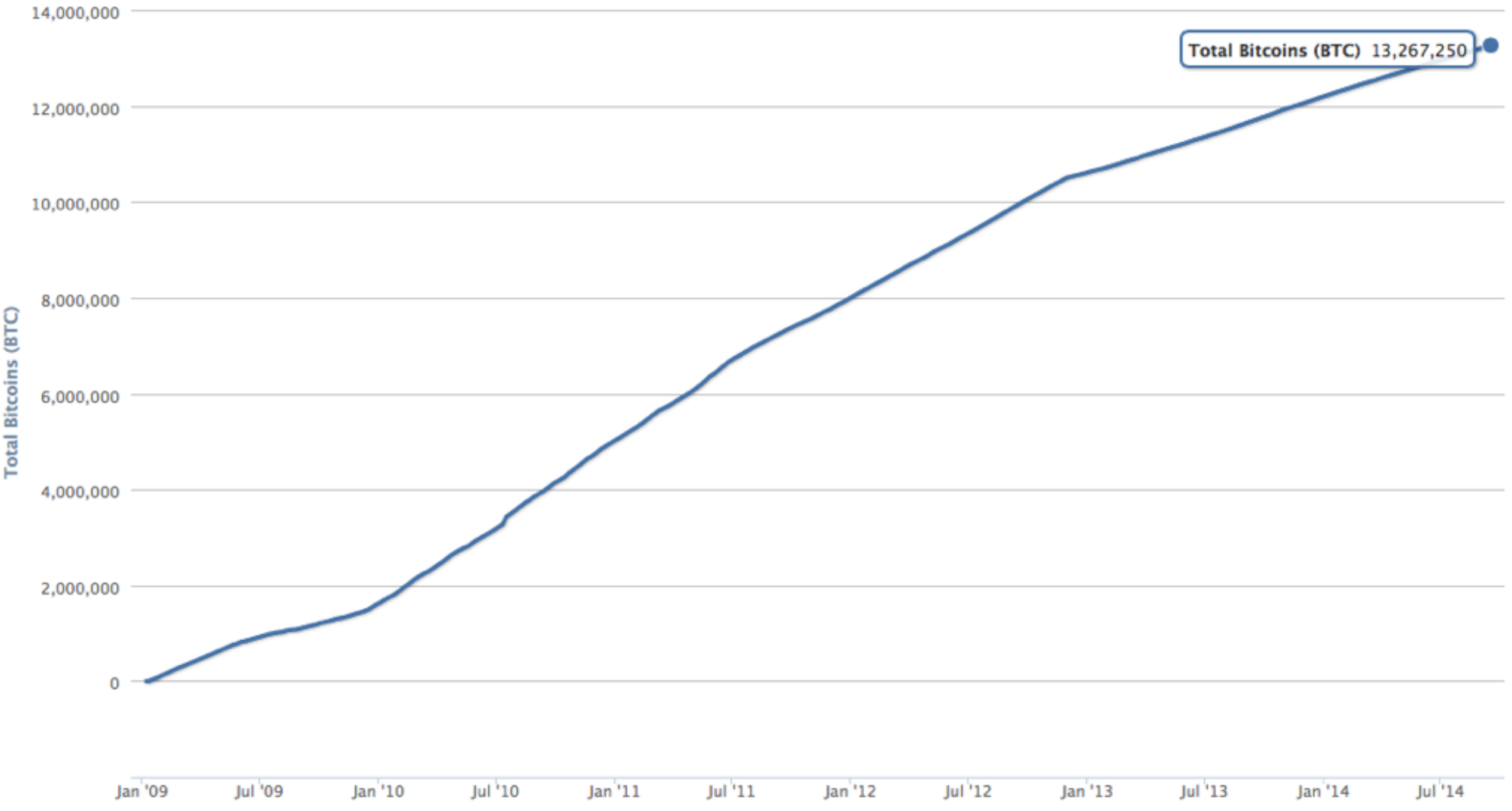
- Emissione moneta controllata

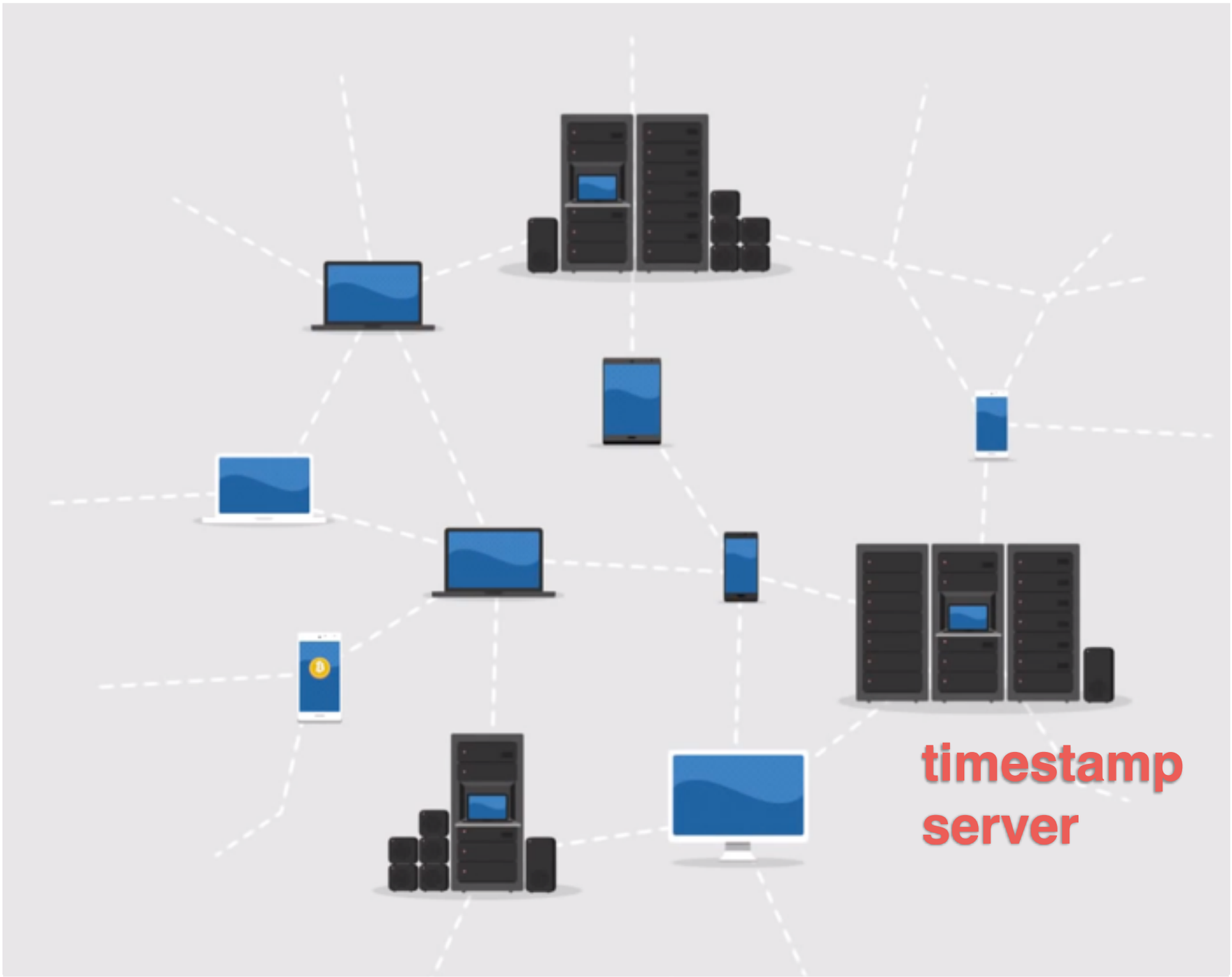
- Nessun sistema centrale

- Anonimato delle transazioni



Bitcoin in circolo





- **Utenti** e **Timestamp Server**
- **Transazioni** tramite chiavi asimmetriche
