



## **Blockchain: innovazione oltre i Bitcoin**

---

***La tecnologia blockchain: dai principi generali di funzionamento agli  
Smart Contract, Token e NFT***

---

**Ing. Francesco Amendola**  
*Presidente della Commissione Smart Mobility  
Ordine degli Ingegneri della Provincia di Roma*

*Roma, 25 marzo 2024*



# Ing. Francesco Amendola



- **Ingegnere elettronico (2003), MBA (2011)**
- **Membro del Direttivo della Consulta Roma Smart City Lab**
- **Innovation Manager Manageritalia-XLabor accreditato MIMiT**
- **Attuale incarico: CTO del Gruppo Harpa (Harpa Italia – Aircare)**
- **Precedenti incarichi: Direttore Sistemi Informativi ATAC – CIO Novomatic Italia**
- **Esperienza professionale di oltre 20 anni in ambito IT, Telecomunicazioni e PA**
- **Docente e relatore in convegni, seminari e corsi universitari e post-universitari su tematiche legate all'innovazione tecnologica ed alla Trasformazione Digitale**
- **Presidente della Commissione Smart Mobility dell'Ordine degli Ingegneri della Provincia di Roma**
- **Program Director del Master in Data Science presso la Rome Business School**



## Disclaimer

- **Tutti i nomi dei prodotti e delle aziende menzionate sono marchi registrati (trademarks™ or registered® trademarks) dei rispettivi proprietari.**
- **L'utilizzo di nomi, marchi e loghi registrati non implica alcuna affiliazione o legame con essi.**



# Oggi parleremo di...





**Che differenza c'è tra**

# **Blockchain e Bitcoin?**



Blockchain  
è la  
tecnologia

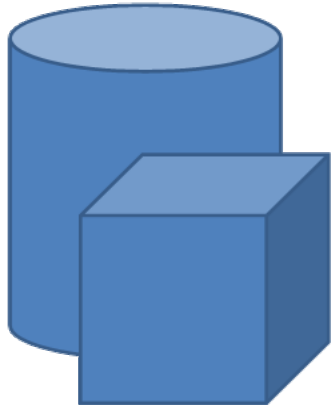
Bitcoin  
è uno dei  
possibili  
prodotti



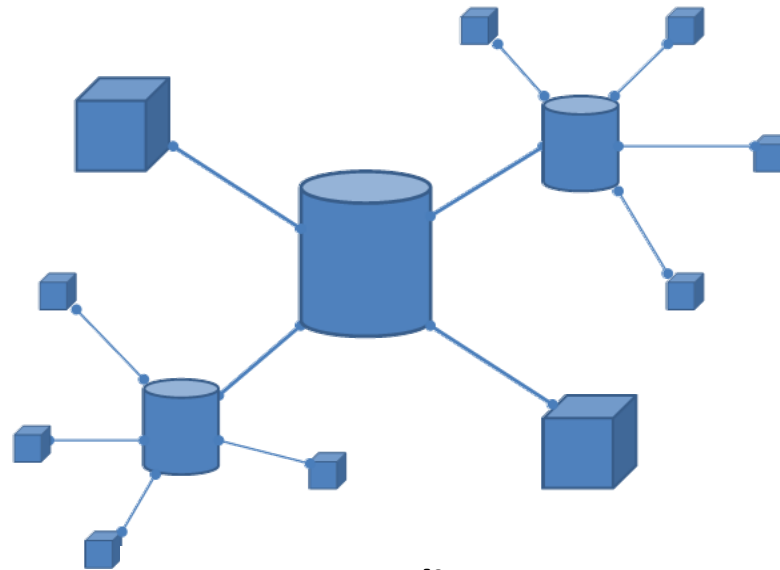
# Quale problema vuole risolvere la Blockchain?



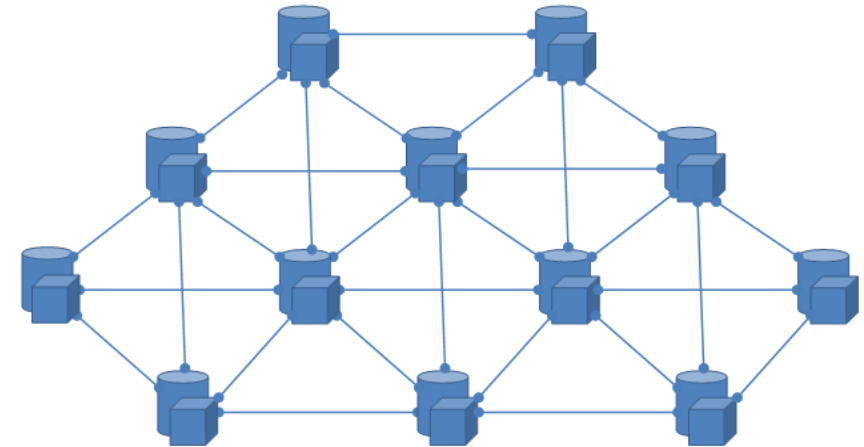
# Soluzioni al problema del **Double Spending**



**Centralizzato**



**Decentralizzato**



**Distribuito**



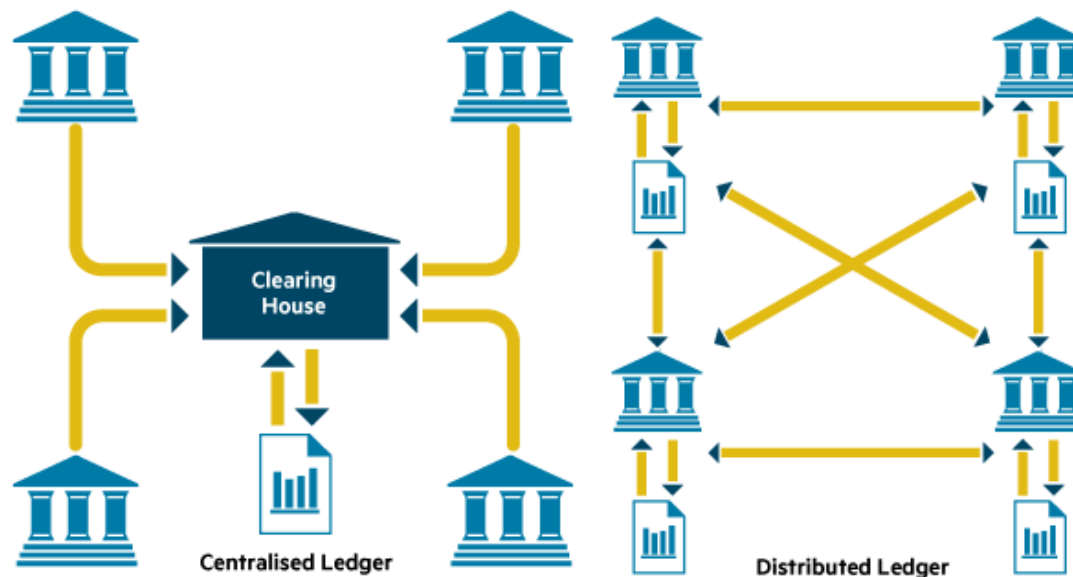
# Che cosa è la Blockchain?

**Tecnologia innovativa, basata su algoritmi matematici e tecniche crittografiche, che consente di memorizzare informazioni in modalità distribuita ed inalterabile**

# La blockchain: implementazione di un Registro Distribuito

## Embedding distributed ledger technology

A distributed ledger is a network that records ownership through a shared registry



In contrast to today's networks, distributed ledgers eliminate the need for central authorities to certify ownership and clear transactions. They can be open, verifying anonymous actors in the network, or they can be closed and require actors in the network to be already identified. The best known existing use for the distributed ledger is the cryptocurrency Bitcoin

FT graphic. Source: Santander InnoVentures, Oliver Wyman & Anthemis Partners

<https://www.process.st/introduction-to-blockchain>

- **Registro digitale distribuito**  
DLT: Distributed Ledger Technologies
- **Crittografia:** garanzia di riservatezza e integrità del dato
- **Resilienza:** ciascuno dei nodi contiene tutte le informazioni



**Qual è il legame tra la  
blockchain ed una pietra  
calcareia a forma di disco  
con un buco al centro?**





# Le origini della **blockchain**



<https://www.financiallounge.com/news/2017/11/13/primo-bitcoin-micronesia>

- Nel 1400 gli abitanti dell'isola di Yap (Micronesia) utilizzavano come moneta delle pietre calcaree chiamate Rai
- Ogni abitante possedeva un registro, il cui contenuto era identico per tutti, che riportava il nome del proprietario di ciascuna pietra Rai



# Le origini della **blockchain**



中本哲史

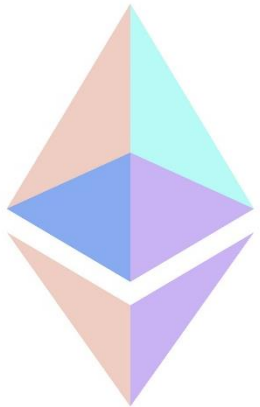
**Satoshi Nakamoto**



# Le origini della **blockchain**



- **Bitcoin:** prima blockchain, realizzata nel 2009 dall'anonimo Satoshi Nakamoto per generare e scambiare la criptovaluta bitcoin



- **Ethereum:** fondata da Vitalik Buterin nel 2015, oltre allo scambio della criptovaluta Ether, consente anche di eseguire applicazioni
- + oltre 2.000 blockchain (Altchain)



# Caratteristiche di Bitcoin

- È possibile «minare» al massimo 21 Milioni di bitcoin
- Ogni giorno ne vengono minati circa 900
- Al momento ne sono stati «minati» circa 19,6 Milioni (93,4%): si prevede il completamento entro il 2140
- L'unità minima è il satoshi, pari a  $10^{-8}$  BTC
- È prevista una ricompensa per il miner che per primo «mina» (valida) un blocco
- Questa ricompensa si dimezza ogni 210.000 blocchi (ca. 4 anni): dal 2020 è pari a 6,25 BTC

## Bitcoin: un sistema di moneta elettronica peer-to-peer

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

Translated in Italian from bitcoin.org/bitcoin.pdf  
by @terzim

**Sommario.** Una versione puramente peer-to-peer di denaro elettronico permetterebbe di spedire direttamente pagamenti online da un'entità ad un'altra senza passare tramite un'istituzione finanziaria. Le firme digitali offrono una soluzione parziale al problema, ma i benefici principali sono persi se una terza persona di fiducia è ancora richiesta per prevenire la doppia spesa. Proponiamo una soluzione al problema della doppia spesa mediante l'utilizzo di una rete peer-to-peer. La rete stampa un marcatore temporale sulle transazioni facendo hashing sulle stesse e incatenandole in una catena di proof-of-work basata sugli hash, formando una registrazione che non può essere modificata senza rifare la proof-of-work. La catena più lunga non solo serve come prova della sequenza di eventi ai quali si è assistito, ma anche come prova che essa proviene dal gruppo più grande di potenza CPU. Fintanto che la maggior parte della potenza CPU è controllata da nodi che non cooperano per attaccare la rete, questi genereranno la catena più lunga e supereranno gli utenti malintenzionati. La rete stessa richiede una struttura minimale. I messaggi sono trasmessi su base best effort, e i nodi possono lasciare e ricongiungersi con la rete a loro piacimento, accettando la catena proof-of-work più lunga come prova di quella che è avvenuta mentre erano non erano presenti.

