

La Blockchain

crittomonete, bitcoin, e altre
applicazioni

Il denaro è ...

una merce di scambio ma non un bene per sé
~~garantito da un corrispettivo in oro o altri beni~~
basato sulla fiducia (che qualcuno lo accetti)

Il denaro è ...

riconoscibile

divisibile

valevole

trasportabile

trasferibile

~~difficile da contraffare~~

il denaro è ...

organizzato in valute nazionali

emesso da autorità riconosciute

legato a vicende politiche

scambiato direttamente solo se contante

scambiato tramite intermediari negli altri casi

Il denaro dovrebbe ...

essere durevole

essere conservabile in modo sicuro

venire emesso in modo stabile e controllato

avere un valore stabile nel tempo

Il Bitcoin ...

è un bene immateriale

ha un valore basato sulla fiducia

puoi scambiarlo con moneta FIAT

non è regolato da un'autorità

Proprietà uniche

E' l'unico pagamento in “contanti” che può avvenire attraverso una rete.

Unico trasferimento di valore che può avvenire interamente dentro la rete

Unico pagamento elettronico che non deve passare da un'autorità intermediatrice

Quanto vale un Bitcoin?

1 Dollaro vale 1 Dollaro

1 Euro vale 1 Euro

1 Bitcoin vale 1 Bitcoin

Bitcoin price (USD) from Coinbase

All



Interest over time



from Google Trends

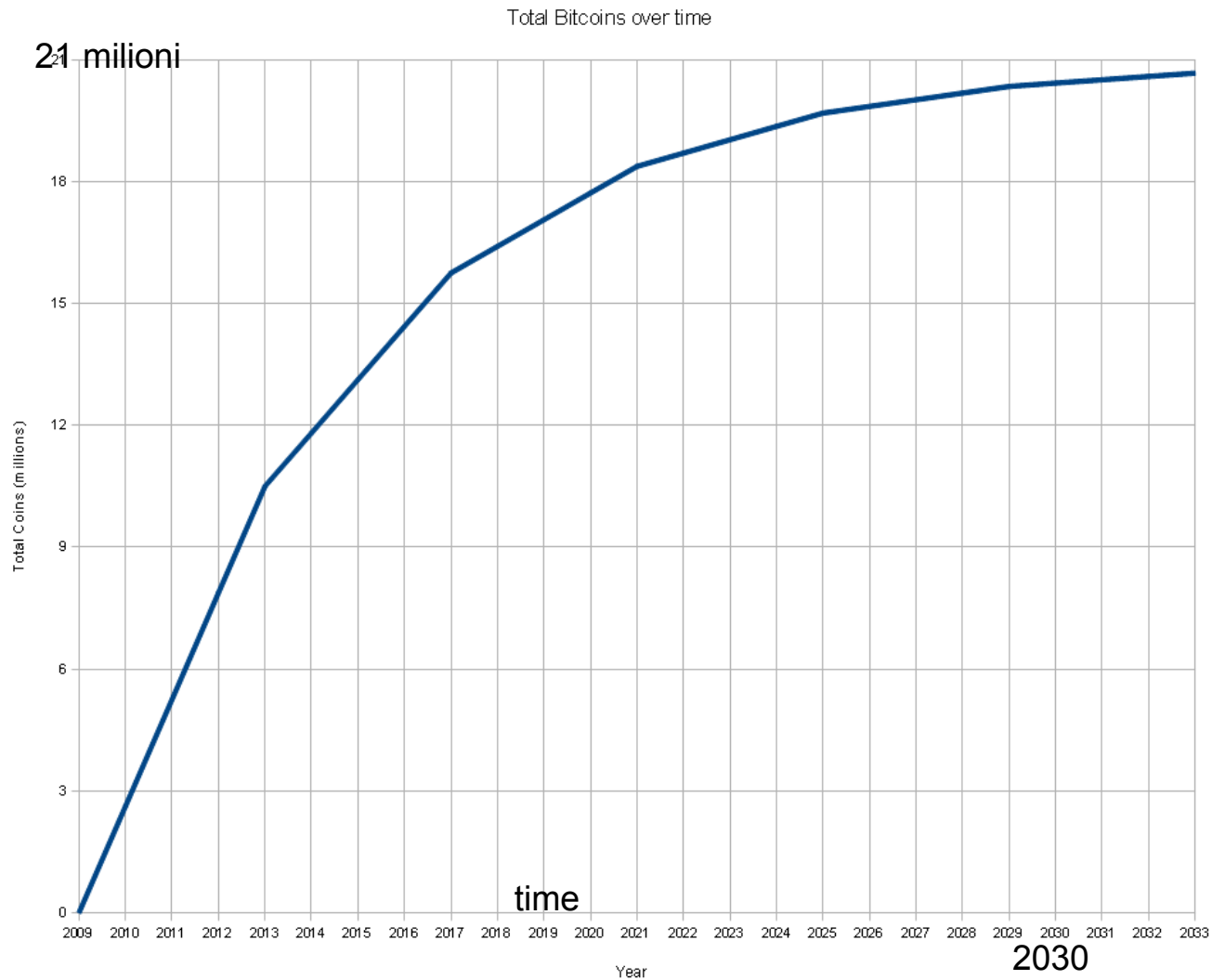
News headlines

Forecast



Quanti?

cap a
21,000,000
circa



Chi è Satoshi Nakamoto?



Chi è Satoshi Nakamoto?

- Un collettivo di Hacker ?



Chi è Satoshi Nakamoto?

- Dorian Satoshi Nakamoto,
- 64 anni
- nippo americano che vive a LA ?

