Cryptovalute: la moneta digitale

Andrea Lisi
Università di Pisa - Informatica
Centro Nazionale delle Ricerche - IIT

BRIGHT 2020
Pisa

Scaletta

Di cosa si parlerà in questa presentazione

- Che cosa sono, e come funzionano le criptovalute
  - Esempio: Bitcoin
- Rispondere ad alcune domande di curiosità

Di cosa **NON** si parlerà in questa presentazione

- Come investire e diventare ricchi con Bitcoin

PREMESSA

Non sono un bancario, finanziario, economista o contabile

Se faccio qualche errore in questo campo, scusatemi in anticipo

Casomai fatemelo notare alla fine, così che possa correggermi in futuro

Che cosa sono le criptovalute?

Che cosa sono le criptovalute?

Contesto storico, siamo nel 2009

Che cosa sono le criptovalute?

Contesto storico, siamo nel 2009

Viene pubblicato online un articolo intitolato

“ Bitcoin: A Peer-to-Peer Electronic Cash System”

firmato da

Satoshi Nakamoto

Bitcoin: A Peer-to-Peer Electronic Cash System

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

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

Che cosa sono le criptovalute?

Che cosa è una **valuta digitale**?

- È una valuta che esiste SOLTANTO in forma digitale, e quindi utilizzabile soltanto da computers[Investopedia]

Che cosa è una **criptovaluta**?

- È una valuta digitale resa sicura grazie a tecniche di crittografia che rendono quasi impossibile spendere due volte la stessa moneta[Investopedia]

Che cosa sono le criptovalute?

Bitcoin è il primo esempio concreto di criptovaluta

- Ma non la prima concezione di valuta digitale (1983)

Ma come si differenzia da un pagamento con Mastercard?

- Un pagamento online in Euro è un processo digitale di trasferimento, transazione, di una moneta fisica tra conti correnti (o altro)

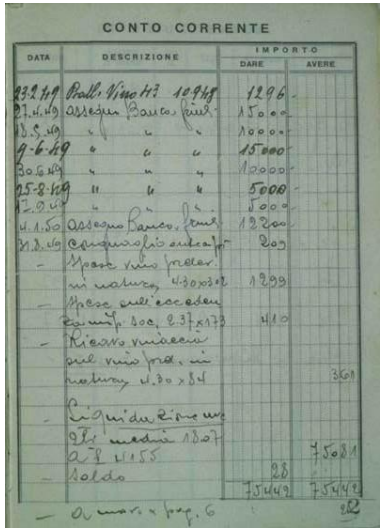
Come funziona Bitcoin?

Come funziona Bitcoin?

Per capire il funzionamento di Bitcoin servono due concetti fondamentali

- **Transazione**

- **Registro, o libro contabile**



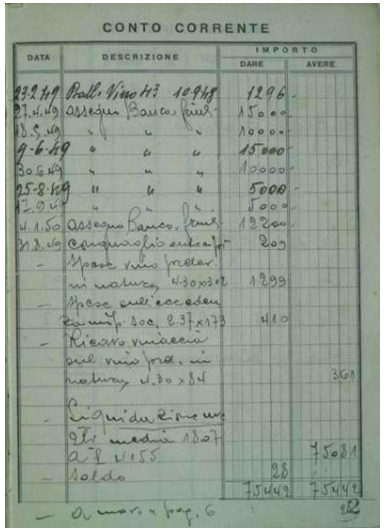
Come funziona Bitcoin?

Pagamento in contanti

- Transazione: il passaggio di banconote o monete
- Libro contabile: un documento personale

Pagamento bancario

- Transazione: un movimento tra conti correnti
- Libro contabile: tenuto dalla banca

