



# Blockchains

Introduzione alla tecnologia blockchain, applicazioni,  
e prospettive future

**Enrico Bacis**

[enrico.bacis@unibg.it](mailto:enrico.bacis@unibg.it)

# • whoami

Enrico Bacis

-----

[enricobacis.com](http://enricobacis.com)

[enrico.bacis@unibg.it](mailto:enrico.bacis@unibg.it)

Dottorando - Università degli Studi di Bergamo

- \* Database/Cloud/Mobile Security
- \* Encryption modes e Blockchains

Unibg Seclab - [seclab.unibg.it](http://seclab.unibg.it)

- \* Progetti europei su cloud data security

- \* Competizioni di (sicurezza) informatica
- \* Membro di BgLUG e Hacklab Bergamo



# Agenda

## Parte I

- Cosa è bitcoin
- Perché ha valore
- Principi di funzionamento
- Come vengono prodotti

## Parte II

- Come si acquistano bitcoin
- Tipi di portafogli
- Come e dove usarli
- Pericoli e Anonimato

## Parte III

- Possibilità
- Smart contracts e ICO

---

## Parte I

# Introduzione e punto di vista tecnico

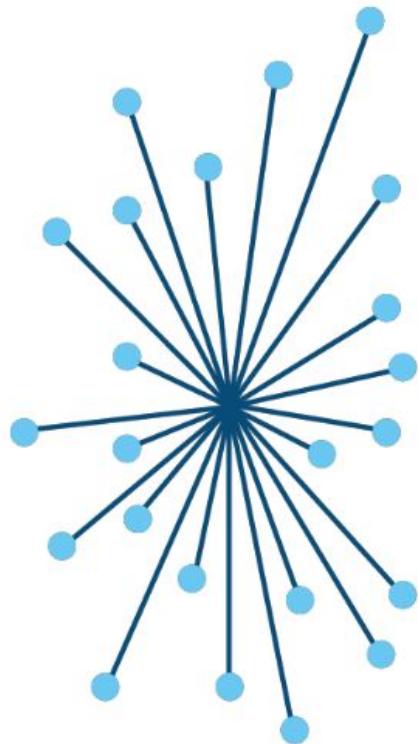
**È possibile creare  
una moneta digitale  
senza una  
autorità centrale?**

**Questa domanda  
è rimasta  
senza risposta  
fino al 2008**

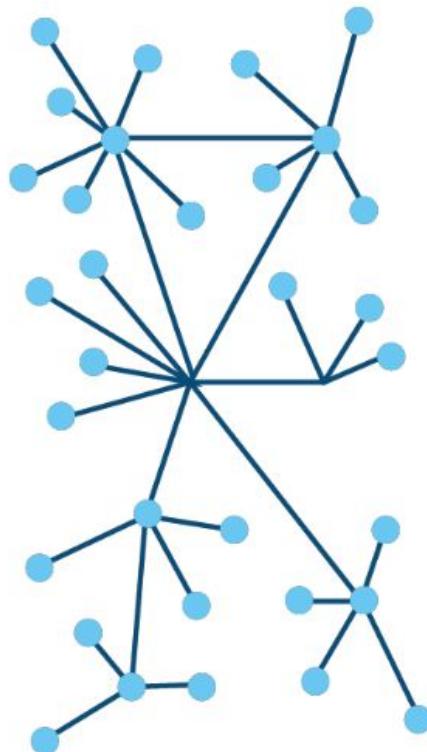
---

**“What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.”**

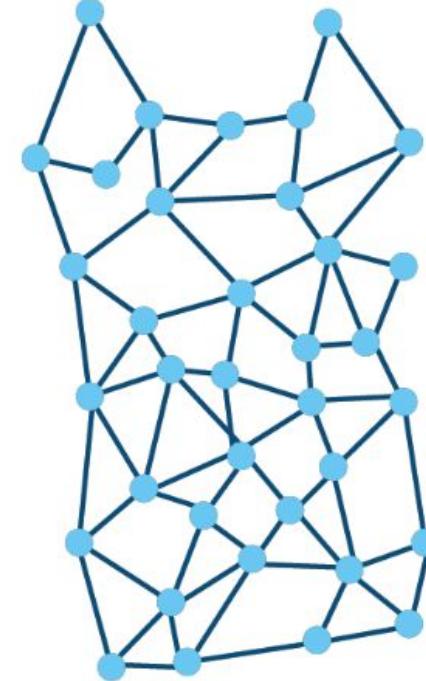
- Satoshi Nakamoto  
*“A peer-to-peer electronic cash system” [2008]*



**Centralized**



**Decentralized**



**Distributed**

# Cosa è Bitcoin?

**un libro mastro (ledger)  
pubblico e distribuito  
basato sul consenso**

---

**1** A vuole inviare denaro a B



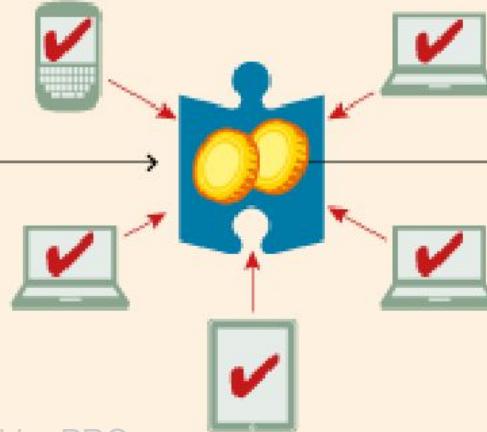
**2** La transazione viene rappresentata come un 'blocco'



**3** Il blocco viene trasmesso a ogni nodo della rete



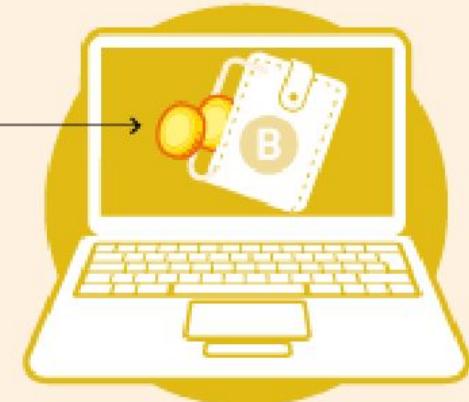
**4** I nodi nella rete approvano la transazione e la convalidano



**5** Il blocco dopo può essere aggiunto alla catena, che fornisce un registro indelebile e trasparante delle transazioni



**6** Il denaro va da A a B



# Chi ha creato Bitcoin?

---

# Satoshi Nakamoto

---

- **31 Ottobre 2008**

Satoshi Nakamoto pubblica l'articolo “*A peer-to-peer electronic cash system*”

- **3 Gennaio 2009**

Satoshi pubblica il codice sorgente di Bitcoin

- **23 Aprile 2011**

Satoshi dice “*Moved onto other things*” e sparisce ...

... senza più utilizzare il suo patrimonio di 980,000 bitcoins



© CoinedBits.com

# Are you Satoshi?

---

## Dorian Nakamoto

- Informatico Giapponese
- Nel 2014 la rivista Newsweek dice di avere le prove del fatto che lui sia Satoshi
- *“I am not Dorian Nakamoto”*  
- satoshi



# Are you Satoshi?

---

**Craig Wright**

- Informatico Australiano
- Nel 2016 si proclama l'inventore di Bitcoin
- Fallisce il Satoshi Test
- Nel 2018 viene denunciato per aver rubato 5 miliardi di dollari in Bitcoin



-\\_(ツ)\_/-

# Are you Satoshi?



Donald J. Trump   
@realDonaldTrump



Following

The failing financial system has disgraced the American people for years. Which is why I gave you Bitcoin, I am Satoshi Nakamoto. Change the financial laws now in favour of Bitcoin.

RETWEETS  
**7,463**

LIKES

**17,361**



6:09 AM - 1



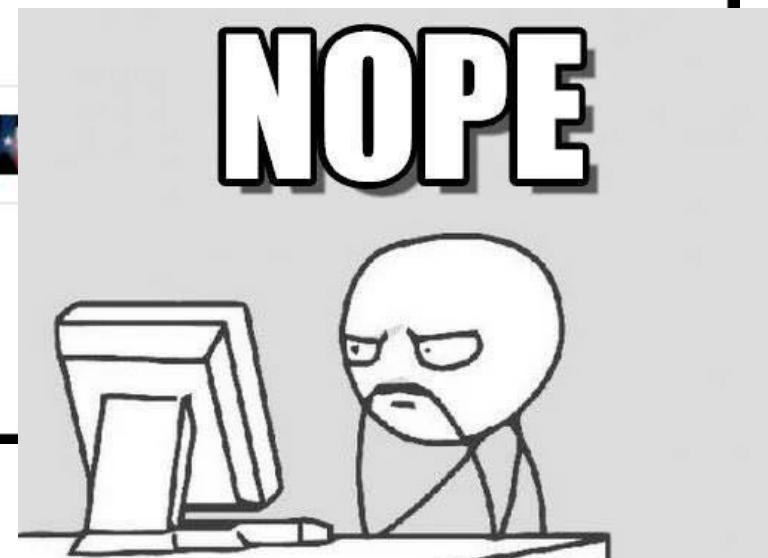


7.5K



17K

...



**NOPE**

# Are you Satoshi?

---



- I dati del suo account lo ritraggono come un uomo di 38 anni che vive in Giappone.
- Estremamente esperto di programmazione in C++, economia, crittografia e reti peer-to-peer.
- Scrive in inglese perfetto. Il suo primo post usa spelling americano, tutti gli altri britannico.
- Legge il “*The Times*”.
- La sua attività non si concentra in un particolare fuso orario.

Si pensa che Satoshi Nakamoto sia lo pseudonimo del gruppo di individui che hanno creato Bitcoin.

# Are you Satoshi?

---



Hal Finney

Dorian Nakamoto

... and many others ...

# Perché Bitcoin ha valore?

---

---

**1. Ha valore tutto ciò  
a cui diverse persone  
attribuiscono valore.**

---

# Il primo acquisto in Bitcoin



**17 Maggio 2010**

Laszlo Hanyecz posta una richiesta per comprare della pizza con Bitcoin

**22 Maggio 2010**

Laszlo conferma di aver effettuato una transazione di 10,000 BTC per queste due pizze.

**2010:** Valore di 10,000 BTC = 41 \$

**2018:** Valore di 10,000 BTC = **60,000,000 \$**

Il 22 Maggio si commemora il **Bitcoin Pizza Day**

- 
1. Ha valore tutto ciò a cui diverse persone attribuiscono valore.
  2. È sia ***commodity*** (*bene*) che ***currency*** (*moneta di scambio*)

# commodity



VS



# Commodity - Bitcoin vs Oro



	<b>Bitcoin</b>	<b>Oro</b>
<b>Risorsa Scarsa</b>	Il numero massimo di Bitcoin in circolazione è fisso	Può ancora essere estratto in quantità difficilmente stimabili
<b>Duraturo</b>	Decentralizzato -> sopravviverebbe ad un attacco nucleare	Ft. Knox no <i>Punto fusione oro: 2856 gradi</i> <i>Esplosione nucleare: <math>10^8</math> gradi</i>
<b>Portabile</b>	Può essere inviato istantaneamente, utilizzando una connessione	Pesante e deve essere dichiarato
<b>Divisibile</b>	Può essere diviso in 100 milioni di pezzi (1 satoshi = $10^{-8}$ bitcoin)	Non può essere diviso in altrettante parti senza distruggerne parte
<b>Verifica di Autenticità</b>	Può essere verificato con algoritmi	Richiede un occhio esperto e test chimici

# Commodity - Bitcoin vs Oro



	<b>Bitcoin</b>	<b>Oro</b>
<b>Conservazione</b>	Bisogna solo salvare le chiavi di cifratura	Conservazione difficile per grandi quantità
<b>Fungibile</b>	Tutti i bitcoin sono uguali, per ognuno si ha la storia completa	Diversi livelli di purezza
<b>Contraffazione</b>	Matematicamente non fattibile	L'oro non può essere contraffatto, ma i lingotti possono essere manomessi
<b>Uso Diffuso</b>	Utilizzato come commodity, inizia ad essere utilizzato come currency	Una volta era una currency, ora solo una commodity (conserva valore)

# currency



vs



# Currency - Bitcoin vs Dollaro



	<b>Bitcoin</b>	<b>Dollaro</b>
<b>Risorsa Scarsa</b>	Il numero massimo di Bitcoin in circolazione è fisso	Esistono 10 trilioni \$ (1.2 circolanti). La Federal Reserve ha triplicato la Monetary Base dal 2008
<b>Duraturo</b>	Bitcoin sono stati persi e rubati, ma mai deteriorati	Le banconote si deteriorano (e vengono sostituite)
<b>Portabile</b>	Può essere inviato istantaneamente, utilizzando una connessione	È facile trasportare denaro contante. Grosse somme richiedono infrastruttura.
<b>Divisibile</b>	Può essere diviso in 100 milioni di pezzi (1 satoshi = $10^{-8}$ bitcoin)	1 dollaro può essere diviso in 100 parti
<b>Verifica di Autenticità</b>	Può essere verificato con algoritmi	La validità della banconota può essere verificata con test ottici / chimici

# Currency - Bitcoin vs Dollaro



	<b>Bitcoin</b>	<b>Dollaro</b>
<b>Conservazione</b>	Bisogna solo salvare le chiavi di cifratura	Conservazione difficile per grandi quantità
<b>Fungibile</b>	Tutti i bitcoin sono uguali, e si conosce la storia completa	Le banconote sono intercambiabili, E <u>non si conosce</u> la storia completa
<b>Contraffazione</b>	Matematicamente non fattibile	La contraffazione delle banconote è una pratica che si combatte da sempre
<b>Uso Diffuso</b>	Utilizzato come commodity, inizia ad essere utilizzato come currency	La valuta assume valore per via di un decreto governativo

# Blockchain e Bitcoin

## Principi di Funzionamento



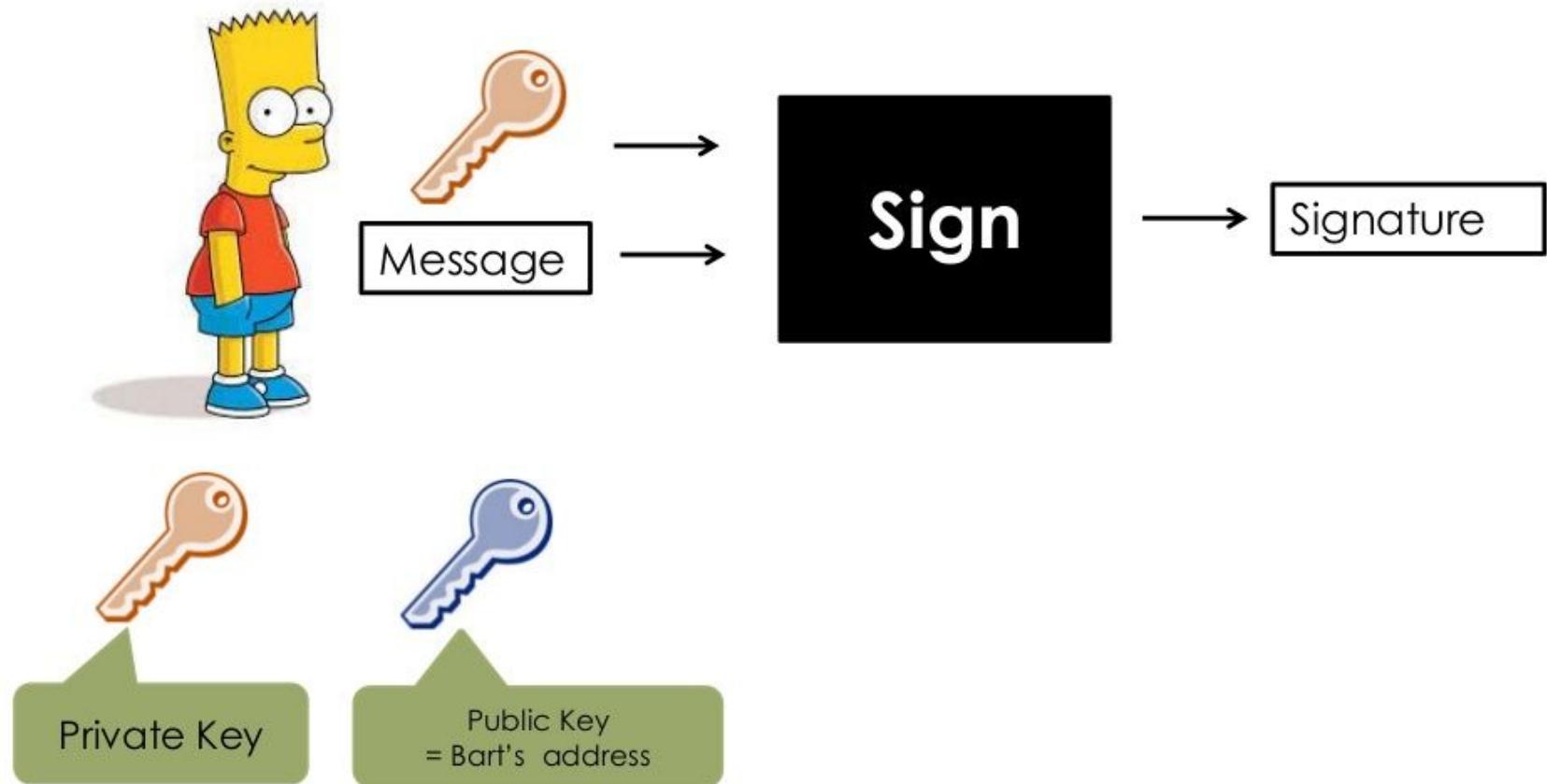


# **Concetti Base e Terminologia**

- 1. Crittografia asimmetrica e firme digitali**
- 2. Indirizzi Bitcoin**
- 3. Blocchi e Transazioni**
- 4. Hash e Controllo di integrità**
- 5. Proof-of-Work e Blockchain**
- 6. Mining**

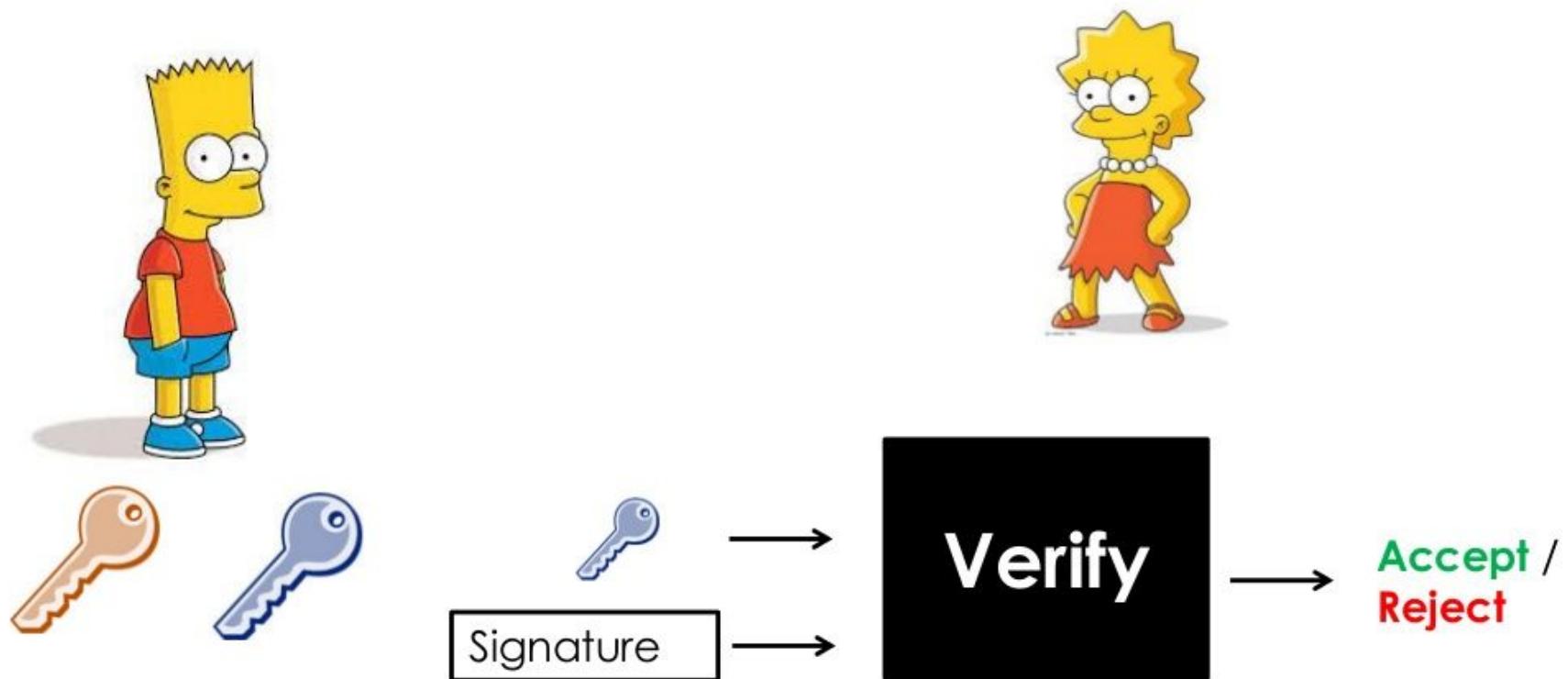
# Crittografia asimmetrica e firme digitali

---



# Crittografia asimmetrica e firme digitali

---



# Crittografia asimmetrica e firme digitali

---



**Non negabile**  
*(non-repudiable)*



**Non falsificabile**  
*(unforgeable)*



## Indirizzi Bitcoin

Un indirizzo Bitcoin è una chiave pubblica (base-58)