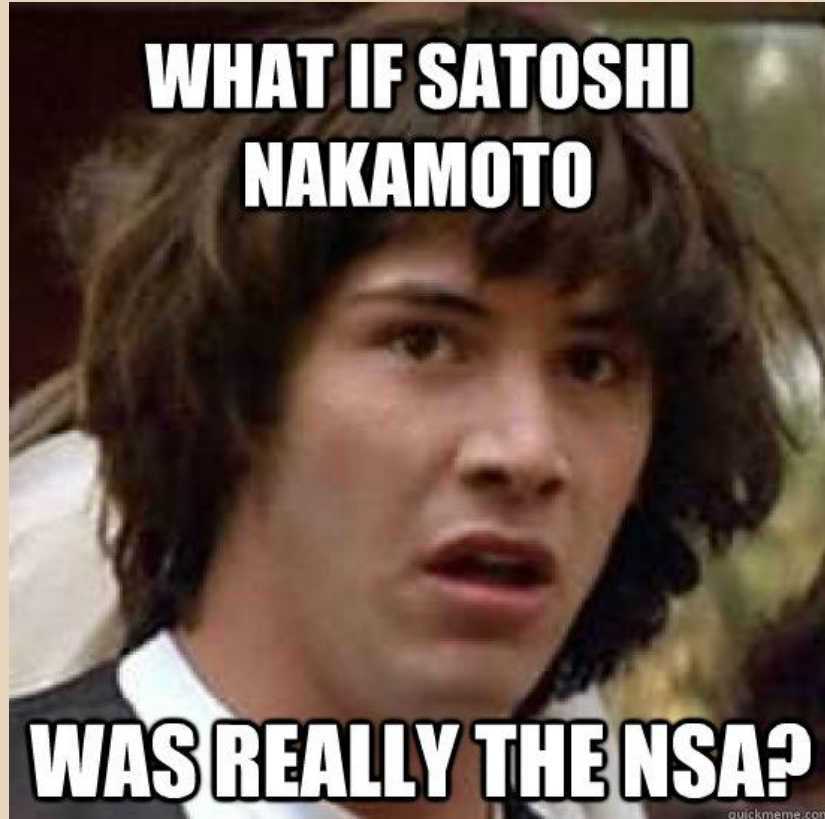


Chi è Satoshi Nakamoto?

- Dorian Satoshi Nakamoto,
- 64 anni
- nippo americano che vive a LA ?



Chi è Satoshi Nakamoto?



Timeline

2008 - paper su Bitcoin, progetto SF, Bitcoin.org

2009 - Bitcoin launch, prima transazione da Satoshi ad Han Finley

2010 - Lazlo acquista una pizza per 10000BTC

Timeline ...

2010 - Nasce MtGox (\$->BTC)

2010 - 1 BTC = 0,50\$

2011 - Bitcoin su TIME

2011 - 1 BTC = 10\$

2011 - Nasce Silk Road

2012 - furto di 50K BTC presso Linode

Timeline ...

2012 - blocco 210,000 la ricompensa scende a 25BTC

2012 - nasce Coinbase

2012 - nasce BoostVC per Bitcoin startups

2012 - nasce la Bitcoin foundation

2012 - Wordpress accetta i Bitcoin

2013 - 1 BTC = 100\$

Timeline ...

2013 - Primo “Bancomat” Bitcoin a San Diego

2013- Coinbase riceve 5M\$ di funding

2013 - FBI “chiude” Silk Road

2013 - A Novembre 1BTC > 1200\$

2013 - La Cina dichiara il Bitcoin illegale

2014 - arresti per riciclaggio

Come guadagno un Bitcoin?

Vendo qualcosa e accetto Bitcoin

Cedo Euro/Dollari in cambio di Bitcoin

Partecipo alla rete e guadagno le commissioni

Partecipo alla rete e conio nuovi Bitcoin

Come ricevo un Bitcoin

Devo avere un indirizzo Bitcoin

Questo indirizzo è associato ad una coppia di chiavi

La chiave privata serve per spendere

Un wallet è un software che gestisce le chiavi

Indirizzo Bitcoin

An example of a Bitcoin address is

3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy

è di fatto la nostra chiave pubblica

Come spendo un Bitcoin

Il wallet usa la chiave privata per firmare una transazione

La transazione viene spedita in rete

...e poi

Come funzionano i Bitcoin?