- **Verifica** corretta transazione
- **Distribuzione** transazione in broadcast

Transazioni

Chiavi asimmetriche (pubblica - privata)

Sistema di firma e verifica

Ogni *bitcoin* è una transazione

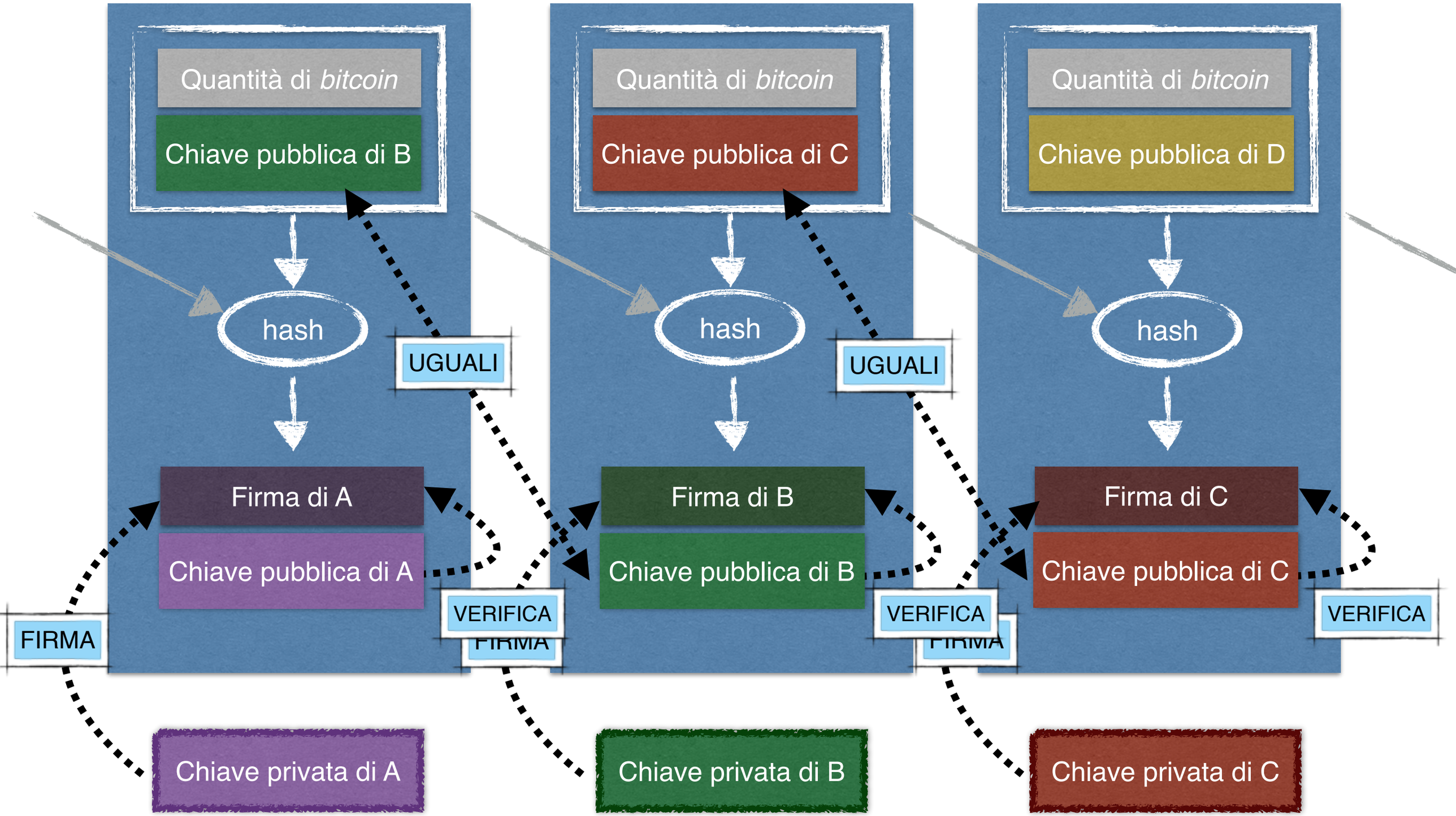
Ogni *bitcoin* è legato ad una transazione precedente