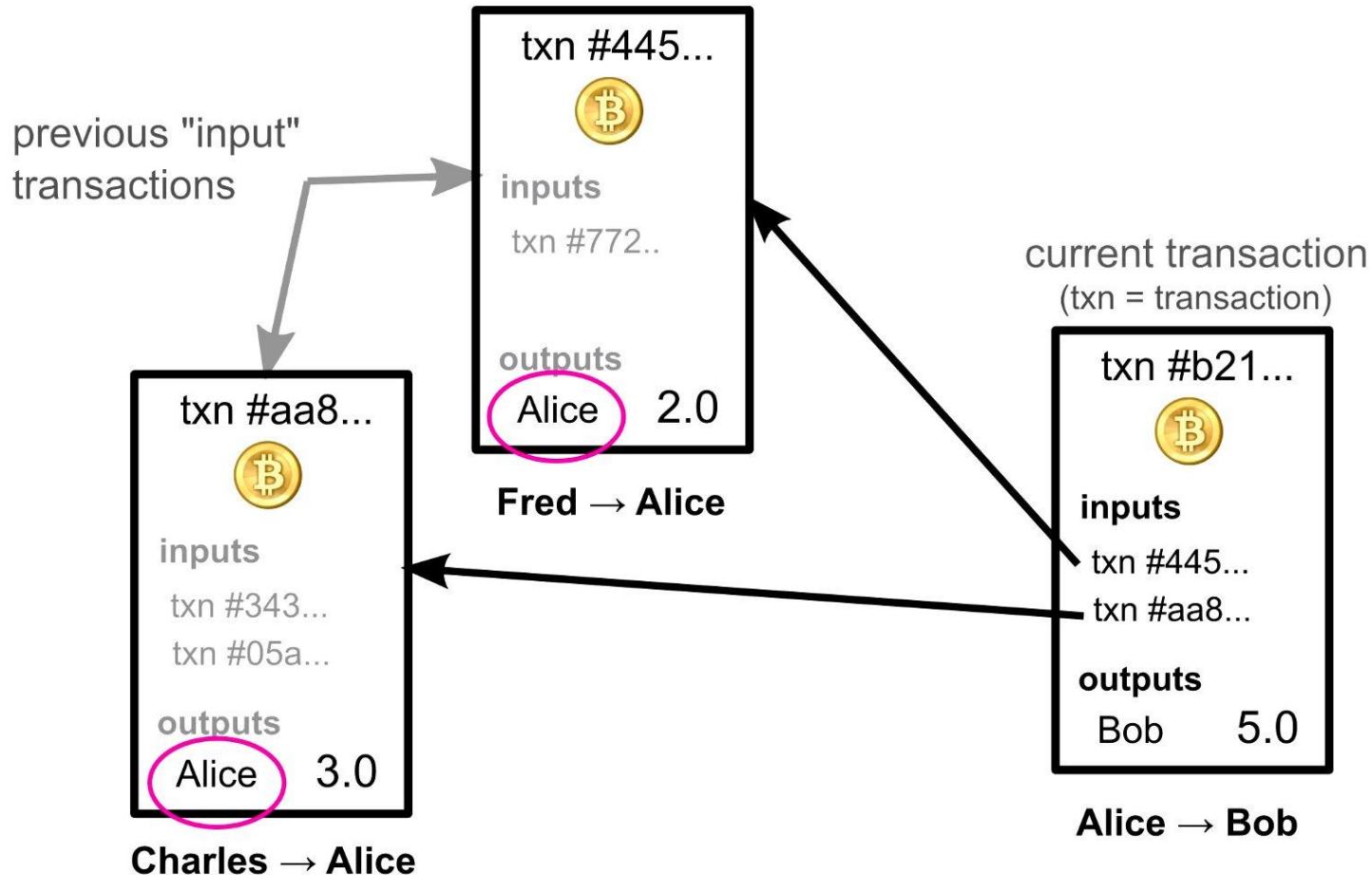
`13NpLwXgEP8d9NpDUHptY6BypFRNXHL3tr`

La chiave privata corrispondente permette di firmare delle transazioni dove si spendono i Bitcoin associati alla chiave pubblica

Indirizzi Bitcoin possono essere creati da chiunque

[www.bitaddress.org](http://www.bitaddress.org)

# Transazioni

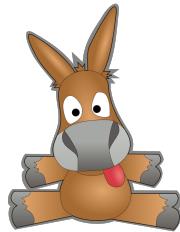


# Invio delle transazioni

---

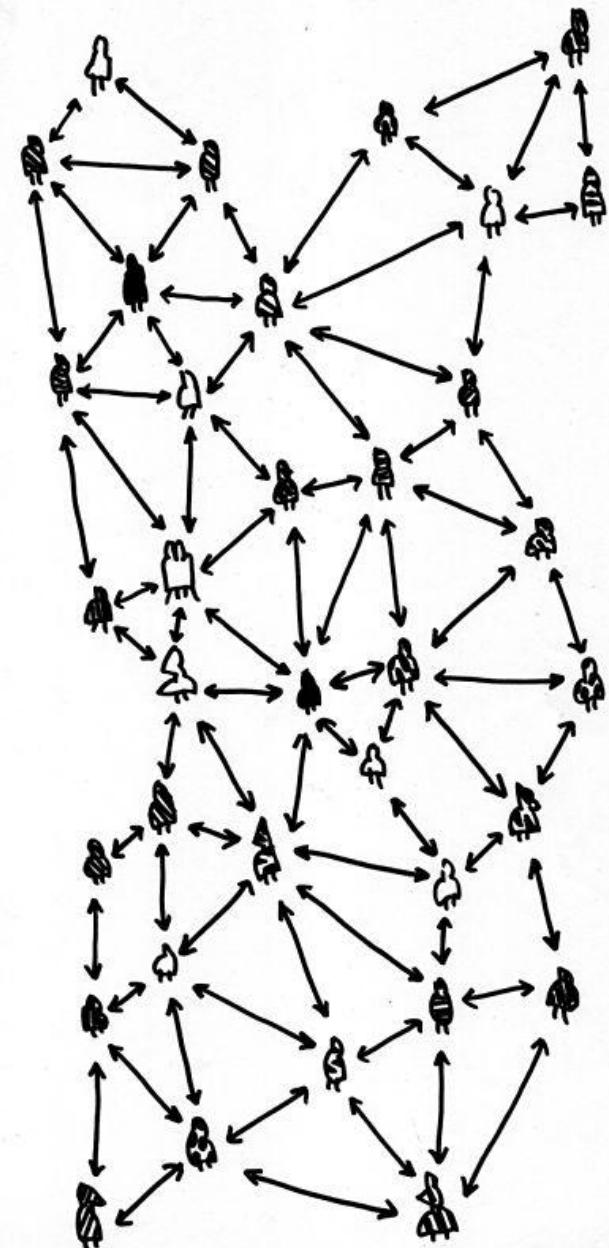
## Peer-to-Peer Network (P2P)

- Le transazioni valide vengono inviate agli altri peers
- In pochi secondi tutti i nodi vengono a conoscenza della transazione



## Come evitare spam e attacchi Denial of Service (DoS)

- Le transazioni vengono validate prima di essere inoltrate

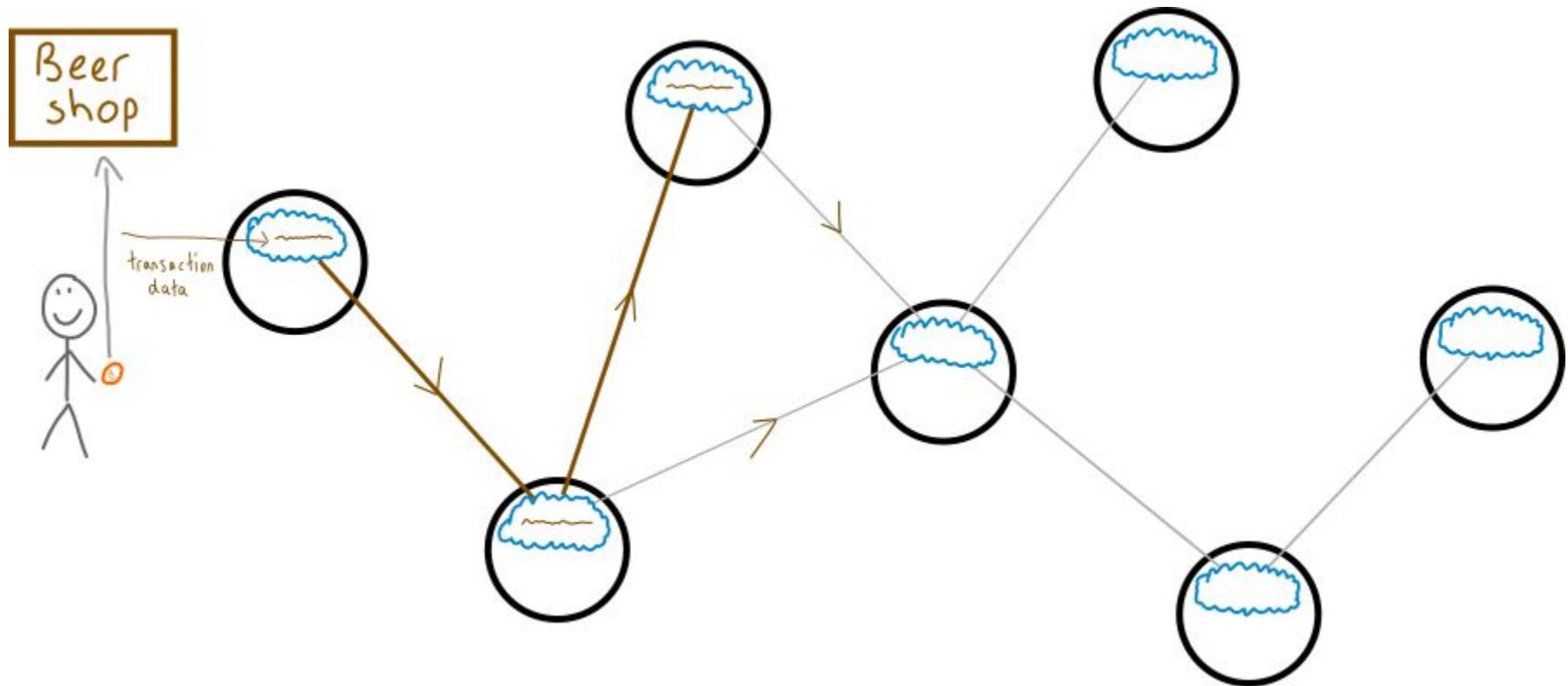


# Il problema del Double Spending

---

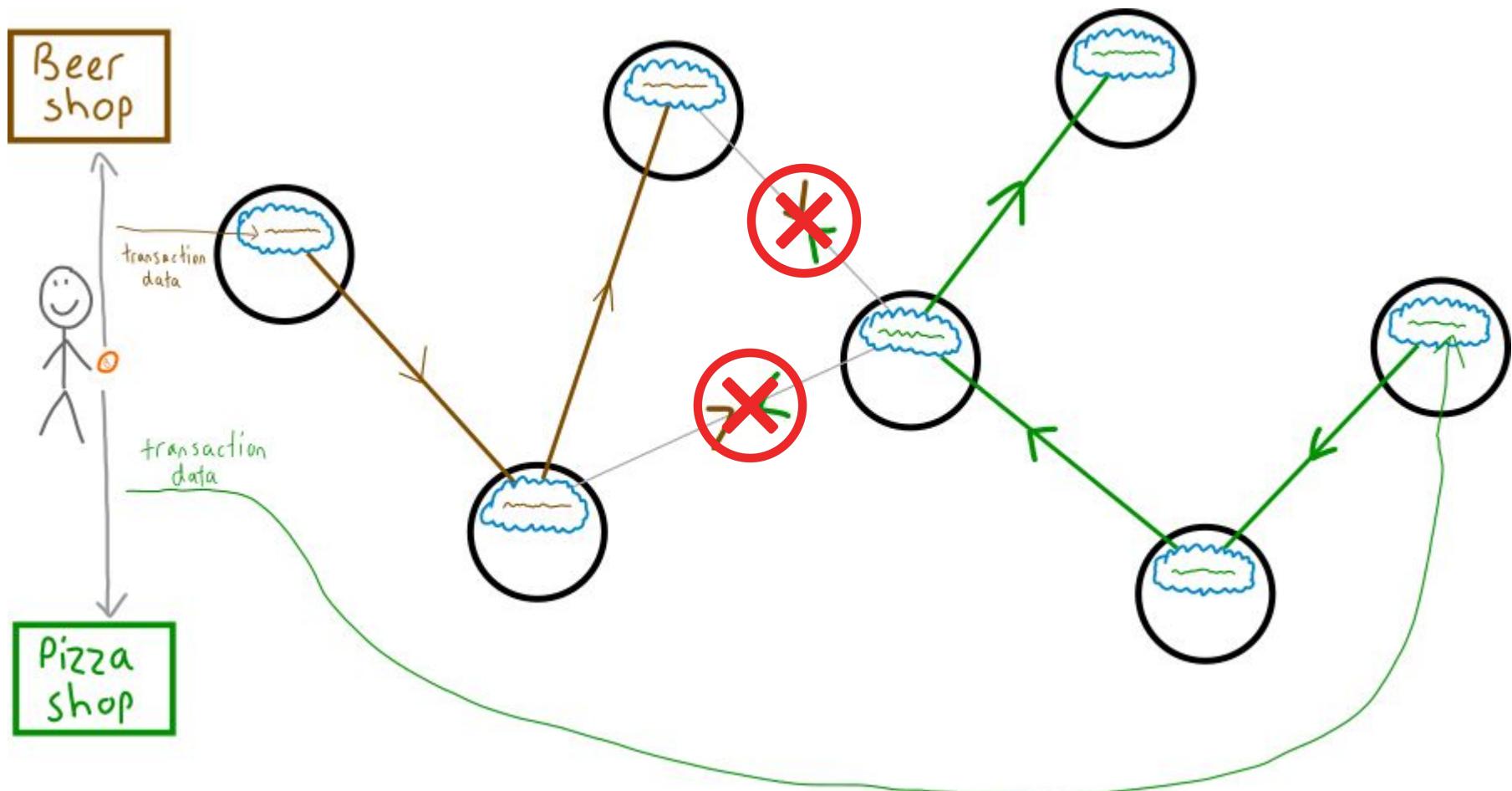
# Double Spending

---



# Double Spending

---

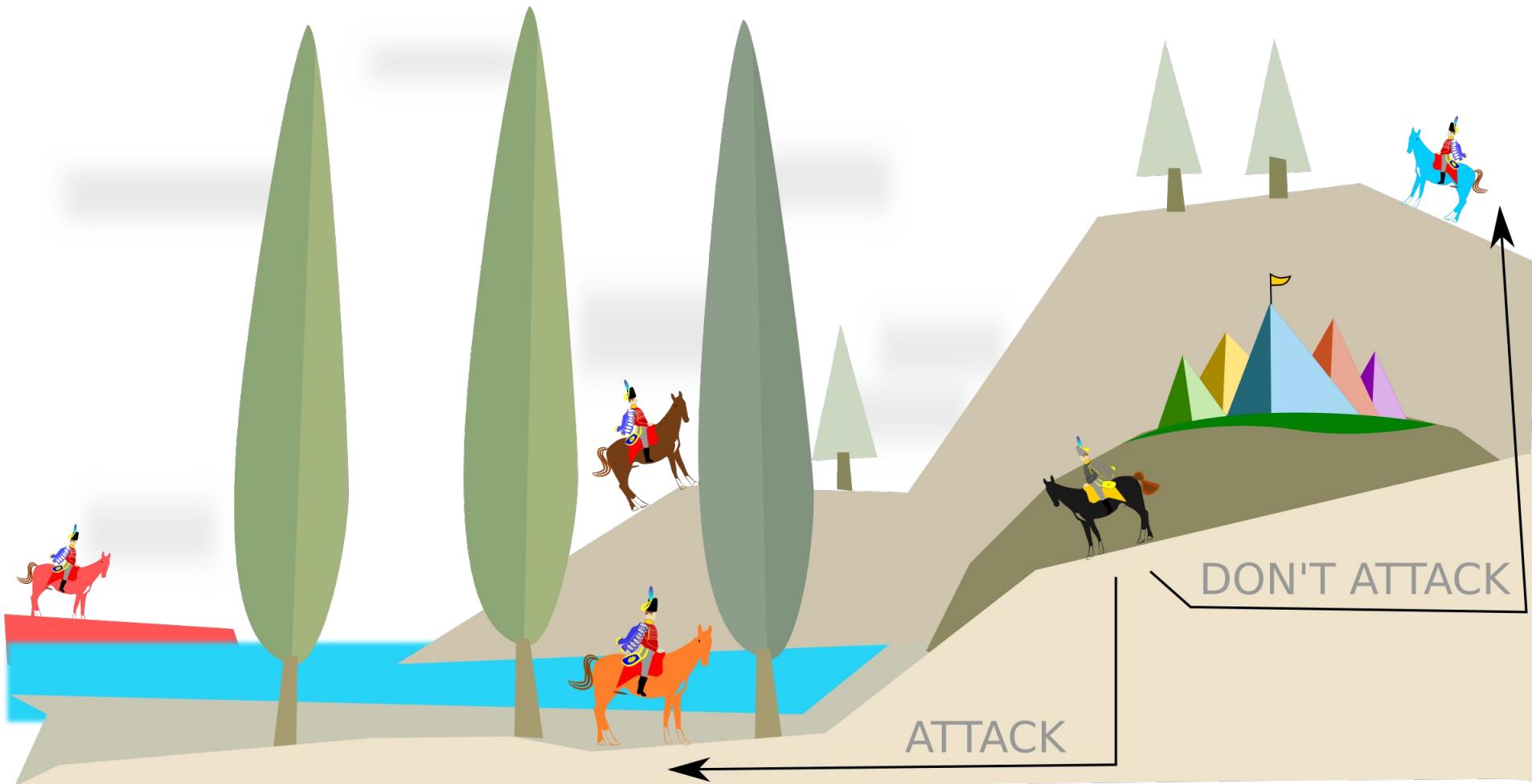


---

# Come raggiungere il consenso in una rete distribuita?

# Problema dei Generali Bizantini

---

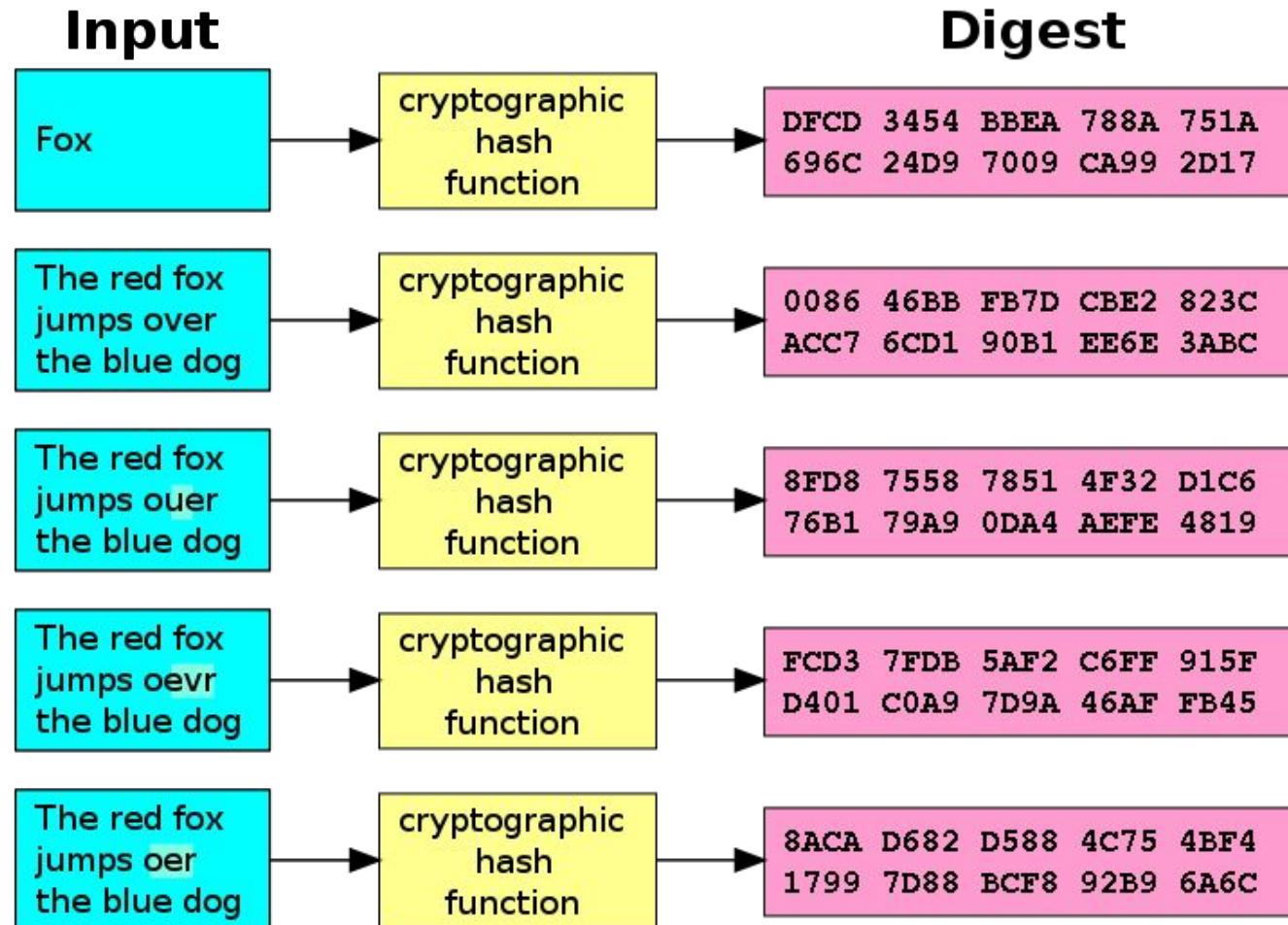


# Blockchain for the win

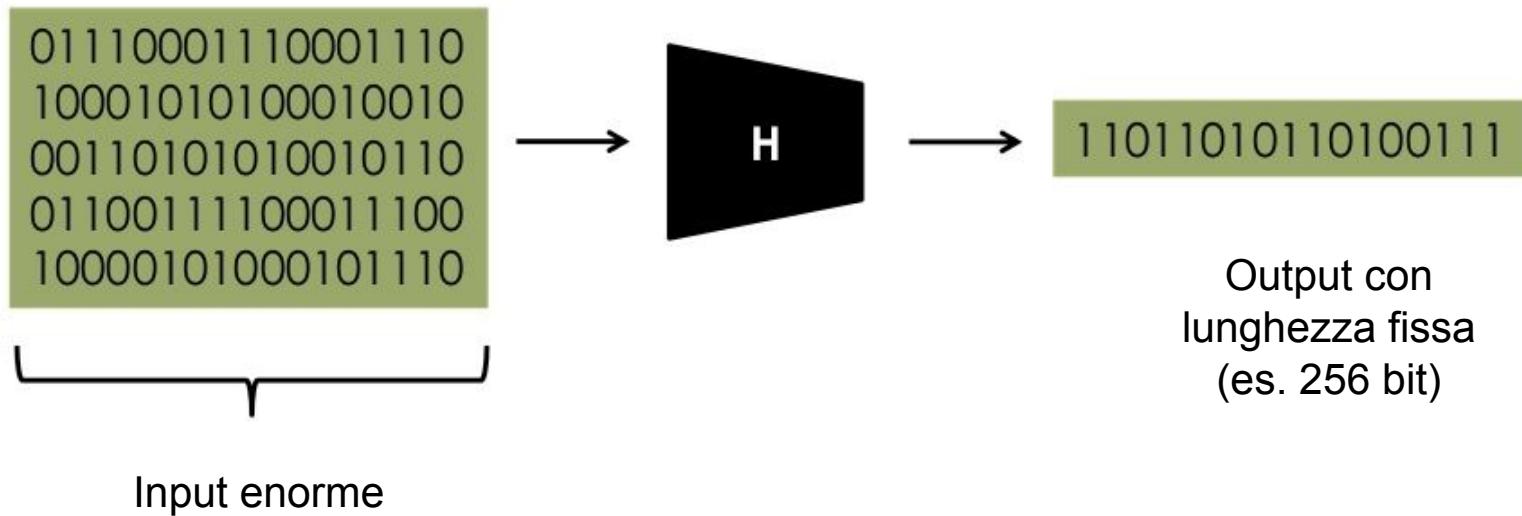
---



# Hash e Controllo di Integrità



# Hash e Controllo di Integrità



- Una modifica di 1 bit in input produce grandi (impredicibili) effetti in output
- Trovare l'inversa è matematicamente non fattibile
- Trovare delle collisioni è matematicamente non fattibile