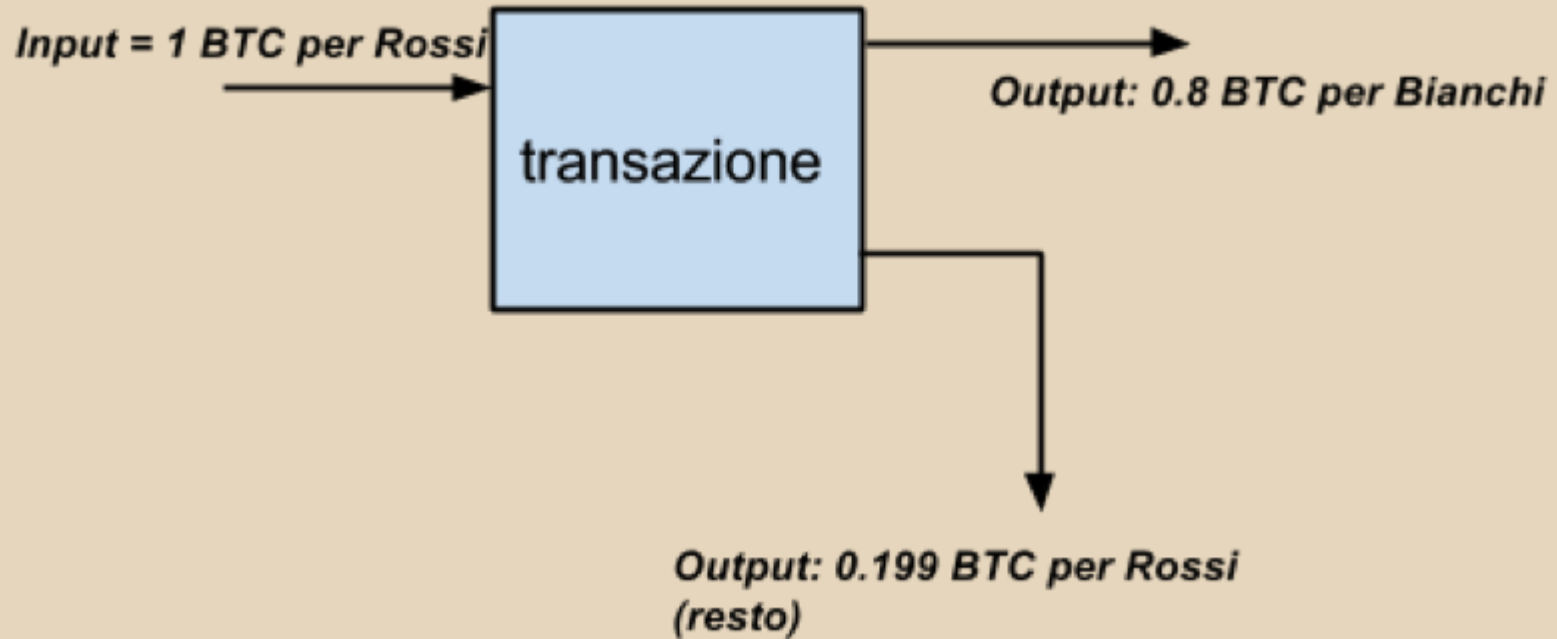
Registro generale delle transazioni

Il registro è **duplicato** in tutti i computer nella rete Bitcoin

Le transazioni sono raccolte in blocchi

Il registro si chiama Blockchain

Transazione



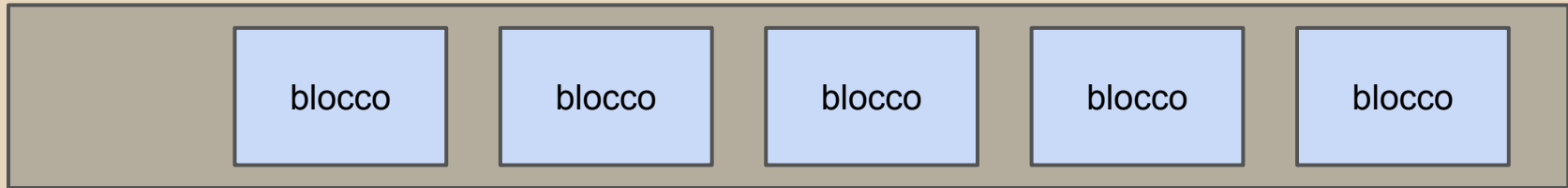
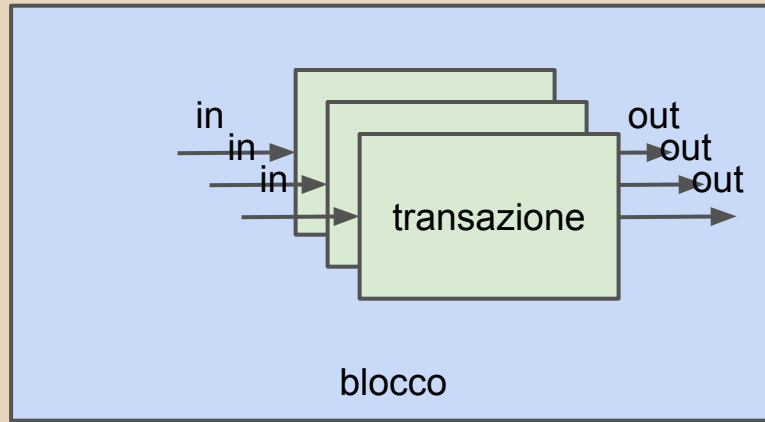
0.001 mancanti sono la “mancia” per chi processa la transazione

Ma chi scrive nella Blockchain

Ogni 10' (in media) qualcuno riesce a risolvere un criptopuzzle detto proof-of-work che gli dà diritto di scrivere un nuovo blocco

Chi scrive un blocco riceve un premio (25BTC)

Ricapitolando



Blockchain

Cos'è la proof-of-work?

~~Permette di scrivere un blocco solo se dimostri di aver fatto una certa quantità “lavoro”~~

Probabilisticamente parlando, puoi scrivere il blocco se hai fatto “tanti” calcoli

Teoricamente parlando, puoi riuscirci al primo tentativo oppure non riuscirci mai

Cos'è la proof-of-work

Es. dati i buffer concatenati **A + nonce**
trovare il **nonce** che genera un hash che inizia
con 10 zeri

$\text{hash}(\text{A+nonce}) = 0000000000345872342642\dots$

FORZA BRUTA!

Minare nuovi Bitcoin

Quindi mediamente ogni 10', l'intera rete riesce a risolvere un blocco e inserirlo nella blockchain.

Se aumentano i partecipanti -> aumenta la difficoltà

Mining

Quindi se accendo il PC e partecipo alla proof-of-work posso coniare dei Bitcoin?