Struttura flessibile

transazione da A a B

transazione da B a C

transazione da C a D



Blocchi

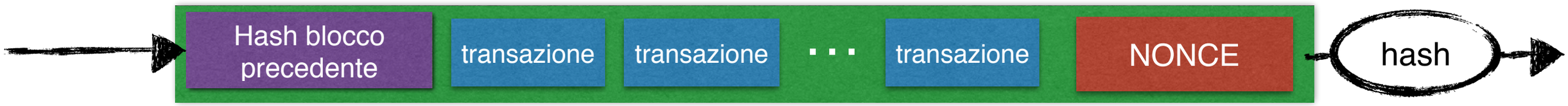
Creati dai timestamp server

Verificano e collezionano transazioni

Richiedono costo computazionale

Distribuiti in broadcast

Blocco



I blocchi sono legati tra loro in una **blockchain**

Proof-of-work: il timestamp server deve trovare un **nonce** che produca un hash inferiore ad un valore target

$$\text{hash}(\texttt{blocco precedente \& nonce}) \leq \texttt{target}$$

Distribuiti in broadcast per essere accettati da almeno il **50% +1** dei timestamp server

I blocchi non accettati vengono scartati nel tempo

Incentivi e limitazioni

Chi produce un blocco accettato riceve *bitcoin*

Inizialmente 50 tbc, ora 25. Ogni 4 anni si dimezza il premio

Per ogni transazione una commissione

La produzione di un blocco deve avvenire in 10 minuti circa

La difficoltà viene incrementata o diminuita ogni 2016 blocchi prodotti

Protocolli crittografici

Più di 100 cryptovalute create con 11 protocolli differenti

	SHA-256	Scrypt	Scrypt-N	CPU-Only	Quark
Algoritmo crittografico	Secure Hash Algoritm	Funzione di derivazione chiave	Adaptive N-Factor	Catene di numeri primi	6 funzioni hash differenti
Principali monete	Bitcoin	Litecoin, Dogecoin	Vertcoin	Primecoin	Quarkcoin

Ecosistema

Consumatori

Venditori

Minatori

Mercati di scambio

Governi

Il prezzo del Bitcoin

Acquirente & Venditore

Vantaggi

- Commissioni minime
- Nessun intermediario
  Banche, conto corrente, carte di credito
- Completo anonimato per acquirente e venditore
- Costo infrastrutture nullo
  Nessun POS

Bancomat Bitcoin - Roma Termini

Acquirente & Venditore

Svantaggi

- Tempo di attesa
- Chiave privata = portafoglio
- Fiscalità ancora non ben definita
- Completo anonimato per acquirente e venditore
  Deep Web

ybp4oezfhk24hxmb.onion

Hitman Network

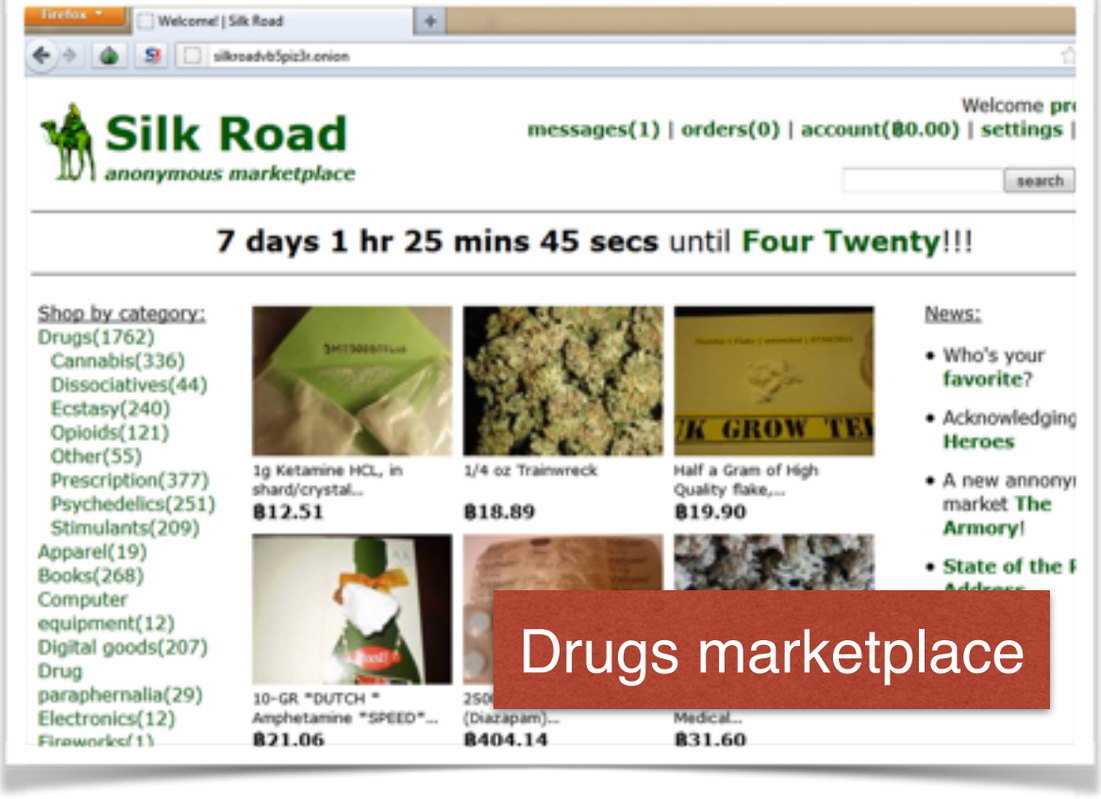
Hitman Network

We are a team of 3 contract killers working in the US (+C
Once you made a "purchase" we will reply to you within 1
within 1-3 weeks depending on target.