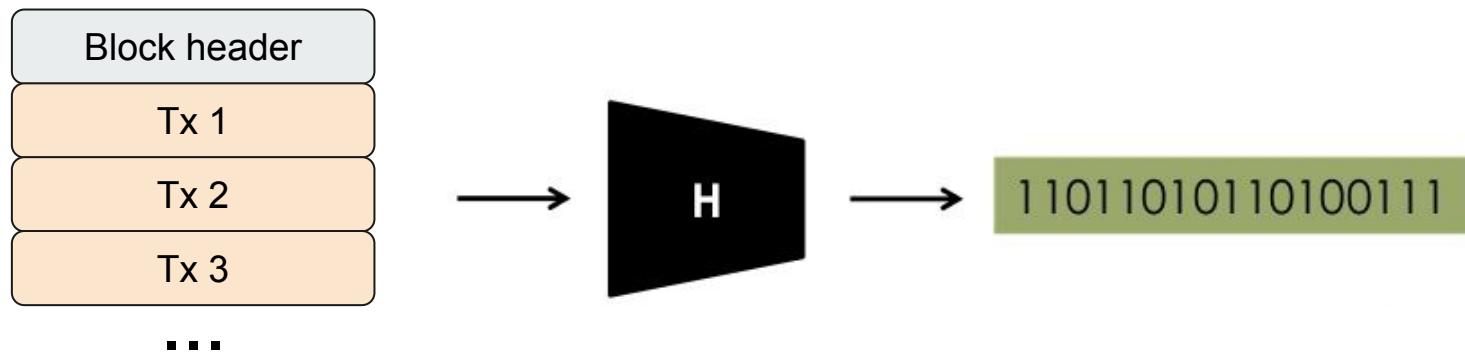
---

*“if every computer ever made by humanity was computing since the beginning of the entire universe, up to now, the odds that they would have found a collision is still infinitely small. So small that it’s way less than the odds that the Earth will be destroyed by a giant meteor in the next two seconds.”*

# Blocco

---

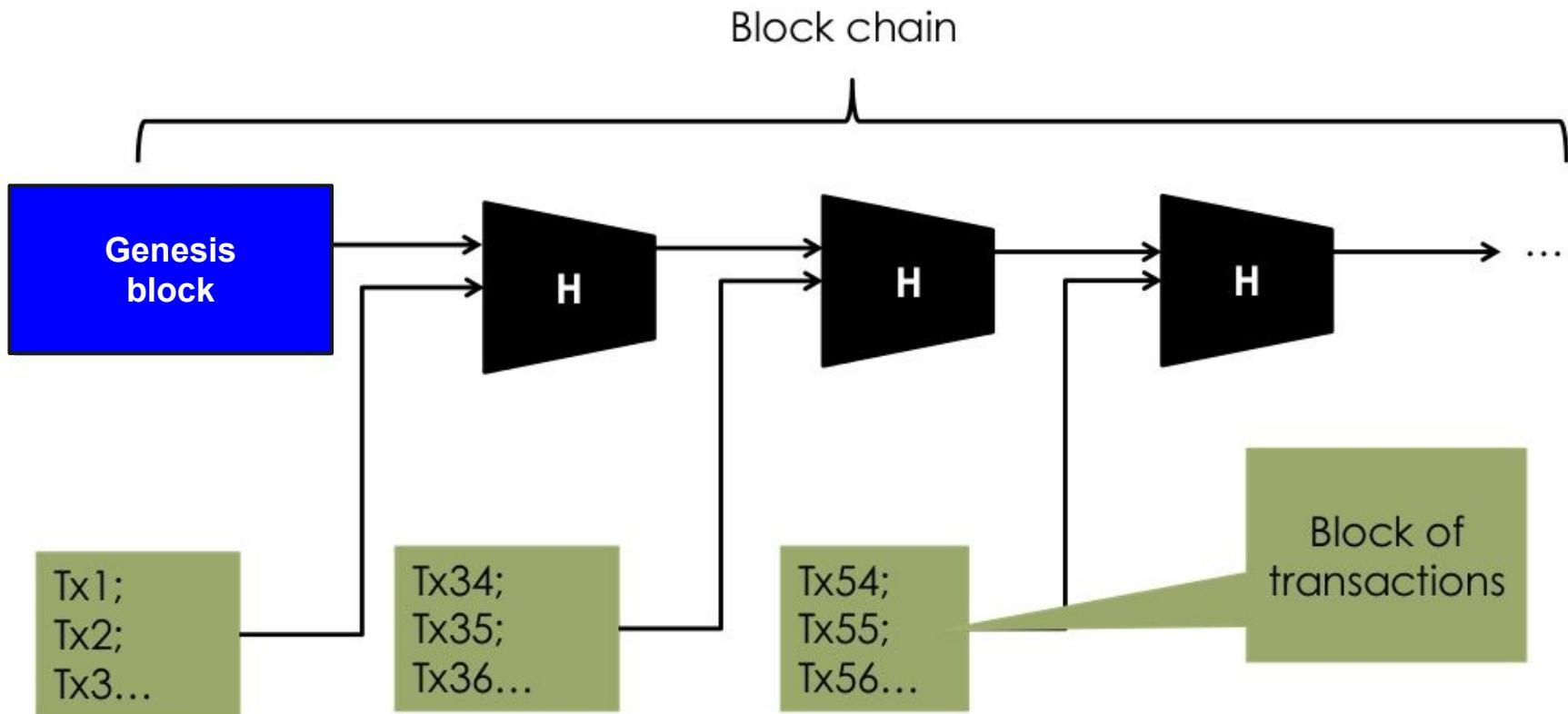
Mettiamo tutte le transazioni in un blocco ...      ... e usiamo questo come input della funzione hash



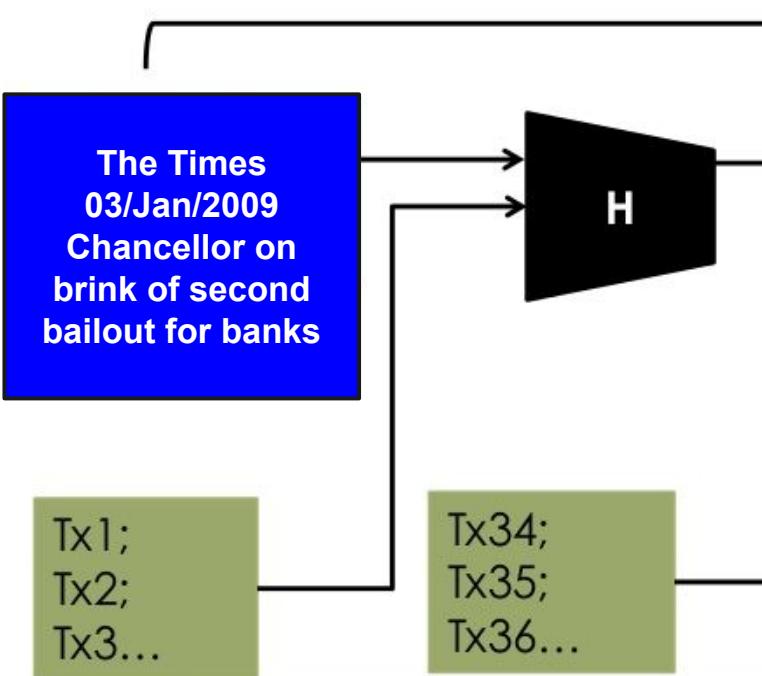
Blocco di  
transazioni

# Blockchain

---



# Bitcoin Genesis



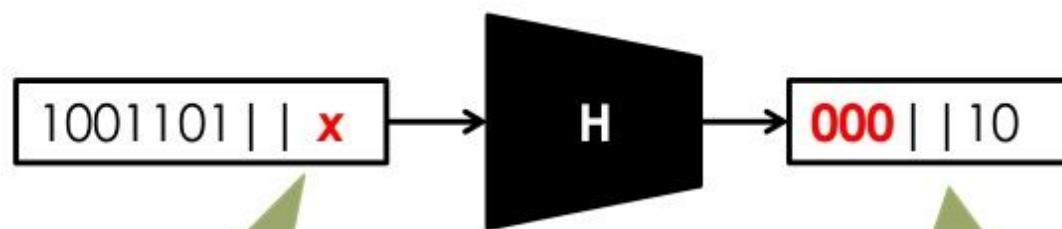
---

## Come ordinare le transazioni?

### Rallentando la generazione dei blocchi

# Proof-of-Work (PoW)

---



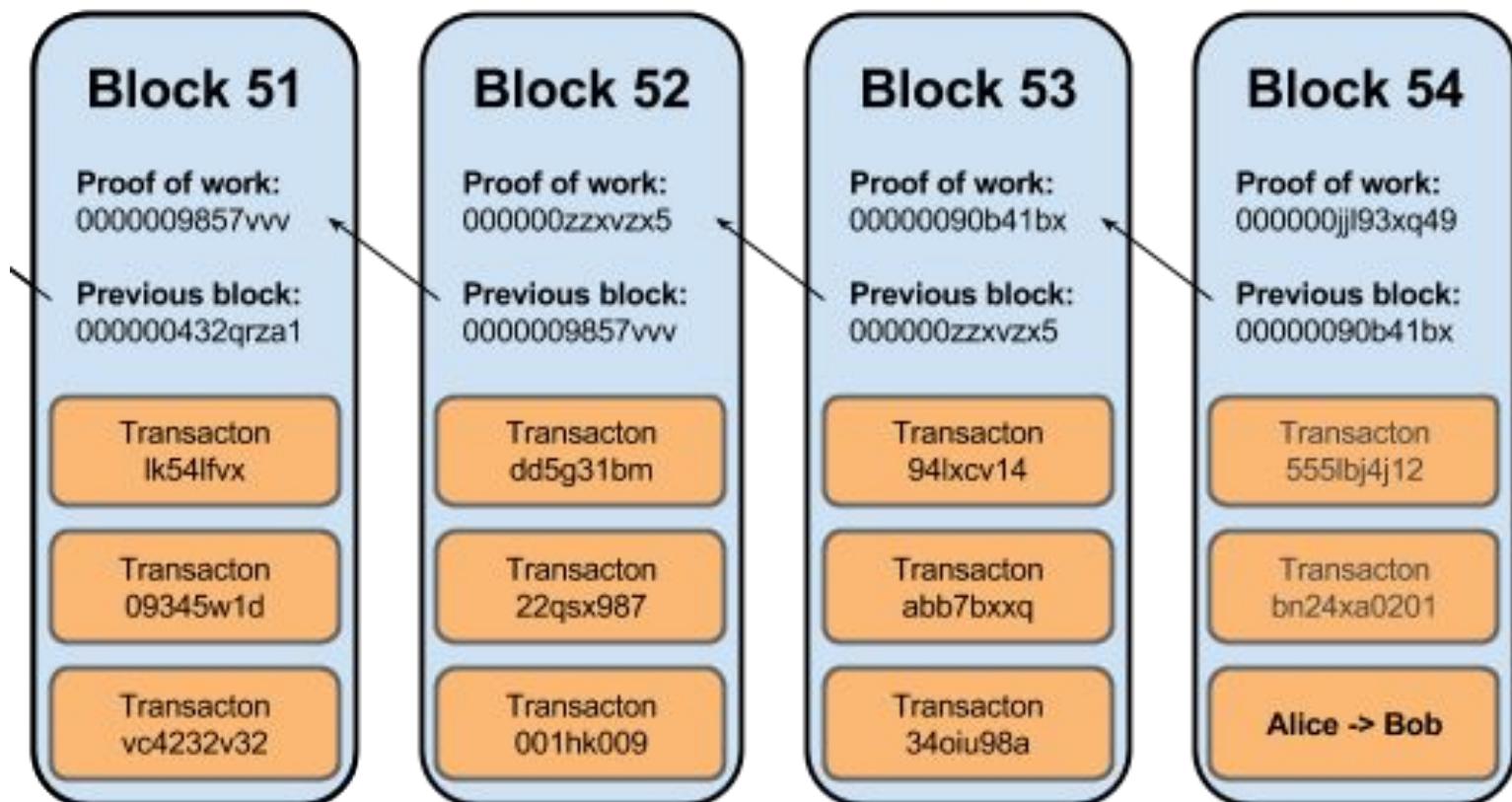
Trova il numero casuale  
(nonce) **x** tale per cui  
l'output inizi con **n** zeri

L'unico modo (\*) per  
trovare una **x** per cui l'output  
inizi con **n** zeri è quello di  
provare circa  $2^{n-1}$  possibilità

(\*) se trovate una soluzione migliore potreste (1) diventare ricchi, (2), diventare famosi (Turing award), o (3) entrambi.

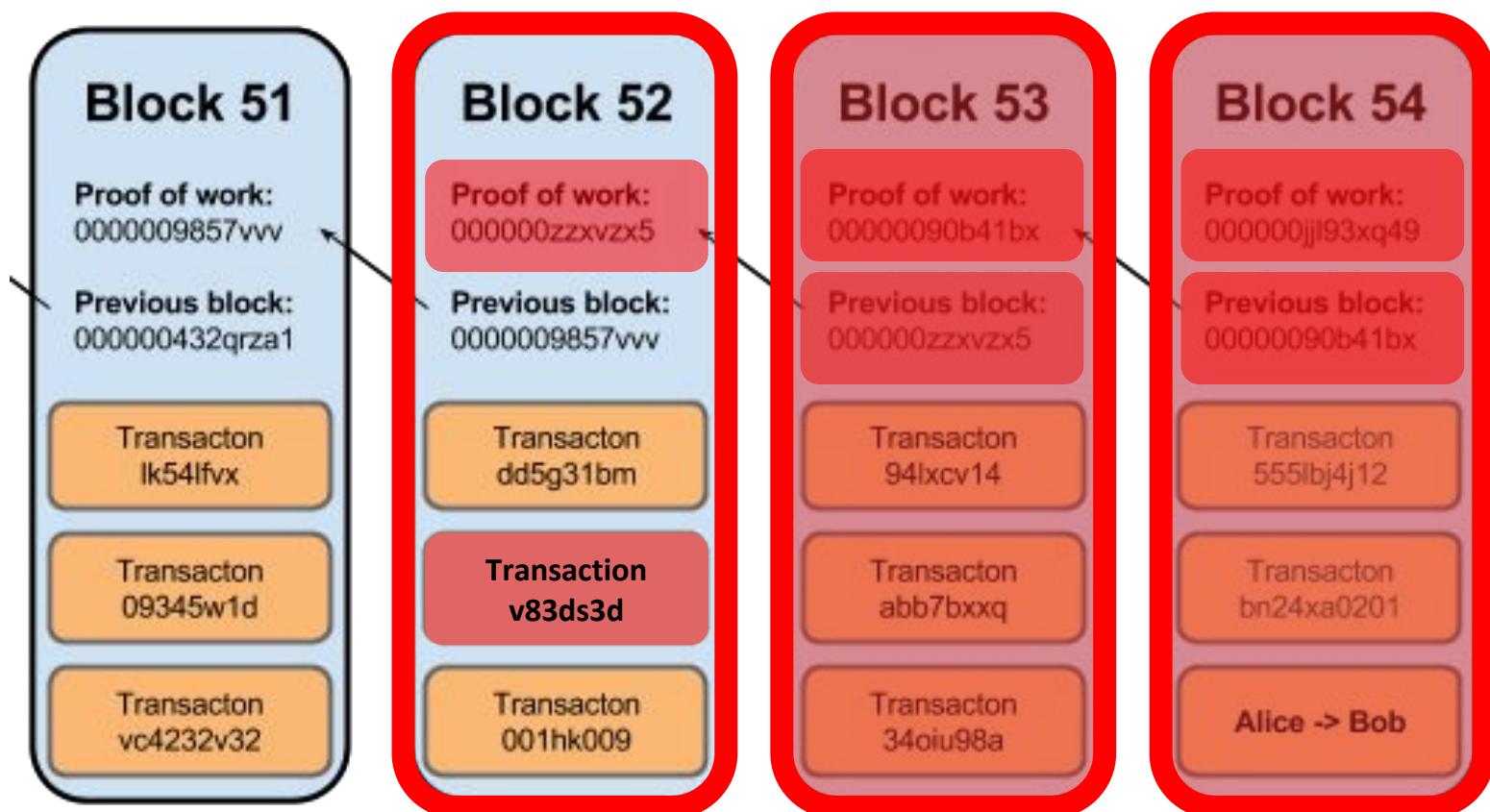
# Blockchain = block chain

---



# Blockchain = block chain

---



La blockchain non è modificabile (a meno di ri-eseguire il Proof-of-Work)

**Bello in teoria,**

**Ma chi butterebbe  
della potenza di calcolo  
per non avere nulla in cambio?**

---



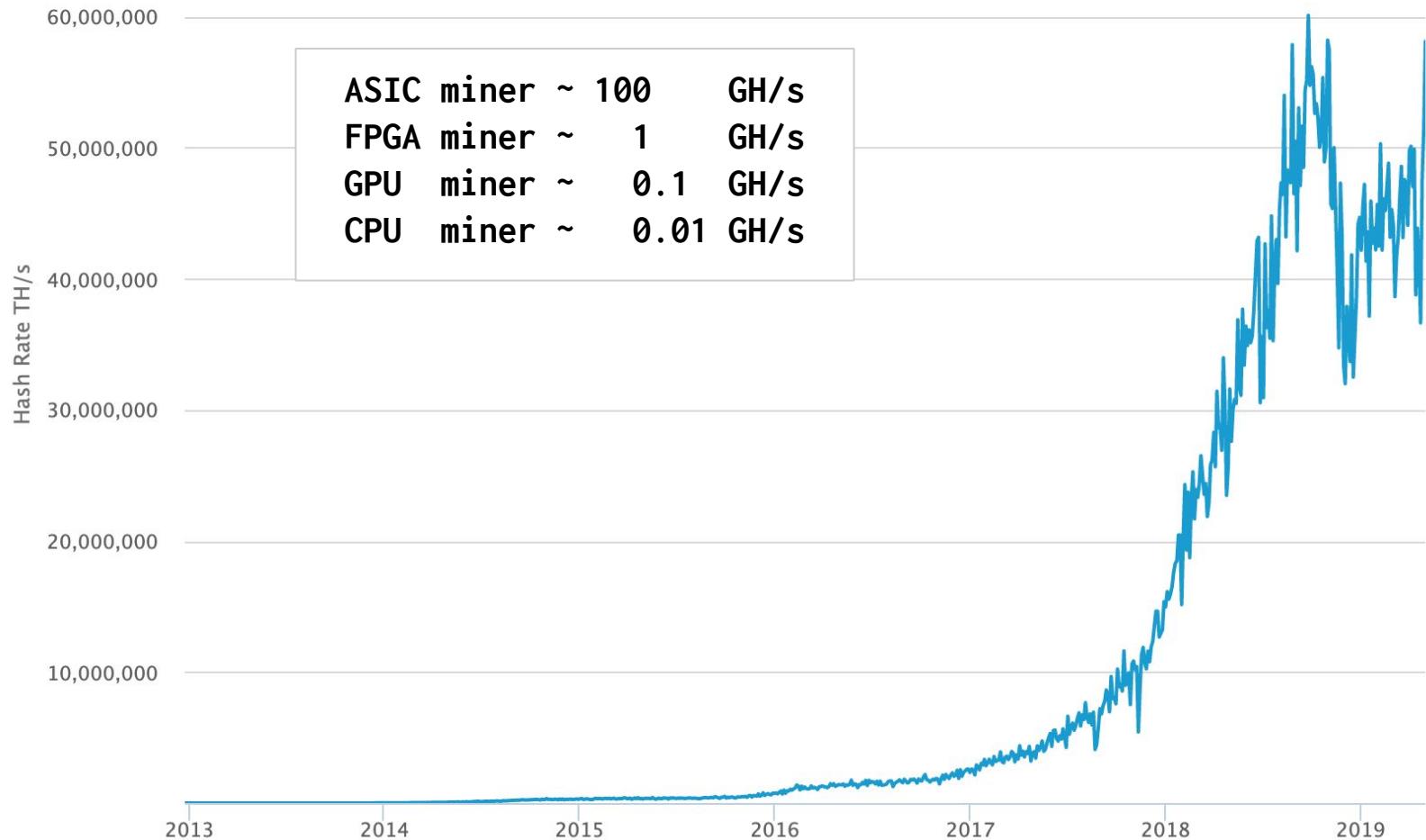
# Bitcoin Mining



# Bitcoin Mining

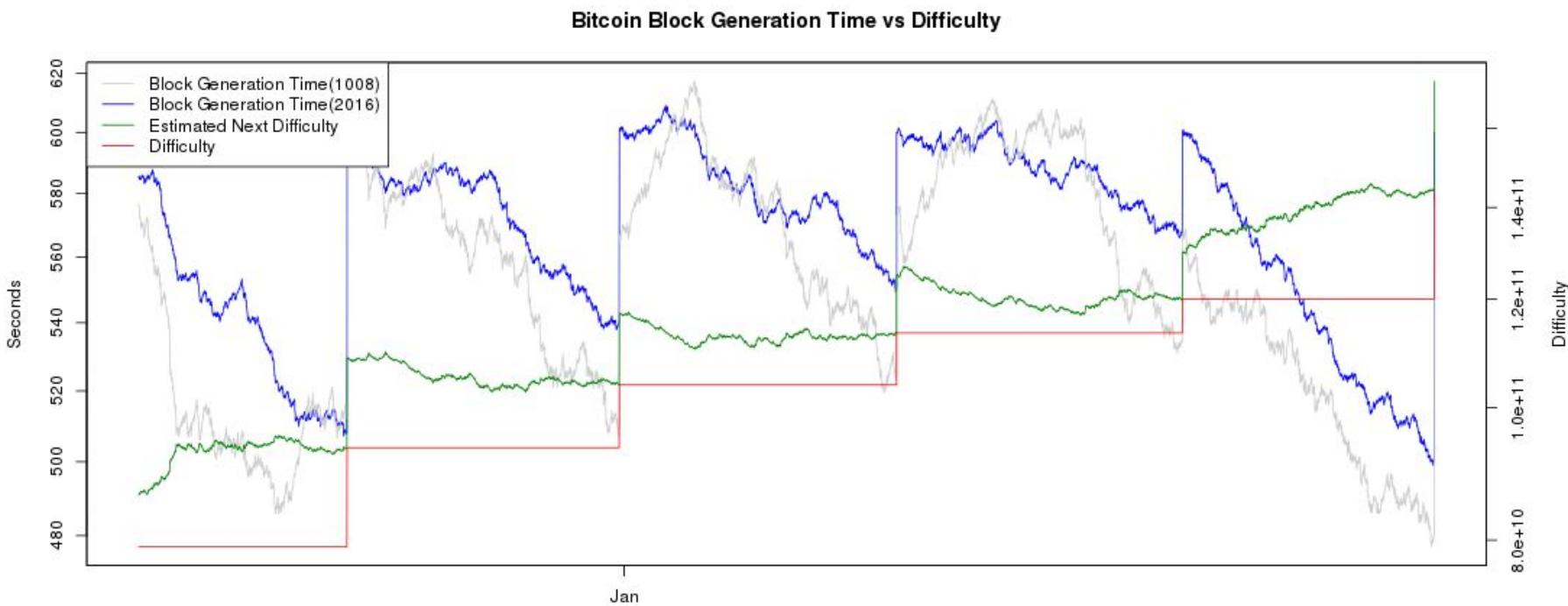
- Chi risolve il blocco è ricompensato con dei Bitcoin
  - Il miner aggiunge una transazione a sé stesso (coinbase) al blocco
  - Tutti i bitcoin sono creati in questo modo
- Qualsiasi abuso è protetto grazie al consenso
- La difficoltà del Proof-of-Work (numero di zeri iniziali nell'hash) viene concordata dai miner in modo da produrre un nuovo blocco ogni 10 minuti.