Difficoltà

il tempo medio di generazione di un blocco

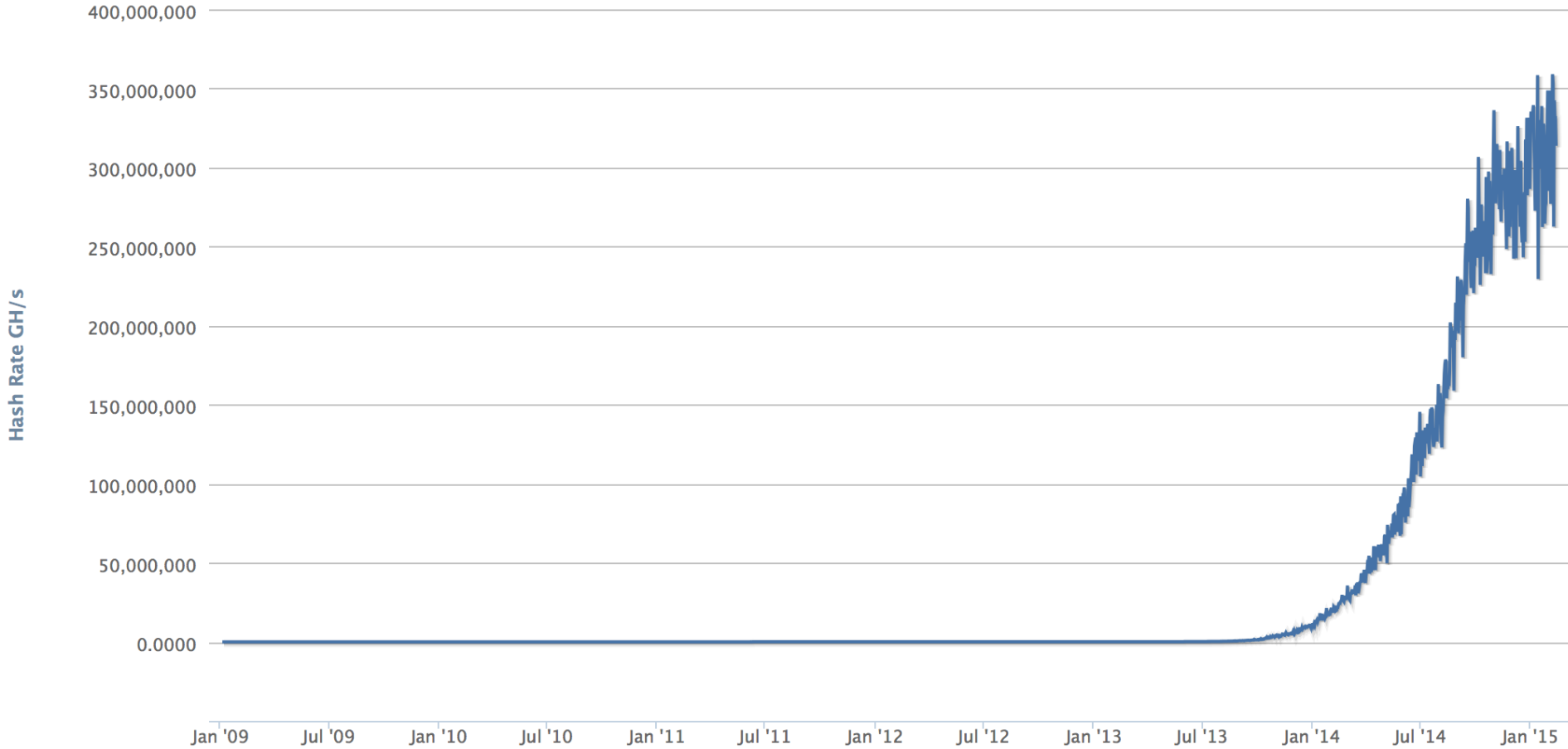
Tempo medio = Difficoltà * 2^{32} / hashrate

1 PC + GPU (1MHash/sec)

data	difficoltà	tempo medio per minare 1 blocco con il PC
gennaio 2010	1	1 ora
gennaio 2012	1E6	136 anni
gennaio 2015	40E9	5 milioni anni

Hash Rate

Source: blockchain.info

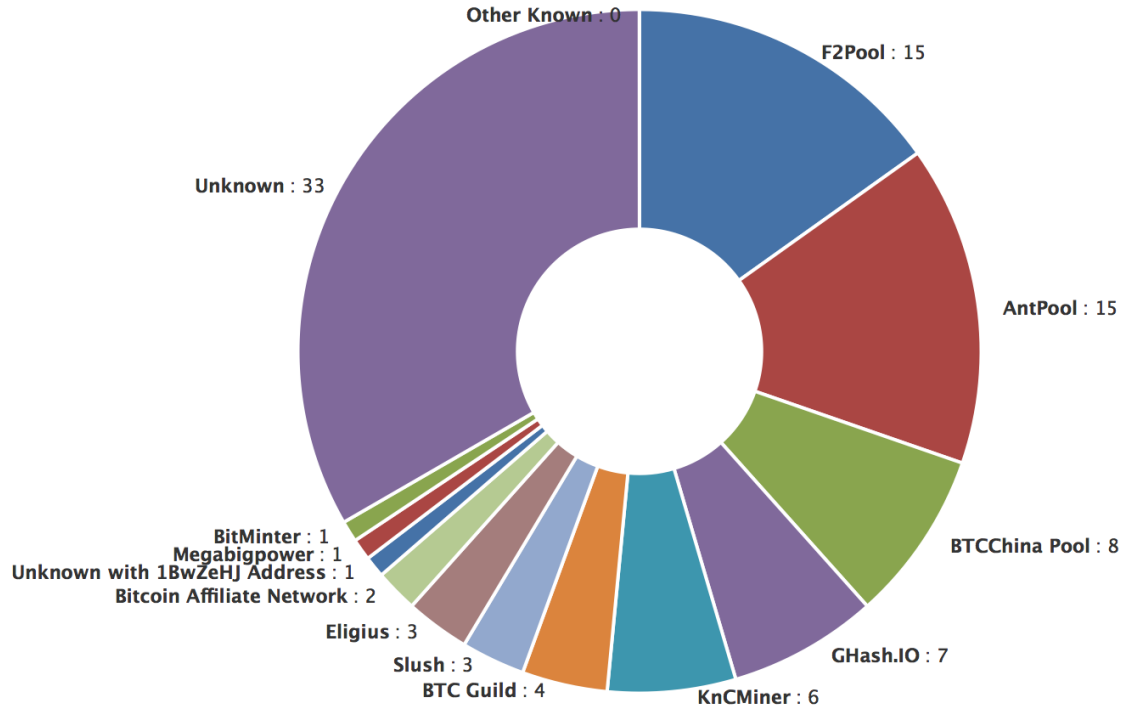


Capacita di hashing della rete Bitcoin

350 PHash/sec

Gennaio 2015

Hashrate distribution (feb 2015)



ASIC



SP35 YUKON POWER SHIPP

\$2,235.00 ~~\$2,795.00~~

We accept payment in Bitcoin, Dollars, or Euro. Prices

Sorry, this product is temporarily out of stock.

