

Bitcoin, anche in pratica

E un piccolo assaggio di altre novità

Marco Amadori <amadori@inbitcoin.it>
<marco.amadori@gmail.com>

InBitcoin.it

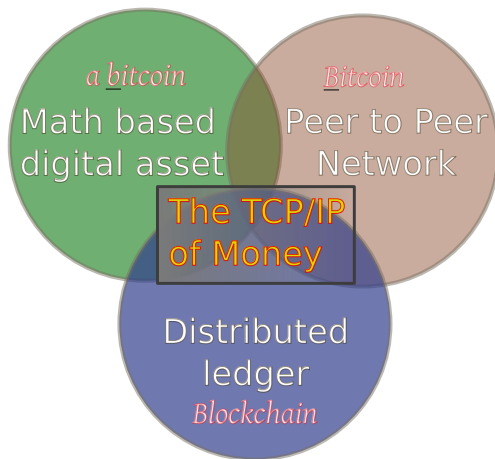
Riva del Garda — 5 Maggio 2015



CONFCOMMERCIO
IMPRESE PER L'ITALIA
TRENTINO

Che cosa è “Bitcoin”

La Valuta, La Rete, La Tecnologia, Il Database



La Valuta

Che cosa è "Moneta"?

Definizioni Aristoteliche

- 1 Dev'essere duratura. La Moneta rimane inalterata nel tempo e agli elementi.
- 2 Dev'essere portabile. Deve valere molto per quanto pesa e ingombrare poco.
- 3 Dev'essere divisibile. Deve essere facile separare e riorganizzare la moneta senza modificarne le caratteristiche fondamentali.
- 4 Deve avere valore intrinseco. Questo valore dev'essere indipendente da altri oggetti e contenuto nella moneta stessa.



La valuta

he cosa è “moneta”?

Definizione più moderna

- Sistema di scambio di valore
- Unità di conto
- Riserva di valore (a breve, a lungo termine)



La valuta

Il Metallo Grigio

“Immaginate un metallo simile all’oro quanto a scarsità di presenza sulla superficie terrestre e quanto a difficoltà di estrazione e con le seguenti proprietà:

- di colore grigiastro, per nulla attraente
- non duttile, non malleabile
- senza funzioni ornamentali o strutturali
- non un buon conduttore, né un buon isolante
- però con una magica proprietà:
può essere trasmesso attraverso un canale di comunicazione.

Satoshi Nakamoto – 27 Agosto 2010



La Valuta

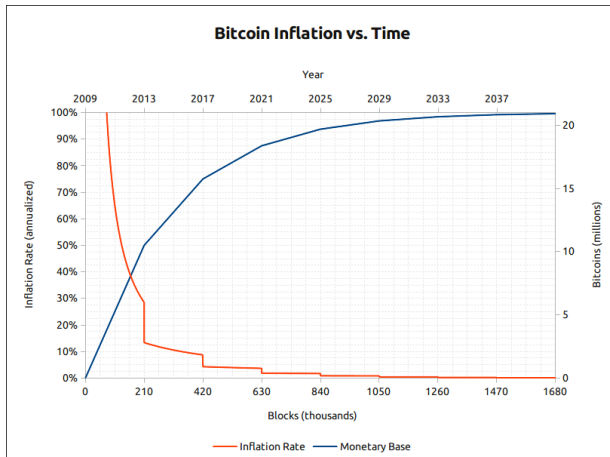
Informazioni economiche

- L'ammontare massimo di bitcoin è pari a 21 M, (ora siamo a ~ 14 M)
- Esistono frazioni di bitcoin, può essere diviso in 100 milionesimi.
- La rete “genera” con il *mining* in media 25 nuovi bitcoin ogni 10 minuti (Ricompensa del blocco o *block reward*)
- La *block reward* è automaticamente dimezzata ogni 4 anni. (210 000 blocchi)
- L'inflazione monetaria è dunque prevedibile con precisione
- 1 BTC = 210 € sui mercati (per auto-arbitraggio)



La valuta

Inflazione monetaria



Un portafoglio di carta

Vis in numeris

Private Key

BIP38 Encrypted



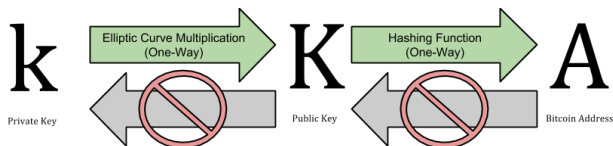
6PRNsJqabLoT73aWNWfSa3hMcX6ML
mx779TPHbKzht4apwqsngkwFcBuKQ