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

[https://bitcoin.org/files/bitcoin-paper/bitcoin\\_it.pdf](https://bitcoin.org/files/bitcoin-paper/bitcoin_it.pdf)

# Come funziona la blockchain: i blocchi



- La blockchain è una «**catena di blocchi**»
- Ciascun blocco è collegato al **solo** blocco precedente con un **particolare Link**
- Il Link al blocco precedente, oltre a formare la catena:
  - *garantisce anche **l'inalterabilità** del blocco precedente*
  - *viene realizzato con una particolare funzione denominata **HASH***



# La funzione di **HASH**

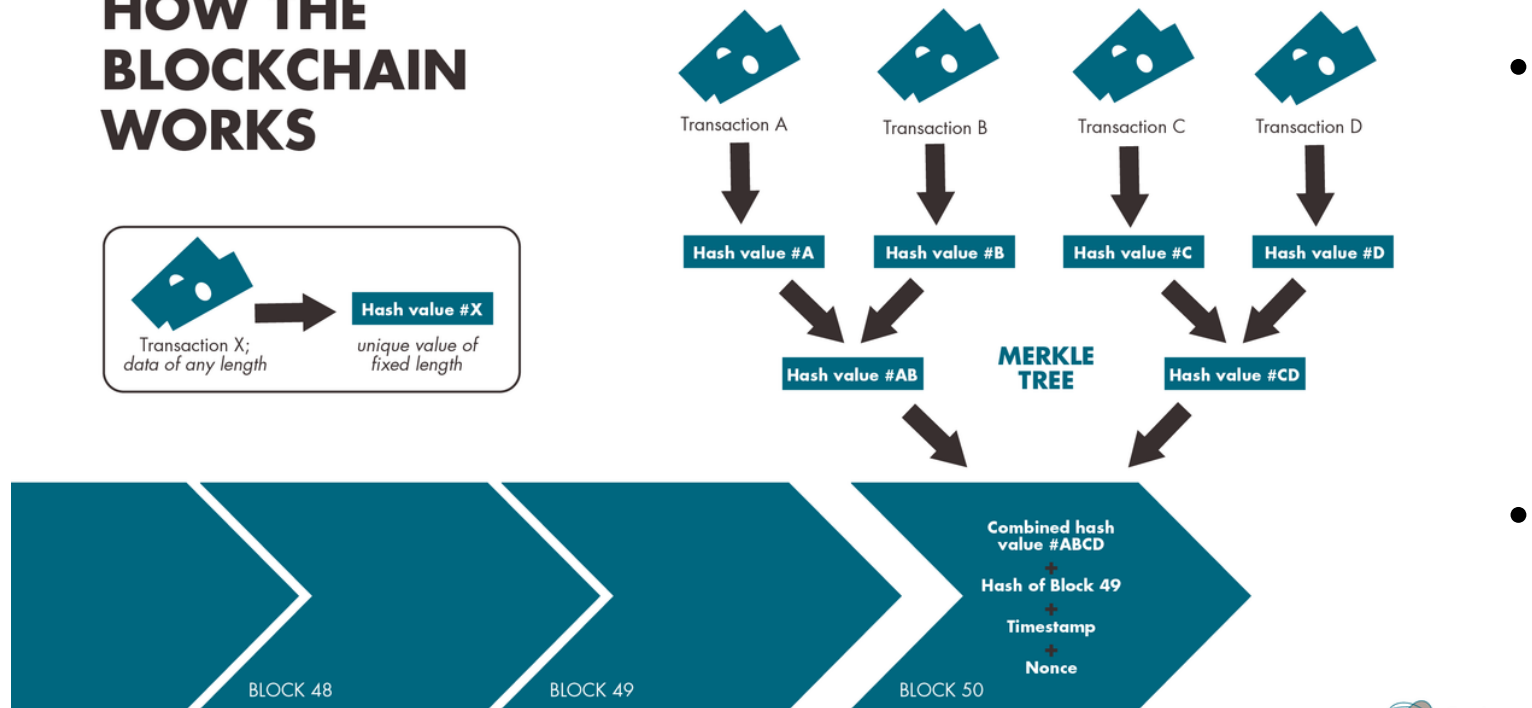
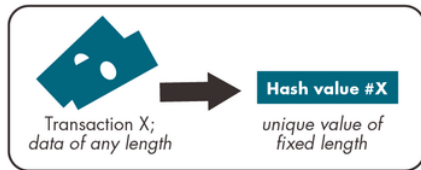


- Hash (**I**ngegnere) =  
= 65dce56252e2da82278999534de124d3561838d7d99e2c128d8ff5c9ff31a646
- Hash (**i**ngegnere) =  
= 036a66e21c964786585c259cc0f1d86a63e6d1f7dbc8bf58b5fce42822c1a250



# Come funziona la blockchain: i blocchi

## HOW THE BLOCKCHAIN WORKS

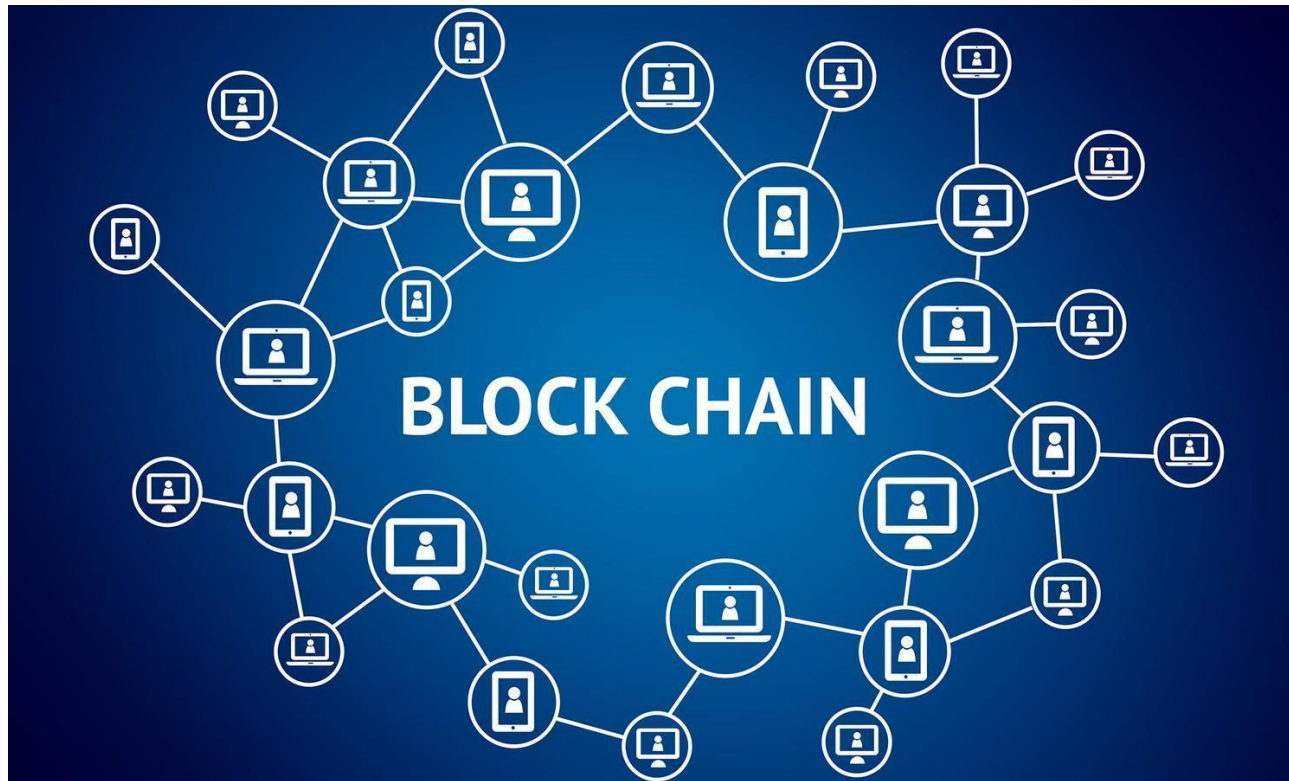


Reproduction of an original figure in "The Great Chain of Being Sure About Things" by the Economist



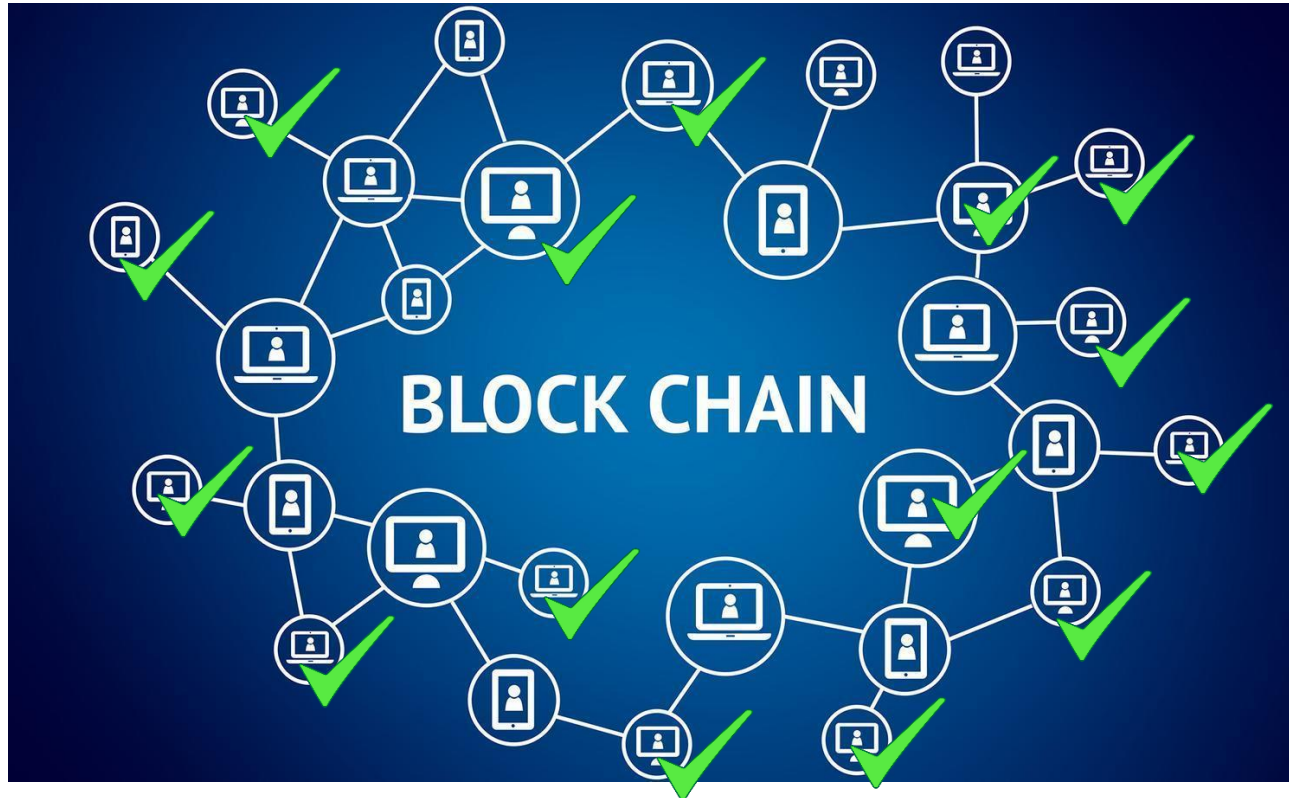
- Catena di blocchi logici
- Ogni blocco è indissolubilmente legato al blocco precedente mediante algoritmi crittografici
- Per modificare il contenuto di un blocco, occorre modificare quello di tutti i blocchi successivi