SHARE:



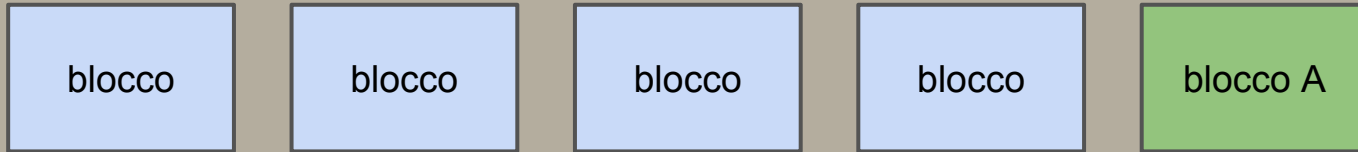
MORE POWER: 5.5 TH/S SHIPPING

solo mining = 400 giorni, può generare circa 2BTC al mese (Feb 2015)

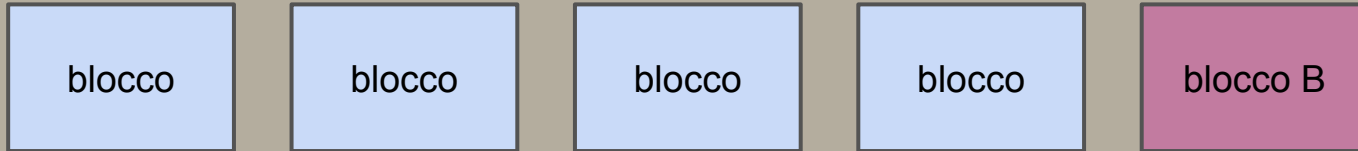
Vulnerabilità - Biforcazioni

Alle 5 viene chiuso il blocco A in Cina

Alle 5 viene chiuso il blocco B in Italia



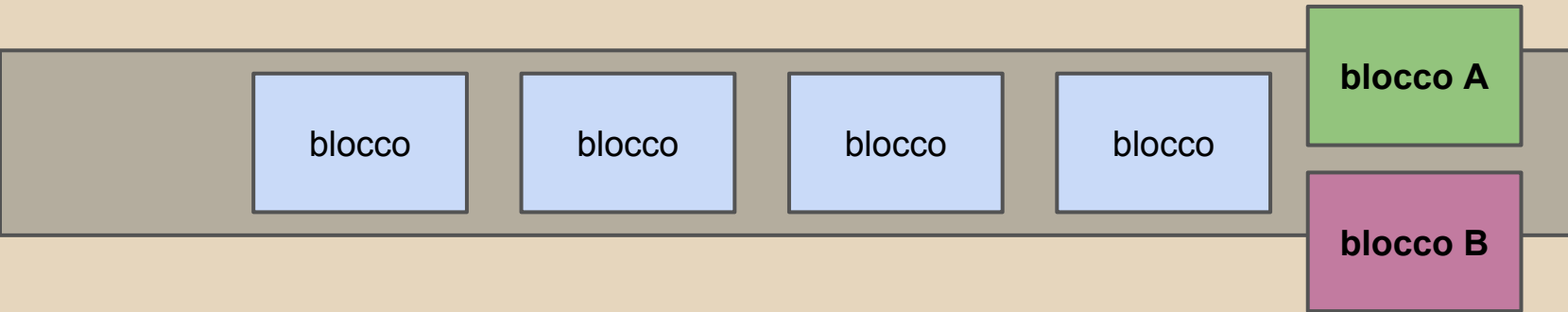
Blockchain propagata dalla Cina



Blockchain propagata dall'Italia

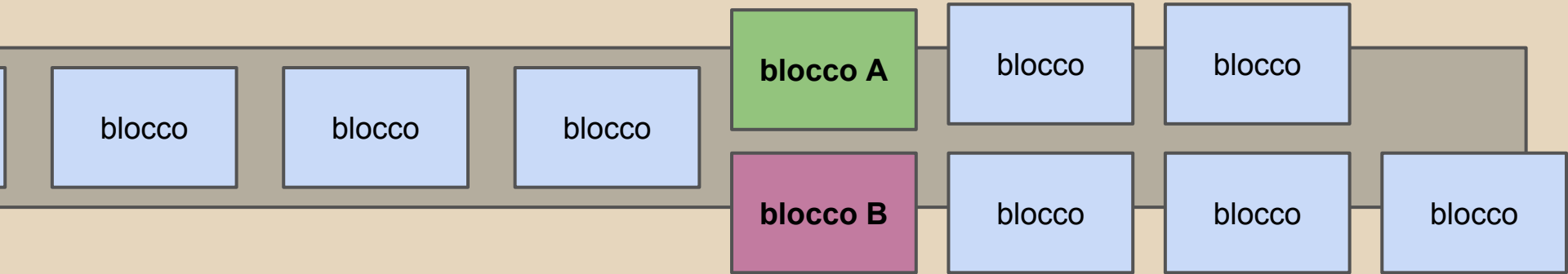
Vulnerabilità - Biforcazioni

Alle 5:01 tutti peer vedono entrambi i blocchi



Vulnerabilità - Biforcazioni

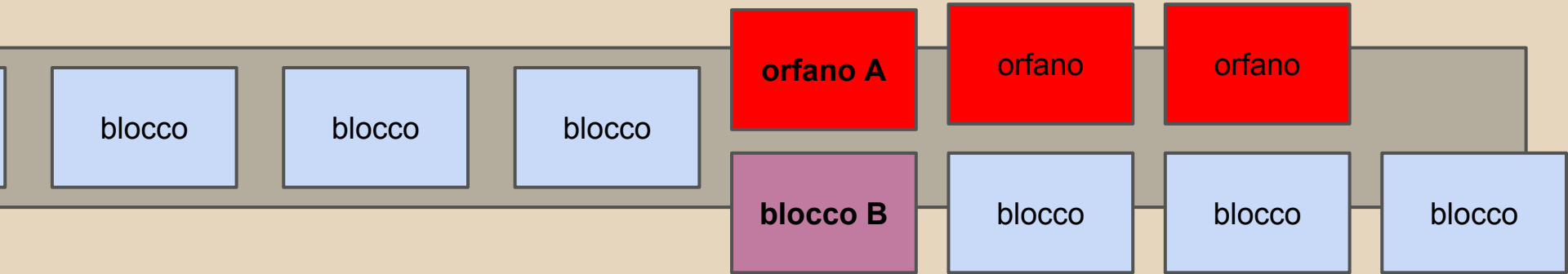
Alcuni decideranno di appendere ad A



Altri decideranno di appendere ad B

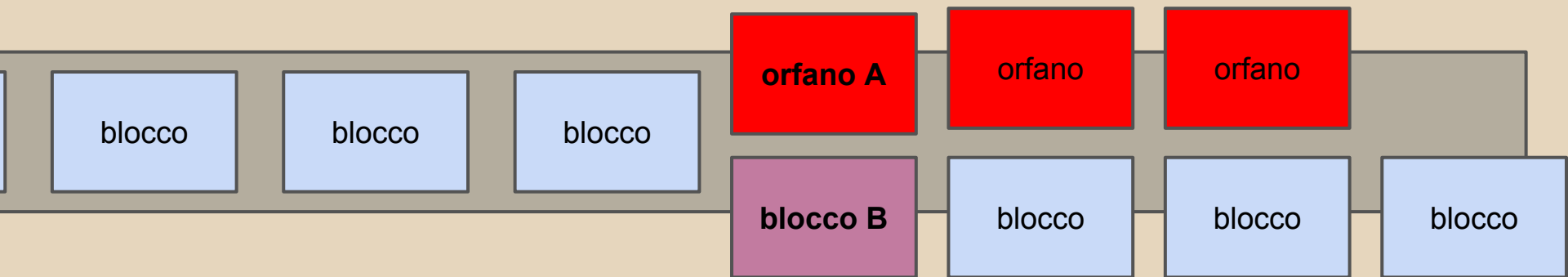
Vulnerabilità - Biforcazioni

Il protocollo stabilisce che il ramo più lungo deve restare, gli altri **devono sparire**



Vulnerabilità - Biforcazioni

Le transazioni dei blocchi orfani sono **invalidate**



Vulnerabilità

Ti rubano le chiavi private

Tracciare la storia di un coin (privacy leak)

DoS sui nodi della rete

Source code bugs (inevitabili)

Sybil attacks (avversario che riempie la rete di bot)

51% attack

Un partecipante con il 51% dell'hashing totale potrebbe:

- revocare i propri pagamenti (double spend)
- impedire la conferma dei pagamenti degli altri

Transaction Malleability

Le transaction contengono campi che non vengono usati per calcolare la “firma” digitale

Un destinatario malevolo potrebbe modificarli prima di inserirli nella blockchain e reclamare che un pagamento non è mai avvenuto

Crittografia (in soldoni)

L'indirizzo è (associato a) una **chiave pubblica**

Le transazioni sono firmate con la **chiave privata** di chi spende

La proof-of-work è basata su **hashing**