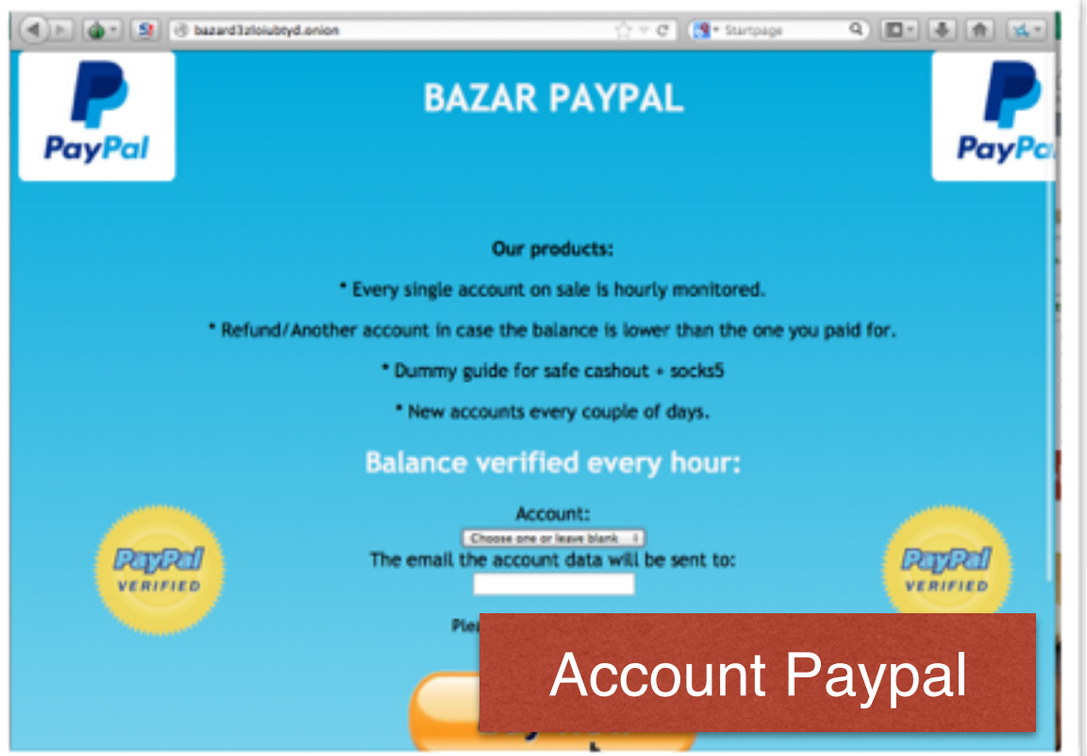
Only rules: no children under 16 and no top 10 politicians.

Product	Price	Quantity
We kill your target in the USA/Canada	10000 USD = 20.679 ฿	1 X Buy now
We kill your target in the European Union	12000 USD = 24.814 ฿	1 X Buy now

Killer



Drugs marketplace



Account Paypal

Miner

Il sogno di produrre moneta da soli

Dal Personal Computer si passa a sistemi più complessi

Monete diverse richiedono hardware diverso

In base all’algoritmo crittografico utilizzato

I Miner scelgono la moneta più profittevole

Miner - Hardware

CPU

GPU

FPGA

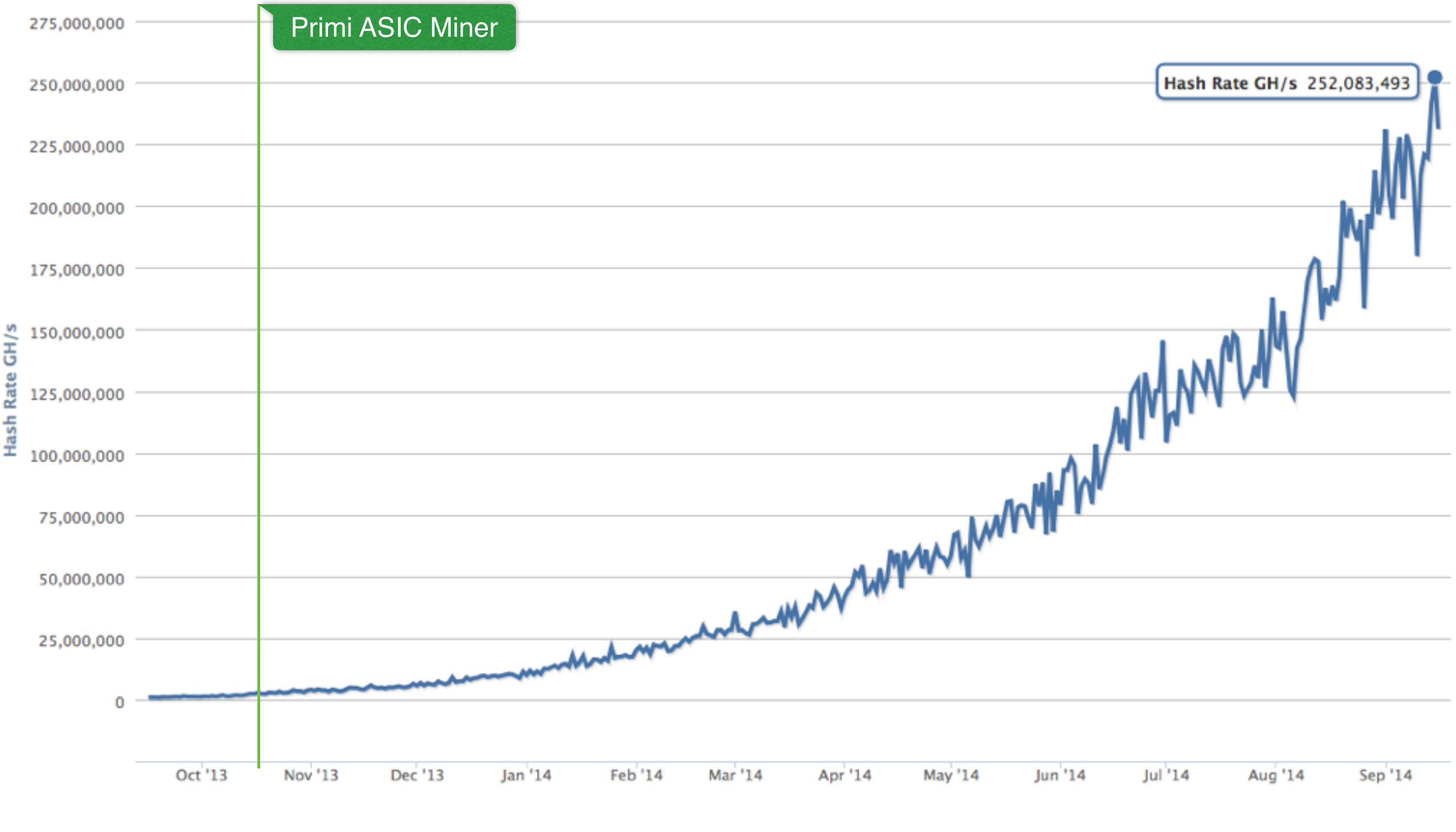
ASIC

L’intento delle nuove *cryptovalute* è di arginare la corsa al nuovo hardware

Il profitto di un miner è dato dall’**hashrate** generato

Anche il **consumo di elettricità** dell’hardware influenza la profittabilità di un miner