# Hash Rate

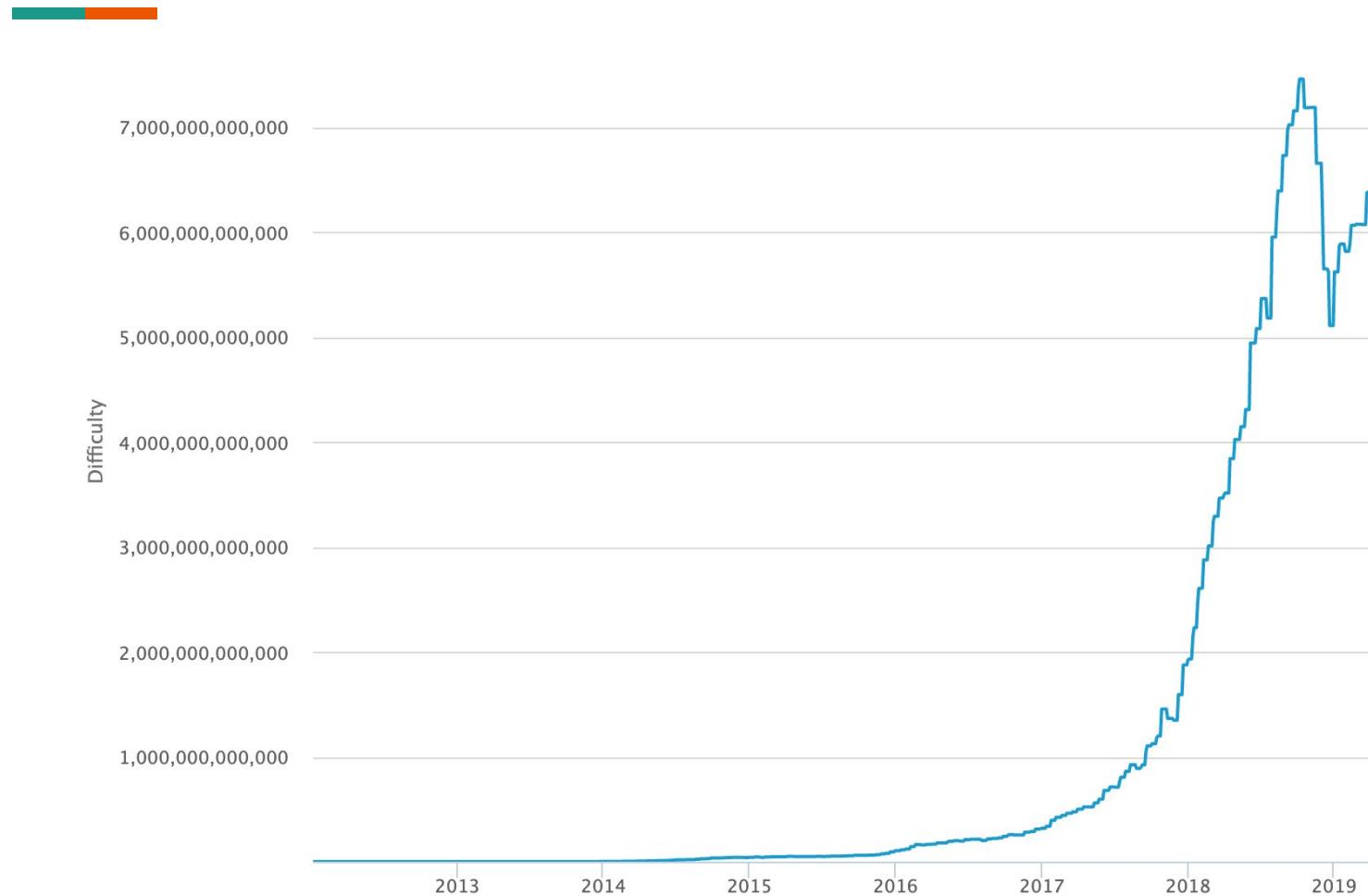


# Difficoltà del Proof-of-Work

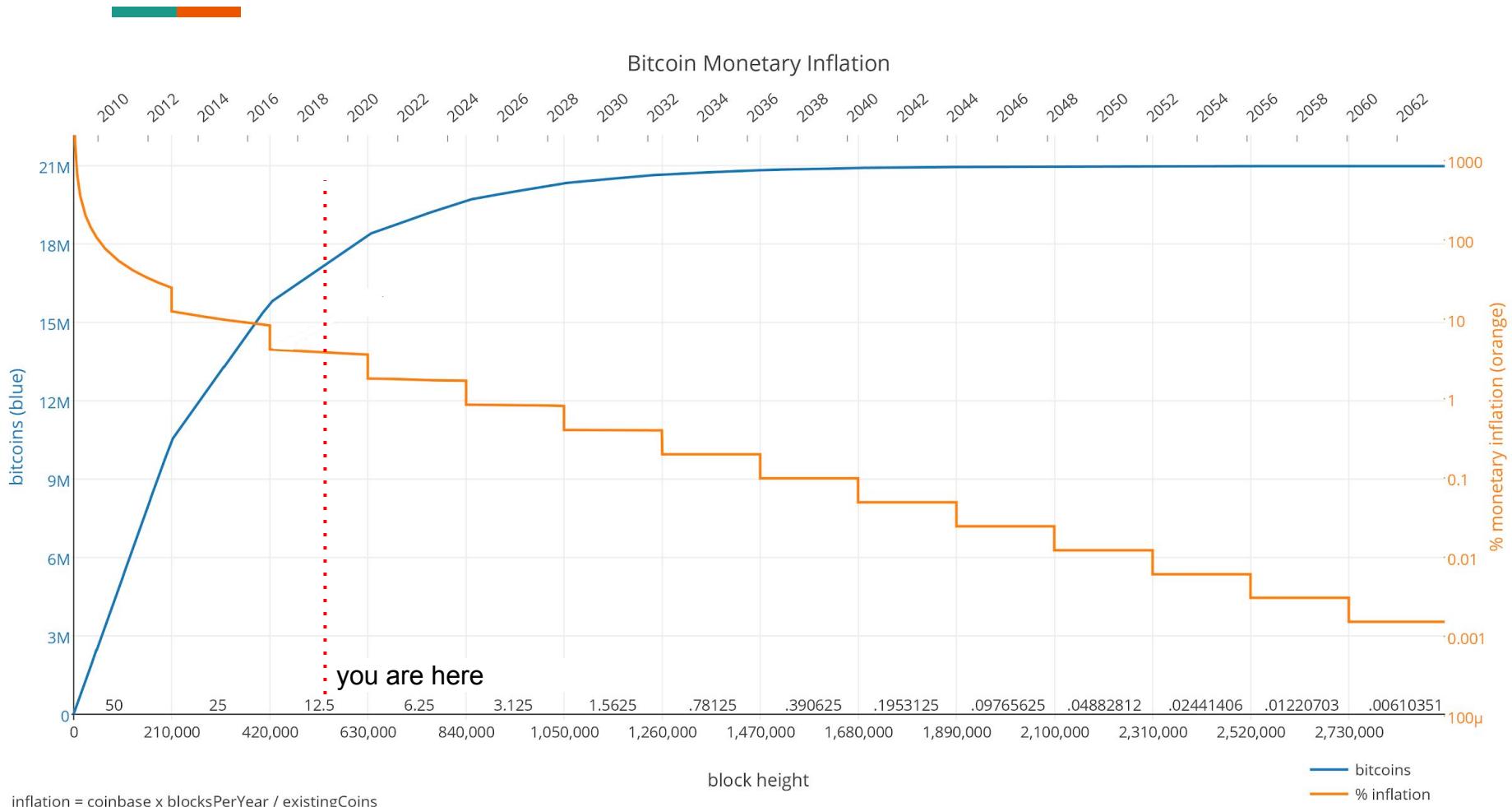
Il tempo di generazione dei blocchi di Bitcoin è regolato dalla difficoltà.



# Difficoltà del Proof-of-Work



# Block Reward - Inflazione controllata

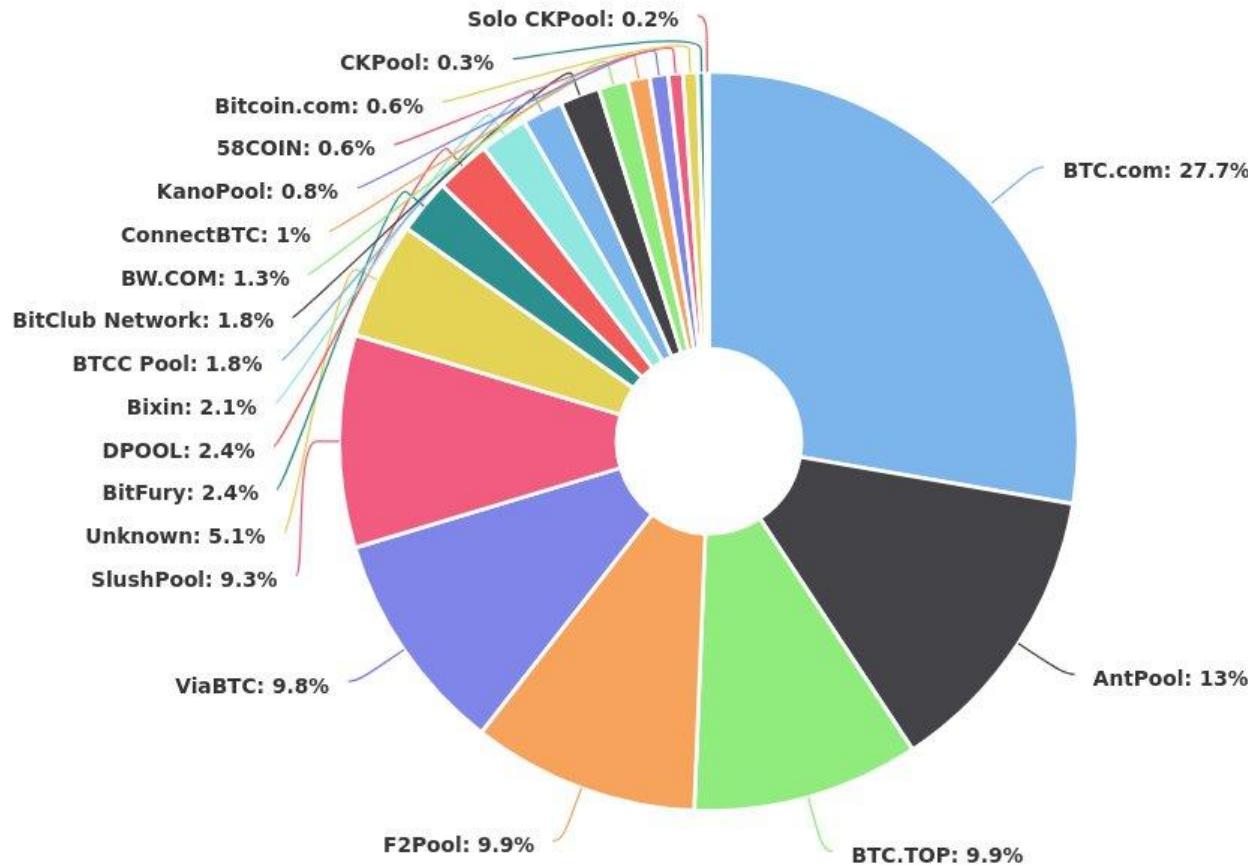


# Transaction Fees

TRANSACTION FEES ARE MEANT TO  
REPLACE BLOCK REWARDS



# Pool Mining

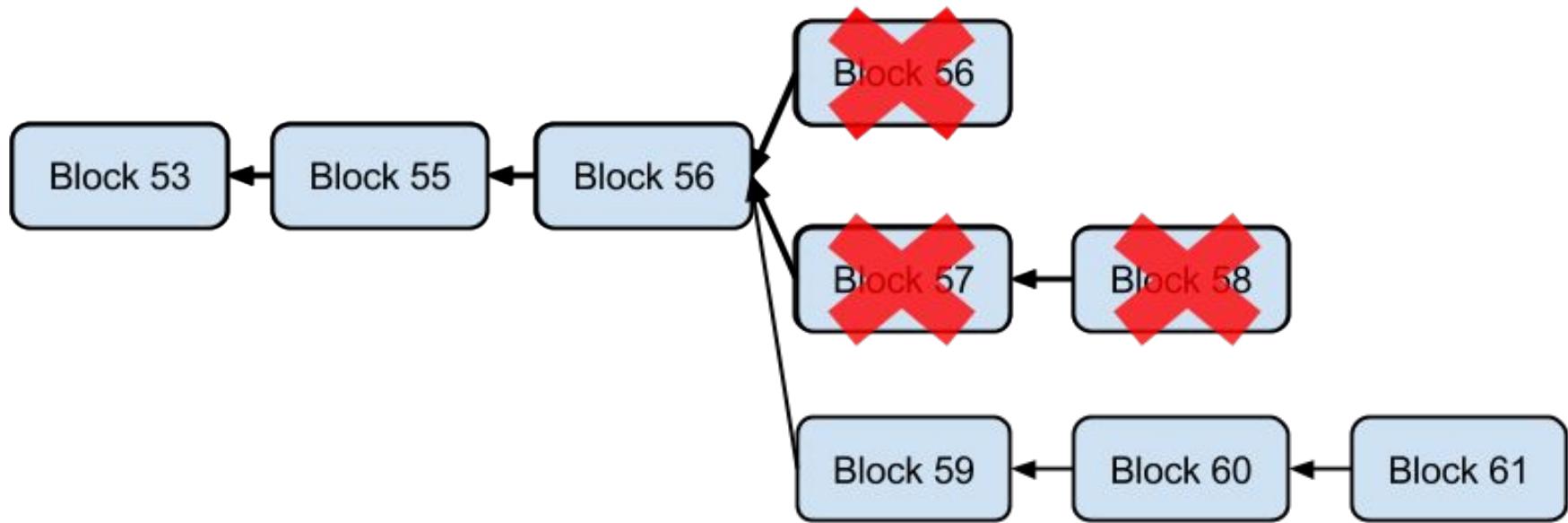


**Cosa succede se due miners  
producono un blocco nello  
stesso momento?**

---

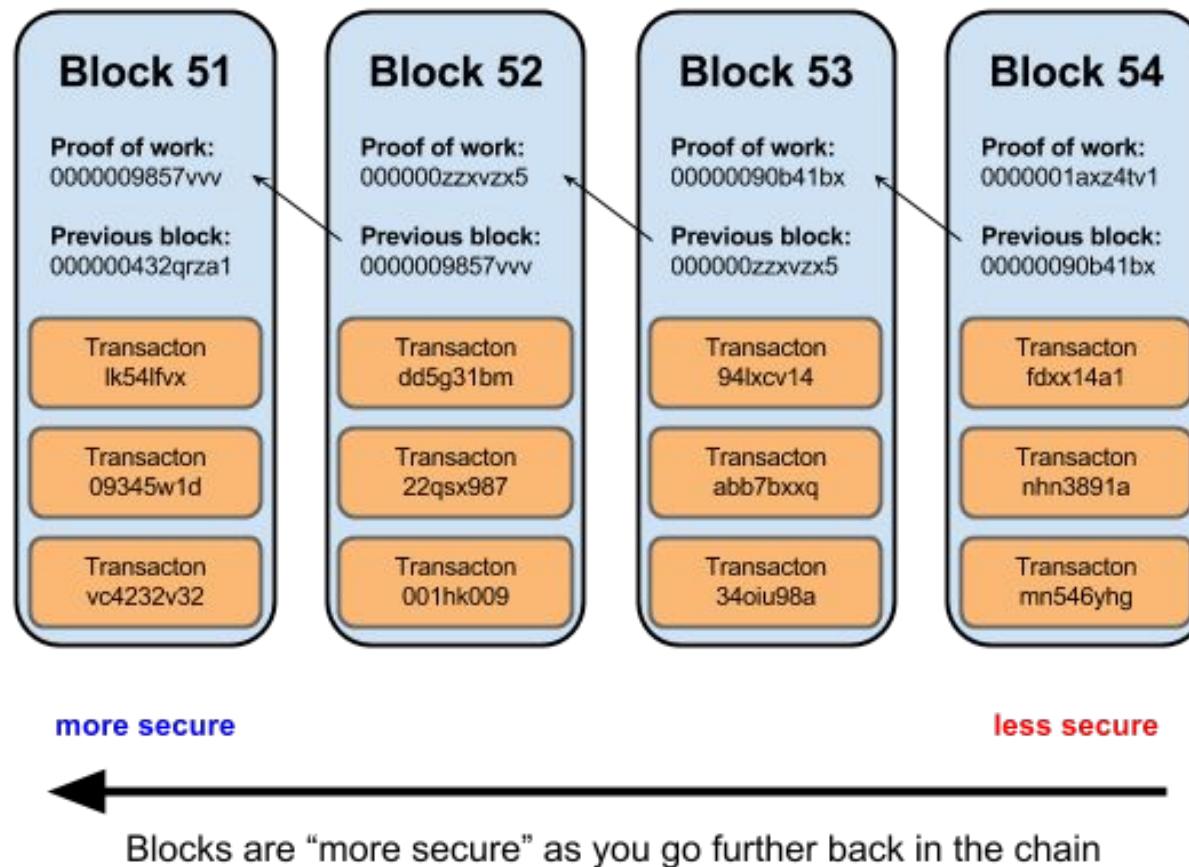
---

## Regola della catena più lunga



# Double Spending

---



# Cosa è Bitcoin?

**un libro mastro pubblico e  
distribuito basato sul consenso**

---

---

## Parte II

# Punto di vista pratico e finanziario



## DISCLAIMER

**Questa lezione non costituisce  
consiglio finanziario / legale.**

# Possesso e gestione di Bitcoin

---

---

## Tipi di Wallet

- App wallet
- Exchange wallet
- Paper wallet
- Hardware wallet



# App Wallet

- Online e mobile
- In molti casi offrono carte di debito associate
- Accettano fiat currency
- Coinbase
- BitPay
- Monaco
- ...



Date	Description	Amount
January 08, 2015	You sent bitcoin to Brian Armstrong	-0.042808
January 02, 2015	You sent bitcoin to New User	-0.0028445
December 21, 2014	You purchased bitcoins	+0.28004
December 14, 2014	You purchased bitcoins	+0.28004
December 12, 2014	You sent a bitcoin gift to Karri	-0.001
December 12, 2014	You sold bitcoins	-0.001
December 12, 2014	You purchased bitcoins	+0.28004
December 11, 2014	You received bitcoin from New	-0.001
December 11, 2014	You received bitcoin from New	-0.001

# Exchange Wallet

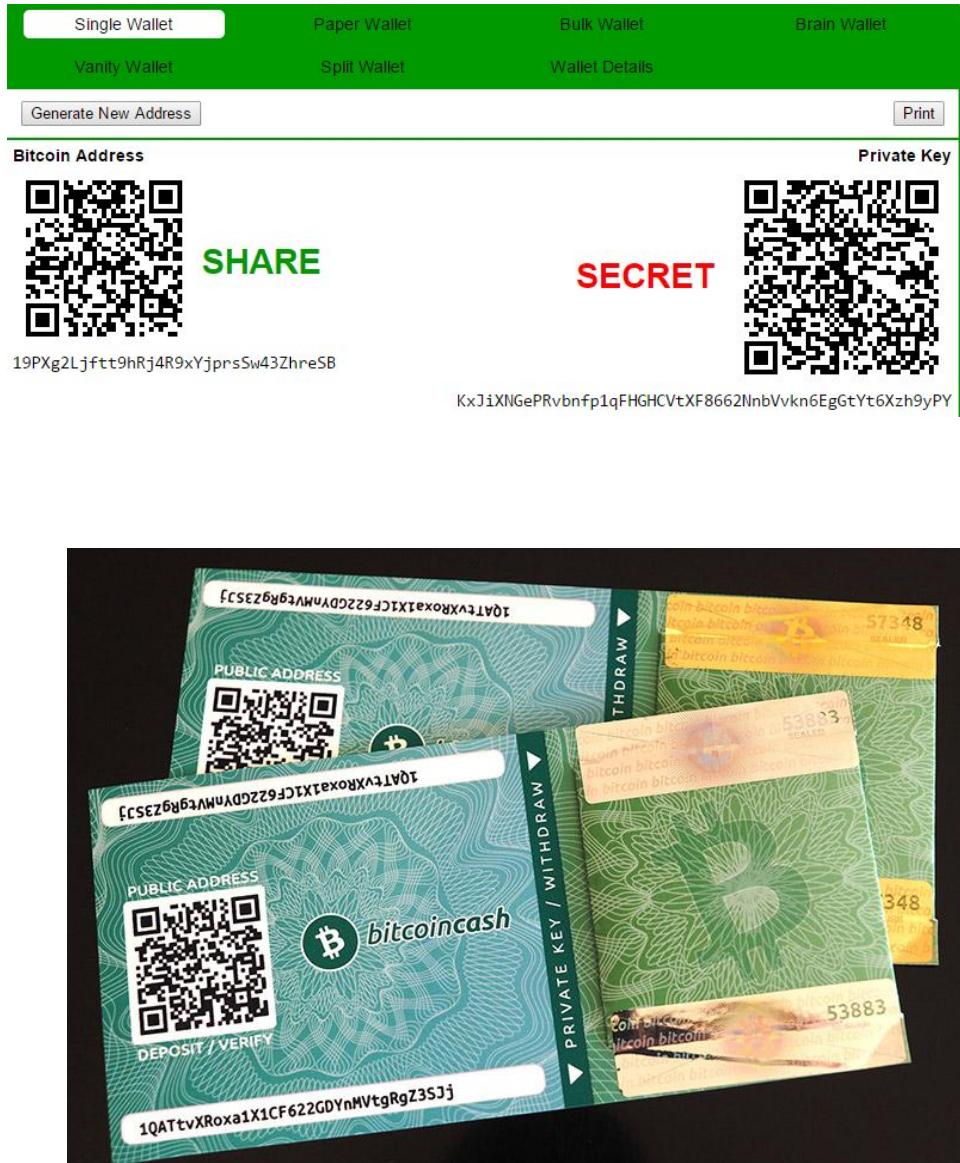
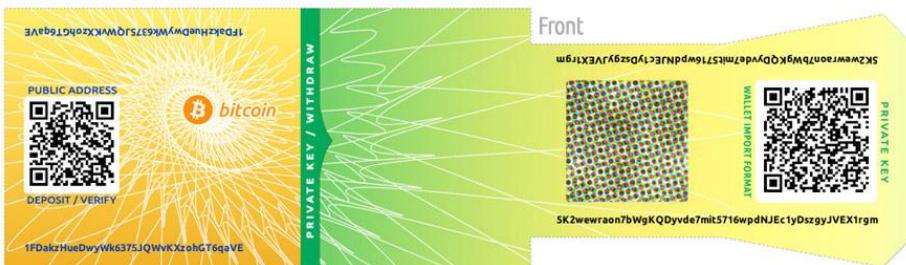
- Il metodo più semplice
- Accettano fiat currency (non tutti)
- Utili per trading
- Kraken
- Poloniex
- eToro
- Gemini
- ...