# Come funziona la blockchain: i nodi



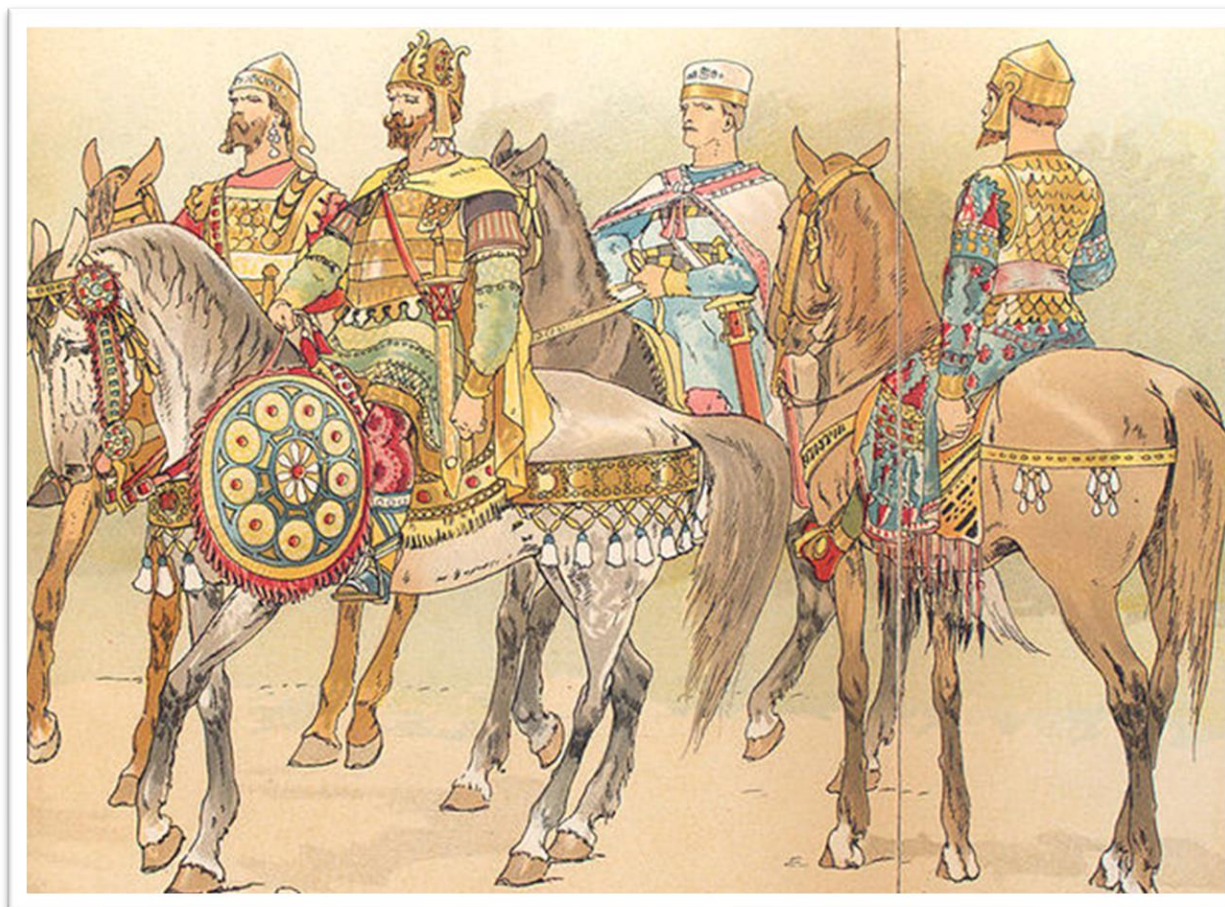
- I **blocchi** logici sono memorizzati su sistemi fisici (server), chiamati **nodi**
- Ogni nodo può interconnettersi con tutti gli altri nodi della rete in modalità P2P (**peer-to-peer**), senza intermediari
- Su ciascun nodo è memorizzato l'intero contenuto della blockchain

# Come funziona la blockchain: i nodi

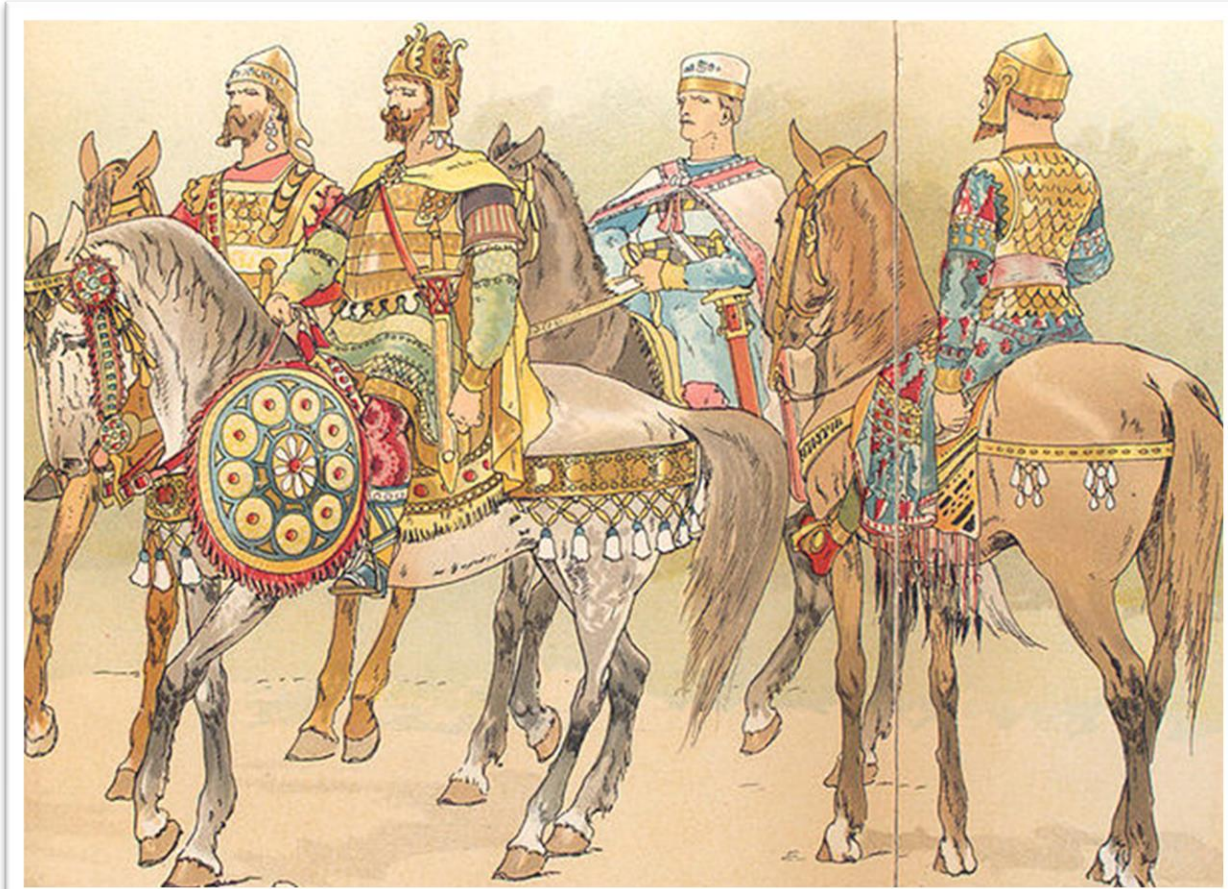


- Affinché un blocco sia aggiunto alla catena, deve essere validato dai nodi secondo il **meccanismo di consenso** previsto dalla blockchain (es. *risorse computazionali* o *valore posseduto*)
- **Attacco al 51%:** controllando il 50% + 1 della blockchain si può alterare lo stato delle transazioni

# Cosa c'entrano i Generali Bizantini?



# Problema dei Generali Bizantini



- I vari generali bizantini devono coordinarsi sull'attacco (se farlo, quando farlo, etc.)
- **Attacco coordinato = successo**
- **Attacco non coordinato = sconfitta**
- Ogni generale è in un luogo diverso: non è possibile prendere una decisione tutti insieme contemporaneamente
- Alcuni generali potrebbero essere dei traditori

# Soluzione: Algoritmo di Consenso

In origine era il **Proof of Work (PoW)**:

Bitcoin (2009), Ethereum (2015)

- *Algoritmo di consenso basato sulla potenza di calcolo posseduta dal nodo minatore (miner)*
- *Rende la blockchain estremamente energivora*
- *È abbastanza lento, ma estremamente efficace, sicuro e affidabile*



# Soluzione: Algoritmo di Consenso

Poi venne il **Proof of Stake (PoS)**:

Peercoin (2012), Ethereum (2022)

- *Algoritmo di consenso basato sulla quantità di criptovaluta (stake) posseduta dal nodo validatore*
- *Più veloce e meno energivoro del PoW*
- *Anche se è estremamente improbabile una validazione non corretta o fraudolenta, in quanto il validatore rischia di perdere il proprio stake, è meno sicuro del PoW perché concentra le validazioni sui nodi con più stake*
- *Ha meno anni di «esperienza sul campo» rispetto al PoW*



# Soluzione: Algoritmo di Consenso

Ulteriori algoritmi di consenso

II **Delegated Proof of Stake (DPoS)**: EOS (2018), Solana (2020)

*Simile al PoS ma con nodi delegati «eletti»*

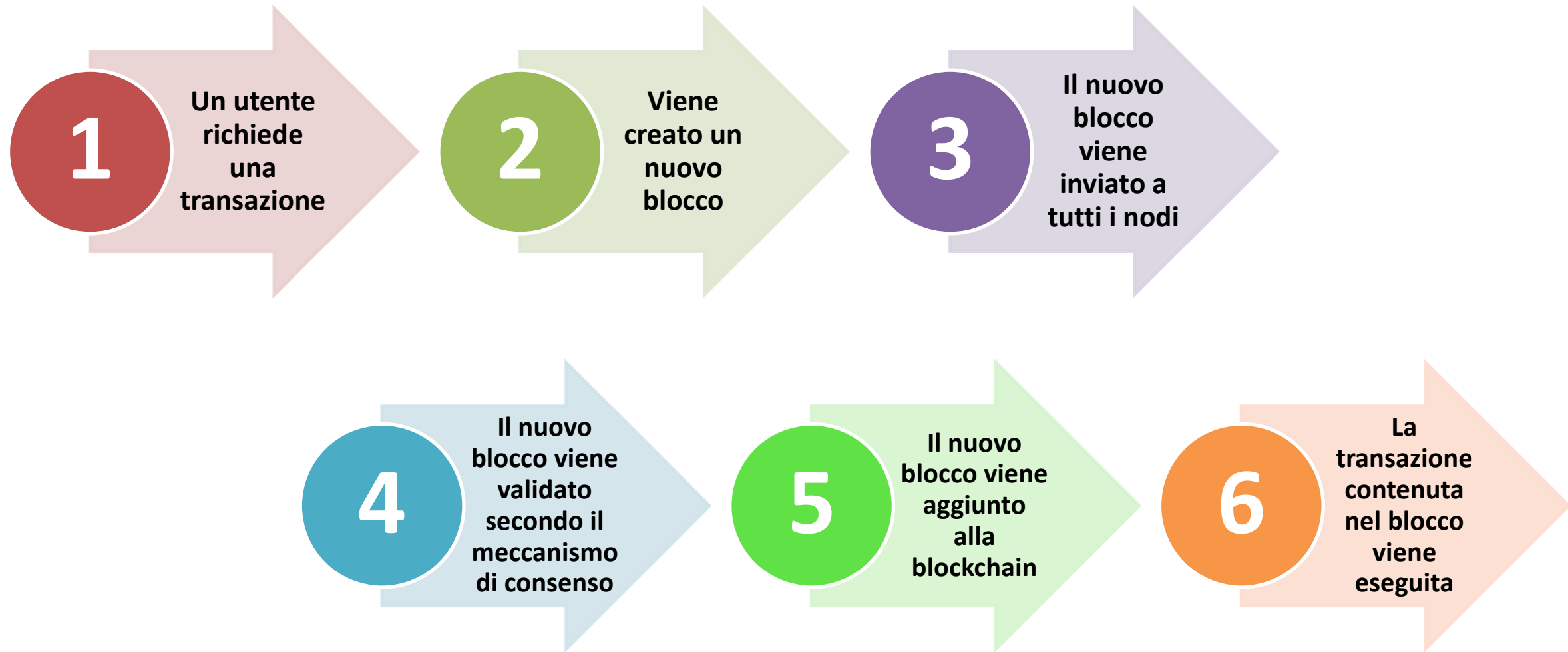
II **Pure Proof of Stake (PPoS)**: Algorand (2019)

*Simile al PoS ma con nodi «estratti a sorte»*

→ *Evitano di concentrare le **validazioni sui nodi con maggiori stake***



# Come funziona la **blockchain**: step-by-step





# Qual è la differenza?

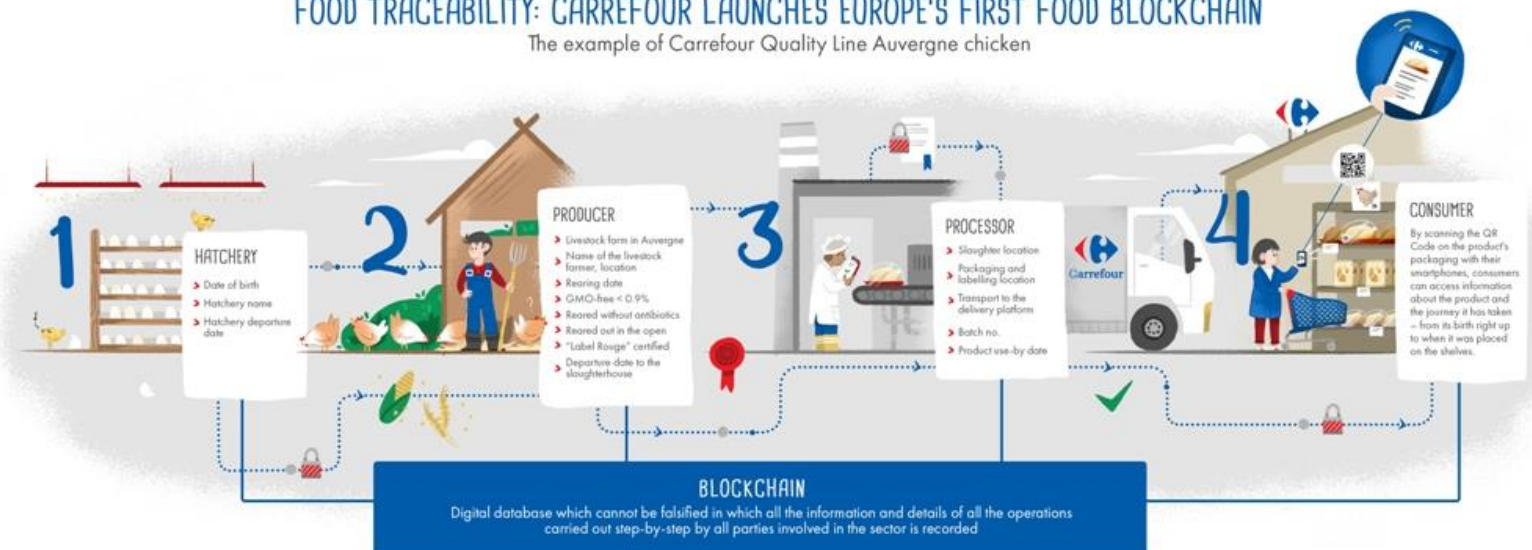


# Agrifood: tracciabilità della filiera



## FOOD TRACEABILITY: CARREFOUR LAUNCHES EUROPE'S FIRST FOOD BLOCKCHAIN

The example of Carrefour Quality Line Auvergne chicken



<https://www.mark-up.it/carrefour-il-pollo-filiera-qualita-tracciato-con-tecnologia-blockchain>