Hashrate globale Bitcoin



GPU Miner


FPGA Miner

Ecoinomist

eMunie, Bitcoin & Litecoin Analyst

GPU Miner

ASIC Miner

KnCMiner ASIC Mining farm

Miner - Software

Le **Pool** sono gruppi di miner che lavorano sulla produzione dello stesso blocco

Il premio è suddiviso in base alla **potenza di calcolo prodotta**

Pool che scelgono la moneta da minare in base alla **profittabilità**

Possono avere delle **commissioni** su ogni blocco prodotto

Politiche diverse di trasferimento del premio

Rendono praticamente impossibile il **mining solitario**

Cloud Mining

Piattaforme di scambio

BTC e

Cryptsy®

coinbase

LocalBitcoins.com

BITFINEX
INVEST IN THE FUTURE

BTer.com

BITSTAMP

kraken

BITTREX

POLONIEX

mintpal

BTC e

Last Price: **464 USD** Low: **460.9049 USD** High: **470 USD**
Volume: **3035 BTC / 1417477 USD** Server Time: **16.09.14 10:58**

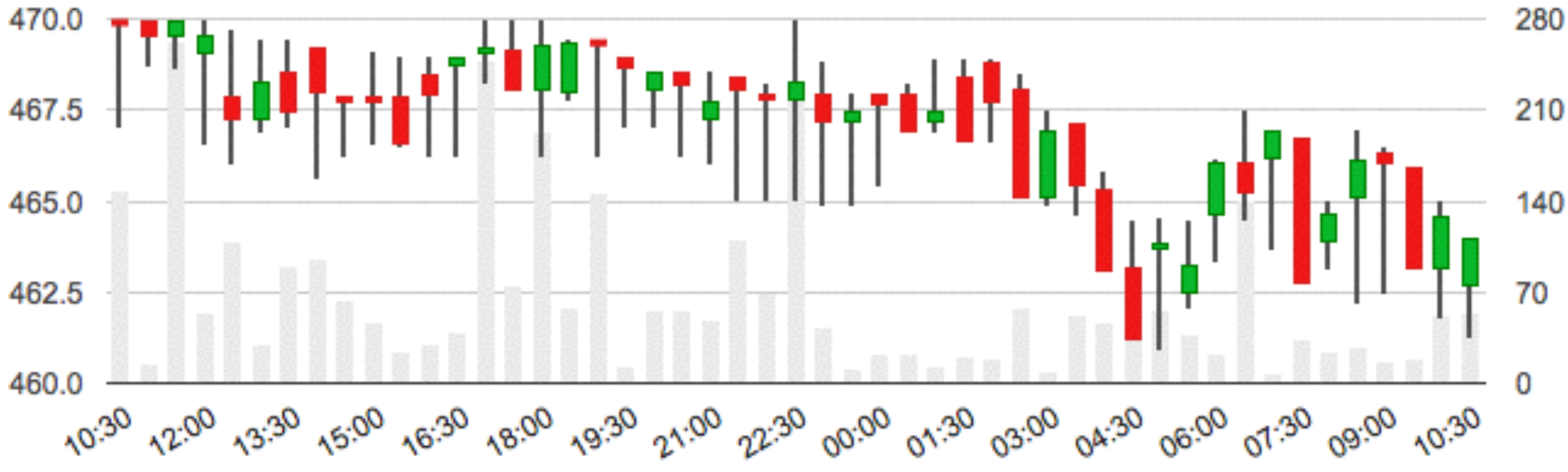
Trade | **News** | **Terms** | **FAQ** | **PAMM**

Latest news:

21/08/14 Profile security settings update 0

15/08/14 **How to protect your account from hacking** 0

BTC/USD 464	BTC/RUR 18839.92	BTC/EUR 373.70662	BTC/CNH 3095.01	BTC/GBP 306.01	LTC/BTC 0.01092	LTC/USD 5.06	LTC/RUR 203.68	LTC/EUR 4.062	LTC/CNH 35.64
LTC/GBP 3.332	NMC/BTC 0.0022	NMC/USD 1.018	NVC/BTC 0.00163	NVC/USD 0.76	USD/RUR 40.13	EUR/USD 1.24438	EUR/RUR 50.12001	USD/CNH 6.75	GBP/USD 1.5114
TRC/BTC 0.00006	PPC/BTC 0.00199	PPC/USD 0.916	FTC/BTC 0.00004	XPM/BTC 0.00052					



Buy BTC

Your balance: **0 USD**

Lowest ask Price **463.999 USD**

Sell BTC

Your bala **0 BTC**

Piattaforma BTC-e

Caso Mt.Gox

Storicamente ha fornito il prezzo più alto di scambio per *bitcoin*

Nel **febbraio 2014** ha interrotto le operazioni bloccando gli account dei propri utenti dichiarando **bancarotta**.

Ad **aprile** ha dichiarato che **850000 bitcoin** erano stati rubati dagli account degli utenti

Hacker, frode o cattiva gestione?

