

QUANT-01



**MATTEO  
MAGGIONI**

- Laureato in Economia delle istituzioni e dei mercati finanziari presso l'Università Cattolica di Milano. Membro dell'International Federation of Technical Analysts (IFTA) e socio della Società Italiana Analisi Tecnica (SIAT).
- Attualmente sono trader istituzionale sui mercati delle commodities.
- Specializzazione in strumenti derivati su indici azionari ed obbligazionari in ottica di breve periodo. Prediligo il trading algoritmico, basato sia su metodi tradizionali che innovativi, tra i quali il machine learning.
- Docente per FinecoBank SpA, per la Società Italiana Analisi Tecnica (SIAT) e per l'Ordine degli Ingegneri della provincia di Roma.
- Faccio parte del comitato scientifico della SIAT.
- Ho tenuto numerose conferenze sul trading in Italia e all'estero, tra cui Expo di Borsa Italiana, ITF di Rimini e Rotary Club.
- Sono autore e coautore di vari libri dedicati al trading e alle strategie di investimento.
- Dal 2012 mi occupo anche di valute digitali e blockchain e sono coautore dei libri "Bitcoin Revolution" e "Tutto su Bitcoin", editi da Hoepli.

**QUANT01.AI@GMAIL.COM**

# **MINING E CARATTERISTICHE DEL NETWORK**

**Lezione 3 - 12/05/2021**

**1**

**INTRODUZIONE AL MINING**

**2**

**STRUMENTI DI LAVORO DEL  
MINATORE**

**3**

**EQUAZIONE DEL MINATORE**

**4**

**IL MINING È PROFITTEVOLE?**



# 1 Introduzione al mining

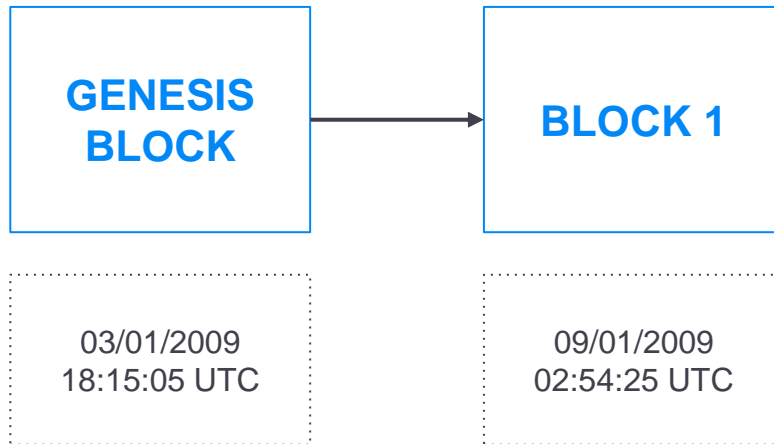
“Una versione puramente **peer-to-peer di denaro elettronico** consentirebbe ai **pagamenti online** di essere inviati da una persona all'altra **senza passare attraverso un'istituzione finanziaria**. Le firme digitali forniscono parte della soluzione, ma i principali benefici si perdono se, per impedire la doppia spesa (**double-spending**), è ancora necessario un terzo soggetto di fiducia. Noi proponiamo una soluzione al problema della doppia spesa usando un network peer-to-peer. Il **network** marca in maniera temporale le transazioni attraverso un codice Hash e le posiziona in una **catena continua** di prove di lavoro (**proof-of-work**) basate su funzioni Hash, formando un registro che non può essere modificato senza rifare la prova di lavoro stessa. La **catena più lunga** serve non soltanto come prova della sequenza di eventi di cui è testimone, ma anche come prova che proviene dal più grande pool di potenza CPU. Fintanto che la maggioranza della potenza CPU è controllata dai **nodi** che non cooperano ad attaccare il network, questi genereranno la catena più lunga e allontaneranno eventuali aggressori. Lo stesso network richiede una struttura minima. I messaggi vengono trasmessi nel miglior modo possibile ed i nodi possono sganciarsi e ricollegarsi al network a propria volontà, accettando la catena di lavoro più lunga come prova di quanto successo, mentre erano assenti.”