<https://www.economyup.it/retail/carrefour-primo-europa-usare-la-blockchain-tracciare-prodotti>

Ing. Francesco Amendola

La tecnologia blockchain: dai principi generali di funzionamento agli Smart Contract, Token e NFT

25/03/2024

pag. 28

# Qual è la differenza?

1

LEGGI IL QR CODE SULLA CONFEZIONE

Inizia il tuo viaggio nel sito web mobile, alla scoperta della filiera di uno **specifico lotto Barilla**.



**2015: nessuna blockchain, piattaforma proprietaria Safety for Food (S4F)**

**2018: Blockchain basata su Ethereum**

<https://www.barillagroup.com/sites/default/files/barilla%20cisco%20internet%20of%20everything%20eng.pdf>  
<https://www.carrefour.fr/engagements/act-for-food/acte-9-garantir-une-tracabilite-complete>

# La crittografia alla base di tutto

Ogni utente possiede una coppia di chiavi crittografiche:

- una pubblica, nota a tutti (**SHARE**), che identifica l'utente sulla blockchain
- una privata, nota solo all'utente proprietario (**SECRET**)

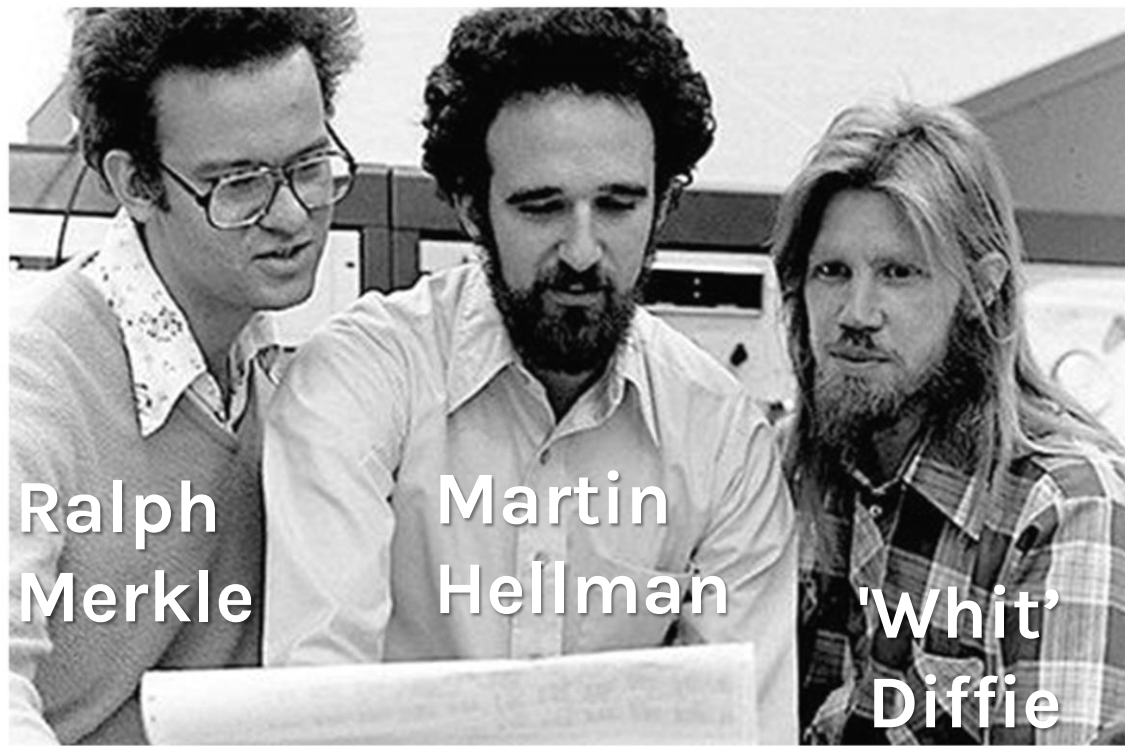
Qualsiasi messaggio cifrato con la chiave pubblica può essere decifrato con la chiave privata, e viceversa!

<https://www.cryptoblock.it/bitcoin-wallet-chiave-privata-pubblica-e-address>

<https://www.criptoinvestire.com/come-funziona-la-crittografia-nelle-blockchain.html>



# La crittografia alla base di tutto



1976 Protocollo **Diffie-Hellman**

1979 **Merkle** tree

1978 Algoritmo **RSA**



# Le blockchain non sono tutte uguali

Oltre 2.000  
blockchain (Altchain)

Oltre 8.000  
criptovalute (Altcoin)

|                           | Open<br>(«permissionless»)              | Closed<br>(«permissioned») |
|---------------------------|-----------------------------------------|----------------------------|
| Who updates               | Everybody                               | Appointed pers./org.       |
| Who produces data         | All users                               | Customers                  |
| Incentive to follow rules | Direct economic (both<br>carrot & whip) | Reputation                 |
| Storage                   | Distributed                             | Centralized                |
| Trust central actors      | No                                      | Yes                        |
| Transaction costs         | -                                       | +                          |
| Capacity/Throughput       | -                                       | +                          |
| Immutability              | +                                       | -                          |
| Currency/token            | Yes                                     | No                         |
| Examples                  | Bitcoin, Ethereum                       | HyperLedger, Corda         |

www.vestforsk.no

<https://www.process.st/introduction-to-blockchain>

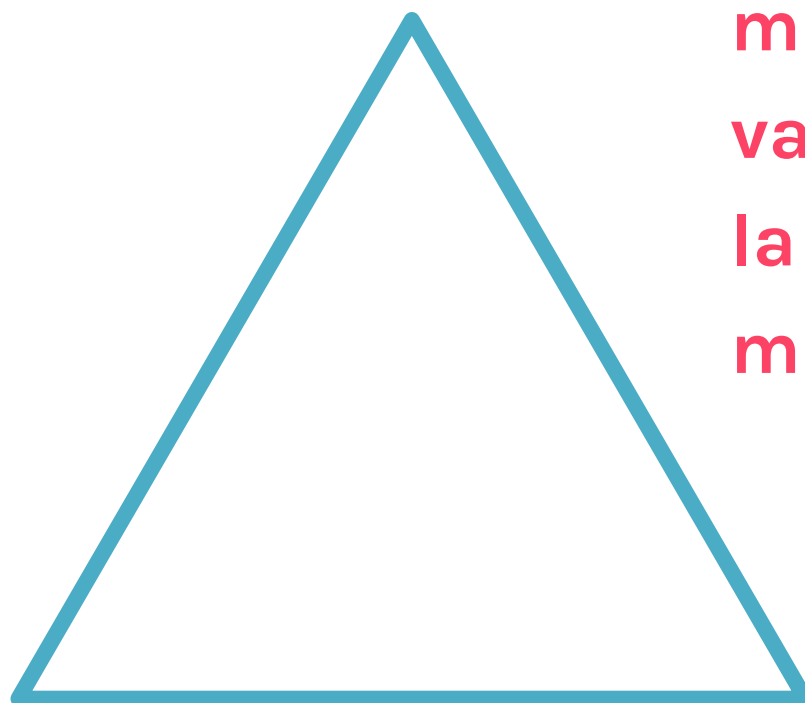


# Il trilemma della blockchain

## Scalabilità

Velocità nel processare le transazioni,  
anche quando il loro volume aumenta

In una blockchain è possibile  
massimizzare solo due delle tre  
variabili per cui, di conseguenza,  
la terza variabile risulta  
minimizzata