Bitcoin Address



1fbk5AYjA7wLdwbru2CunWEuToBu1USsX

<https://blockchain.info/address/1fbk5AYjA7wLdwbru2CunWEuToBu1USsX>



Crittografia a Curva Ellittica – Sicurezza oltre il Militare, Termodinamica



Tipi di Portafoglio - Wallet Bitcoin

- Online, Proprietario, modello “bancario”, l'utente non ha il controllo delle chiavi segrete
- Online Wallet con controllo delle chiavi private o multifirma `GreenAddress.it`
- Desktop Wallet (PC) – Electrum, Multibit
- Smartphone Wallet – Android Wallet, GreenAddress, Mycelium
- Multi Asset Wallet
- Cold Storage (wallet disconnessi)
- Hardware Wallet (le chiavi private non sono mai esposte)



Come si ottengono bitcoin

- In cambio di beni e servizi, solitamente tramite Payment Processor (es: Video POS NFC)
- Si possono comprare in cambio di Euro o Dollari
 - Su mercati online, via bonifico, es: kraken.com, bitstamp.net
 - Via ricarica postepay o superflash alle poste o al tabacchino, es: bitboat.it
 - Da dei “bancomat” (Bitcoin ATM) come quello di Rovereto presso Ottica Guerra, dove si possono comprare bitcoin in contanti.
- Scambiandoli per altri “crypto asset” o altre monete matematiche
- ~~“Minandoli”, con il proprio computer — hardware specifico~~



Pagamenti in Bitcoin

Come fare ad accettarli?

N.B. Si **emette sempre lo scontrino in euro**, non (ancora) in bitcoin. Poi si sceglie tra 2 opzioni:

- Usando un wallet direttamente, senza intermediari ma richiede know-how.
- Usando un App di un Payment Processor



Pagamenti in Bitcoin

Payment Processor

Pagamenti Euro su Euro

- 1 Il commerciante richiede Euro al cliente su un App (o in altro modo)
- 2 Il Cliente paga “tramite” bitcoin dal cellulare (ma anche tablet, da un dispositivo dedicato bitcoin o dal PC per il commercio online)
- 3 Il servizio di PP vende per lui i bitcoin sul mercato
- 4 Il PP invia entro 1,2 giorni lavorativi un bonifico SEPA sul CC del commerciante ed ottiene Euro in conto corrente pari all'importo richiesto (anche 0% commissioni)



Pagamenti via Bitcoin

Svantaggi

- Richiede (ancora) un accordo commerciale con l'azienda che fornisce il servizio, non Trustless
- I volumi sono ancora bassi



Pagamenti via Bitcoin

Vantaggi

- È sicuro per design – Push Vs Pull
- È ubiquo, disponibile ovunque
- Scherma il negoziante dalla volatilità del bitcoin come valuta
- Ha costi bassi o nulli per il commerciante
- Permette di ricevere pagamenti da una clientela globale
- Cattura per attuale scarsità di offerta il bitcoiner Olandese, Tedesco, Inglese..
- Marketing, Immagine Aziendale
- Permette Innovazione (mesh-network, nfc tags, micropagamenti, nanopagamenti, etc..)



Citazioni a caso

Per prendere fiato

“Il Bitcoin è una notevole conquista crittografica e la capacità di creare qualcosa che non è duplicabile nel mondo digitale ha un valore enorme.”

— Eric Schmidt (ex CEO di Google)

“Non aver avuto una strategia per Internet nel 1995 è equivalente a non avere una strategia per il Bitcoin ora.”

— Moe Levin (CEO di Bitpay Europa)

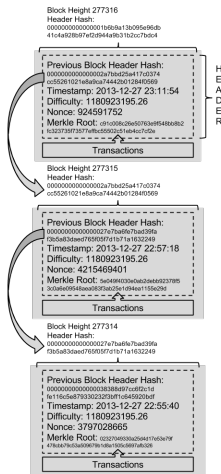
“Entro il 2005 sarà chiaro che l'impatto di Internet sull'economia non sarà stato più grande di quello del fax.”

— Paul Robin Krugman – Nobel Memorial Prize in Economic Sciences (1998)



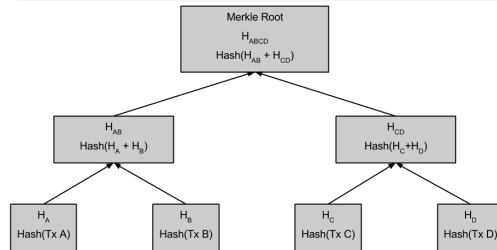
Chain of Blocks

A Distributed Ledger



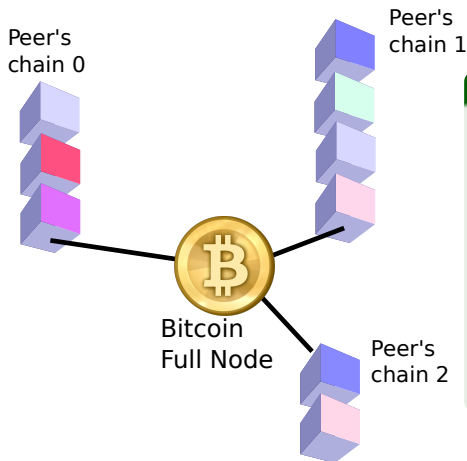
Secure Hash Algorithm – SHA256

The proof of work used in Bitcoin takes advantage of the apparently random nature of cryptographic hashes. A good cryptographic hash algorithm converts arbitrary data into a seemingly-random number.