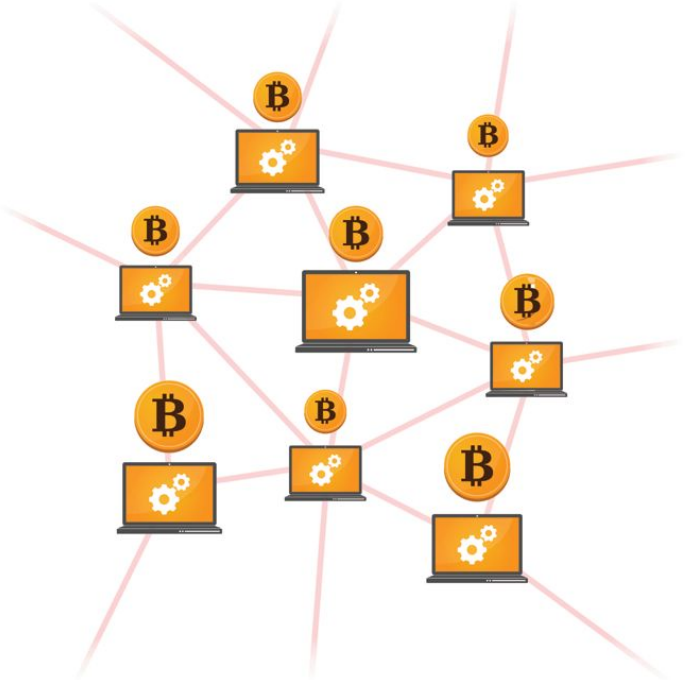


Come funziona Bitcoin?

Bitcoin è formata da una rete di computer connessi tra di loro grazie ad un software

Ogni computer è autorizzato ad eseguire una transazione

Ogni computer memorizza **IL** libro contabile **dell'intera rete Bitcoin**



Come funziona Bitcoin?

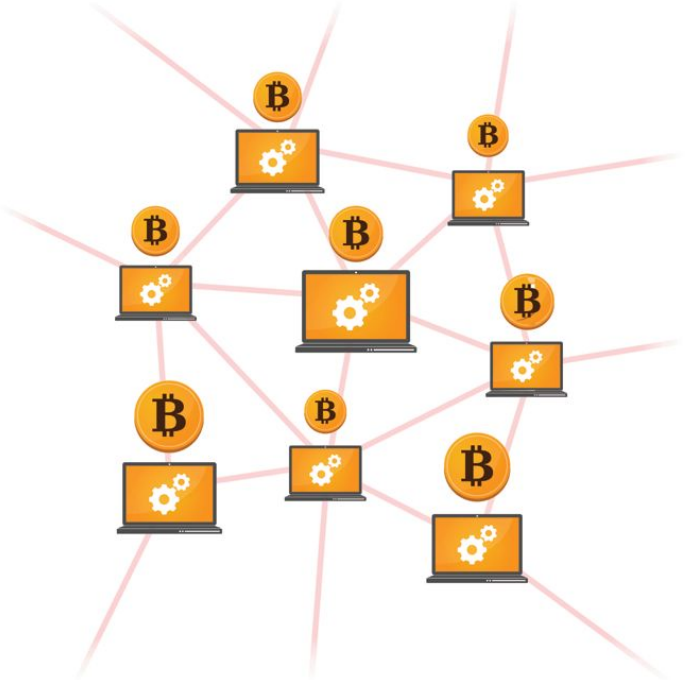
Bitcoin è formata da una rete di computer connessi tra di loro grazie ad un software

Ogni computer è autorizzato ad eseguire una transazione

Ogni computer memorizza **IL** libro contabile **dell'intera rete Bitcoin**

Problema

Se ogni computer ha **IL** libro contabile, come viene aggiornato?



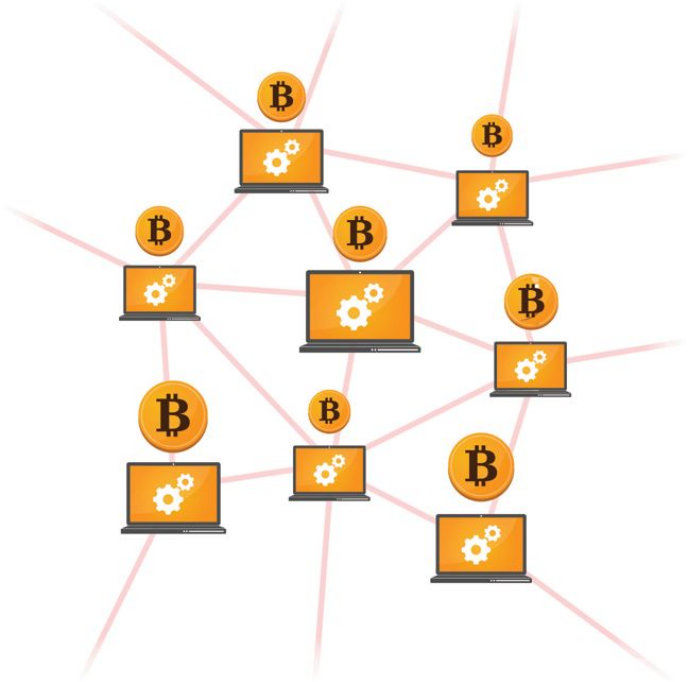
Come funziona Bitcoin?