## Sicurezza

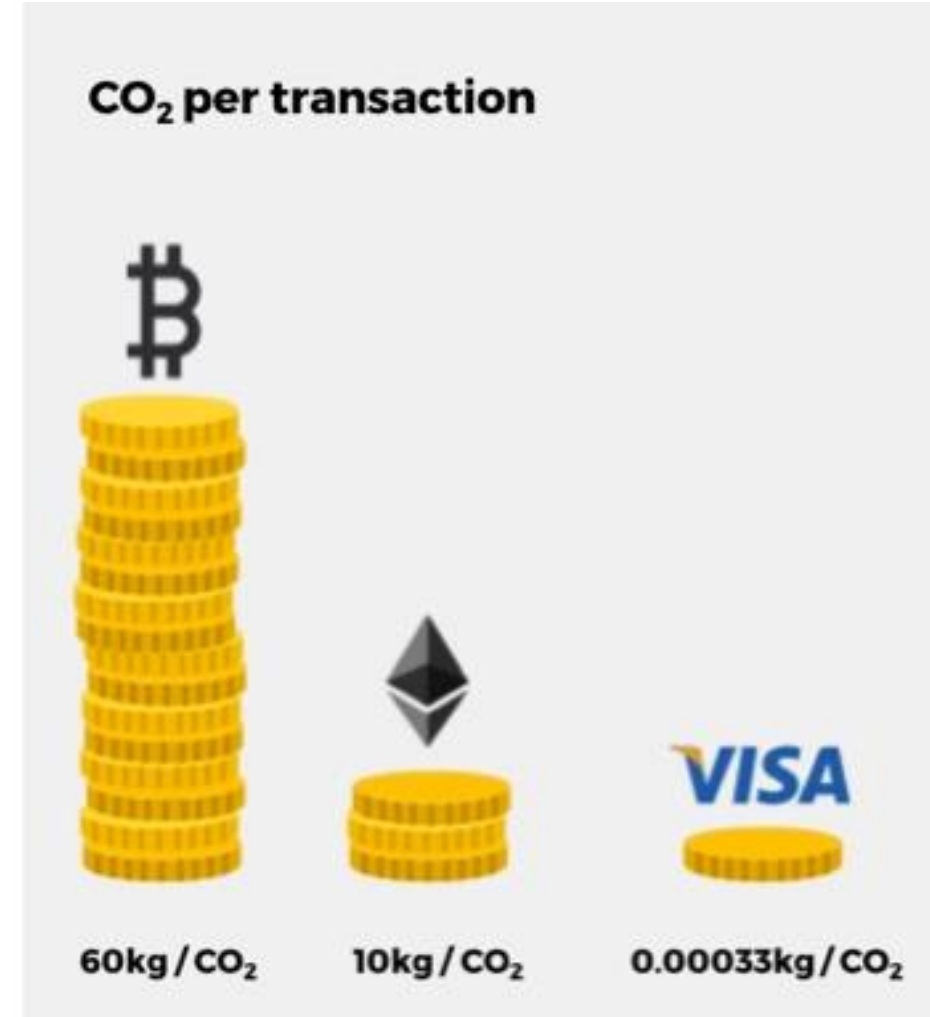
Capacità di resistere agli attacchi

## Decentralizzazione

Nodi distribuiti, resilienza

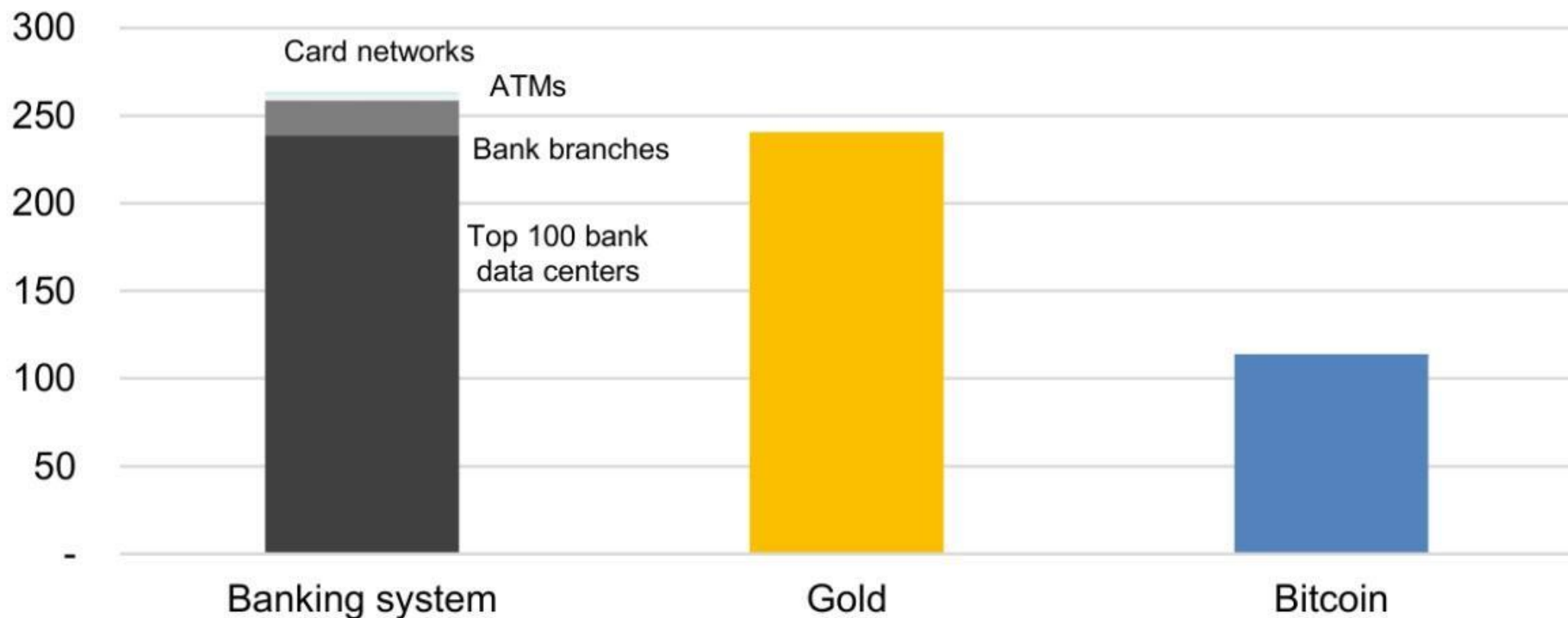
# La blockchain è una tecnologia energivora ?

- L'attuale consumo per l'estrazione di bitcoin (149 TWh) è pari a quello di uno Stato come la Malesia o la Svezia
- La tendenza dei miner è sfruttare energia alternativa sotto-utilizzata
- **Occorre bilanciare i costi sostenuti con i benefici ed i risparmi conseguiti**



# La blockchain è una tecnologia energivora ?

Stima del **consumo elettrico** annuo (TWh/anno)



Fonte: Galaxy Digital

# The Merge - Ethereum

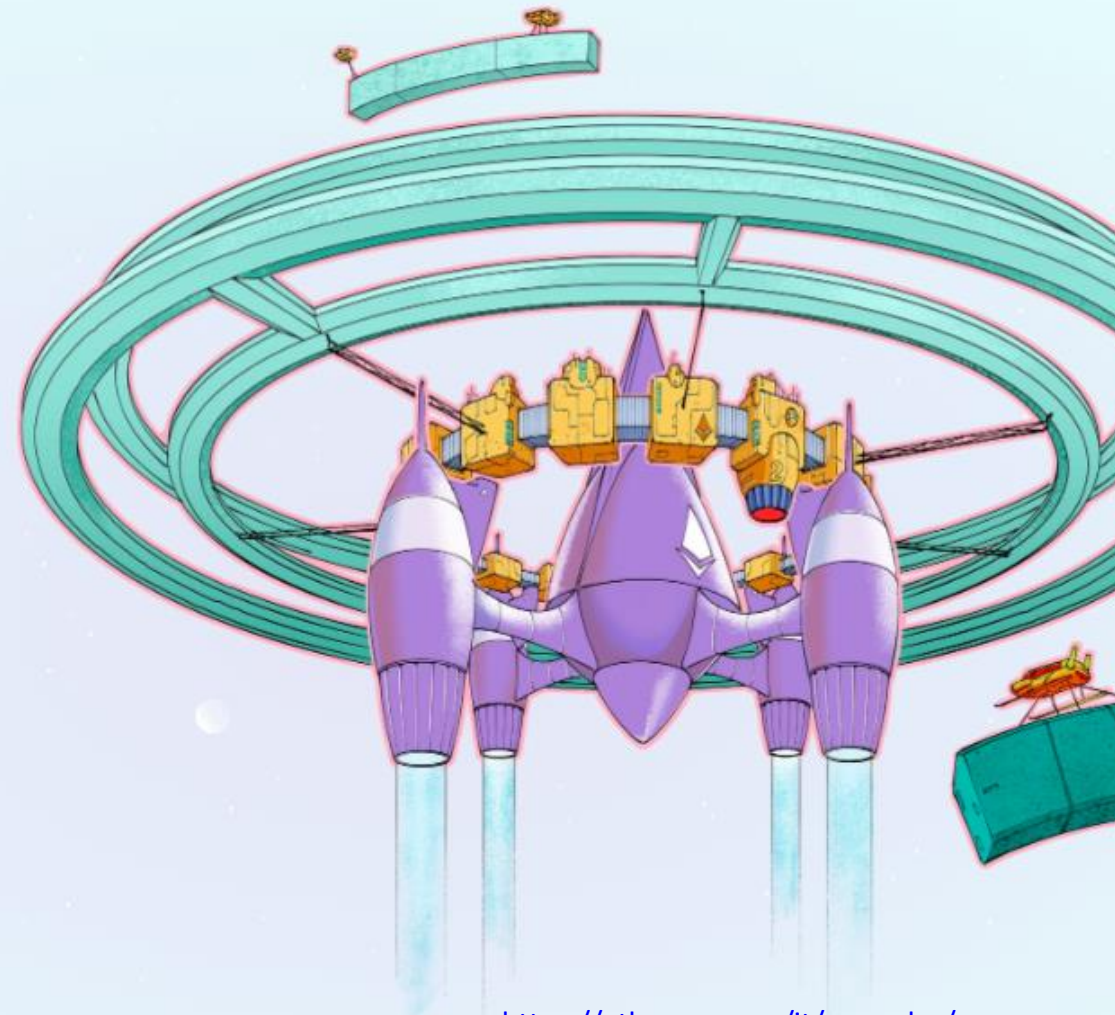
15 settembre 2022, dopo circa 7 anni...

AGGIORNAMENTI / FUSIONE

## La Fusione

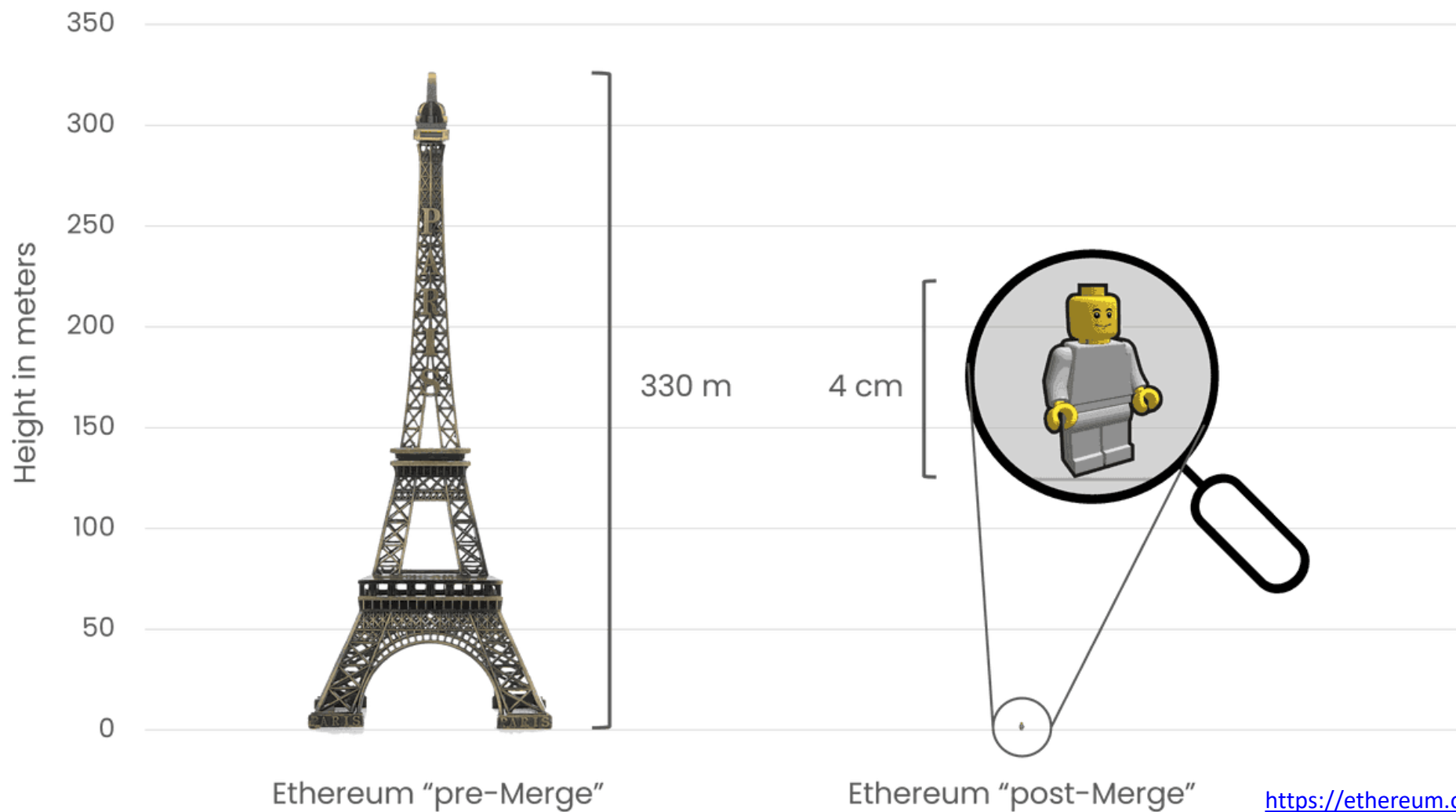
- La Rete principale di Ethereum usa il Poof of stake, ma non è sempre stato così.
- La transizione dal meccanismo originale di Proof of Work al Proof of stake è stata chiamata La Fusione.
- La Fusione si riferisce al momento in cui la Rete principale originale di Ethereum è divenuta parte di una blockchain di Proof of stake separata, detta Beacon Chain, ora esistente come un'unica catena.
- La Fusione ha ridotto il consumo energetico di Ethereum di circa il 99,95%.