La blockchain (= catena di blocchi) è composta da blocchi collegati ed ordinati cronologicamente.

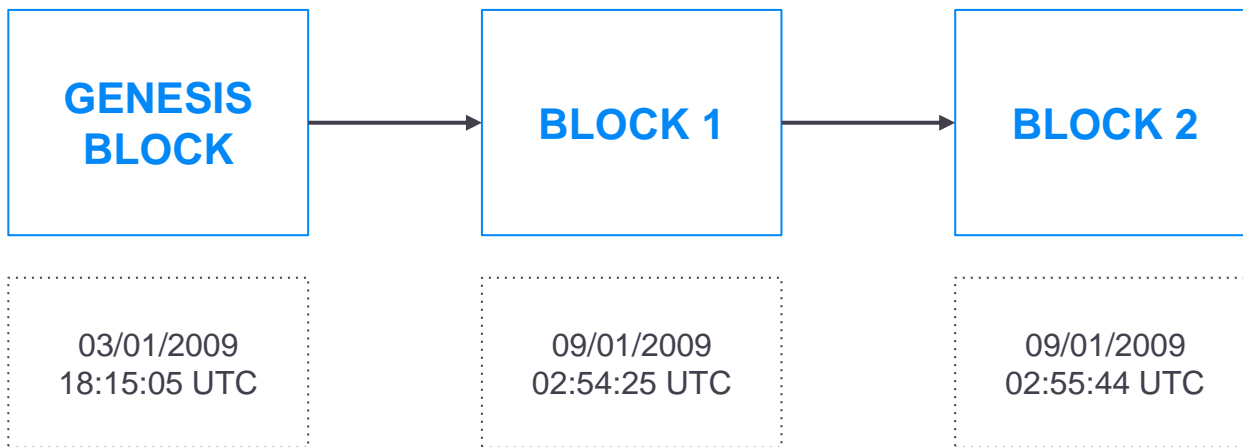
**GENESIS  
BLOCK**

03/01/2009  
18:15:05 UTC

La blockchain (= catena di blocchi) è composta da blocchi collegati ed ordinati cronologicamente.

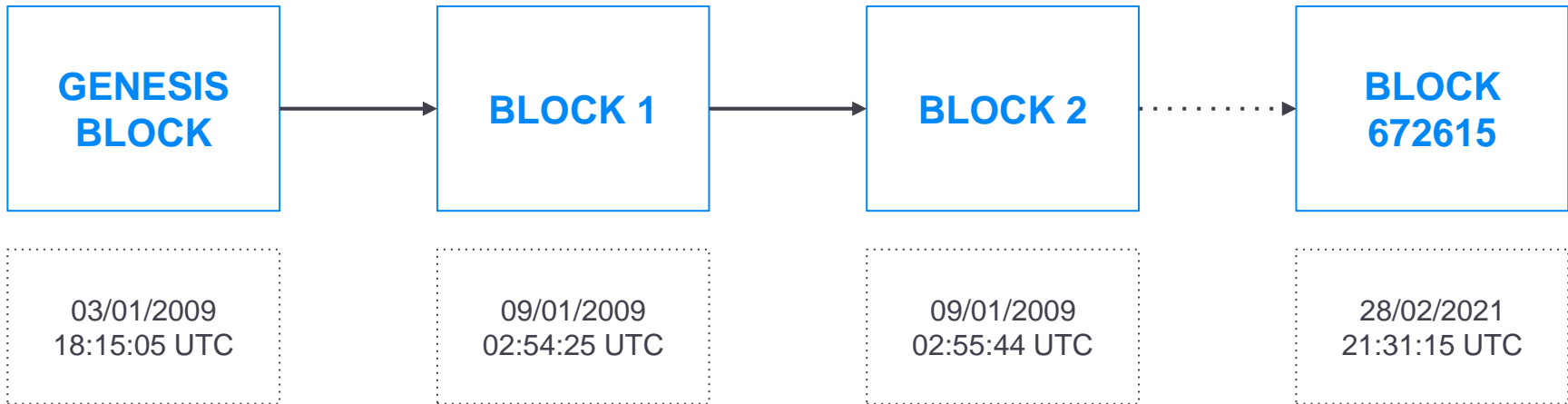


La blockchain (= catena di blocchi) è composta da blocchi collegati ed ordinati cronologicamente.