Tutti i computer devono essere d'accordo

- Ovvero, inserendo le stesse transazioni nello stesso ordine

Una nuova pagina viene prodotta ad intervalli

- Circa 15 minuti



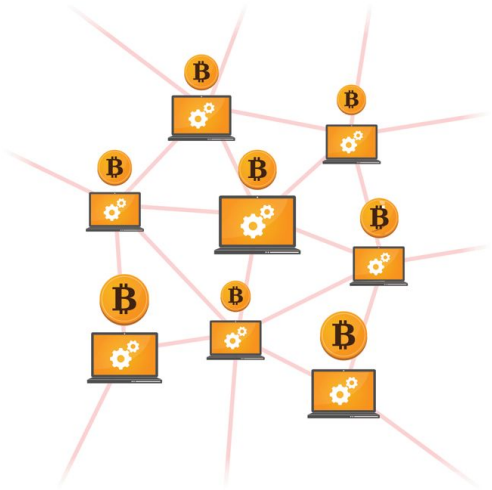
Come funziona Bitcoin?

Come funziona Bitcoin?

FASE 1: Scelta di un leader tramite un consenso

Il leader proporrà la nuova pagina del libro contabile con le transazioni

- Competizione tra i computer della rete



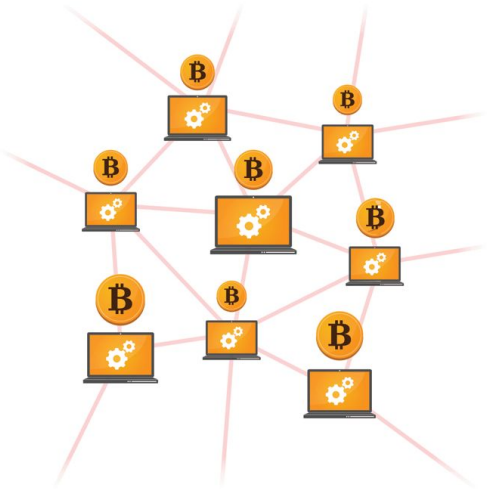
Come funziona Bitcoin?

FASE 1: Scelta di un leader tramite un consenso

Il leader eletto sarà colui che per primo risolverà un puzzle

- Un puzzle è difficile da risolvere, ma una volta risolto è facile vedere se è risolto bene
- Il sudoku funziona con lo stesso principio

5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9



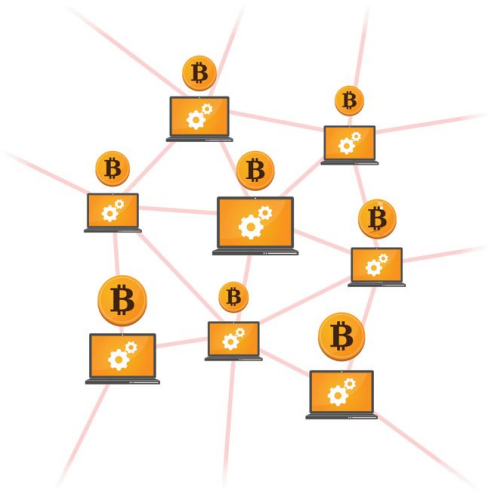
Come funziona Bitcoin?

FASE 1: Scelta di un leader tramite un consenso

In Bitcoin il puzzle è crittografico, la cui difficoltà viene bilanciata nel tempo così che la risoluzione impieghi circa 15 minuti di tempo

- Un po' come aumentare o diminuire le tessere "cielo blu" in un puzzle

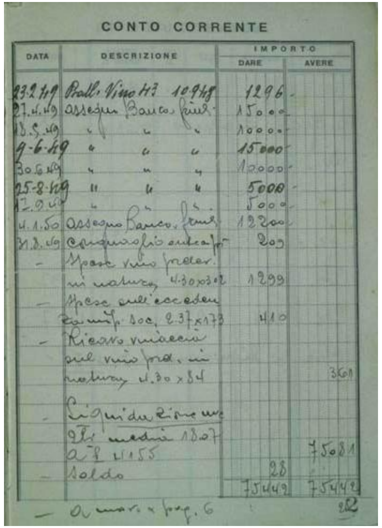
- Se è troppo facile, la rete diventa inconsistente
- Se è troppo difficile, nessuno partecipa



Come funziona Bitcoin?