Criticità

- Speculazioni finanziarie
- Sicurezza
- Utilizzo
- Protocollo

Pump & Dump

Tecnica di speculazione finanziaria su azioni di società

Prevede micro-acquisti che tendono ad **aumentare il prezzo** di un bene (azioni, metalli, ecc)

Al raggiungimento di un prezzo fissato viene **venduta in blocco** una ingente quantità del bene

L'anonimato delle transazioni rende difficile l'individuazione dei responsabili di questi fenomeni sulle cryptomonete

E' possibile riconoscere dei pattern specifici

Markus

```
2-6-2013 9:16 - UID: 698630 Type: sell Currency: USD BTC: 31.69415842 Fiat: 3781.11
2-6-2013 9:16 - UID: 698630 Type: sell Currency: USD BTC: 1.40911659 Fiat: 168.11
2-6-2013 9:16 - UID: 698630 Type: sell Currency: USD BTC: 0.79253306 Fiat: 94.55
2-6-2013 9:16 - UID: 698630 Type: sell Currency: USD BTC: 0.54 Fiat: 64.42
2-6-2013 9:16 - UID: 698630 Type: sell Currency: USD BTC: 8.45390963 Fiat: 1008.55
2-6-2013 9:16 - UID: 698630 Type: sell Currency: USD BTC: 49.6 Fiat: 5917.28
2-6-2013 9:16 - UID: 698630 Type: sell Currency: USD BTC: 10.0 Fiat: 1193.0
2-6-2013 9:17 - UID: 698630 Type: sell Currency: USD BTC: 9.7 Fiat: 1157.21
2-6-2013 9:17 - UID: 698630 Type: sell Currency: USD BTC: 16.84 Fiat: 2009.01
2-6-2013 9:17 - UID: 698630 Type: sell Currency: USD BTC: 21.2 Fiat: 2529.16
2-6-2013 9:17 - UID: 698630 Type: sell Currency: USD BTC: 18.07269924 Fiat: 2156.07
2-6-2013 9:17 - UID: 698630 Type: sell Currency: USD BTC: 31.0 Fiat: 3698.3
2-6-2013 9:17 - UID: 698630 Type: sell Currency: USD BTC: 1.0 Fiat: 119.3
2-6-2013 9:17 - UID: 698630 Type: sell Currency: USD BTC: 50.0 Fiat: 5965.0
2-6-2013 9:18 - UID: 698630 Type: sell Currency: USD BTC: 101.66851471 Fiat: 12129.05
2-6-2013 9:18 - UID: 698630 Type: sell Currency: USD BTC: 0.18436186 Fiat: 21.99
2-6-2013 9:18 - UID: 698630 Type: sell Currency: USD BTC: 20.0 Fiat: 2386.0
2-6-2013 9:18 - UID: 698630 Type: sell Currency: USD BTC: 2.5 Fiat: 298.25
2-6-2013 9:18 - UID: 698630 Type: sell Currency: USD BTC: 4.5964668 Fiat: 548.36
2-6-2013 9:18 - UID: 698630 Type: sell Currency: USD BTC: 7.0495 Fiat: 841.01
2-6-2013 9:19 - UID: 698630 Type: sell Currency: USD BTC: 1625.7115664 Fiat: 194624.99
2-6-2013 9:38 - UID: 698630 Type: buy Currency: USD BTC: 1000.00000001 Fiat: 7395.38
2-6-2013 9:38 - UID: 698630 Type: buy Currency: USD BTC: 96.22498428 Fiat: 1728.39
2-6-2013 9:38 - UID: 698630 Type: buy Currency: USD BTC: 107.54895109 Fiat: 1008.23
2-6-2013 9:39 - UID: 698630 Type: buy Currency: USD BTC: 21.0 Fiat: 288.07
2-6-2013 9:39 - UID: 698630 Type: buy Currency: USD BTC: 6.10669614 Fiat: 1626.59
2-6-2013 9:39 - UID: 698630 Type: buy Currency: USD BTC: 1712.52851334 Fiat: 1711.05
2-6-2013 9:39 - UID: 698630 Type: buy Currency: USD BTC: 1218.26221811 Fiat: 2137.32
2-6-2013 9:39 - UID: 698630 Type: buy Currency: USD BTC: 41.3318567 Fiat: 158.78
2-6-2013 9:39 - UID: 698630 Type: buy Currency: USD BTC: 19.60589386 Fiat: 8.08
2-6-2013 9:39 - UID: 698630 Type: buy Currency: USD BTC: 60.0 Fiat: 21.69
2-6-2013 9:39 - UID: 698630 Type: buy Currency: USD BTC: 10.67659713 Fiat: 46.04
2-6-2013 9:39 - UID: 698630 Type: buy Currency: USD BTC: 362.51169969 Fiat: 243.83
2-6-2013 9:39 - UID: 698630 Type: buy Currency: USD BTC: 113.76591175 Fiat: 2.97
2-6-2013 9:39 - UID: 698630 Type: buy Currency: USD BTC: 43.03001695 Fiat: 0.21
2-6-2013 9:40 - UID: 698630 Type: buy Currency: USD BTC: 9.785 Fiat: 0.03
```

- Serie di micro-acquisti e vendite
- 290000 bitcoin acquistati
- Spesa totale pari a 4 milioni $