Ogni blocco contiene l'**hash** del precedente
(link crittografico)

Comprare Coin con Paypal?

Nessuno li vende ... perché?

Le transazioni Bitcoin sono irrevocabili, quelle paypal sono revocabili.

Stesso discorso per carte di credito

Comprarli con Dollari Linden

VirWox, Paypal <-> Linden \$ <-> BTC

Problemi:

- Alte commissioni, per piccole cifre si perde
- Non consente di usare i centesimi di euro quindi un account di 7,34 EUR per esempio ne usi 7,00 per gli scambi e i 0,34 restano lì senza utilità alcuna.

Comprarli su Coinbase, Bitstamp, etc

Sono piattaforme di scambio EUR/BTC

Hai un saldo in EUR ed uno in BTC

Devi associare un conto bancario vero

Problema: **sicurezza** dei tuoi dati personali

I've been Goxed

7.2.2014, all Bitcoin withdrawals were halted

24.2.2014, suspended all trading, site down

28.2.2014 Mt. Gox filed for bankruptcy protection in Tokyo.

The company said they had lost almost 750,000 of its customers' bitcoins

Oltre al danno la beffa

<http://pastebin.com/u5N0W9nH>

Mt. Gox database sale: steps to remove yourself from dump before sales.

Most around here know we are selling gox customer info. Many have contact us requesting to pay to have their data removed before we sell. We are doing this for a cost of 0.25 BTC per person removed. We have already sold and release 20% of data to 2 buyers, so if you are apart of that it's too late for you.

Comprarli su Facebook

Ci sono gruppi appositi

Si individuano le persone serie dagli scammers

Si prova con un piccolo acquisto (ricarica postepay)

Si dà un feedback sul gruppo

Comprarli dal vivo

Si incontra il venditore

Gli si danno i soldi in mano

Lui ti spedisce i coin dal cellulare







Altcoins ...