The screenshot shows the Poloniex exchange wallet interface. It features three main forms: 'BUY ETH', 'STOP-LIMIT', and 'SELL ETH'.  
1. 'BUY ETH': Fields include Price (0.02706373 BTC), Amount (ETH), Total (BTC), and Fee (0.2% Fee, ETH). A red box highlights the 'Buy' button.  
2. 'STOP-LIMIT': Fields include Price (0.02706379 BTC), Stop (BTC), Limit (BTC), Amount (ETH), and Total (BTC).  
3. 'SELL ETH': Fields include Price (0.02700003 BTC), Amount (ETH), Total (BTC), and Fee (0.2% Fee, BTC).  
Below these forms is a 'NOTICES' section containing a message from a user named 'Talmyon' about a mod position and an announcement about a maker-taker fee schedule starting March 20th.

# Paper Wallet

- Coppia di chiavi generata localmente e stampata su carta
- Si possono solo fare trasferimenti
- Sicuri
- bitaddress.org



# Hardware Wallet

---

- Metodo più sicuro
- Trezor
- Ledger Nano S
- KeepKey
- ...



 **TREZOR**



# Buy Bitcoin

---

Oltre ai metodi appena visti ne esistono altri in cui le valute vengono acquistate “di persona”

- ATM ([coinatmradar.com](http://coinatmradar.com))
- [localbitcoins.com](http://localbitcoins.com)



# Rischi

---

## Mt. Gox Allegedly Hacked: "This Could Be the End of Bitcoin"

February 25, 2014 // 07:30 AM EST

- Hacking
  - Mt.Gox
  - Bitfinex
  - BitGrail
  - ...
- Truffe
  - Bitconnect
  - OneCoin
  - ...



Ponzi crypto coins @bccponzi · 13h

Why are crypto experts like  
[@VitalikButerin](#) and [@SatoshiLite](#) not  
speaking out their concerns about  
Bitconnect? They could make a  
difference!

12

9

33



Vitalik Buterin ✅ @VitalikButerin · 2h

I actually have no idea what bitconnect  
is.



Ponzi crypto coins @bccponzi · 33m

1% interest compounded daily would  
make your \$1000 investment worth \$50  
million+ in 3 years, does that sound  
sustainable to you?

1

2

3



Vitalik Buterin ✅ @VitalikButerin · 14m

Yeah, if 1%/day is what they offer then  
that's a ponzi.

1

7

14



# Conseguenze



- Nessun risarcimento
- Crollo del prezzo
- Fork?



Francesco The Bomber @bomberfrancy · 27m  
NANO on BitGrail have been stolen.

Unfortunately there is no way to give it back to you at 100% (we only got 4 MLN XRN right now).

The devs, as you have guessed, dont want to collaborate



118



4

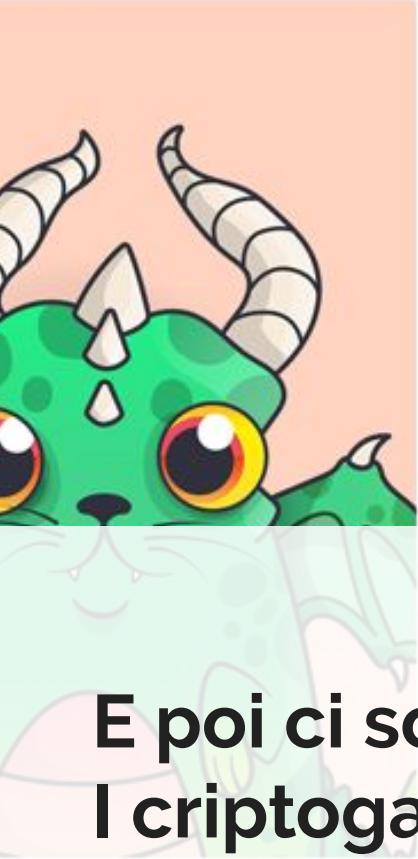
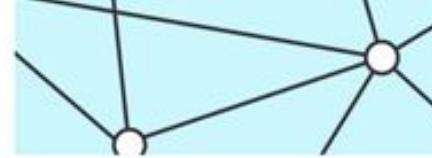


2



# CryptoKitties

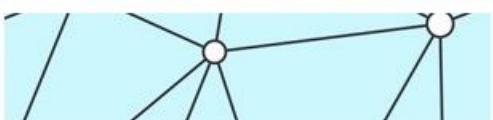
E poi ci sono  
I criptogattini ...







\$2500



\$115,000



\$54



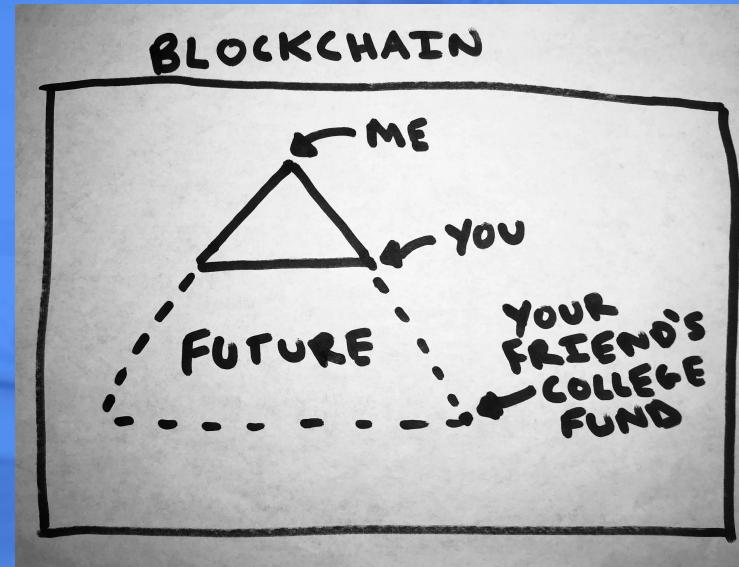
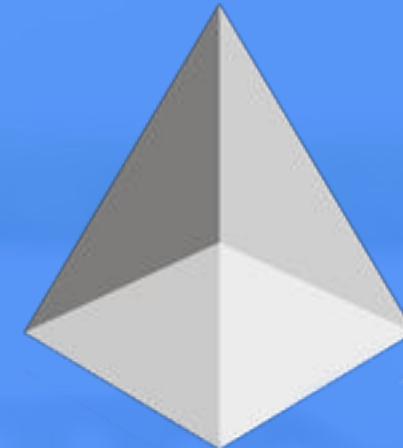




# The World's First Legitimate Ponzi Scheme

Because money doesn't grow on trees... unless you're BitFinex

Learn More





# Create your own coin! (i.e., attenti alle truffe)

bitcoin / bitcoin

Watch 3,380 Unstar 32,651 Fork 19,631

Code Issues 546 Pull requests 265 Projects 7 Insights

Bitcoin Core integration/staging tree <https://bitcoin.org/en/download>

bitcoin c-plus-plus p2p cryptocurrency cryptography

17,422 commits 7 branches 197 releases 551 contributors MIT

Branch: master New pull request Create new file Upload files Find file Clone or download

MarcoFalke Merge #13506: Qt: load wallet in UI after possible init aborts ... Latest commit 6579d80 44 minutes ago

.github Make default issue text all comments to make issues more readable 7 months ago

.tx tx: Update transifex slug for 0.16 5 months ago

build-aux/m4 ax\_boost\_{chrono,unit\_test\_framework}.m4: take changes from upstream 3 months ago

contrib Merge #13454: Make sure LC\_ALL=C is set in all shell scripts 2 days ago

# Create your own coin! (i.e., attenti alle truffe)

## Fork It Till You Make It

This is a Bitcoin fork coin generator. Use at your own risk. Please read the [Terms of Service](#) and [FAQ](#).

The screenshot shows a web-based application for generating a Bitcoin fork coin. The interface is designed to look like a standard Bitcoin wallet application.

**Header:** BitcoinCobaltExtreme Core - Wallet

**Navigation Bar:** Overview, Send, Receive, Transactions

**Send Form:**

- Pay To:** Enter a BitcoinCobaltExtreme address (e.g. FTG7aX1m13XM5T63MDQ5JamKbZR4jVdPDQ)
- Label:** Enter a label for this address to add it to your address book
- Amount:**  BCX  Subtract fee from amount

**Fee Section:** Transaction Fee: 0.00020000 BCX/kB  Warning: Fee estimation is currently not possible.

**Action Buttons:** Send, Clear All, Add Recipient

**Balance:** 0.00000000 BCX

**Status Bar:** Syncing Headers (17.3%)...  BCX HD ⚙️ ⚙️

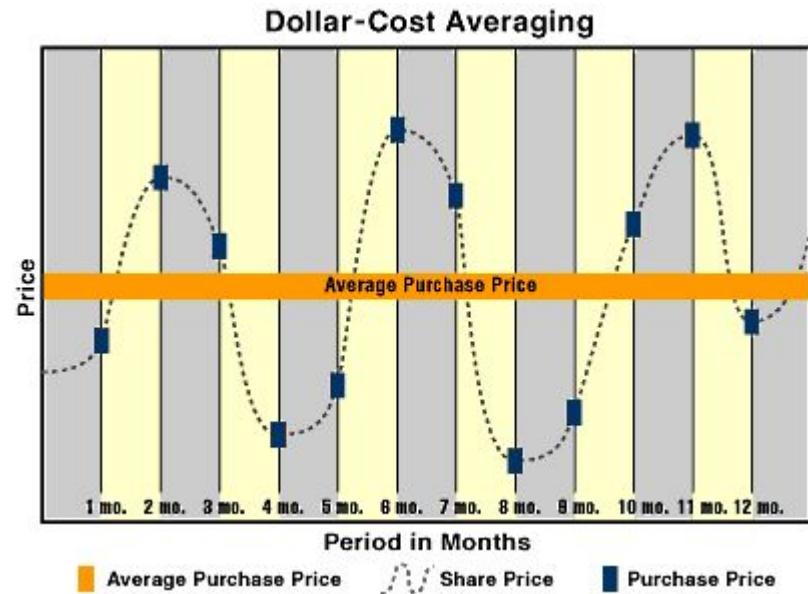
For too long it has been extraordinarily difficult, even for [leading developers](#), to fork the Bitcoin blockchain. The need to change source code and to use a compiler has been an excessive burden. Forkgen was created to allow innovation to break free of the central planning stranglehold of Core. Inspired by successful forks like Bitcoin Gold, Bitcoin Diamond and BCash, and the visionary leadership of Craig Wright, Forkgen is the embodiment of Satoshi's True Vision™ where if big blocks are good for scaling then **many chains** are even better.

# Utilizzi di Bitcoin

---

# Trading finanziario

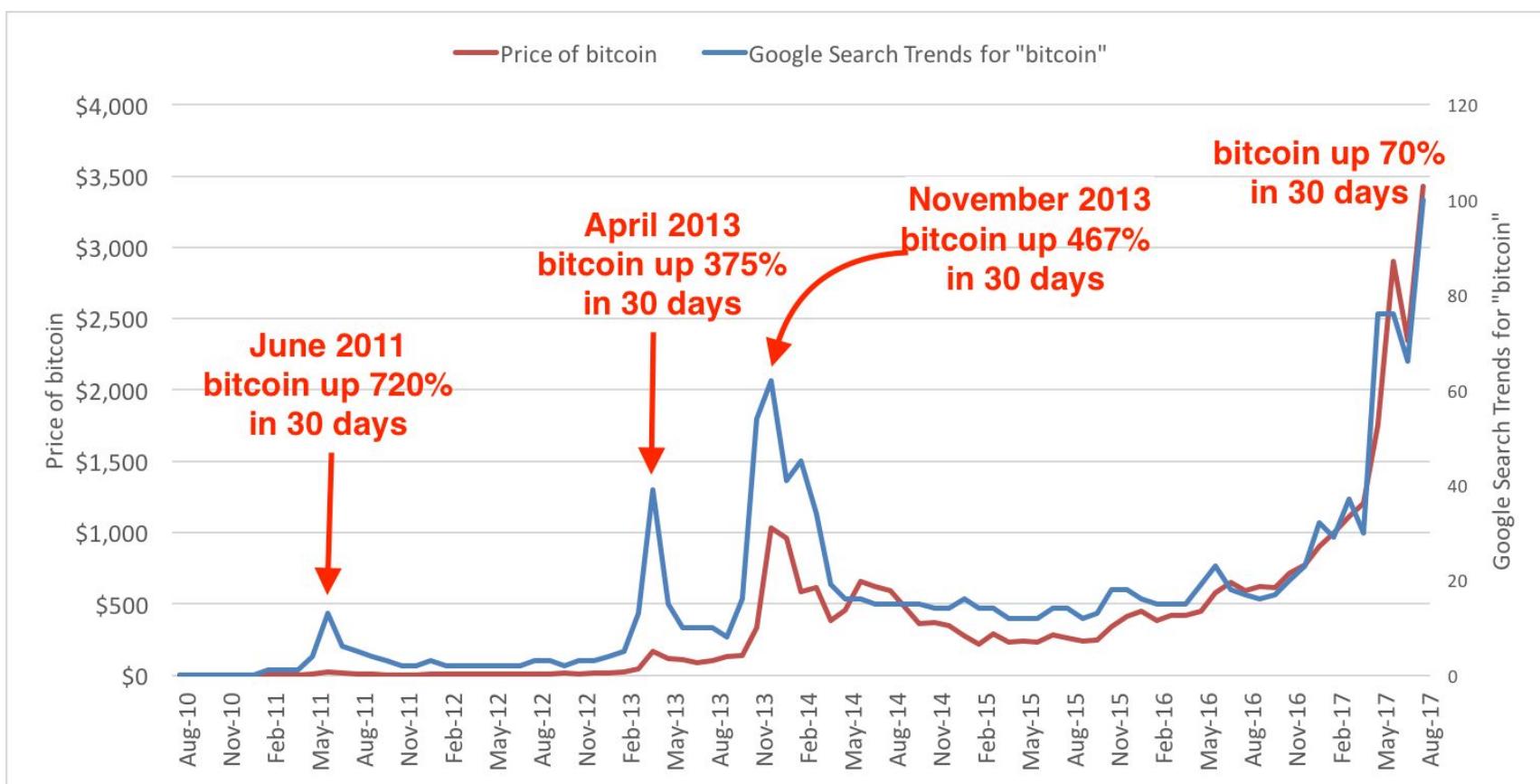
- Facile usando gli exchange
- Forex
  - Strategie applicate a valute reali
  - Cost averaging
  - Buy limit/Sell limit
  - Stime (AI?)
- Prezzi diversi su exchange diversi (arbitraggio)
  - cryptocompare.com
  - coinmarketcap.com



**MY FINANCIAL ADVISOR IS  
AN ALGORITHM**



# Google Trends



# Acquisto di beni

- Shopping Online
  - Shopify
  - Expedia/Microsoft/...
  - Openbazaar.org
- On site
  - Negozi che accettano bitcoin
  - Coinmap.org
- Attività ludica
  - Giochi (Cryptokitties, ...)
  - Scommesse (Bitcoin Lotto, ...)
  - Gioco d'azzardo (BitCasino, ...)

The screenshot shows the OpenBazaar interface. At the top, there is a search bar with the placeholder "Search for markets or products..." and a "Search" button. Below the search bar, there is a navigation menu with links to Home, Messages, Orders, Notarizations, Contracts, and Settings. A user profile icon is also visible.

In the main area, there is a section titled "My Contracts". This section contains a table with two rows of data. The columns are labeled "Product", "Images", "Quantity", "Price", "Shipping", and "Control".

Product	Images	Quantity	Price	Shipping	Control
<b>Stuffed Animal</b> This is a stuffed totoro. It is 8" tall and has no known diseases.		1	฿ 0.5	฿ 0.02	<a href="#">Edit</a> <a href="#">Remove</a>
<b>One Mouser</b> This is a mouser from TMNT. The 80s one, not the messed up new version of the show. It will not actually catch mice, no		1	฿ 0.01	฿ 0.01	<a href="#">Edit</a> <a href="#">Remove</a>



# Attività Illeggali

- Commercio illegale
  - Silkroad
  - Empire Market
  - ...
- Malware
  - Ransomware (Cryptolocker, WannaCry, ...)
  - Crypto mining (ads, estensioni, app, ...)

Welcome OzFreelancer!

messages(0) | orders(0) | account(\$0.00) | settings | log out

MARCH | W(0)

Silk Road  
anonymous marketplace

Shop by category:

- Drugs(1582)
  - Cannabis(271)
  - Dissociatives(33)
  - Ecstasy(217)
  - Opioids(106)
  - Other(65)
  - Prescription(274)
  - Psychedelics(306)
  - Stimulants(190)
  - Apparel(37)
  - Art(1)
  - Books(300)
  - Computer equipment(9)
  - Digital goods(218)
  - Drug paraphernalia(33)
  - Electronics(13)
  - Erotica(165)
  - Fireworks(1)
  - Food(1)
  - Forggeries(34)
  - Hardware(1)
  - Home & Garden(5)
  - Lab Supplies(5)
  - Medical(3)
  - Money(89)
  - Musical instruments(2)
  - Pawnshops(11)

10-Grams high grade MDMA 80+%  
B61.17

Amphetamines sulfate / Speed freebase...  
SALE!!!!  
B28.59

2g Jack Frost (weed) \*420  
B8.54

Dr Amsterdam  
Michael Jackson

5 Grams of pure MDMA crystals  
B42.04

100 red Y tablets 111mg (lab tested)...  
B97.77

3.5g Albino Rhino (weed)  
B12.37

500 mg Xanax  
B3.22

10mg Flexeril (muscle relaxant)...  
B3.22

\*\*\*10gr. Amphetamine Sulphate.  
B33.19

News:

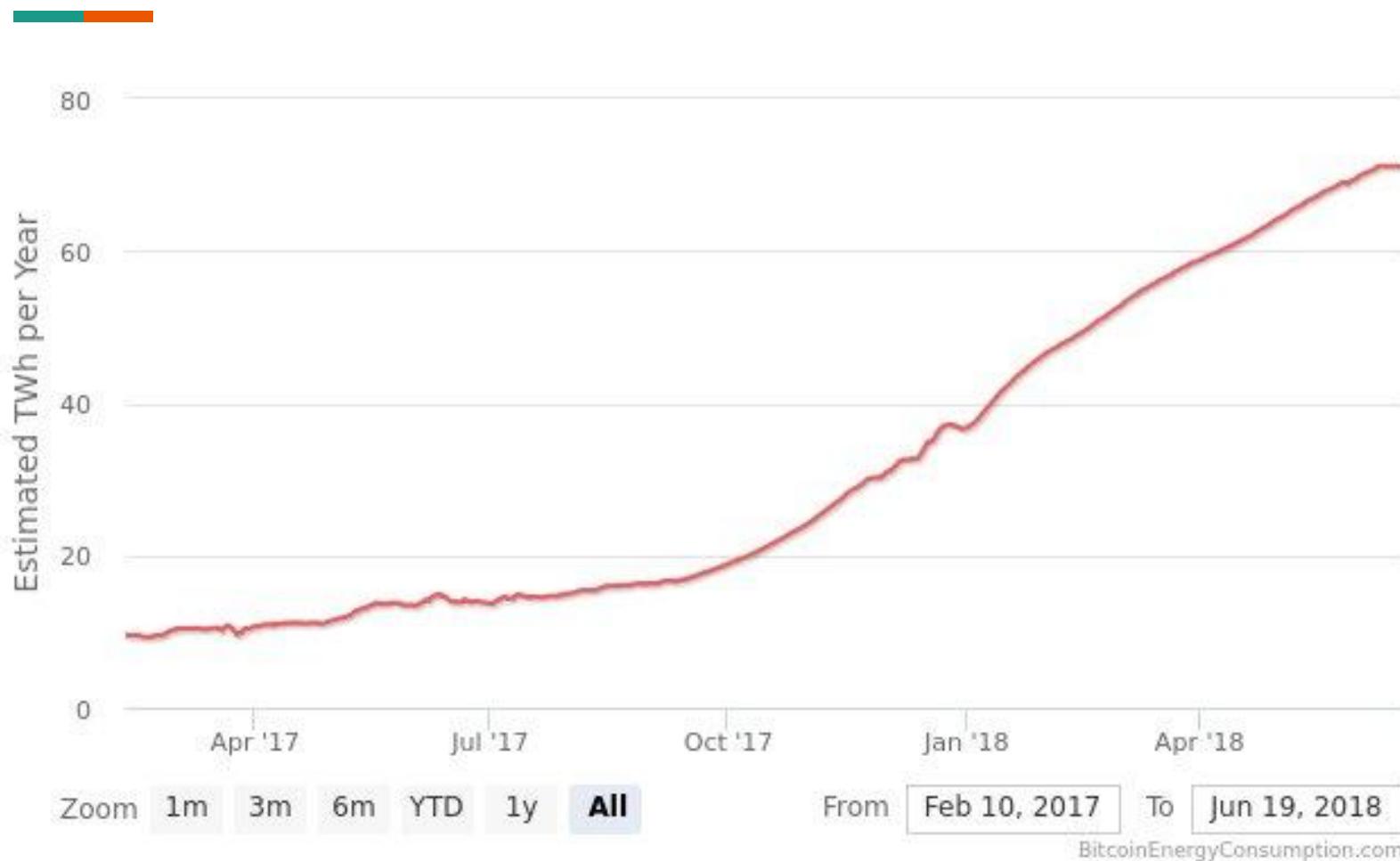
- The gift that keeps on giving
- Who's your favorite?
- Acknowledging Heroes
- A new anonymous market The Armory!
- State of the Road Address