Ultimo aggiornamento pagina: 14 ottobre 2022

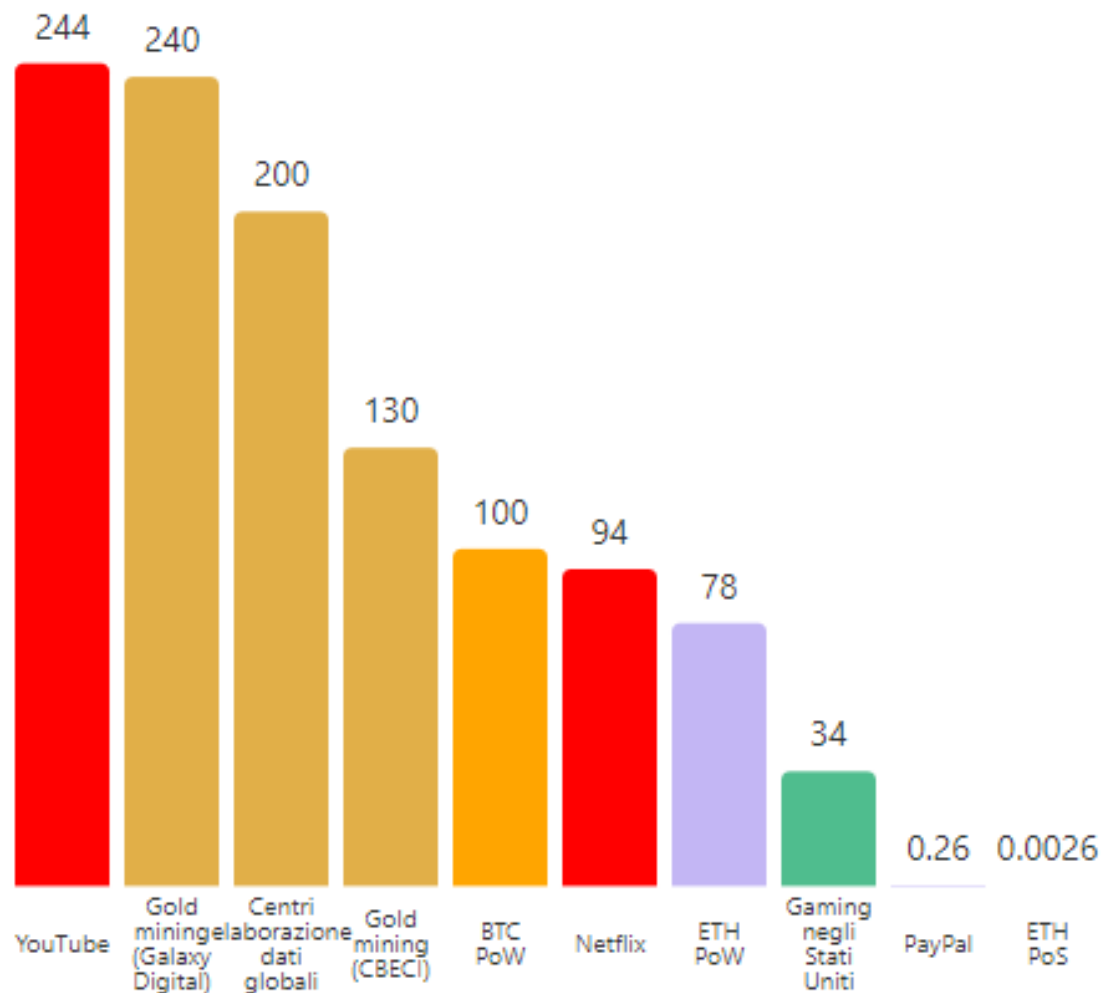


<https://ethereum.org/it/upgrades/merge>

# Il debito carbonico di Ethereum

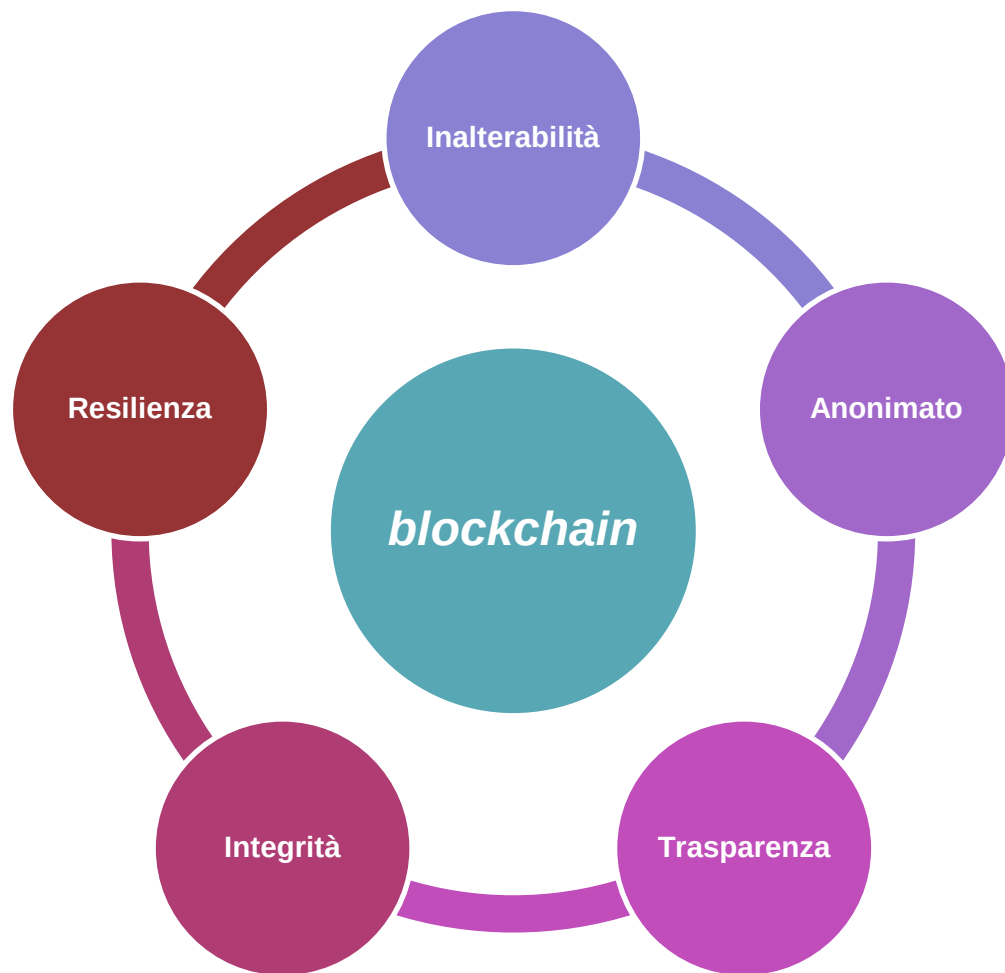


# Consumo di **energia** annuale in TWh/anno



<https://ethereum.org/it/energy-consumption>

# Caratteristiche della **blockchain**



... in modalità  
**distribuita**  
senza intermediari



# Cosa posso realizzare con la blockchain?

- **Criptovalute**
- **Token**
- **Smart Contract**
- **Non-fungible Token**

**Prodotti digitali, servizi e soluzioni uniche**

# Cosa sono gli Smart Contract?



- Programmi (codice software) eseguiti sui nodi di una blockchain **(IFTTT – If This Then That)**
- La tecnologia blockchain garantisce la **trasparenza**, l'**integrità** e l'**immodificabilità** dei risultati
- A differenza dei contratti, **non** hanno necessariamente **valenza legale**

# Come è fatto uno Smart Contract?

```
Purchasing.sol
1  pragma solidity ^0.5.0;
2
3  contract Purchasing {
4
5      address [6] public buyers;
6
7      function purchase(uint artId) public returns (uint) {
8          require(artId >= 0 && artId <= 5);
9
10         require (buyers[artId] == address(0x0));
11
12         buyers[artId] = msg.sender; |
13
14         return artId;
15     }
16
17     function getBuyers() public view returns (address[6] memory) {
18         return buyers;
19     }
20
21 }
22
```

- Esempio di Smart Contract per certificare l'acquisto delle opere d'arte
- Il linguaggio di programmazione più diffuso è Solidity su Ethereum

<https://cryptonomist.ch/2019/08/24/come-creare-dapp-ethereum-smart-contract>

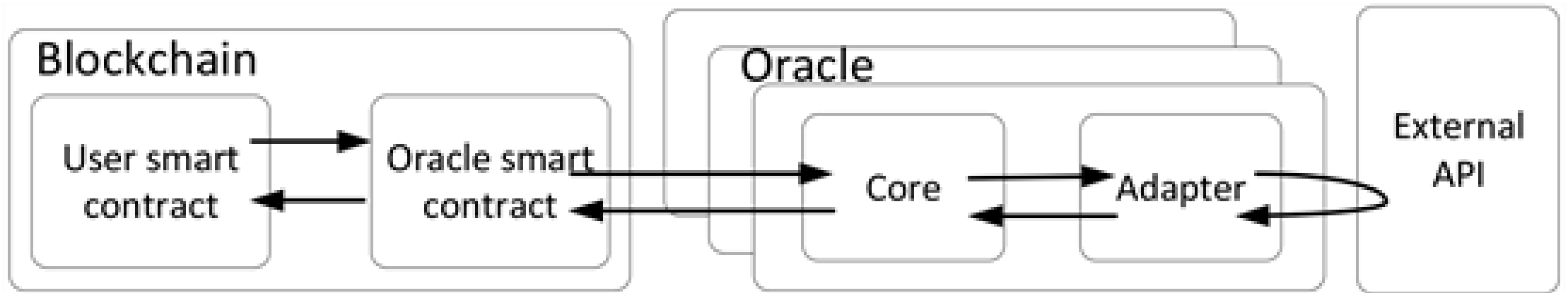


# Esempi di Smart Contract

- Assicurazione di viaggio che automaticamente rimborsa l'utente in caso di ritardo dell'operatore (treno, aereo, etc.)
- Trading (valute, azionario, etc.)
- Definizione automatica delle regole di pricing in base al livello della domanda
- Gestione Fideiussioni
- Definizione di vincoli per l'Intelligenza Artificiale
- **Oracoli**
- **Creazione e gestione dei Token**

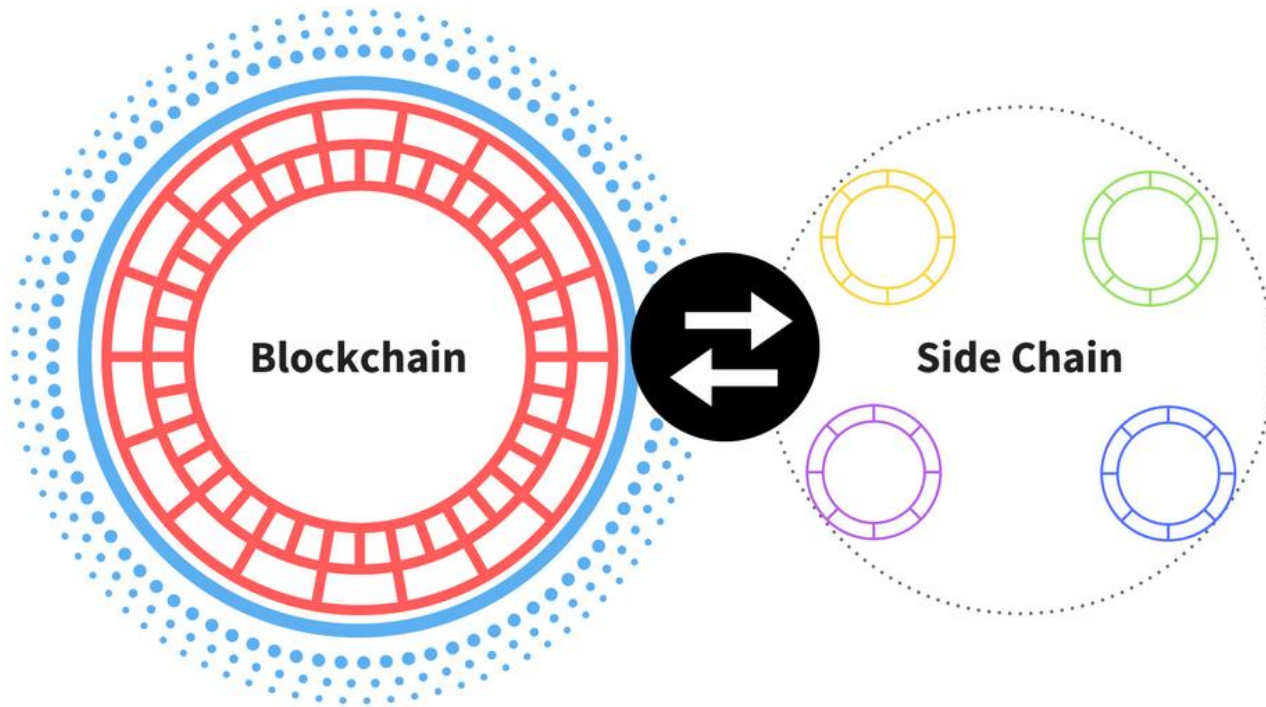
# Gli Oracoli

- Fungono da tramite tra una blockchain ed il mondo esterno
- Rendono possibile l'esecuzione di Smart Contract con dati esterni (es. valore delle azioni, esisti scommesse, etc.)