Come funziona Bitcoin?

FASE 2: Creazione di una nuova pagina del libro contabile



Il computer vincitore, il leader, è in carica di collezionare una porzione delle transazioni richieste dalla rete, e compilare così la nuova pagina del libro contabile

Il leader comunica a tutta la rete la nuova pagina

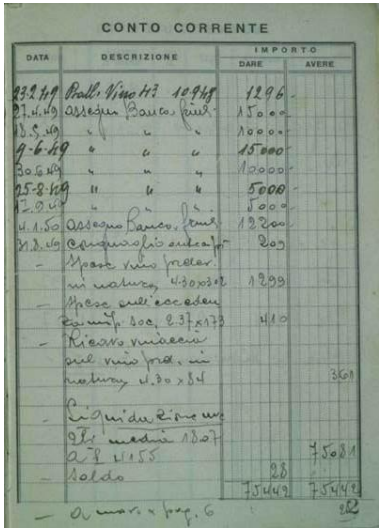
Come funziona Bitcoin?

Come funziona Bitcoin?

FASE 3 Verifica della correttezza della pagina da parte della rete

Tutti i computer della rete ricevono la pagina e, basandosi sulla propria copia del libro contabile, controllano che le transazioni inserite siano corrette

- Se lo sono, accettano la pagina
- Altrimenti la rifiutano



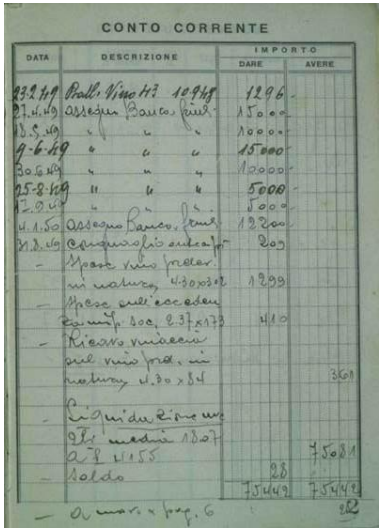
Come funziona Bitcoin?

Come funziona Bitcoin?

FASE 4 Aggiornamento di ogni libro contabile, e ricompensa del leader

Ogni computer aggiorna il proprio libro contabile con la nuova pagina

La nuova pagina conterrà una transazione speciale che ricompensa il leader con una quantità fissa di Bitcoin come premio per aver vinto la competizione

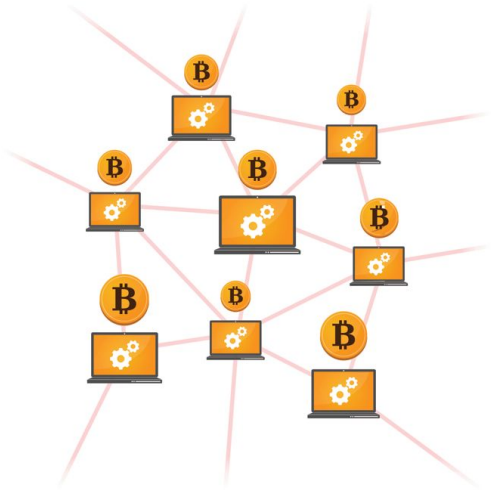


Come funziona Bitcoin?

La ricompensa è la motivazione principale per la quale i computer competono

- Risolvere il puzzle crittografico richiede una grande quantità di energia elettrica

Inoltre, il leader trattiene una piccola commissione da ogni transazione



Come funziona Bitcoin?

Bitcoin vive grazie agli incentivi

- I partecipanti sono intenzionati a giocare secondo le regole per poter guadagnare

- Se giocare sporco fa scappare gli utenti, il valore di Bitcoin crollerebbe e non ci sarebbe nessun guadagno

Domande frequenti

Ma come ottengo Bitcoin?

Il modo più naturale è scaricare il software e metterlo in competizione per diventare leader

MA …

- Il libro contabile di Bitcoin è grande circa 300 GB
- I partecipanti a Bitcoin al giorno d'oggi non sono portatili, ma interi palazzi di computer
- Servirebbe il computer in esecuzione 24 ore su 24 sempre
    - Poi chi la sente l'Enel?

Ma come ottengo Bitcoin?

Esistono dei broker di finanza che accettano Euro, Dollari etc in cambio di Bitcoin

- Vari siti web

Farseli dare da chi li possiede già

- Magari come pagamento di un servizio

Ma come utilizzo Bitcoin?