# I Problemi di Bitcoin

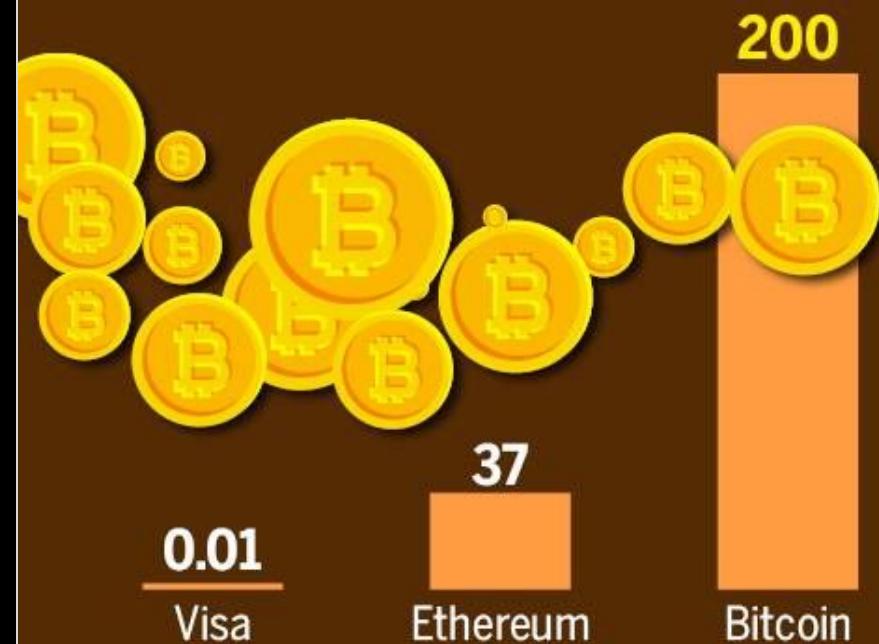
---

# Energia consumata





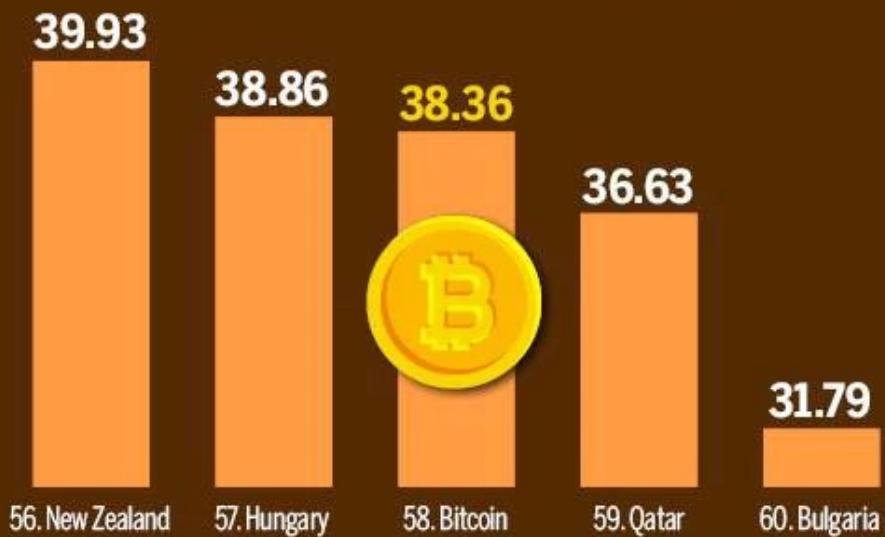
### Estimated kwh used per transaction



### Energy consumption: If bitcoin was a country

(At year end: projected)

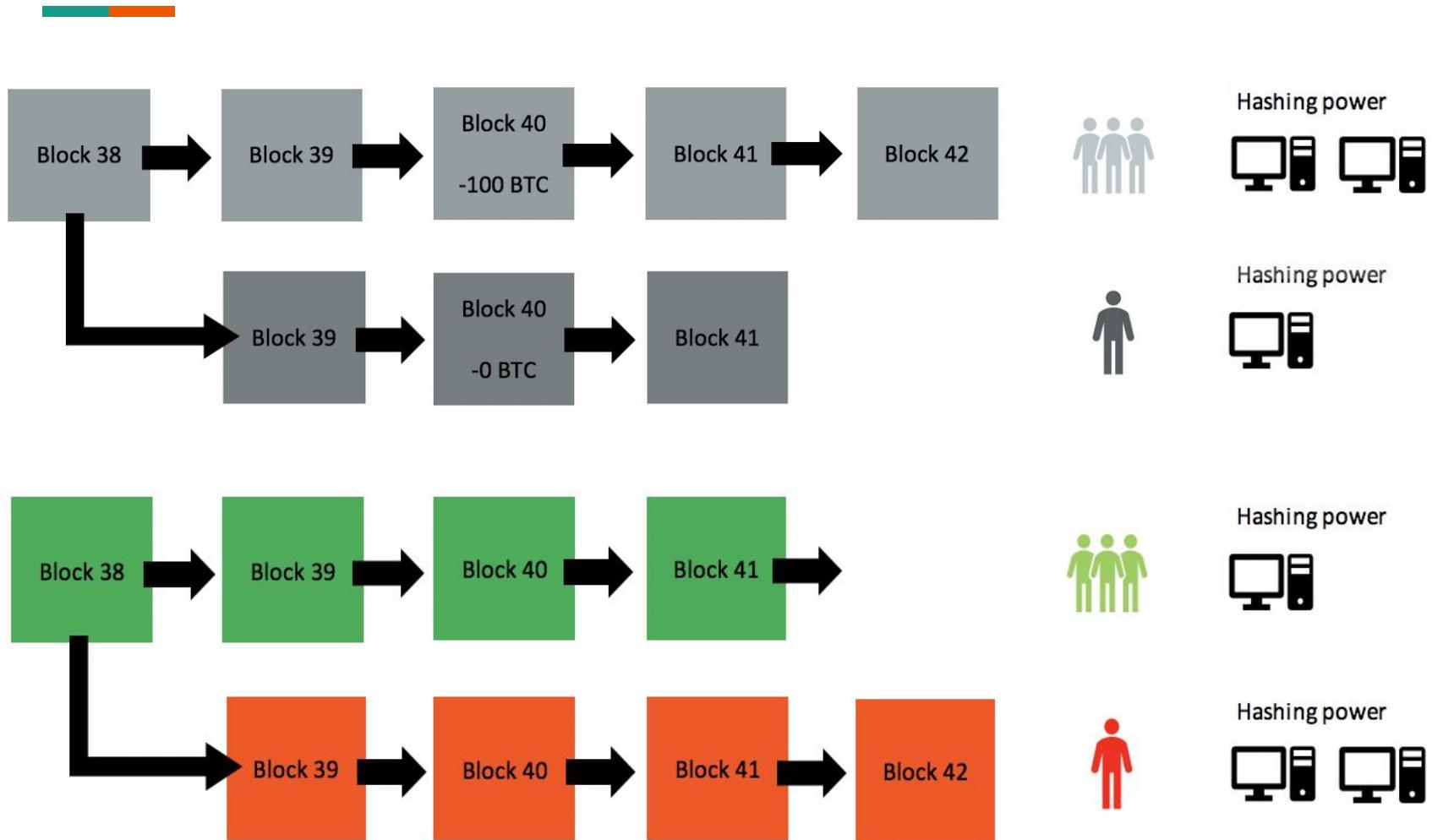
Total electricity consumption in a year (in TWH)



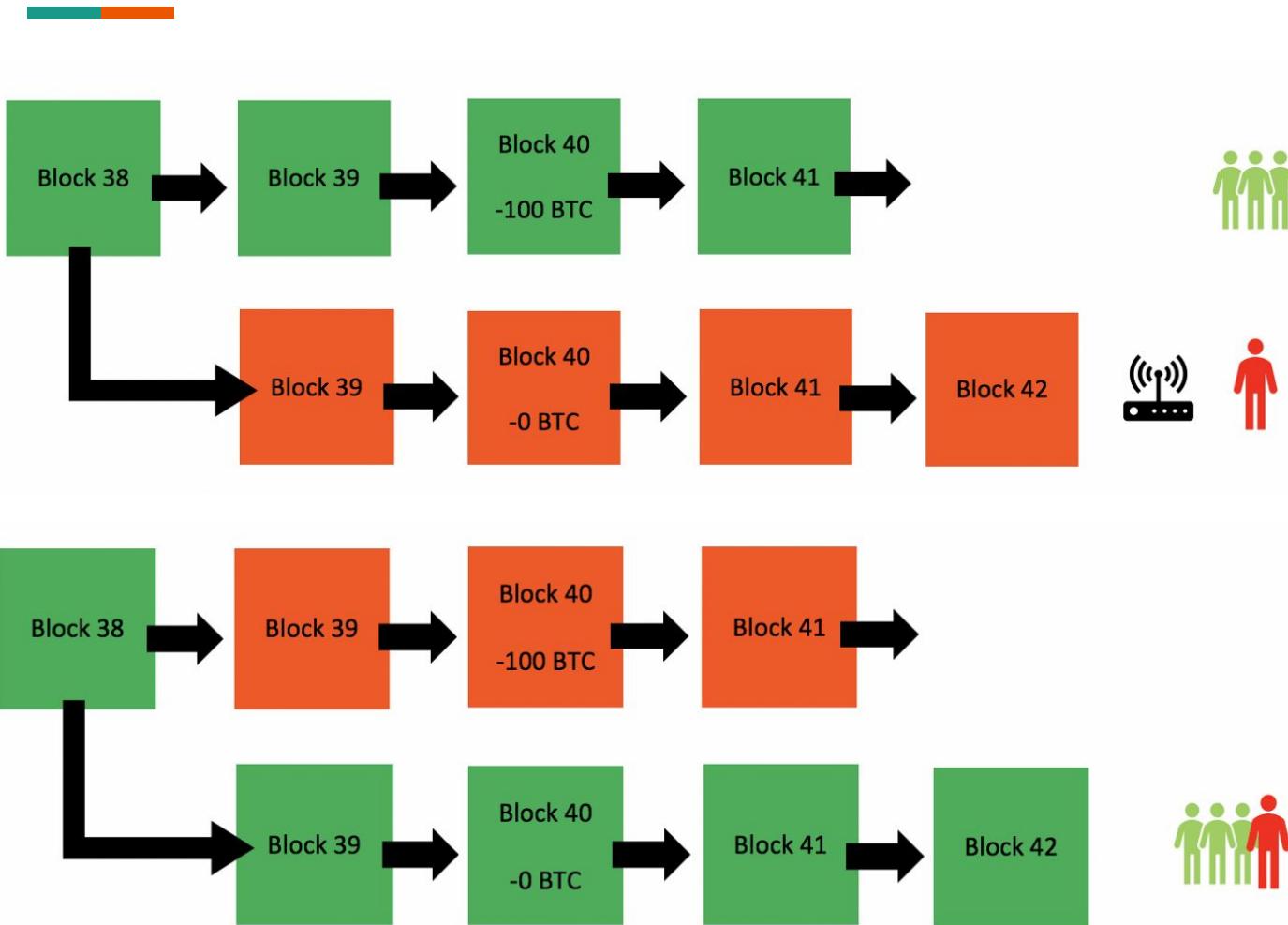
# 51% Attack



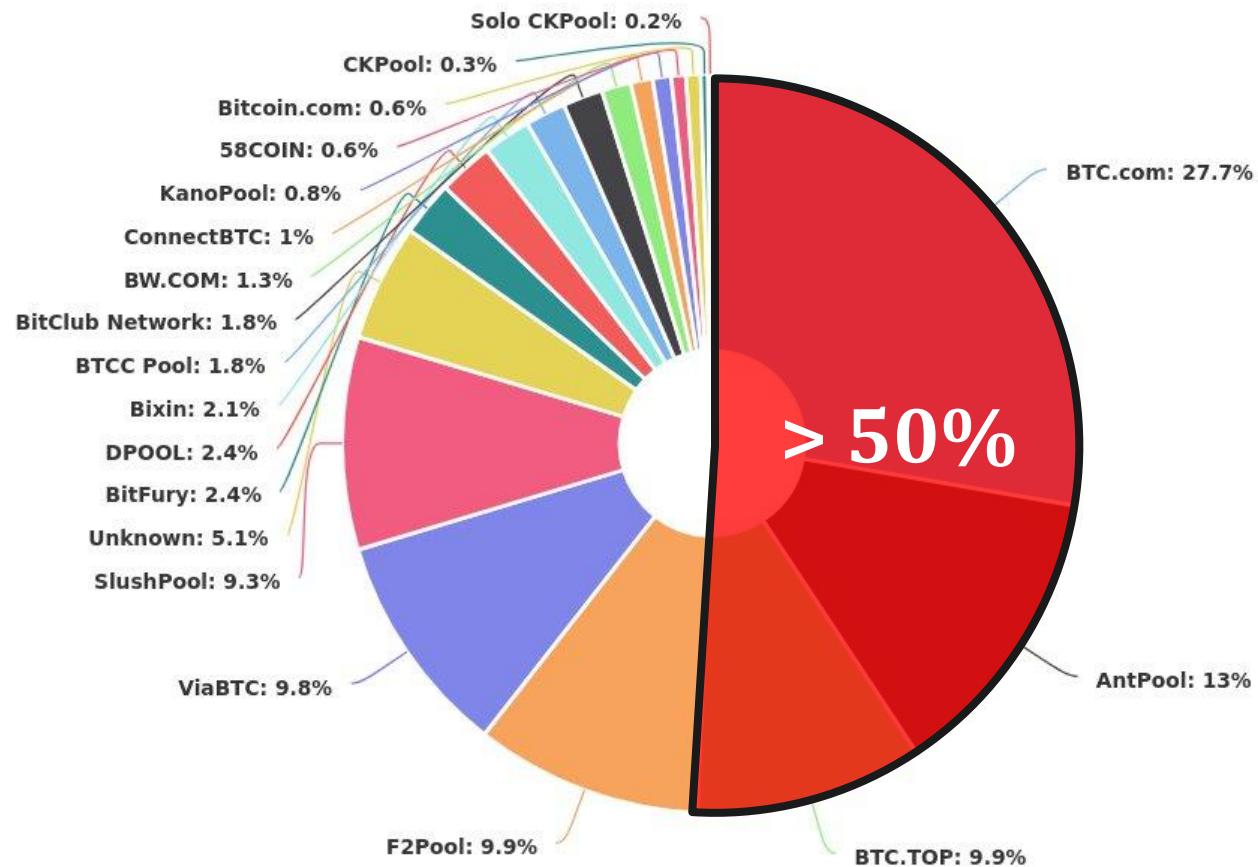
# 51% Attack



# 51% Attack



# Mining Pool - 51% Attack



# PoW 51% Attack Cost

This is a collection of coins and the theoretical cost of a 51% attack on each network.

[Learn More](#)[!\[\]\(88c219f0311903581e21b213e11a0f99\_img.jpg\) Tip](#)

Name	Symbol	Market Cap	Algorithm	Hash Rate	1h Attack Cost	NiceHashable
Bitcoin	BTC	\$106.49 B	SHA-256	48,136 PH/s	\$451,284	0%
Ethereum	ETH	\$18.60 B	Ethash	137 TH/s	\$90,971	5%
BitcoinCashABC	BCH	\$5.39 B	SHA-256	2,254 PH/s	\$21,134	2%
Litecoin	LTC	\$4.82 B	Scrypt	350 TH/s	\$51,437	3%
Monero	XMR	\$1.20 B	CryptoNightR	314 MH/s	\$5,574	5%
Dash	DASH	\$1.10 B	X11	3 PH/s	\$4,761	15%

---

Come risolvere questi problemi?

Proof-of-Work → Proof-of-Stake

# PROOF OF WORK



The probability of mining a block depends on the amount of work a miner does



Takes more energy than Proof of Stake



One example is Mining, which uses computer cycle time to validate new transactions



Stakeholders validate new blocks by utilizing their share of coins on the network



The first example of Proof of Stake was Peercoin



A user would need to own a majority of all coins in order to attack the network

COMPARING

PROOF

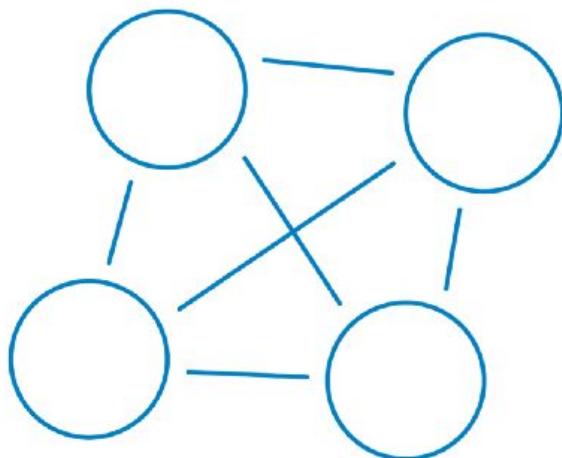
ALGORITHMS

Proof of work & Proof of stake are methods of verifying the authenticity of transactions, without the need for a centralized third party.

**WHAT ARE THEIR MAIN DIFFERENCES?**

# PROOF OF STAKE

## PROOF OF WORK



### Centralized

Users organize in mining pools

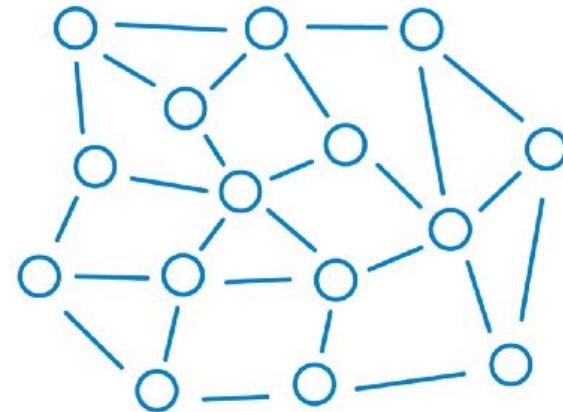


Hardware tools  
ASICS and CPUs



Energy  
high consumption  
Unsustainable concept

## PROOF OF STAKE



### Decentralized

Users remain in control of their tokens



Hardware tools  
no necessary

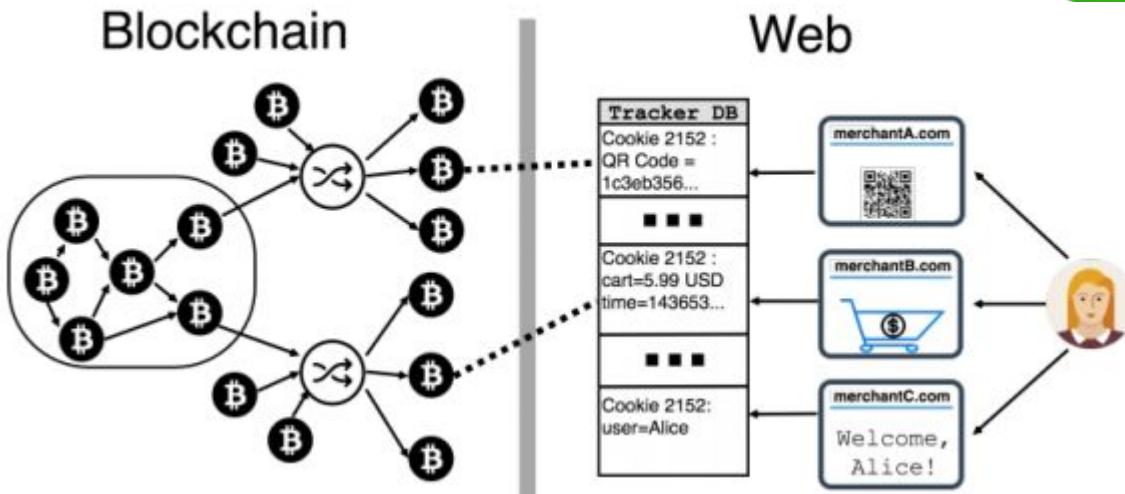


Energy  
low consumption  
Sustainable concept

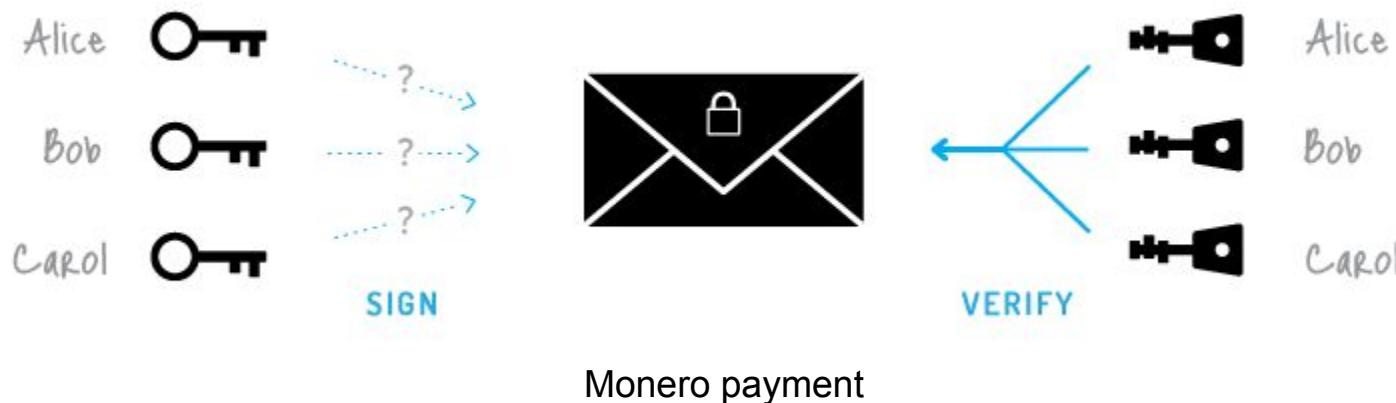


# Realmente Anonimo?

- Indirizzo IP
- Credenziali su app ed exchange wallet
- Storia delle transazioni
- Bitcoin mixer
- Altcoin anonime (Monero)

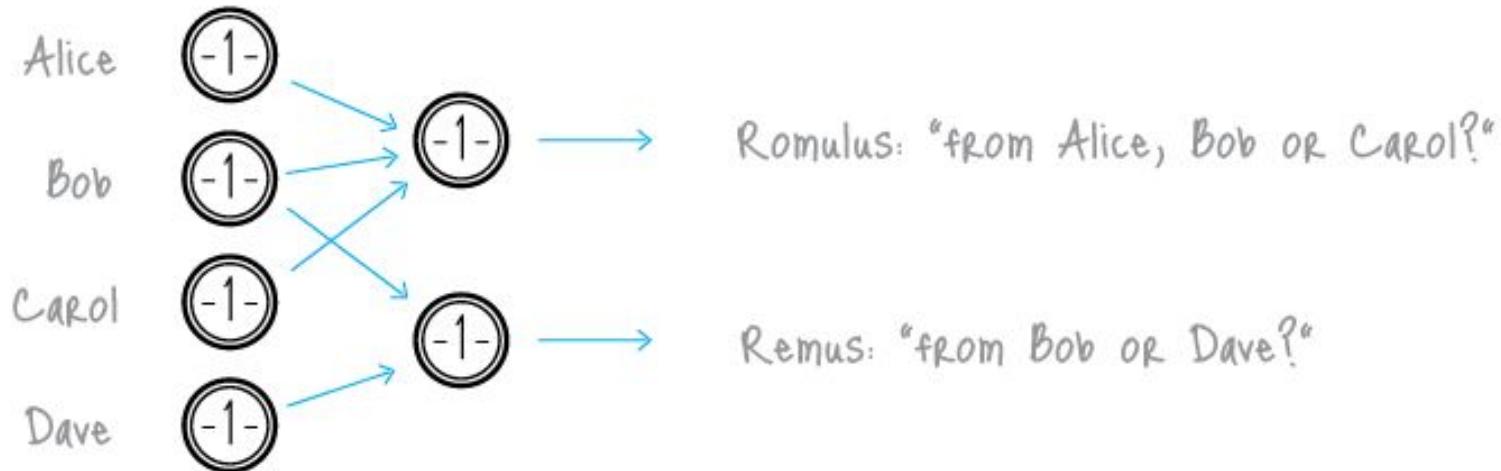


# Untraceable payments



# Untraceable payments

---





**Daily Meme Supply** @DailyMemeSupply · 16h

\*buys 0.000001 bitcoin\*

\*changes bio\*

investor & entrepreneur 💰 \$BTC 💵 living life in the sky ✈️ ☁️ eat, sleep, bitcoin