<https://academy.binance.com/it/articles/blockchain-oracles-explained>

# Soluzione del Trilemma con gli Smart Contract



- Sidechain: **blockchain** **secondarie** connesse bi-direzionalmente ad una blockchain principale
- Offrono **caratteristiche specifiche** (es. maggiore velocità/scalabilità, a scapito di sicurezza e/o decentralizzazione)
- Esempio: ricorso alla sidechain per la molteplicità delle transazioni (es. micro-pagamenti veloci), riportando sulla blockchain principale solo il **saldo delle operazioni**

# Rischio di attacchi hacker

## Attacchi al 51%

- Ethereum Classic      2020      \$5,6 milioni
- Bitcoin Cash      2019      (bloccato in tempo)
- Bitcoin Gold      2018      \$18 milioni

## Attacchi su Smart Contract

- The DAO      2016      \$55 milioni
- Polynetwork      2021      \$611 milioni (restituiti)
- DAO Maker      2021      \$7 milioni

## Attacchi su Wallet utenti/Exchange

- Miliardi di \$ **sottratti continuamente** dai Wallet degli utenti o dalle piattaforme di intermediazione (Exchange)



**PolyNetwork**



<https://99bitcoins.com/51-percent-attack>  
<https://sicurezza.net/cyber-security/blockchain-no-prova-hacker>

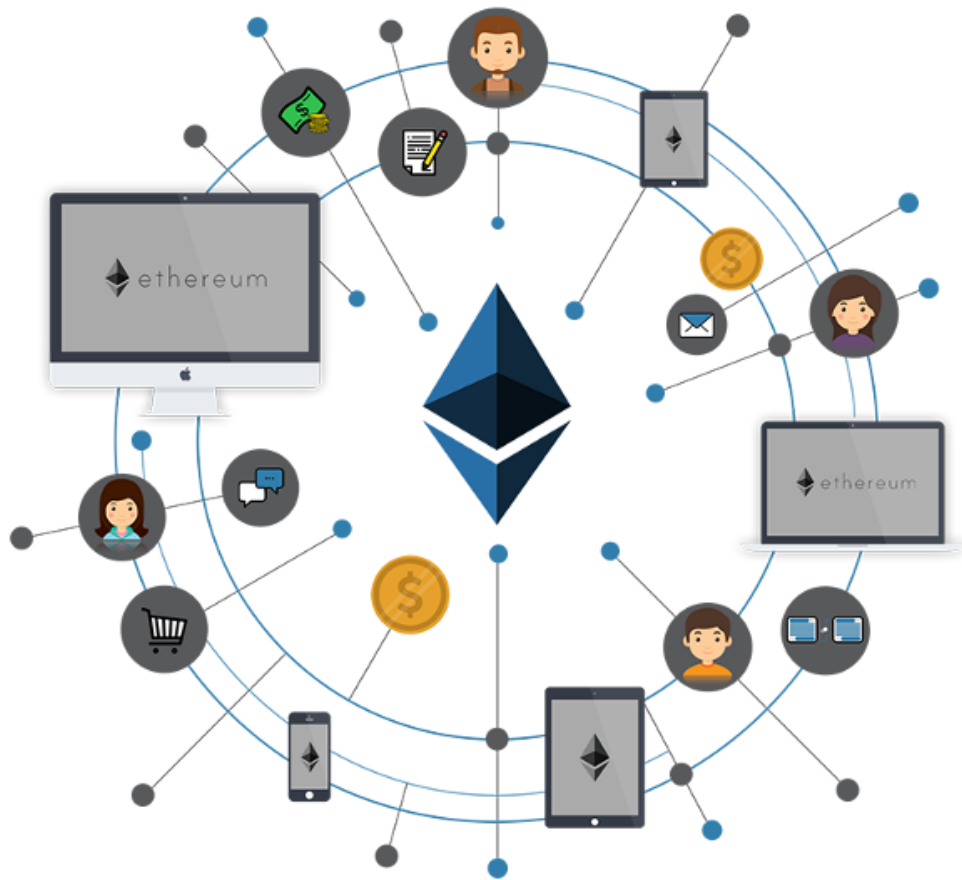


# Non solo criptovalute...



... ma anche **gettoni**

# Cosa sono i Token?



- **Definizione:** informazioni digitali rappresentative di una qualche forma di diritto
- **Esempi:**
  - la proprietà di un bene (asset)
  - l'accesso ad un servizio
  - denaro o titoli



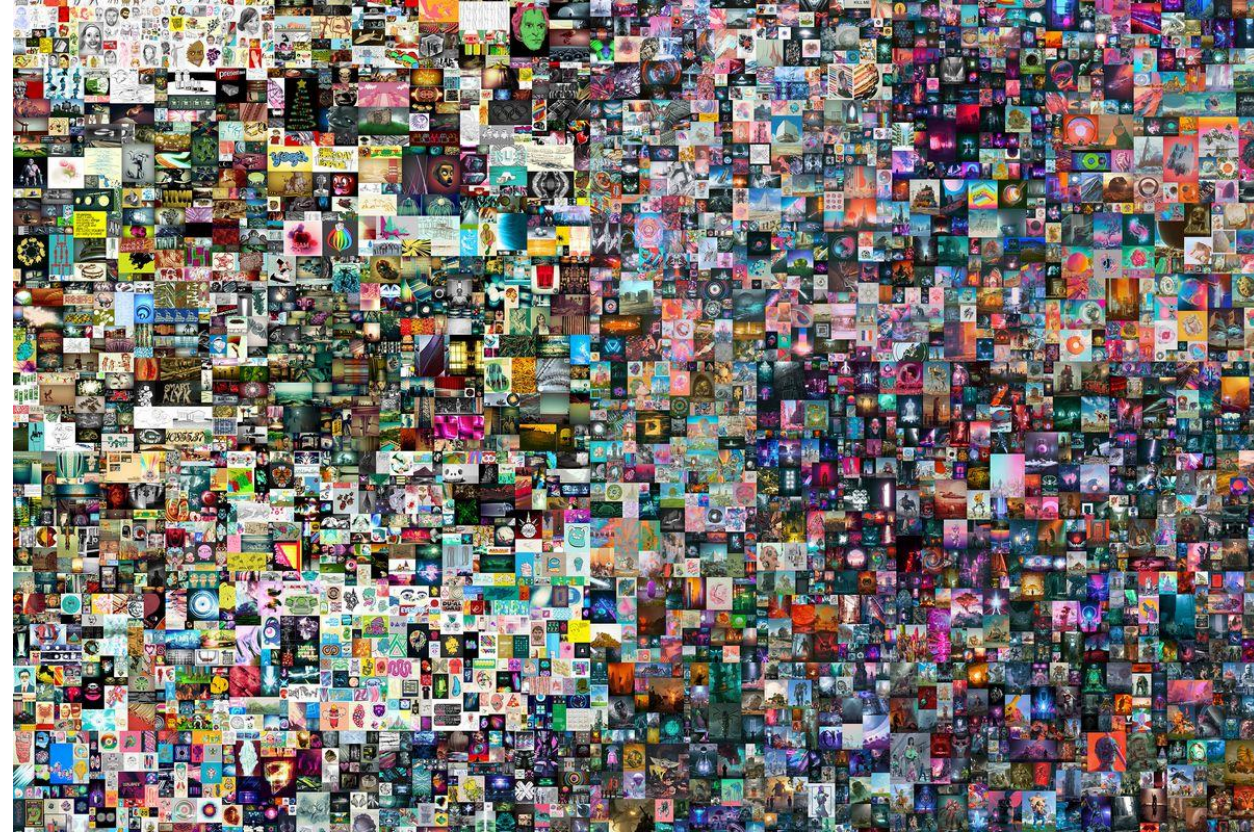
# Token fungibili ed infungibili



# Token fungibili ed infungibili



**Femme au Chien (olio su tela)**  
**Pablo Picasso, 1962**



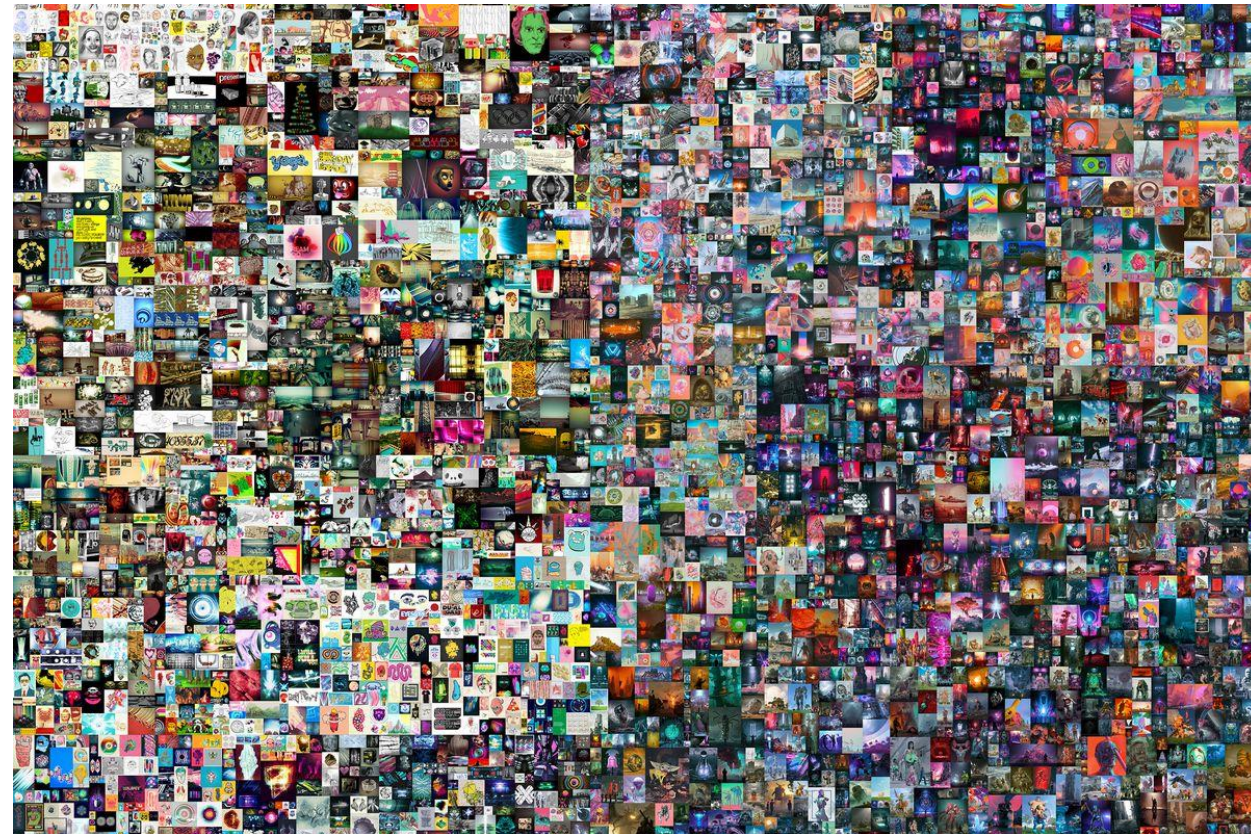
**Everydays: the First 5000 Days (opera digitale)**  
**Mike Winkelmann (Beeple), 2021**