700+

molte delle quali derivate dal progetto Bitcoin

COM≡HTTP

Advanced Tables

Logo	Abbr	Name
	10-5	TenFive Coin
	21	21
	2CH	2chcoin
	365	365Coin
	42	FourtyTwoCoin
	66	66Coin

Confronto a tre

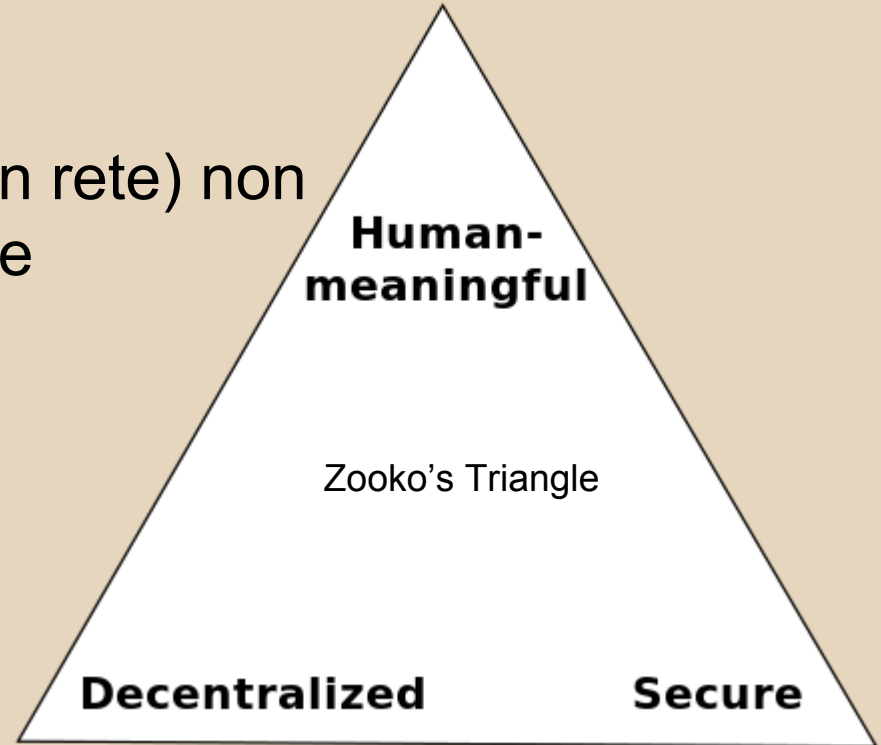
	Bitcoin	Litecoin	Namecoin
hashing	SHA256	Scrypt	SHA256
cap	21 milioni circa	84 milioni circa	21 milioni
value*	250 \$	2 \$	0,5 \$
T di conferma	10 minuti	2 minuti	10 minuti

(*) al 18 Febbraio 2015

Come nasce Namecoin

Congettura: uno spazio di nomi (in rete) non può essere contemporaneamente

**mnemonico,
decentralizzato
sicuro (ovvero globale)**



La congettura di Zooko sembra vera



...ma non lo è

Namecoin permette di salvare nella blockchain una coppia chiave, valore

Quindi

è un DNS decentralizzato, mnemonico e sicuro (globale)

Namecoin

- domini **.bit** -- es. **davide.bit**
- occorre un plugin nel browser chiamato **FreeSpeechMe**
- per un dominio si paga **0.01NMC**
- scade dopo **36000** blocchi (ca. 200 giorni)

Anonimato

Bitcoin non è nato per anonimizzare gli utenti
Ogni utente può avere uno o più pseudonimi

Un pagamento in Bitcoin è anonimo quanto scambiarsi una banconota in una piazza affollata. Qualcuno potrebbe riconoscere la nostra faccia

Per l'anonimato c'è Darkcoin

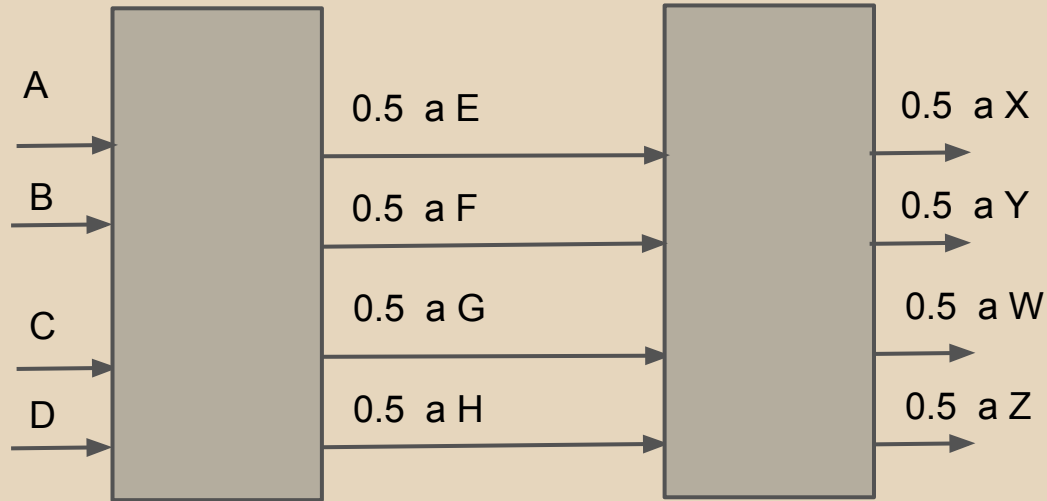
Un pagamento in Darkcoin è anonimo quanto scambiarsi una banconota indossando un cappuccio in testa ed in mezzo ad altri che fanno la stessa cosa vestiti come noi