Willy

```
29-11-2013 0:07 - UID: 817985 Type: buy Currency: USD BTC: 16.61124644 Fiat: 18709.31
29-11-2013 0:12 - UID: 817985 Type: buy Currency: USD BTC: 17.49854918 Fiat: 19402.8
29-11-2013 0:20 - UID: 817985 Type: buy Currency: USD BTC: 12.01301395 Fiat: 13346.46
29-11-2013 0:30 - UID: 817985 Type: buy Currency: USD BTC: 14.04190796 Fiat: 15172.05
29-11-2013 0:33 - UID: 817985 Type: buy Currency: USD BTC: 18.03482617 Fiat: 19785.76
29-11-2013 0:38 - UID: 817985 Type: buy Currency: USD BTC: 10.02069695 Fiat: 11011.54
29-11-2013 0:47 - UID: 817985 Type: buy Currency: USD BTC: 16.80501168 Fiat: 18256.07
29-11-2013 0:56 - UID: 817985 Type: buy Currency: USD BTC: 13.46333525 Fiat: 15078.58
29-11-2013 1:01 - UID: 817985 Type: buy Currency: USD BTC: 14.60390798 Fiat: 16324.46
29-11-2013 1:10 - UID: 817985 Type: buy Currency: USD BTC: 18.89383201 Fiat: 21909.61
29-11-2013 1:15 - UID: 817985 Type: buy Currency: USD BTC: 12.63500728 Fiat: 14339.39
29-11-2013 1:21 - UID: 817985 Type: buy Currency: USD BTC: 15.36861265 Fiat: 17395.3
29-11-2013 1:30 - UID: 817985 Type: buy Currency: USD BTC: 13.69985504 Fiat: 15469.14
29-11-2013 1:40 - UID: 817985 Type: buy Currency: USD BTC: 16.24860284 Fiat: 18411.35
29-11-2013 1:46 - UID: 817985 Type: buy Currency: USD BTC: 13.08811052 Fiat: 14901.38
29-11-2013 1:53 - UID: 817985 Type: buy Currency: USD BTC: 15.95674773 Fiat: 18116.97
29-11-2013 2:01 - UID: 817985 Type: buy Currency: USD BTC: 13.37224115 Fiat: 15224.97
29-11-2013 2:10 - UID: 817985 Type: buy Currency: USD BTC: 19.88618992 Fiat: 22699.37
29-11-2013 2:16 - UID: 817985 Type: buy Currency: USD BTC: 14.53897264 Fiat: 17228.68
29-11-2013 2:24 - UID: 817985 Type: buy Currency: USD BTC: 13.06074749 Fiat: 15496.65
29-11-2013 2:31 - UID: 817985 Type: buy Currency: USD BTC: 17.2701824 Fiat: 20845.52
29-11-2013 2:40 - UID: 817985 Type: buy Currency: USD BTC: 12.01285719 Fiat: 14394.19
29-11-2013 2:46 - UID: 817985 Type: buy Currency: USD BTC: 19.62848432 Fiat: 23689.59
29-11-2013 2:51 - UID: 817985 Type: buy Currency: USD BTC: 13.97077125 Fiat: 16812.95
29-11-2013 2:59 - UID: 817985 Type: buy Currency: USD BTC: 19.77464431 Fiat: 23685.61
29-11-2013 3:09 - UID: 817985 Type: buy Currency: USD BTC: 10.17565522 Fiat: 12203.29
29-11-2013 3:16 - UID: 817985 Type: buy Currency: USD BTC: 11.89824686 Fiat: 14354.39
29-11-2013 3:22 - UID: 817985 Type: buy Currency: USD BTC: 16.92208158 Fiat: 20475.47
29-11-2013 3:30 - UID: 817985 Type: buy Currency: USD BTC: 18.01251461 Fiat: 21922.58
29-11-2013 3:30 - UID: 817985 Type: buy Currency: USD BTC: 10.02355348 Fiat: 12202.57
29-11-2013 3:40 - UID: 817985 Type: buy Currency: USD BTC: 11.82919942 Fiat: 14420.03
29-11-2013 3:49 - UID: 817985 Type: buy Currency: USD BTC: 16.60023461 Fiat: 20132.04
29-11-2013 3:55 - UID: 817985 Type: buy Currency: USD BTC: 15.49602936 Fiat: 18765.48
29-11-2013 4:01 - UID: 817985 Type: buy Currency: USD BTC: 17.65075674 Fiat: 21445.28
29-11-2013 4:07 - UID: 817985 Type: buy Currency: USD BTC: 18.53672501 Fiat: 22522.71
29-11-2013 4:16 - UID: 817985 Type: buy Currency: USD BTC: 18.75286685 Fiat: 22811.56
```

- Serie di micro-acquisti
- Per ogni periodo 2,5 milioni di $ spesi
- 270000 bitcoin acquistati
- Spesa totale pari a 112 milioni $

Pump & Dump


"Willy" & "Markus"
1150
1100
1050
1000
950
900
850
800
750
700
650
600
550
500
450
400
350
300
250
200
150
100
50
12.75
200000
150000
100000
50000
0
2013
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
2014
Feb
Mar
Apr
May
Now

Pump & Dump

Il prezzo del *bitcoin* è fortemente influenzato da queste operazioni

Gli account che mettono in atto queste operazioni sono temporanei

Stranamente non risentono di **downtime** del network

Effettuano un cambio di valuta **da yen a dollari**

Coincidono con le **bolle di Aprile e Novembre 2013**

Wallet

Il proprio **Wallet** di *cryptomonete* diventa un vero portafoglio

Chi ha la chiave privata è proprietario della moneta

Wallet nel cloud possibile soluzione. Ma c’è da fidarsi?

Soluzione: ente di autorizzazione per i trasferimenti. Doppia firma per le transazioni

Pool > 50% +1

Ha raggiunto il **55%** dell'hashrate nel giugno 2014 per almeno 24h

Possibile riscrittura della storia del bitcoin

Nessun vincolo per le pool nel protocollo

Soluzioni: Two Phase Proof of Work, Multi-PPS

100 cryptomonete

Variano protocollo di crittografia, tempo di produzione di un blocco e aggiornamento difficoltà

Miner mossi solo dalla moneta più profittevole

Mercati con poca liquidità sono a rischio Pump&Dump

	Crypto Currency Current Profitability Position		Current Difficulty 14 Day Difficulty Chart	Est. Coins (Current / 24 Hr Avg)
1	JackpotCoin (JPC) **Network Hashrate:** 6.05 GH/s **Block Reward:** 13,508.517175 **Blocks:** 773,771 **Block Time:** 2.00 minute(s)	JHA	140.6519 +20.44 %	27,048.5481 / 33,997.2830
2	WankCoin (WKC) **Network Hashrate:** ? **Block Reward:** 50.00 **Blocks:** 55,123 **Block Time:** 10.00 minute(s)	SHA-256	5,809,809.6179 -25.13 %	0.1731 / 0.1296
3	Battlecoin (BCX) **Network Hashrate:** 3.14 TH/s **Block Reward:** 50.00 **Blocks:** 213,844 **Block Time:** 2.00 minute(s)	SHA-256	69,232.4096 -30.00 %	14.5283 / 10.1698
4	Peercoin (PPC) **Network Hashrate:** ? **Block Reward:** 86.36661851 **Blocks:** 132,992 **Block Time:** 10.00 minute(s)	SHA-256	179,656,365.3445 +0.44 %	0.0097 / 0.0097
5	Bitcoin (BTC) **Network Hashrate:** 231.52 PH/s **Block Reward:** 25.00 **Blocks:** 320,940 **Block Time:** 10.00 minute(s)	SHA-256	29,829,733,124.0404 0.00 %	0.0000 / 0.0000
6	TEKcoin (TEK) **Network Hashrate:** 15.78 TH/s **Block Reward:** 1.00 **Blocks:** 543,128 **Block Time:** 1.00 minute(s)	SHA-256	259,924.1738 -7.64 %	0.0774 / 0.0715
7	OpenSourcecoin (OSC) **Network Hashrate:** 2.56 TH/s **Block Reward:** 12.50 **Blocks:** 524,651 **Block Time:** 1.00 minute(s)	SHA-256	41,370.7245 +4.47 %	6.0781 / 6.3623