Consensus via Proof of work

Longest chain wins



The "Work" is called "mining"

- 1 $\text{SHA256}(\text{SHA256}(\text{block header}) + \text{nonce}) < \text{target} ?$
- 2 The Bitcoin Network will reward me (25 BTC)

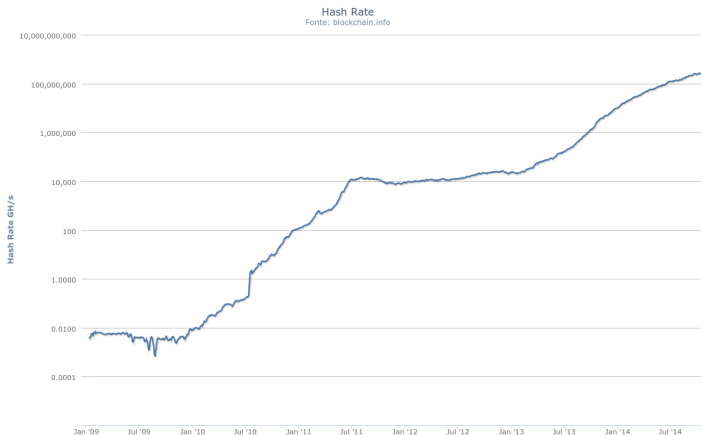
This is a new type of Cryptographic Signature, a **DMMS** — *Dynamic Membership Multi-party Signature*

Difficulty ("inverse" of target) will adapt to global hashrate every ~ 2 weeks (2016 blocks)



Historical Hashrate

Logarithmic Scale



Usage Metrics

Latest quarter

	Quarterly			Last 12 Months	
	Sep-14	Jun-14	Q/Q Δ	Sep-13	Δ
Commerce					
Wallets	6,559,978	5,427,688	21%	1,353,201	5x
Merchants	76,000	63,000	21%	10,000	8x
Merchants' annual revenue (\$bn)	86	29	196%	0	N/A
ATMs	251	103	144%	0	N/A
Unique bitcoin addresses	184,554	136,152	36%	61,734	3x
Industry					
All-time VC investment (\$m)	317.0*	225.3	41%	30.4	10x
Number of VC-backed startups	66*	50	32%	14	5x
Media					
Mainstream media mentions	9,398	9,024	4%	1,794	5x
Technology					
Network Hash Rate (billion/second)	261,900,382	111,194,683	136%	1,213,246	216x
Github no. of updated repositories	18,753	15,109	24%	1,573	12x
Valuation					
Bitcoin market capitalization (\$bn)	5.2	8.3	-37%	1.5	3x

*Includes recent Q4 deals (eg Blockchain \$30.5m).

Sources: CoinDesk, [Blockchain.info](#), [BitcoinPulse](#), [Github](#), [Coin ATM Radar](#). Figures used are as of end of quarter.

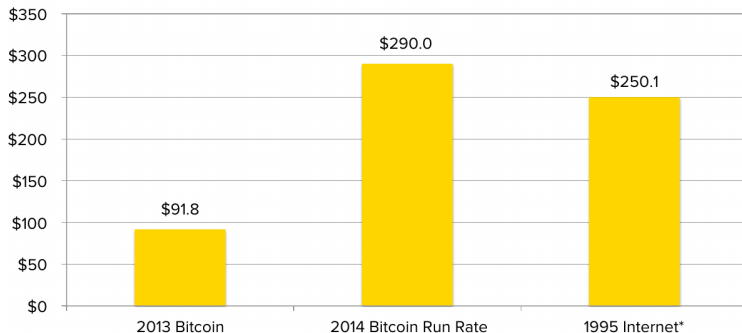
• <http://coinmap.org/>



What is happening?