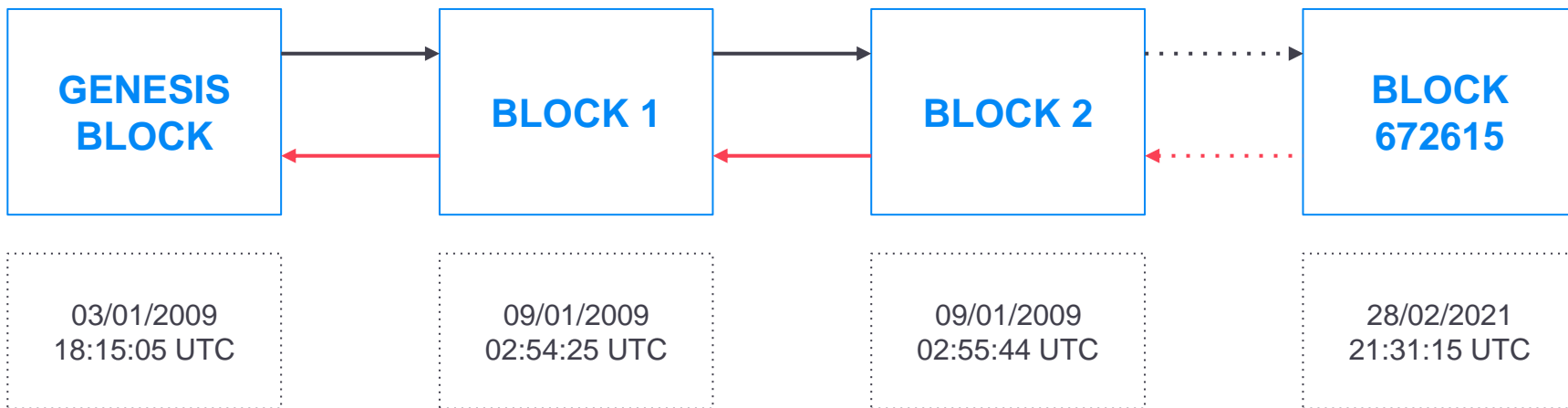




La blockchain (= catena di blocchi) è composta da blocchi collegati ed ordinati cronologicamente.



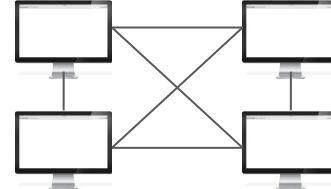
La blockchain è **bidirezionale**: dal primo blocco è possibile salire fino a quello più recente e viceversa.



Un sistema informatico è un sistema in grado di effettuare delle elaborazioni su una serie di dati con lo scopo di fornire dei risultati in modo automatico.



**Un singolo computer**

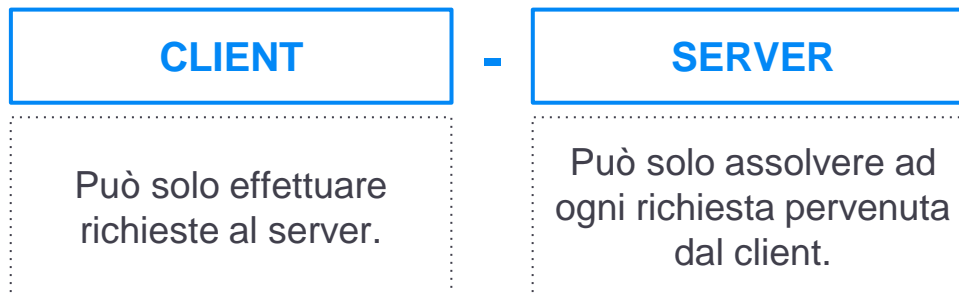


**Un insieme di computer interconnessi**



**ARCHITETTURA DI UN  
SISTEMA INFORMATICO**

L'architettura più diffusa di un sistema informatico con cui si realizzano le interconnessioni tra i diversi computer è quella:



**HARDWARE**

È composto da client, server ed infrastruttura di rete.