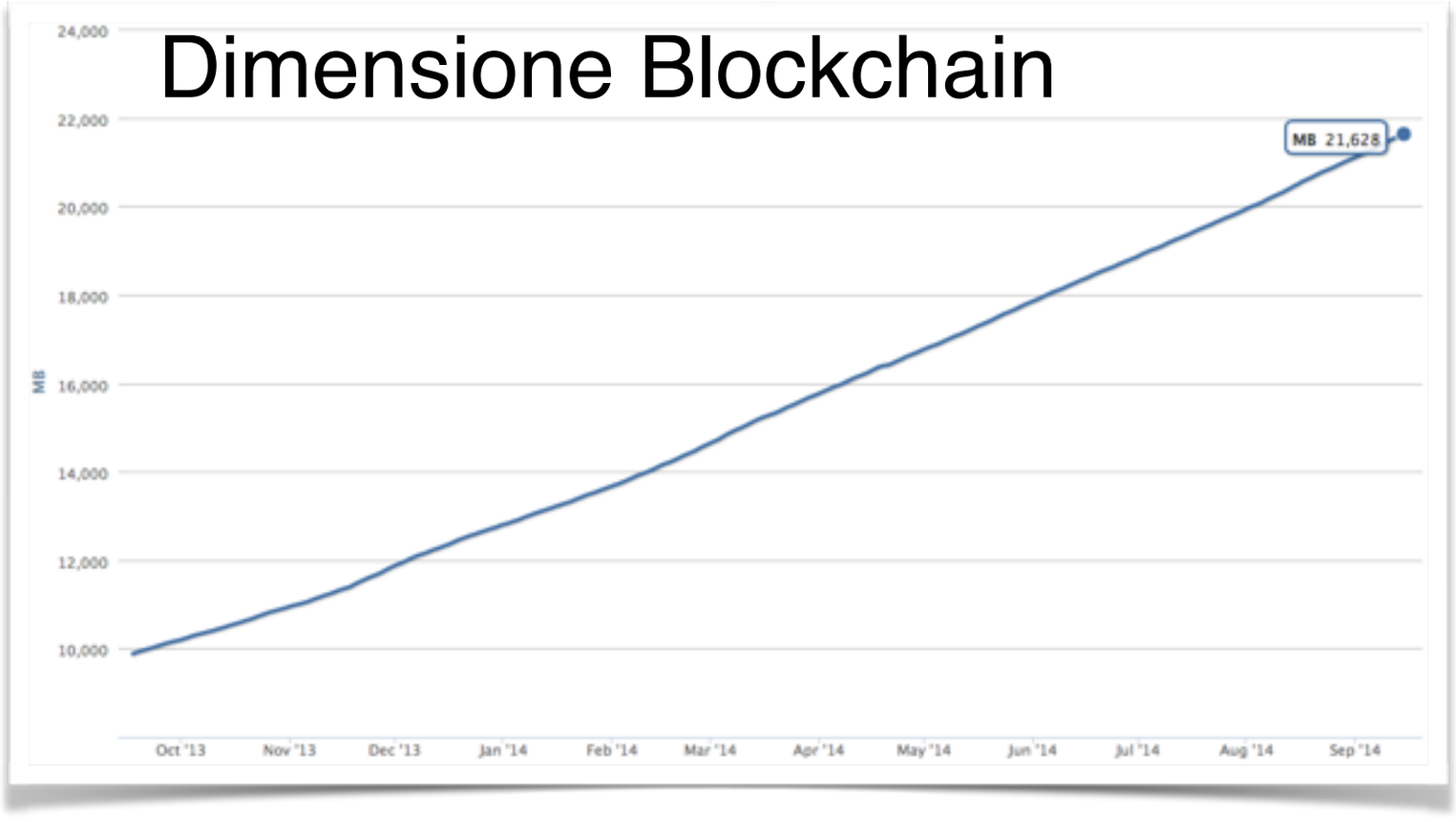
Il protocollo

6 blocchi per avere piena conferma di una transazione = 1 ora

Risorse fisiche ed energetiche sprecate

ENERGIA

125 GigaWatt/s



Evoluzione

- Protocollo
- Commerciale
- Anti-Speculazione

Protocollo green

Sfruttare potenza di calcolo e risorse fisiche per bene comune

Modifiche che migliorino il bitcoin e che non aggiungano nuove monete

Diminuire la quantità di energia utilizzata dal protocollo

Permacoin

Concedere spazio di
archiviazione invece di risolvere
puzzle crittografici

Minore spreco di energia

Proof of Retrievability

Possibilità di distribuire la Libreria
del Congresso americano
circa 2000 TB

Pagamenti sicuri

Sviluppo **protocolli** di pagamento **sicuri**

Protezione per **wallet con crittografia**

Wallet con **firma digitale**

Protocolli per **backup chiavi private**

Mining attivo

Eliminare il mining passivo

Legare il mining ad un’attività

Evitare la corsa all’ASIC limitando a CPU la possibilità di mining

Rivedere il concetto di pool

Game Mining

Le copie pirata di Watch Dogs sui siti di torrent includono un malware che mina Bitcoin (PC)

di *Rosario Grasso*, pubblicata il 27 Maggio 2014, alle 09:01

"Questo malware usa la capacità di calcolo di CPU e GPU per permettere dei guadagni in termini di Bitcoin a terzi. "

Il gaming richiede molte risorse di calcolo e di elaborazione grafica

Impossibile il mining passivo

Giocare richiede la presenza di una persona sul computer

Possibile anche in software di grande utilizzo: Office, Spotify, ecc

Social Mining

Sfruttare il tempo passato sui social per minare

Software mining via Javascript

Possibile sfruttare WebCL e WebGL

Bitcoin ha una difficoltà troppo elevata