Status of Venture Capitals

Bitcoin vs Early Internet VC Investment (millions)



*Includes first sequence venture deals but excludes late-stage 1995 internet investments (\$257.6m). For additional disclosure on methodology see <http://www.coindesk.com/following-money-trends-bitcoin-venture-capital-investment/>

Source: CoinDesk, [PricewaterhouseCoopers](#)



Permissionless Innovation

Bitcoin and Internet

- Before Internet, point-to-point communication between computers was available
- You needed a contract or permission from a Telco in order to innovate
- Low level of Innovation, fax-machine, poor video conferences, not much more
- Bitcoin opens an era of financial Innovation (programmable money)
- The Blockchain permits Decentralized Computing
- Internet of Things: IBM's "Adept" will use the Blockchain



Blockchain as DB

Permanent Storage

- You could write important data in the Blockchain (for free or for a small fee)
- What is written in the Blockchain is “forever”
- No one can remove or alter Blockchain information
- Example Application: Proof of Existence, Decentralization of Notary services

<http://www.proofofexistence.com/detail/>

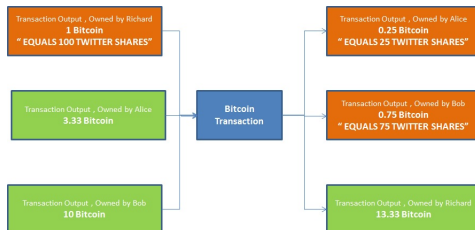
e3c21569e6ba5b488d5c416e8fc6ea166551cf64076f8f337ddc8cc8f9936bc0



Generic Asset Ledger

Coloring Coins

- Tracking bitcoin transaction to allow generic asset trading
- “coloring coins” enables distributed exchanges
- anyone can issue a colored coin



Multisignatures











Enabling Smart Contracts

- Wallets that need more than one signature to send a transaction
- k/n multisignatures are available in Bitcoin since 2012
- Smart Contracts are Trustless Unbreakable Agreements
- Example: micro and nanopayments trustless channels
- Example: decentralized escrow (OpenBazaar is a decentralized Ebay)
- Example: Smart Properties



Crypto currencies

640 currencies should be enough for everyone

#	Name	Market Cap	Price	Available Supply	Volume (24h)
1	 Bitcoin	€ 3.681.775.431	€ 273.33	13,470,025 BTC	€ 11.075.275
2	 Ripple	€ 112.521.946	€ 0.003882	28,989,252,282 XRP *	€ 235.763
3	 Litecoin	€ 97.392.370	€ 2.90	33,563,705 LTC	€ 2.052.311
4	 BitSharesX	€ 27.824.896	€ 0.013913	1,999,883,512 BTSX *	€ 286.588
5	 Dogecoin	€ 17.085.031	€ 0.000180	95,166,195,027 DOGE	€ 392.888
6	 Nxt	€ 16.067.217	€ 0.016067	999,997,096 NXT *	€ 26.691
7	 Peercoin	€ 13.629.943	€ 0.623657	21,854,853 PPC	€ 41.736
8	 Counterparty	€ 9.303.871	€ 3.51	2,647,154 XCP *	€ 31.952
9	 Namecoin	€ 7.163.043	€ 0.705097	10,158,950 NMC	€ 12.924
10	 Darkcoin	€ 6.840.358	€ 1.42	4,832,408 DRK	€ 41.911

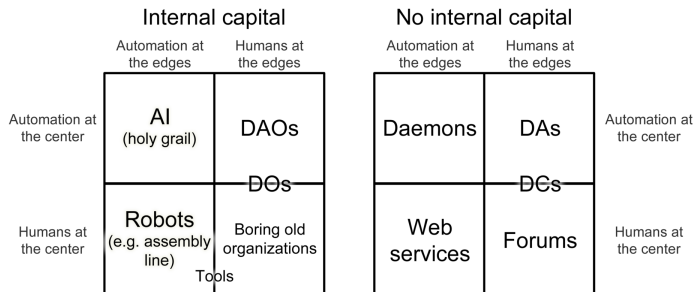
- Initially forks of bitcoin codebase
- Purpose-Specific or Experimental testbed
- Different parameters or hash Algorithm
- Due to being tied to bitcoin, they become real money too (crypto exchanges)
- Less network effect, no real threat to Bitcoin



Appcoins

Ethereum example

- Bitcoin full nodes execute a Non-Turing Complete script (handling of transactions, signatures)
- What if the script is Turing Complete?
- A platform for Smart Contracts <http://www.ethereum.org>
- Distributed Applications
- Distributed Autonomous Corporations



Bitcoin for good

Payment system for developing countries

- 50 % of the world is unbanked
- Kenya: 40 % of GDP is transacted via Mpesa, SMS money
- Remittances: ~400 B\$ market, 8% average fee
- Microcredits



Domande

Dubbi?

- Sicurezza?
- Futuro della tecnologia?
- **Chiedete pure.**

Queste slides

<http://goo.gl/BbzHTT> [github: mammadori, branch “riva”]

Contatti

Marco Amadori <marco.amadori@gmail.com>

<http://inbitcoin.it> — <http://pagoinbit.it>