**SOFTWARE**

È la parte logica del sistema informatico.

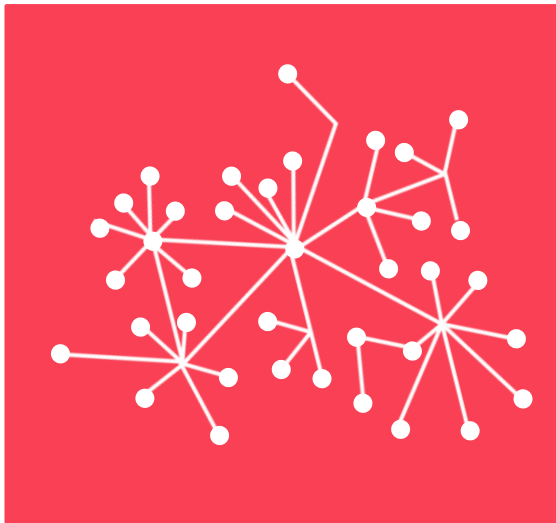
## Tipologia di sistema informatico



**CENTRALIZZATO**

- È presente un solo server centrale che assolve a tutte le richieste dei client connessi alla stessa rete.
- È un sistema che accentra su di un singolo computer sia servizi che dati da fornire ai client.
- Esempio: rete di una piccola azienda in cui i computer dei dipendenti sono collegati ad un unico server centrale.

## Tipologia di sistema informatico



**DECENTRALIZZATO**

- È un sistema che presenta molti server collegati tra loro ognuno dei quali fornisce particolari servizi o dati.
- Un singolo server non è autonomo, ma necessita della collaborazione di tutti o di alcuni degli altri server.
- Più server collaborano per fornire la risposta ai client.
- Esempio: posta elettronica.

## Tipologia di sistema informatico



**DISTRIBUITO**

- Ogni server è autonomo ed autosufficiente e non esiste un server dedicato a particolari servizi.
- Tutti i server della rete forniscono un medesimo servizio e contengono le medesime informazioni.
- I server sono connessi tra loro attraverso un software (middleware) che permette il coordinamento delle attività e di conseguenza il client ha una percezione di un unico sistema informatico integrato.
- È noto anche come sistema di rete peer to peer (P2P).
- Esempio: BitTorrent.

## LEDGER

Libro mastro

Registro contabile

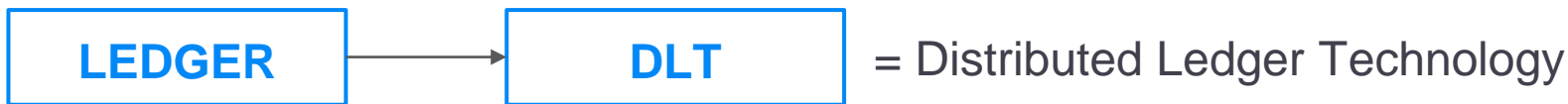
Fino a non pochi decenni fa, i ledger erano esclusivamente fisici e di conseguenza caratterizzati da una struttura centralizzata.

- Qualcuno inseriva i dati
- Qualcuno gestiva i sistemi
- Qualcuno estraeva i dati

Negli anni della digitalizzazione i processi non sono radicalmente cambiati, così come la struttura dei dati che è sempre stata concepita in modo analogico. Quello che invece si è verificato è stata una velocizzazione di alcuni passaggi.