È possibile partecipare in maniera “light” tramite programmi “portafoglio” leggeri

Questi portafogli creano una speciale coppia di chiavi per poter ricevere ed inviare Bitcoin

- Una chiave **privata**, quindi da non comunicare a nessuno, permette di firmare una transazione ed inviare Bitcoin
- Una chiave **pubblica**, quindi nota a tutti, che permette di ricevere Bitcoin
    - Concetto della cassetta della posta

Ma come utilizzo Bitcoin?

Attenzione 1

Non esiste una banca! Ogni Bitcoin inviato per sbaglio non è rimborsabile

Attenzione 2

La perdita della chiave privata significa la perdita di tutti i Bitcoin associati, e non è recuperabile facilmente

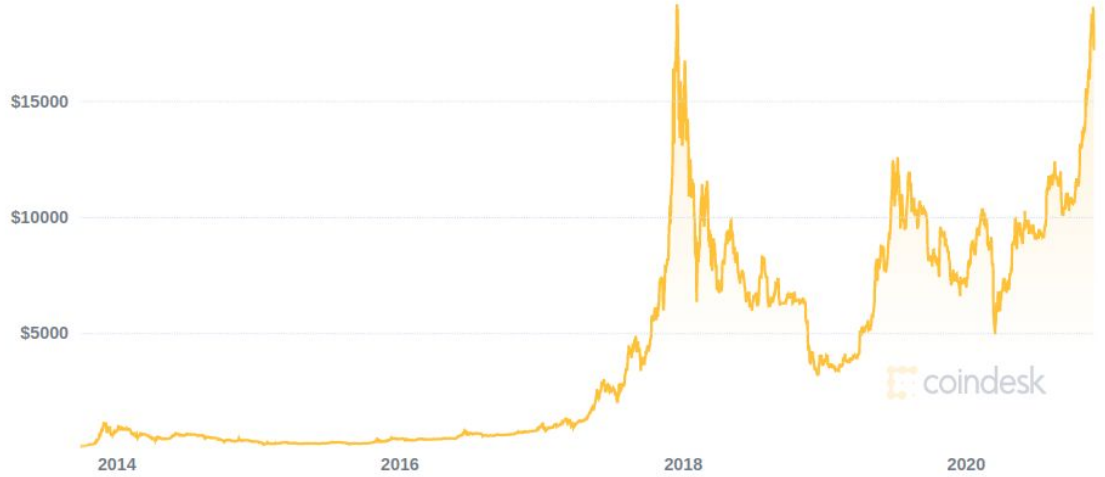
Ma quanto valgono i Bitcoin?

Oggi 1 Bitcoin vale circa 14.000€

Ci sono circa
15 Milioni di Bitcoin

Per un valore totale di
260 Miliardi di €

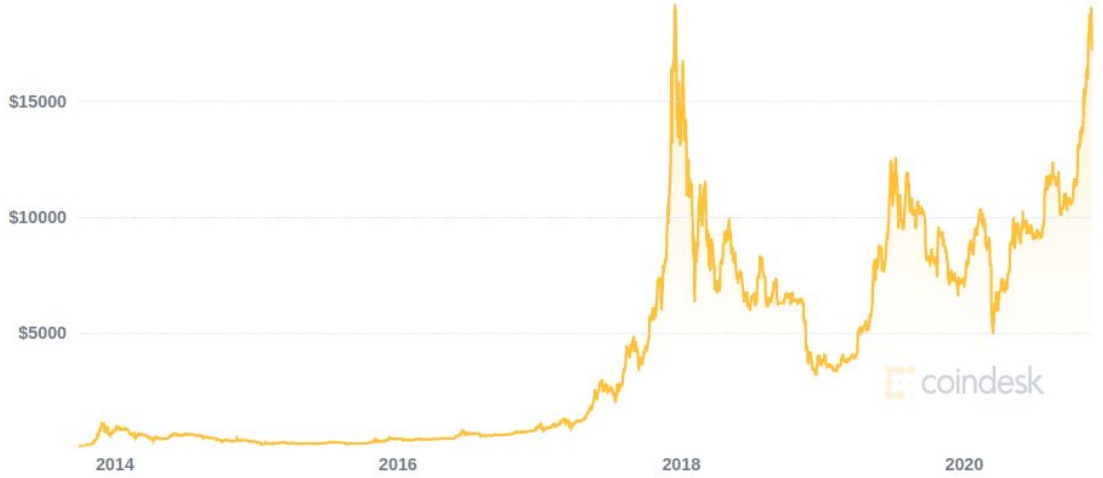
[Coindesk, 27 Novembre]



Chi decide il valore di Bitcoin?