Mixare 2 transazioni in una



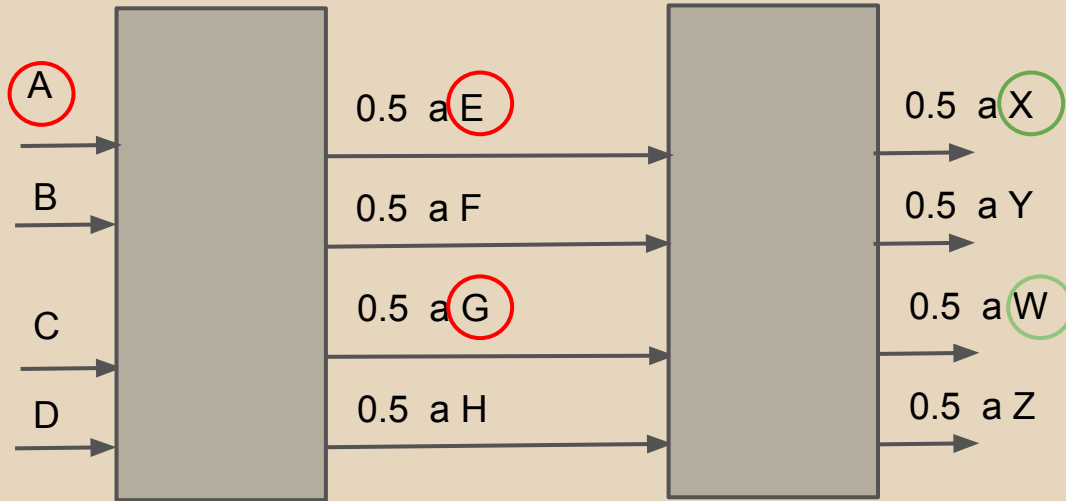
Chi paga chi?

Mixare N pagamenti in una trans



Alice paga a Bob 1 coin. Lo vedete?

Mixare N pagamenti in una transactn



Sì se sapete che Alice controlla i rossi e Bob i verdi

Oltre i pagamenti

IBM/Samsung **ADEPT**, Internet of things on BC
<https://www.theprotocol.tv/adept-demo-ibm-samsung/>

D-CENT is a Europe-wide project creating privacy-aware tools and applications for direct democracy <http://dcentproject.eu/>

Oltre i pagamenti

Storj - The Future of Cloud Storage. affitta spazio sul tuo hard drive in cambio di valuta digitale: <http://storj.io>

GeoCoin, analisi dati territoriali <http://geocoin.cash/> GeoCoin Currency, Bringing GIS technologies to the blockchain!

Piattaforme per smart contracts

Ethereum -- <https://www.ethereum.org/>

NXT -- <http://nxt.org/>

Oltretomba

Think about your testament

Your bitcoins can be lost forever if you don't have a backup plan for your peers and family. If the location of your wallets or your passwords are not known by anyone when you are gone, there is no hope that your funds will ever be recovered. Taking a bit of time on these matters can make a huge difference.

(from [Bitcoin.org](https://bitcoin.org))

E' legale?

Pareri della Banca d'Italia

Gli exchange orientati a rendere istituzionale bitcoin e le altre Monete Digitali e che fin dall'inizio si sono adeguati **alle norme anti-riciclaggio** possono regolarmente essere serviti dalle banche italiane come soggetti leciti.

E' legale?

Pareri della Banca d'Italia

Gli exchange e i **sistemi che permettono di acquistare bitcoin** al di fuori delle norme anti-riciclaggio, ovvero senza fare un corretto riconoscimento del cliente per le somme rilevanti (oltre i 999€), dovrebbero vedersi tagliati i ponti con le banche italiane

E' legale?

Pareri della Banca d'Italia

l'Autorità Bancaria Europea (EBA) ha individuato numerosi profili di rischio derivanti dall'utilizzo o dalla detenzione delle Valute Virtuali

La Banca d'Italia condivide l'opinione dell'EBA di scoraggiare le banche e gli altri intermediari vigilati dall'acquistare, detenere o vendere Valute Virtuali.

La storia dell'italiano che ha fondato una startup con 45 bitcoin

Thomas Bertani, 24 anni, ha fondato Oraclize, una startup che potrebbe rivoluzionare i pagamenti digitali. E ha scelto di usare i bitcoin come capitale sociale.

Community italiana

- Gruppone Facebook **Bitcoin Italia**
- **Associazione AssoBit**
- **Bitcoin Talk sezione ITA**

persone chiave:

Franco Hostfat Cimatti, Stefano Pepe, Carola Frediani, Giacomo Zucco, Andrea Medri (TRT), Lawrence Nahum

Community sarda

Sardegna Bitcoin

<http://www.bitcoinsardegna.it/>

Mauro Pili,
Luigi Angotzi,
Stefano Lai,
Vineria Enò

Referenze

Il paper originale di Satoshi Nakamoto

<https://bitcoin.org/bitcoin.pdf>

Il wiki con tutta la doc aggiornata

<http://bitcoin.it/>

Libri



Bitcoin: cosa sono e come ottenerli: viaggio nel mondo della criptovaluta

2014 | eBook Kindle

di Carlo Denaro

Formato Kindle

EUR 2,42

include IVA (dove applicabile)



Compra ora con 1-Click®

Disponibile per il download immediato



Dizionario Bitcoin - Italiano: Glossario ragionato sul mondo Bitcoin

di Davide Carboni

Formato Kindle

EUR 0,00 kindleunlimited

Per gli abbonati è previsto un servizio di lettura gratuito. [Ulteriori informazioni.](#)

EUR 2,37 da acquistare

include IVA (dove applicabile)



Compra ora con 1-Click®

Disponibile per il download immediato

Libri



Investire BITCOIN: Come capire e gestire questa nuova forma di ricchezza

di Stefano Pepe

Formato Kindle

EUR 9,99

include IVA (dove applicabile)



Compra ora con 1-Click®

Disponibile per il download immediato



Senza Banche - Bitcoin la moneta di Internet 27 feb. 2013 | eBook Kindle

di Fabio Vita

Formato Kindle

EUR 0,00 kindleunlimited

Per gli abbonati è previsto un servizio di lettura gratuito. [Ulteriori informazioni.](#)

EUR 3,66 da acquistare

include IVA (dove applicabile)



Compra ora con 1-Click®

Disponibile per il download immediato