69

2.6K

10.1K



---

## Parte III

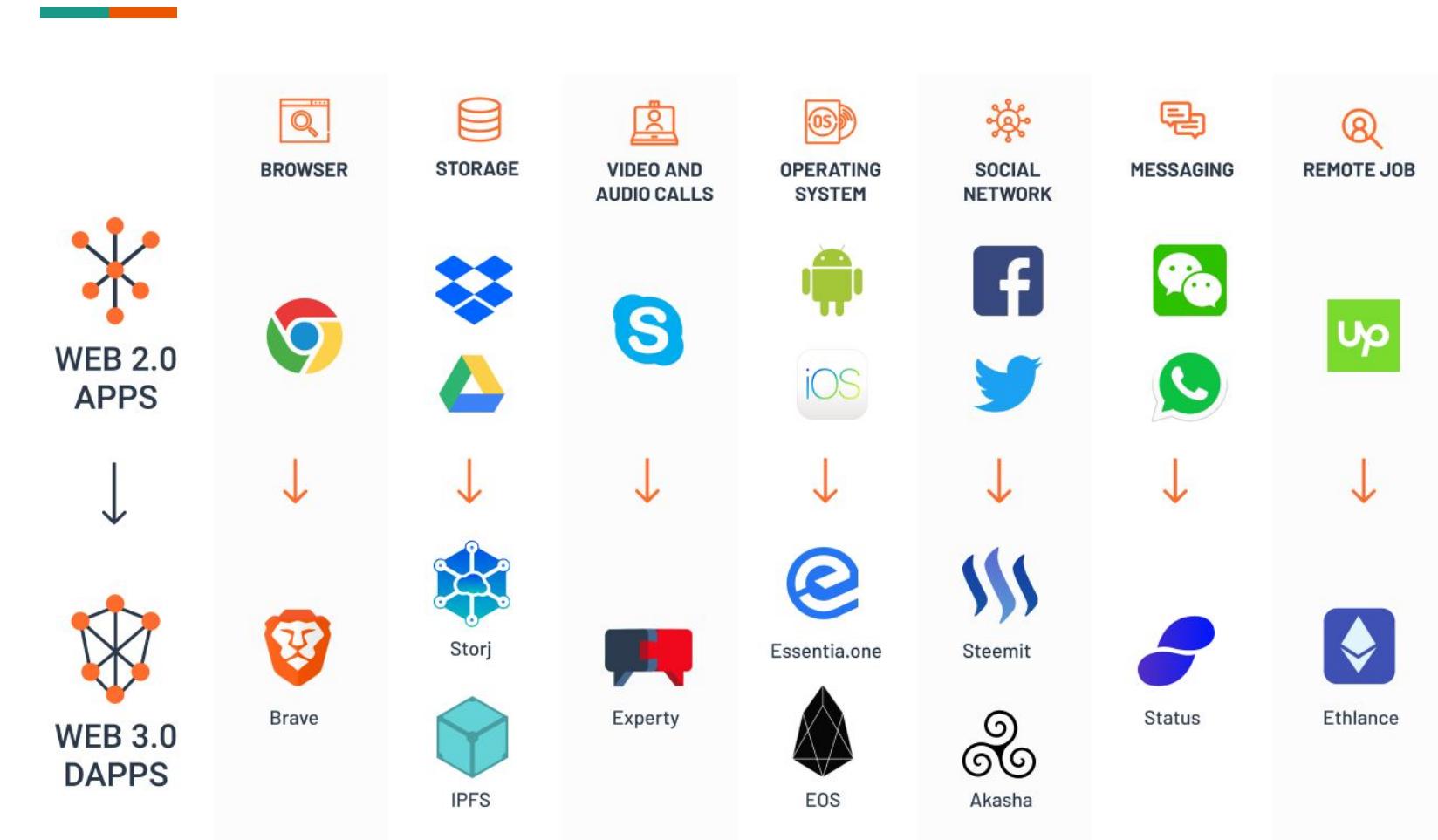
# Prospettive future

# Altcoins e Internet 3.0

---



# Internet 3.0



# Smart Contracts

*( programming the blockchain )*

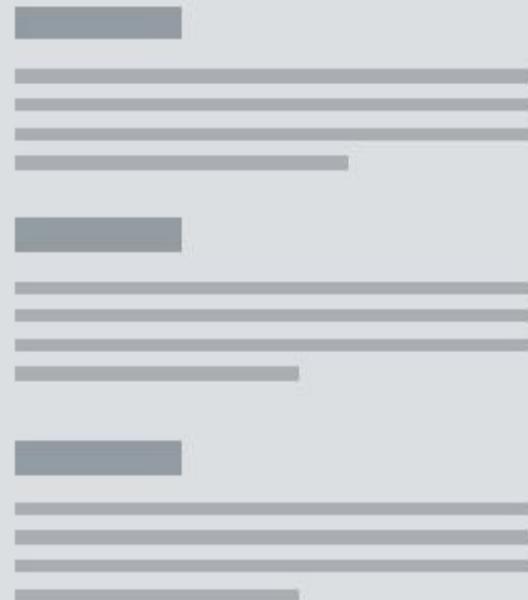
---

## Smart Contracts

Attraverso gli smart contract si possono **automatizzare** le **clausole** contrattuali in modo parziale o completo.

Si tratta di contratti digitali atti a scambiare proprietà, denaro, azioni o altri asset di valore in modo trasparente, sicuro e senza intermediari.

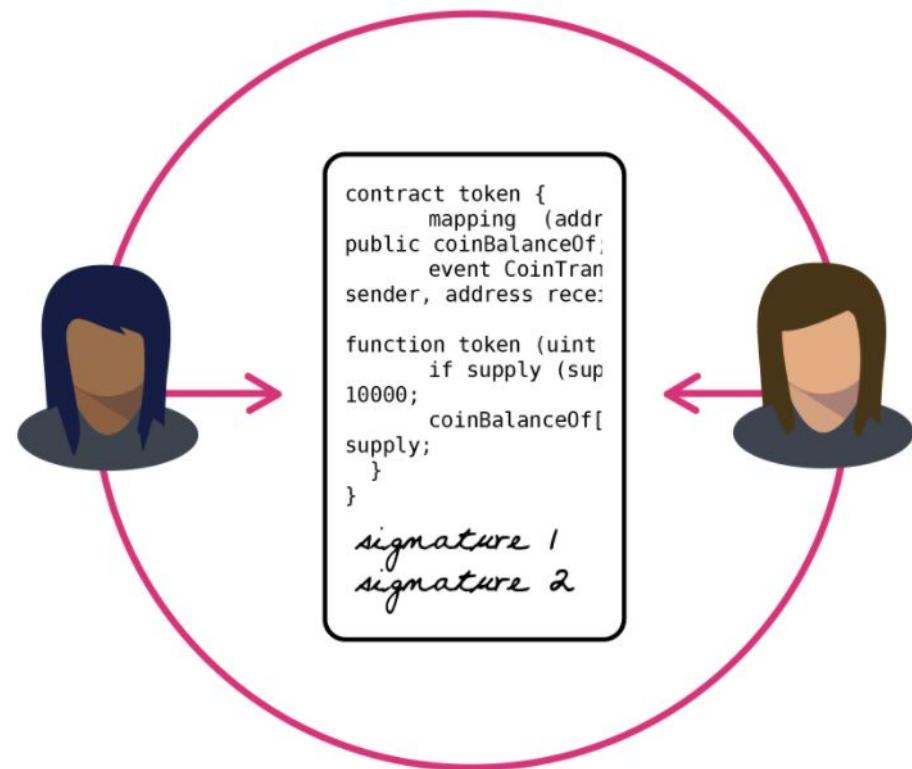
## CONTRACT



# Ethereum



e t h e r u m



# Ethereum - MyCoin

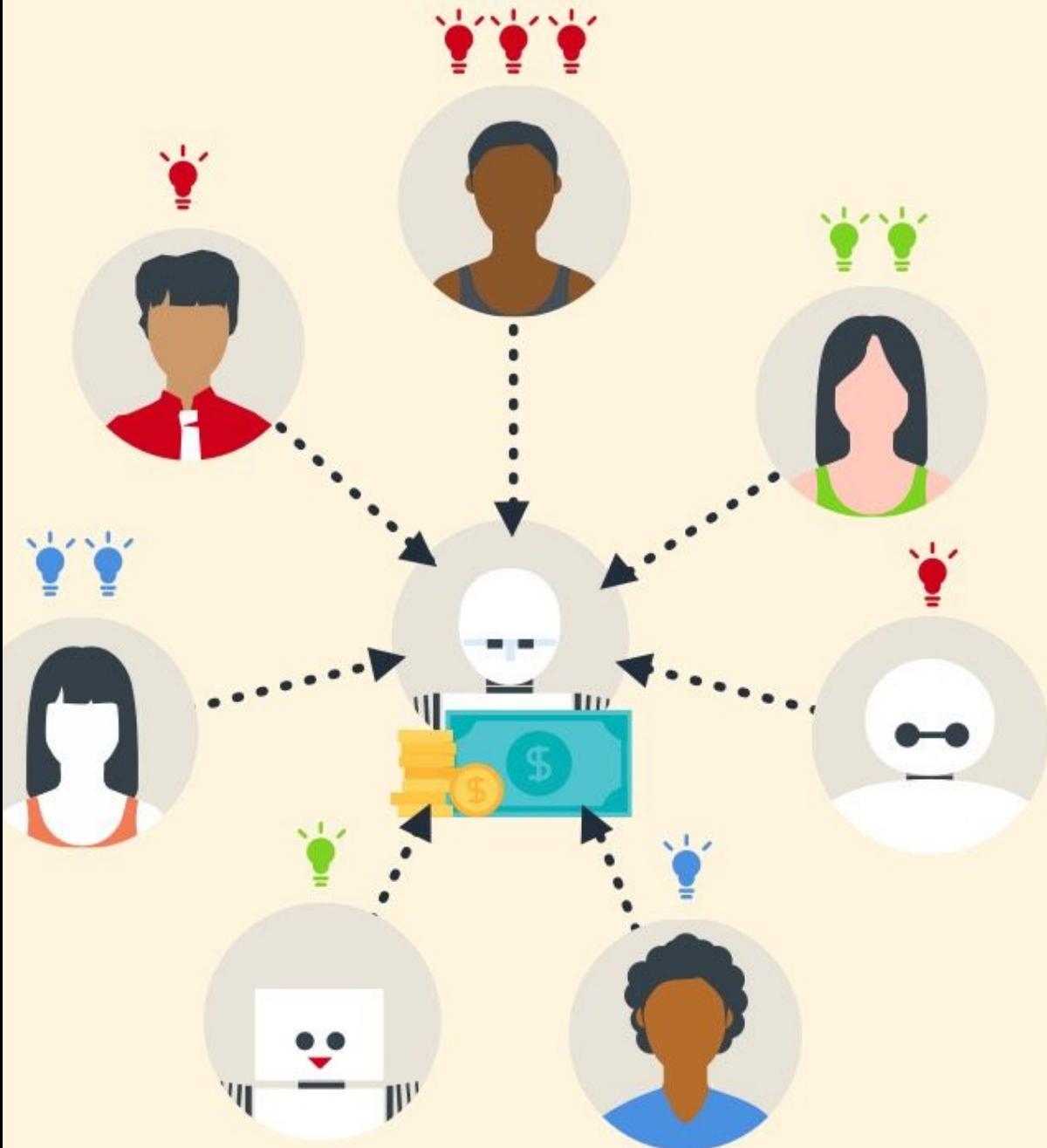
---

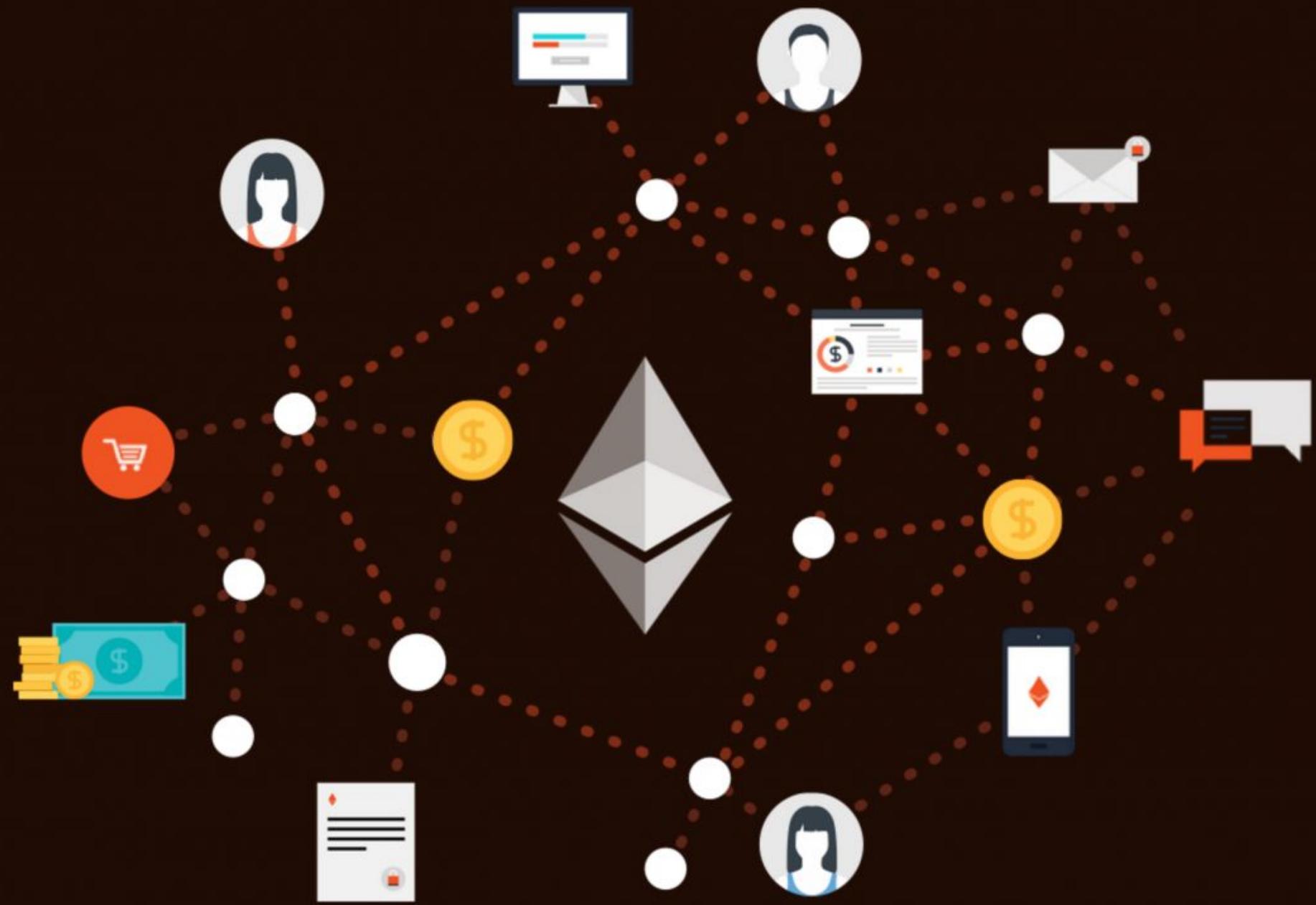
```
contract MyCoin {  
    /* This creates an array with all balances */  
    mapping (address => uint256) public balanceOf;  
  
    /* Initializes contract with initial supply coins to the creator of the contract */  
    function MyCoin(  
        uint256 initialSupply  
    ) public {  
        balanceOf[msg.sender] = initialSupply;  
    }  
  
    /* Send coins */  
    function transfer(address _to, uint256 _value) public {  
        require(balanceOf[msg.sender] >= _value); // Check if the sender has enough  
        require(balanceOf[_to] + _value >= balanceOf[_to]); // Check for overflows  
        balanceOf[msg.sender] -= _value; // Subtract from the sender  
        balanceOf[_to] += _value; // Add the same to the recipient  
    }  
}
```

# Decentralized Autonomous Organization

*Sarebbe possibile creare una democrazia digitale basata sul consenso?*

<https://www.ethereum.org/dao>





# CryptoZombies

CryptoZombies è un corso di programmazione interattivo e gratuito che ti insegna a creare giochi su Ethereum.

Viene utilizzato il linguaggio Solidity per creare smart contracts.

Il corso è progettato per partire dalle basi assolute.

[cryptozombies.io](https://cryptozombies.io)



# Cosa è ERC-20?

- Prima che venisse creato lo standard dell'ERC-20, si erano verificati diversi problemi di compatibilità tra le varie forme di token di Ethereum. **Ogni token possedeva uno smart contract completamente unico.**
- ERC-20: **Standard** per la creazione di token Ethereum.
- I token possono fungere da quote in un progetto, certificati di proprietà di asset, punti fedeltà o persino criptovalute vere e proprie (hanno indirizzi ETH).
- Facili da creare:  
<https://coinlaunch.market/coincreator>
- **Contro:** porta ad un'abbondanza di token molto simili e rende il processo di selezione da parte di possibili investitori più complesso e confusionario.



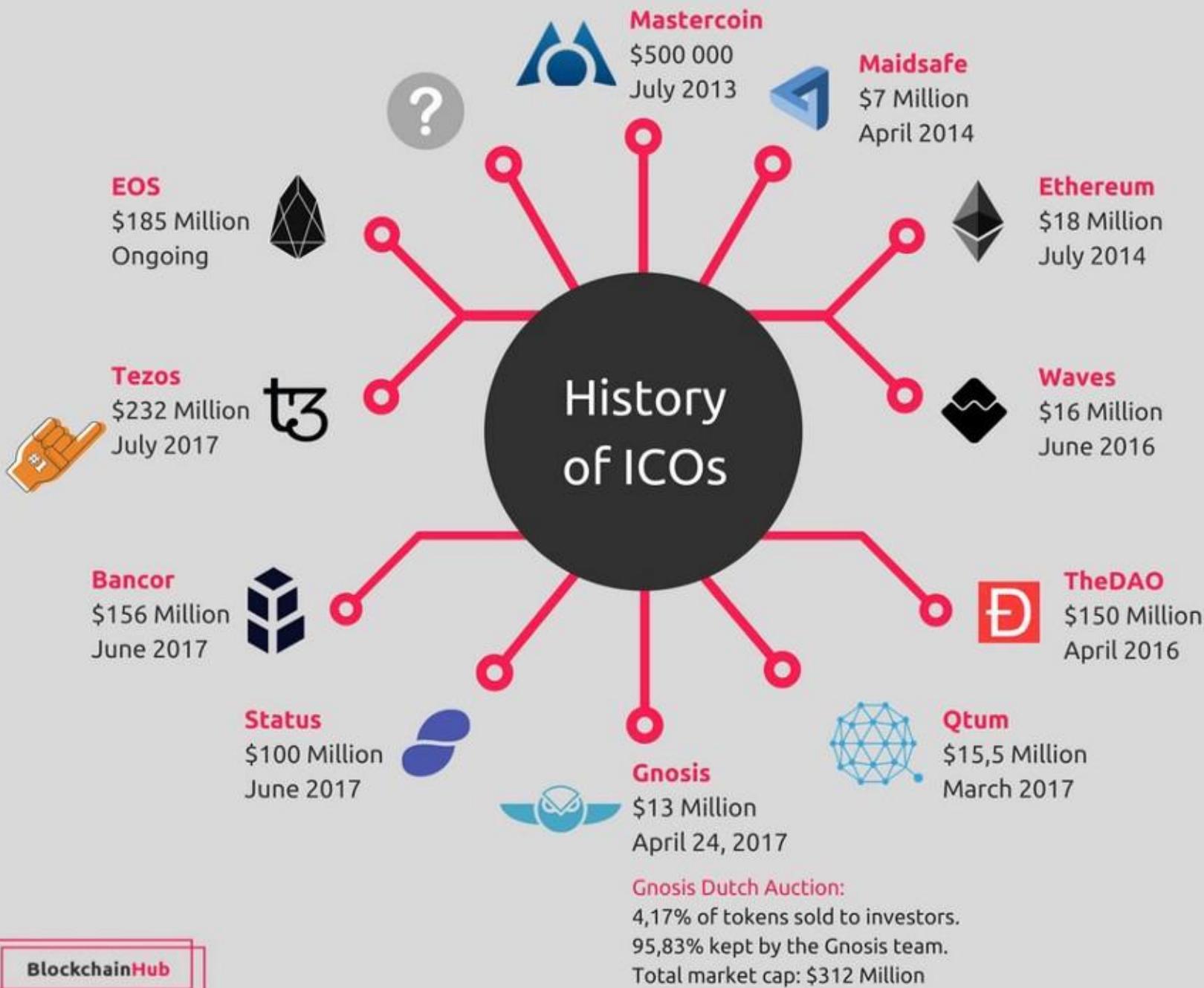
## Initial Coin Offering / Token Sale

---

# ICO



Its a bit like a mix between an  
IPO and Online Crowdfunding,  
but for Cryptocurrency.





## ParkinGO lancia GOT: il suo Token Digitale!

Il GOToken è una moneta che permette di acquistare tutti i servizi offerti dalla piattaforma ParkinGO.

È partita la [token sale](#) pubblica che si concluderà il 3 luglio.

Dal **04 luglio 2018**, potrai pagare i servizi ParkinGO con i GOToken usufruendo di esclusivi vantaggi.

---



# Permissionless

## Vs

# Permissioned

Le reti Blockchain possono essere categorizzate in due classi:

- **Permissionless:** Tutti possono partecipare alla rete ed inviare le transazioni. La fiducia è garantita dal protocollo crittografico.

**Esempio:** bitcoin

- **Permissioned:** Un membro ha bisogno di essere autenticato per partecipare alla rete e sottomettere delle transazioni.