Il mercato, pura
domanda / offerta

I Bitcoin non sono legati
a nessun asset (tipo l'oro)



Quanti bitcoin ci saranno?

Come accennato, ci sono circa 15 Milioni di Bitcoin a giro

- Ogni 15 minuti vengono “creati” nuovi, che sono quelli della ricompensa al leader

Massimale: 21 Milioni di Bitcoin

- La ricompensa viene dimezzata ogni 4 anni
- È iniziata con 50 Bitcoin, a Giugno 2020 c’è stato il terzo dimezzamento, ora è di 6.25 Bitcoin
- 21 Milioni verranno raggiunti circa nel 2140

Quale è il futuro di Bitcoin?

Difficile preverderlo...

Quale è l’impatto di Bitcoin?

L’insieme di tecniche per l’aggiornamento del libro contabile hanno avuto un incredibile riscontro

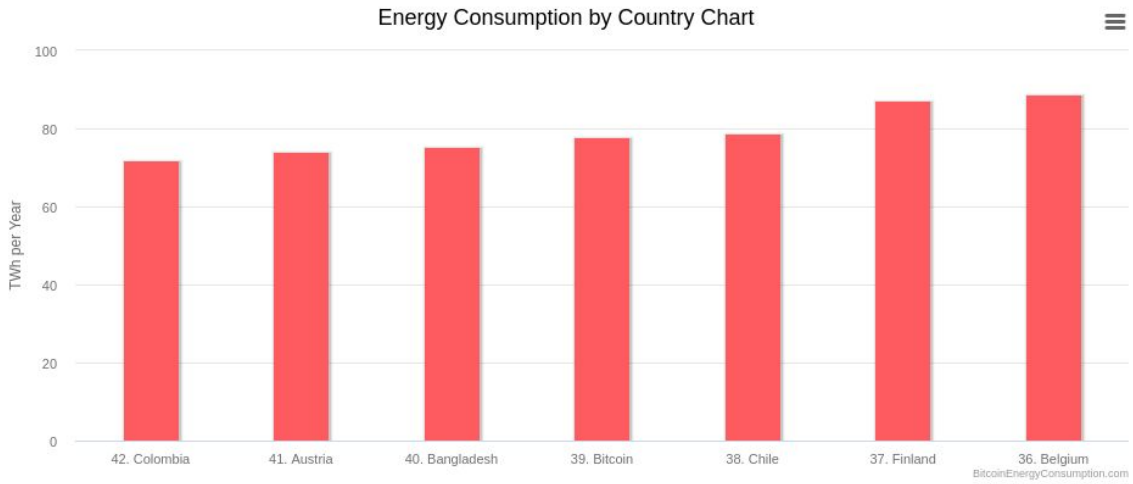
- Sia nel mondo della ricerca universitaria
  - Migliorare Bitcoin, utilizzare i concetti su altri problemi
- Sia nel mondo dell’industria
  - Creare una rete di computer aziendali per migliorare i processi produttivi
    - Esempio: filiere alimentari

Quanto consuma Bitcoin?

Ad Agosto 2020, sottostima

Rete mondiale di Bitcoin paragonabile a Austria e Finlandia
[Digiconomist, 11 Novembre]

La ricerca sta studiando alternative meno esose



Parole chiavi già lette (forse)

Blockchain
È il libro contabile descritto prima, cui ogni pagina è chiamata “blocco” (da qui catena di blocchi)

Mining, o miners
Il processo di soluzione del puzzle ed elezione del leader (mining, scavare, per scoprire nuovi Bitcoin)

Proof of Work
L’algoritmo di consenso per la scelta del leader

Quante criptovalute esistono?

Troppe...

Cosa portare a casa

Cosa portare a casa

Bitcoin è una criptovaluta

- Valuta digitale con crittografia

Non esiste una banca, e tutte le transazioni vengono effettuate in cooperazione tra partecipanti di una rete di computer

La responsabilità è interamente nelle mani dell'utente

- Assenza di banche vuol dire più libertà ma meno tutele

I numero di Bitcoin in circolazione è destinato ad arrestarsi nel 2140

Grazie!