# Token fungibili ed infungibili



**Femme au Chien (olio su tela)**  
**Pablo Picasso, 1962**



**Everydays: the First 5000 Days (opera digitale)**  
**Mike Winkelmann (Beeple), 2021**

# Token fungibili ed infungibili



**Femme au Chien (olio su tela)**  
**Pablo Picasso, 1962**



**Everydays: the First 5000 Days (opera digitale)**  
**Mike Winkelmann (Beeple), 2021**



# Quale problema risolvono gli NFT?

**La mancanza di scarsità nativa degli asset digitali**

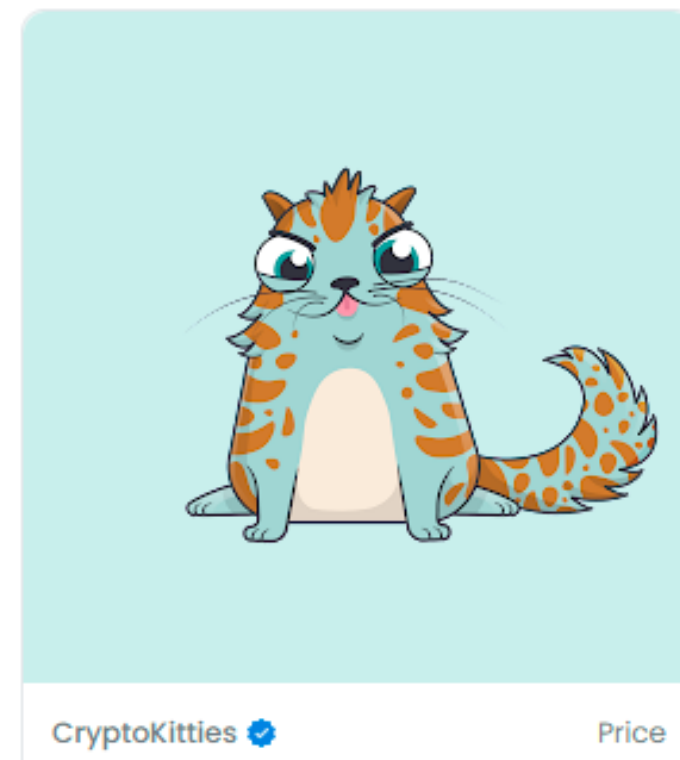
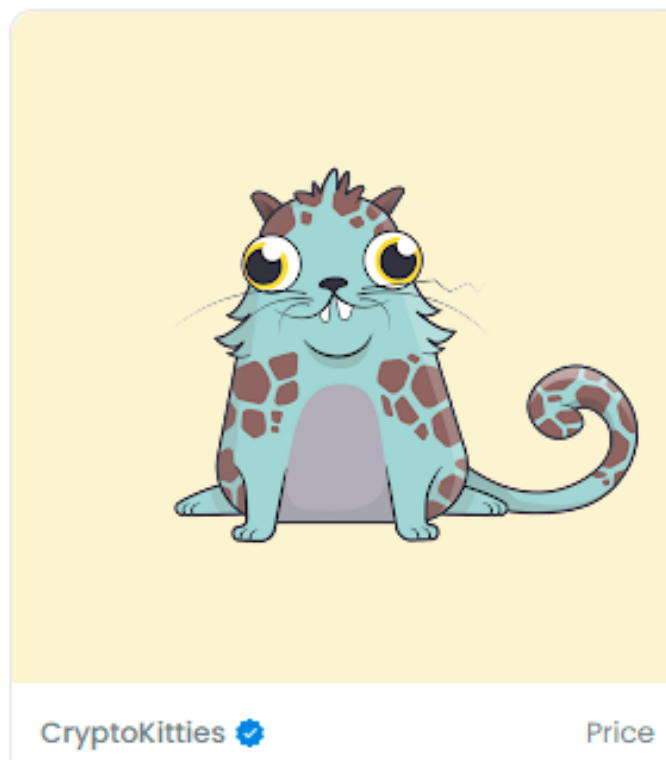
**Digital Scarcity**

# NFT di asset digitali unici



## What is CryptoKitties?

CryptoKitties is a game centered around breedable, collectible, and oh-so-adorable creatures we call CryptoKitties! Each cat is one-of-a-kind and 100% owned by you; it cannot be replicated, taken away, or destroyed.



<https://www.cryptokitties.co/>

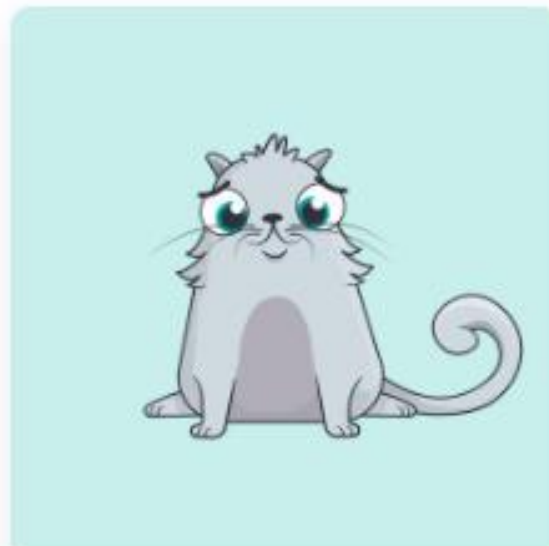
# NFT di asset digitali unici



Cecil Teamust

Price

0.002



Rare & Boy

Price

240

Last sale: 0.002

## Cecil Teamust

Owned by [Gytukas](#) 99 views 1 favorite

Sale ends November 18, 2022 at 7:37am GMT+2

Current price

0,002 \$2,62

Add to cart

Make offer

## Rare & Boy

Owned by [MIAJOERG](#) 60 views 2 favorites

Sale ends November 19, 2022 at 8:14am GMT+2

Current price

240 \$314,800,80

Add to cart

Make offer

<https://opensea.io/collection/cryptokitties>

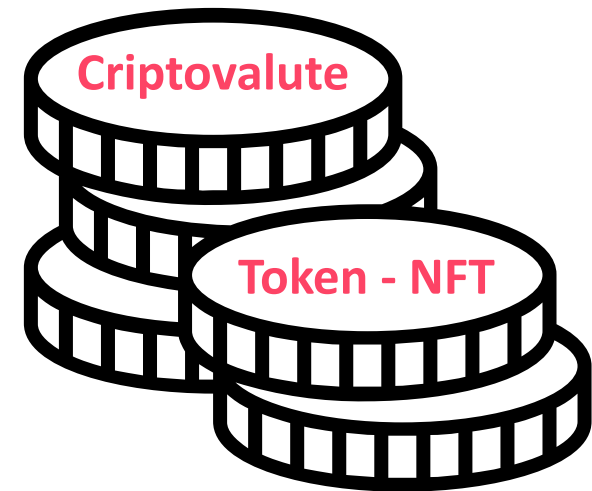
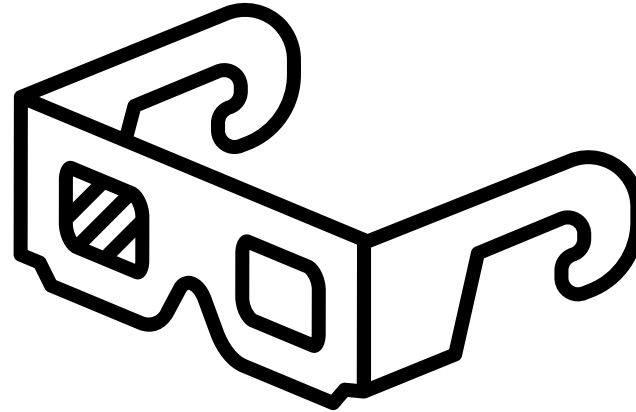
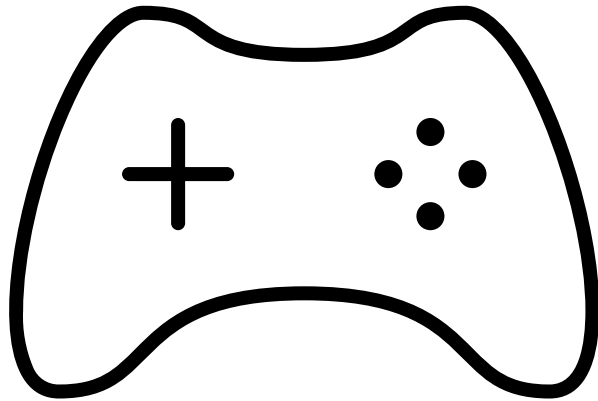
# Esempio di NFT: 2 al prezzo di 1

- Primo cripto-francobollo, emesso da La Posta Svizzera
- Oltre al francobollo tradizionale, si riceve la sua versione digitale NFT





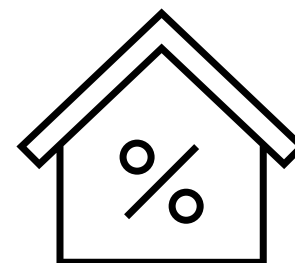
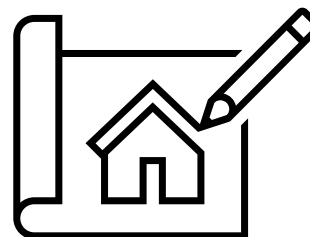
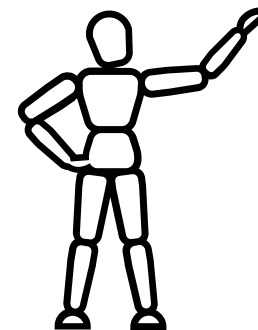
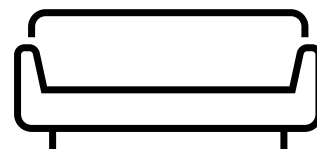
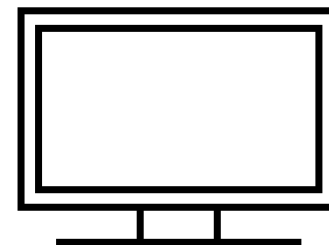
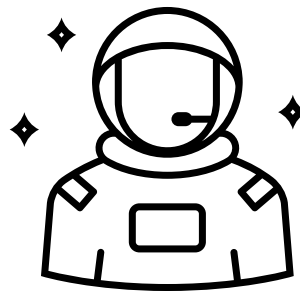
# Gaming P2E: dal Play-to-Win al Play-to-Earn



# Metaverso e Digital Scarcity

## Asset digitali «scarsi»

- Avatar e accessori
- Arredamento
- Opere d'arte
- Collezionismo
- Virtual Real Estate





## Web 1.0 – fruizione

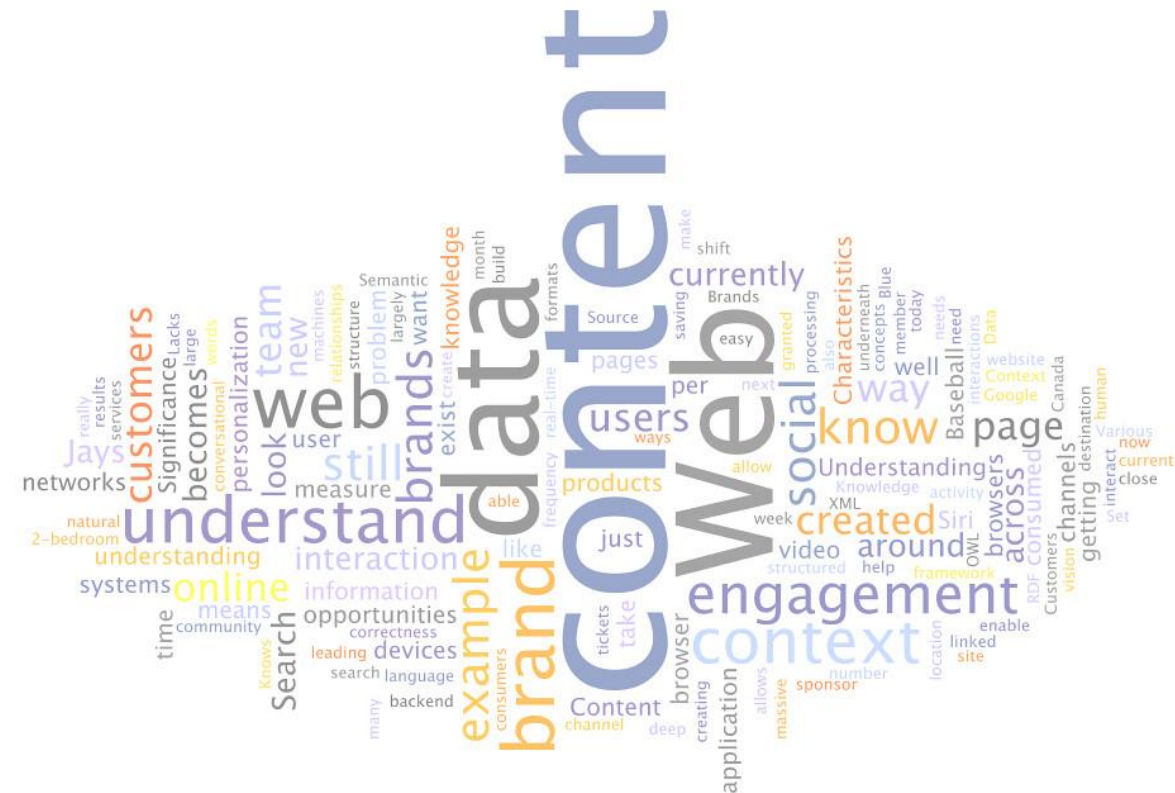
## Information economy

## Web 2.0 – contribuzione (social)

## Platform economy

## Web 3.0 – partecipazione

## Token economy





# GRAZIE PER L'ATTENZIONE

**Ing. Francesco Amendola**  
[info@ingamendola.com](mailto:info@ingamendola.com)