**Esempio:** Hyperledger fabric

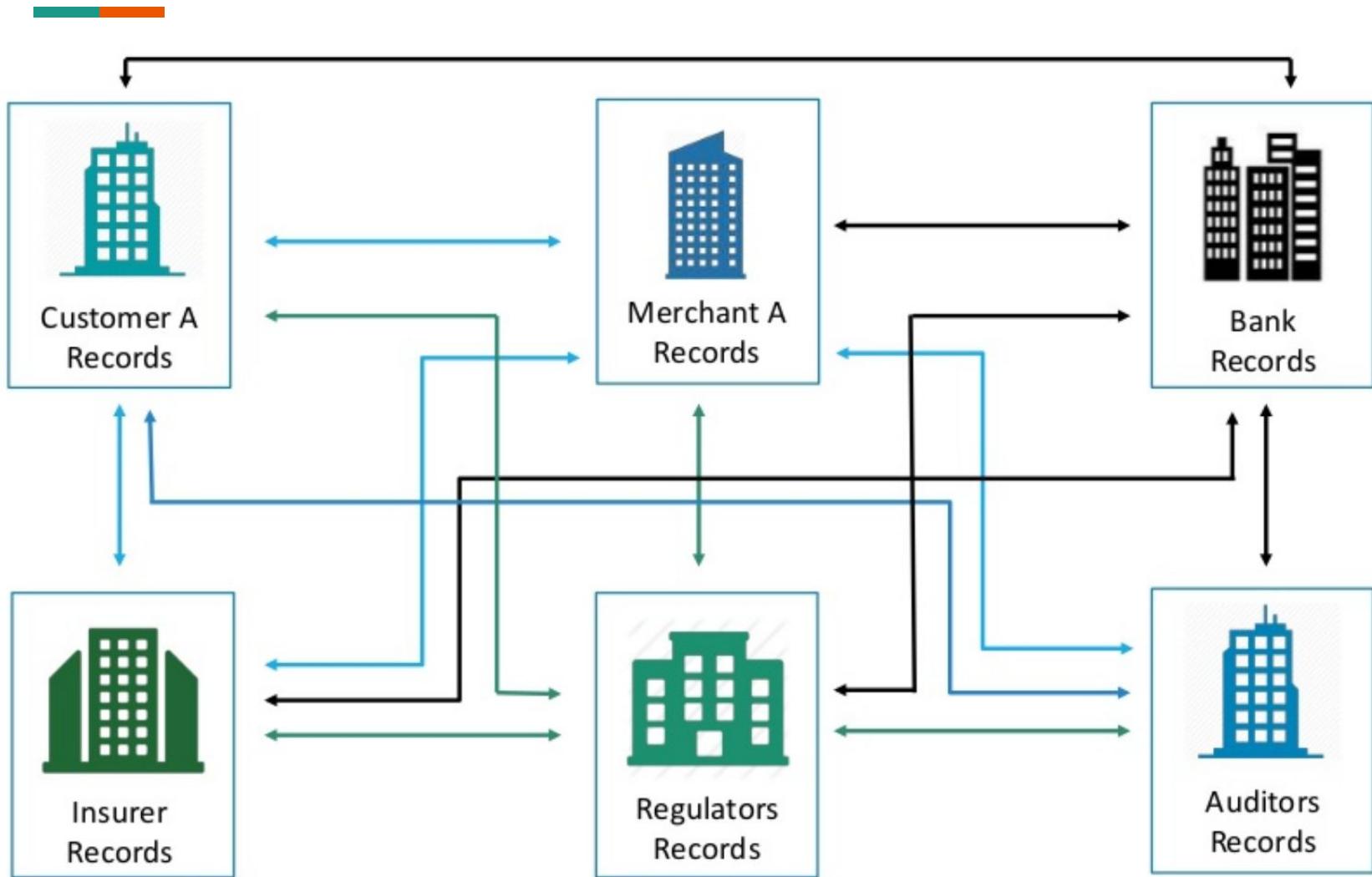
---



# Hyperledger

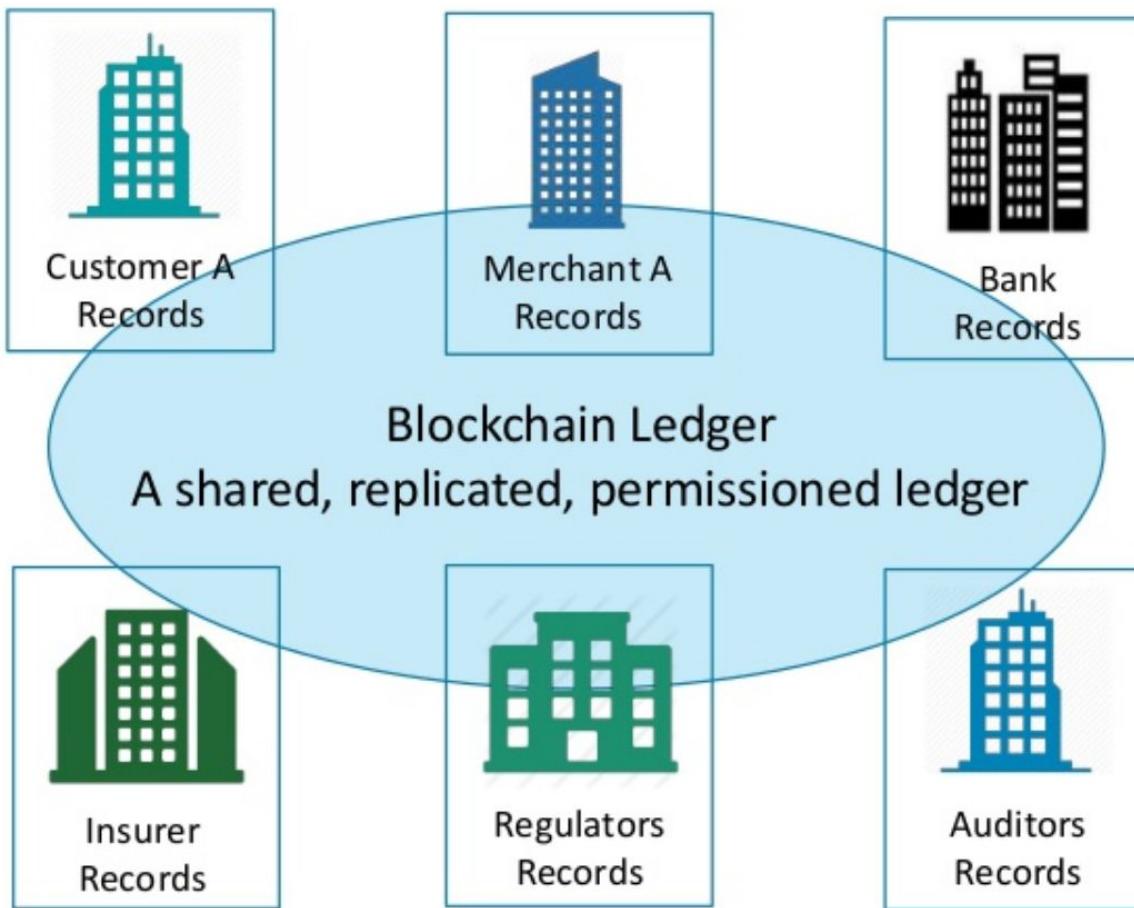
---

# Problema



# Problema

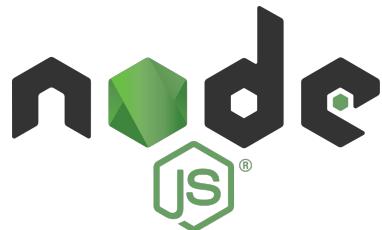
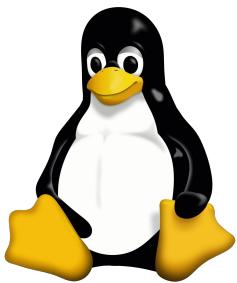
---



- ✓ Consensus
- ✓ Immutability
- ✓ Provenance
- ✓ Finality



# HYPERLEDGER



CLOUD FOUNDRY



# Hyperledger members

## Premier



## Associate



© 2018

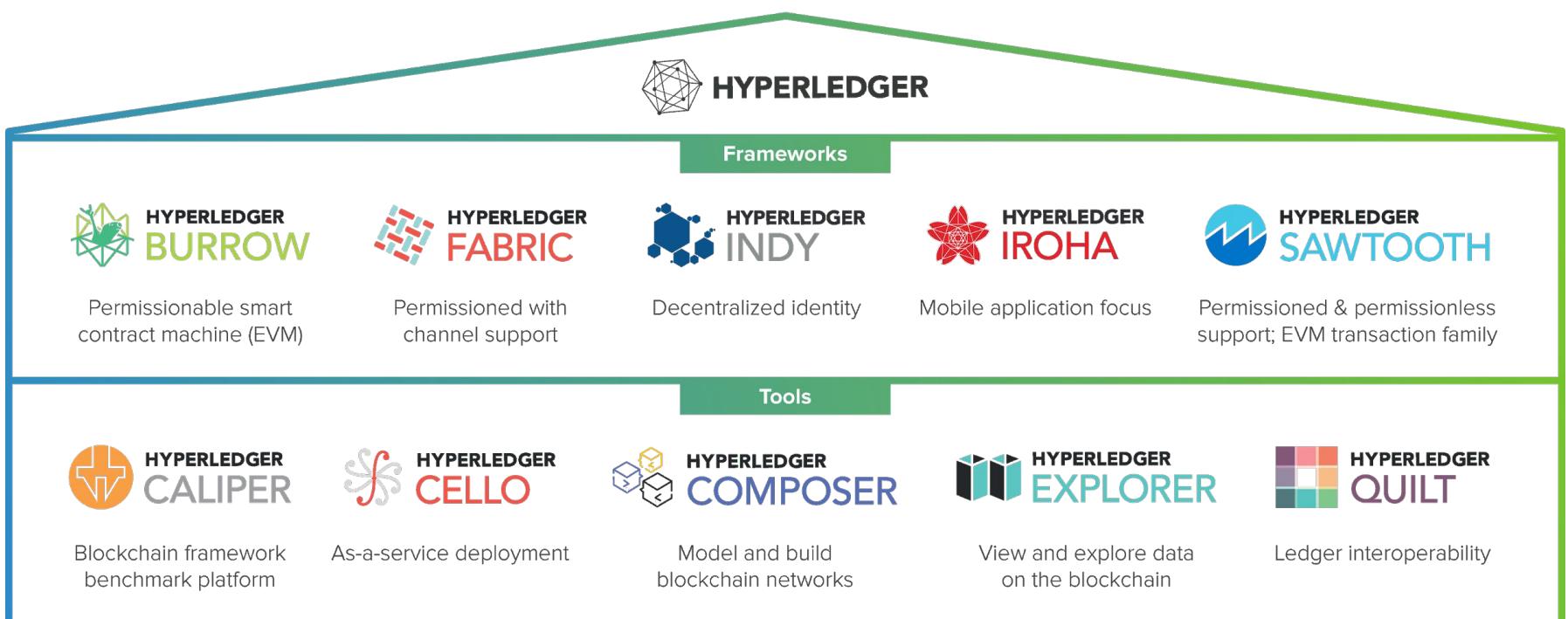
## General



Source: <https://www.hyperledger.org/about/members>  
Updated 14 February 2018

IBM Blockchain

# Hyperledger Foundation



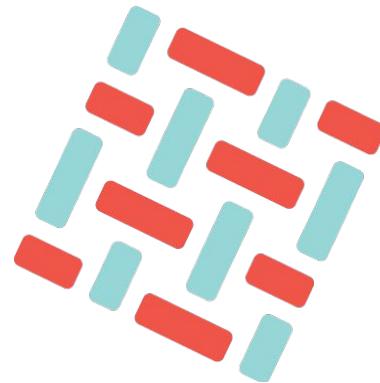
**HYPERLEDGER**



# Hyperledger Fabric

---

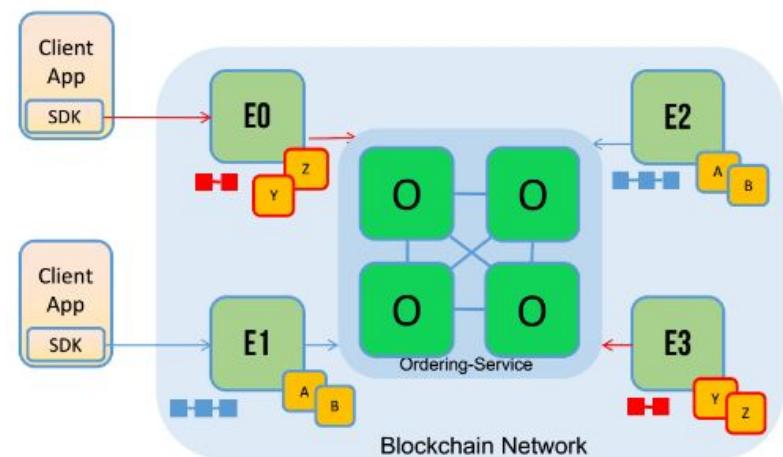
- Permissioned Blockchain  
(utenti autorizzati - no PoW)
- Transazioni private
- Servizio principale: distributed ledger e ordinamento delle transazioni
- Veloce e scalabile
- Nessuna criptovaluta associata
- Gestione di smart contracts



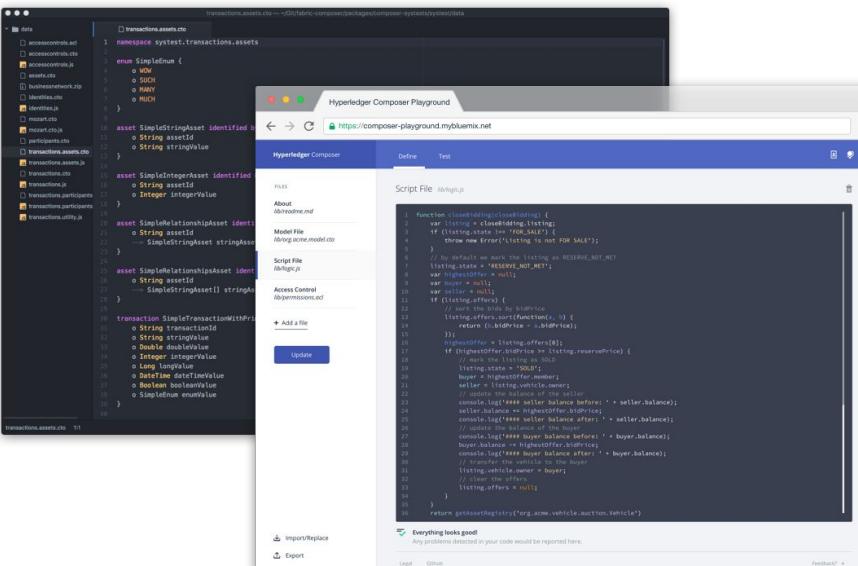
**HYPERLEDGER**  
**FABRIC**

# Hyperledger Fabric - Canali privati

- Hyperledger Fabric è basata su canali (gruppi di due o più membri della blockchain).
- L'identità dei membri è verificata.
- I canali permettono di scambiare transazioni che sono validate e possono fare parte di smart contracts.
- Le transazioni nei canali rimangono private (ma con ordine definito e vincolanti).



# Hyperledger Composer



The screenshot shows the Hyperledger Composer Playground interface. On the left, there's a file tree for a project named 'transactions.assets.cdt'. The main area has two tabs: 'Define' and 'Test'. Under 'Define', there's a 'Script File' tab containing the following JavaScript code:

```
function closeListing(closeListing) {
    var listing = closeListing.asset;
    if (listing.state === 'FOR-SALE') {
        throw new Error('Listing is not for sale');
    }
    // by default we mark the listing as RESERVE-NOT-MET
    listing.state = 'RESERVE-NOT-MET';
    var buyer = null;
    var seller = null;
    if (listing.offers) {
        // avoid triggering the update function, so
        // return the old price + bidPrice - bidFee;
        listing.offers[0].bidPrice = listing.reservePrice;
        highestOffer = listing.offers[0];
        if (highestOffer.bidPrice > listing.reservePrice) {
            listing.state = 'CLOSED';
            listing.buyer = buyer;
            seller = listing.vehicle.owner;
            // update the balance of the seller
            console.log(`***** seller balance before: ${seller.balance}`);
            seller.balance += highestOffer.bidPrice;
            console.log(`***** seller balance after: ${seller.balance}`);
            // update the balance of the buyer
            console.log(`***** buyer balance before: ${buyer.balance}`);
            buyer.balance -= highestOffer.bidPrice;
            console.log(`***** buyer balance after: ${buyer.balance}`);
            listing.vehicle.owner = buyer;
            // clear the offers
            listing.offers = null;
        }
    }
    return getAssesmentList('org.acme.vehicle.auction.Vehicle');
}
```

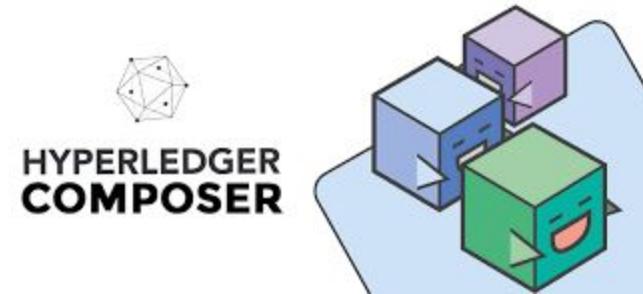
Below the code editor, there are buttons for 'Import/Replace' and 'Export'. At the bottom, there's a status bar with 'Everything looks good' and a note: 'Any potential errors in your code would be reported here.'

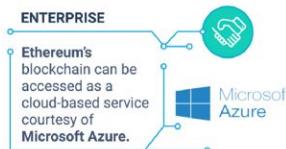
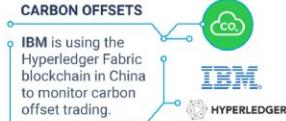
<https://hyperledger.github.io/composer>

Hyperledger Composer è un framework che permette di comporre delle applicazioni su Hyperledger Fabric.

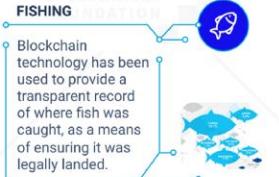
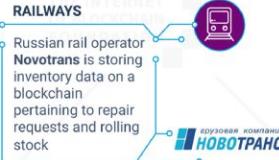
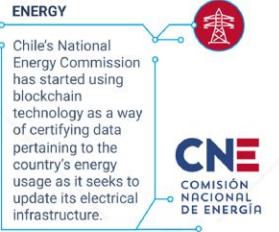
Guida l'utente nella modellazione del suo problema di business tramite la definizione di: **assets**, **partecipanti** e **transazioni**.

Permette di portare la propria soluzione in produzione in tempi rapidi.





# 50+ BLOCKCHAIN REAL WORLD USES CASES

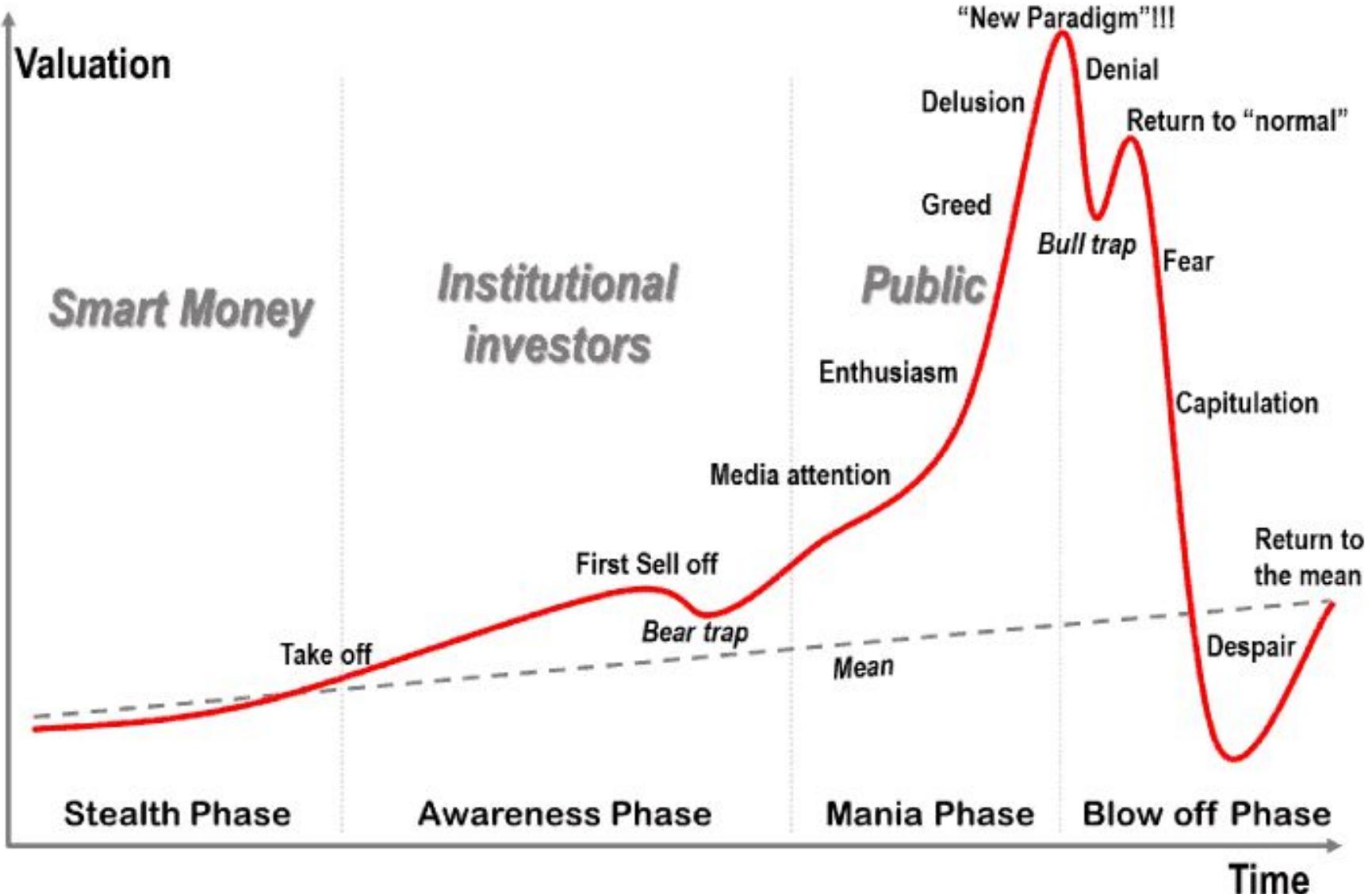


MATTEO GIANPIETRO ZAGO



---

Is the Blockchain  
a bubble?



## Bitcoin price index from October 2016 to October 2018 (in U.S. dollars)



Source  
CoinDesk  
© Statista 2018

Additional Information:  
Worldwide; CoinDesk



# Tulip price index 1636-37

200

150

100

50

25

Nov 12

Nov 25

Dec 1

Dec 12

Feb 3

Feb 5

Feb 9

May 1

De Bal Gewooge  
440 Aars  
658 —

# Dot-com bubble



# Demo Time

---

- <https://anders.com/blockchain>
- <https://coindemo.io>
- <https://blockchaindemo.io>



# Thanks!

**Enrico Bacis**  
enricobacis.com  
enrico.bacis@unibg.it

**Unibg Seclab**  
seclab.unibg.it  
seclab@unibg.it