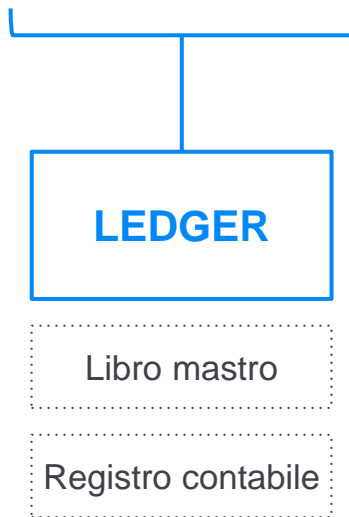
È con l'avvento della blockchain che si è avuta un'accelerazione significativa nello sviluppo dei ledger:



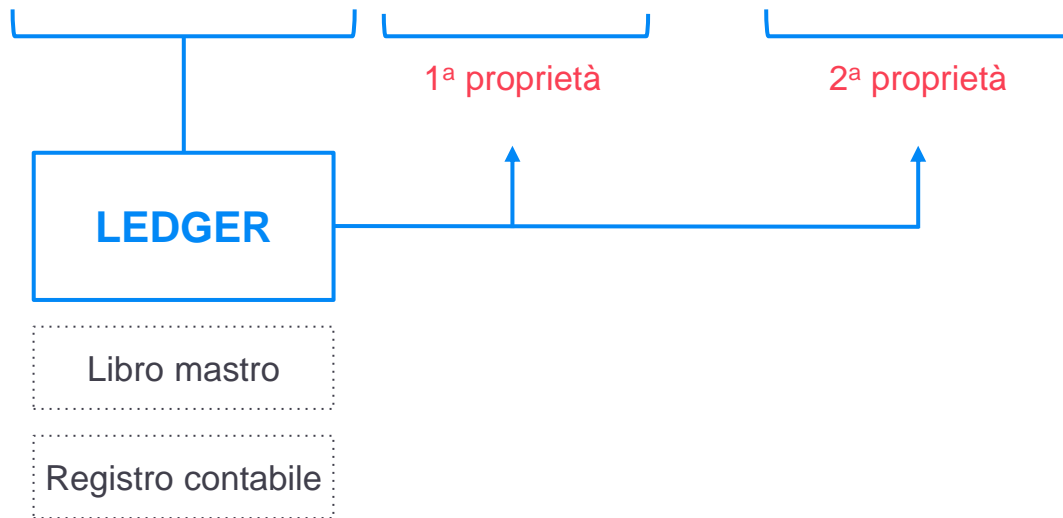
È un sistema distribuito che attraverso un meccanismo di consenso coinvolge tutti i nodi della rete per garantire univocità, persistenza e condivisione dei dati presenti nel ledger.

La blockchain è una struttura dati distribuita ed immutabile.

La blockchain è una struttura dati distribuita ed immutabile.



La blockchain è una struttura dati **distribuita** ed **immutabile**.



In sintesi la struttura elementare della blockchain è formata da:

**DATABASE  
DISTRIBUITO**

**1**

**CONSENSO**

**2**

**PREMIO DI  
CONVALIDA**

**3**

## 1 - Database distribuito



1

### PERMISSIONED LEDGER

- È un registro in cui per l'accesso è necessario registrarsi ed identificarsi e di conseguenza è prevista una sorta di ente centrale che abiliti gli accessi.
- Il consenso è semplice: ad esempio nel caso di aggiunta di una nuova transazione, si verificata la validità e si vota a maggioranza.

2

### PERMISSIONLESS LEDGER



- È un registro in cui chiunque può accedere senza autorizzazione.
- Il consenso è complesso (Proof of Work, Proof of Stake...) per evitare che un soggetto malevolo possa influenzare il processo di modifica del registro.

## 2 - Consenso



Per funzionare autonomamente, un sistema distribuito richiede che gli interessi dei vari attori siano allineati ed in particolare che siano d'accordo su due principali elementi:

1. Regole del protocollo
2. Storia delle transazioni



### **ALGORITMO DI CONSENSO**

È un meccanismo mediante il quale si garantisce che tutte le regole di un protocollo distribuito siano rispettate.

### PRINCIPALI ALGORITMI DI CONSENSO



#### **Proof of Work (PoW)**

i minatori risolvono un problema matematico per poter aggiungere blocchi alla blockchain Questa attività richiede molto tempo ed energia.



#### **Proof of Stake (PoS)**

I partecipanti che possiedono una partecipazione significativa sono selezionati in modo pseudocasuale per coniare i blocchi e aggiungerli alla blockchain.



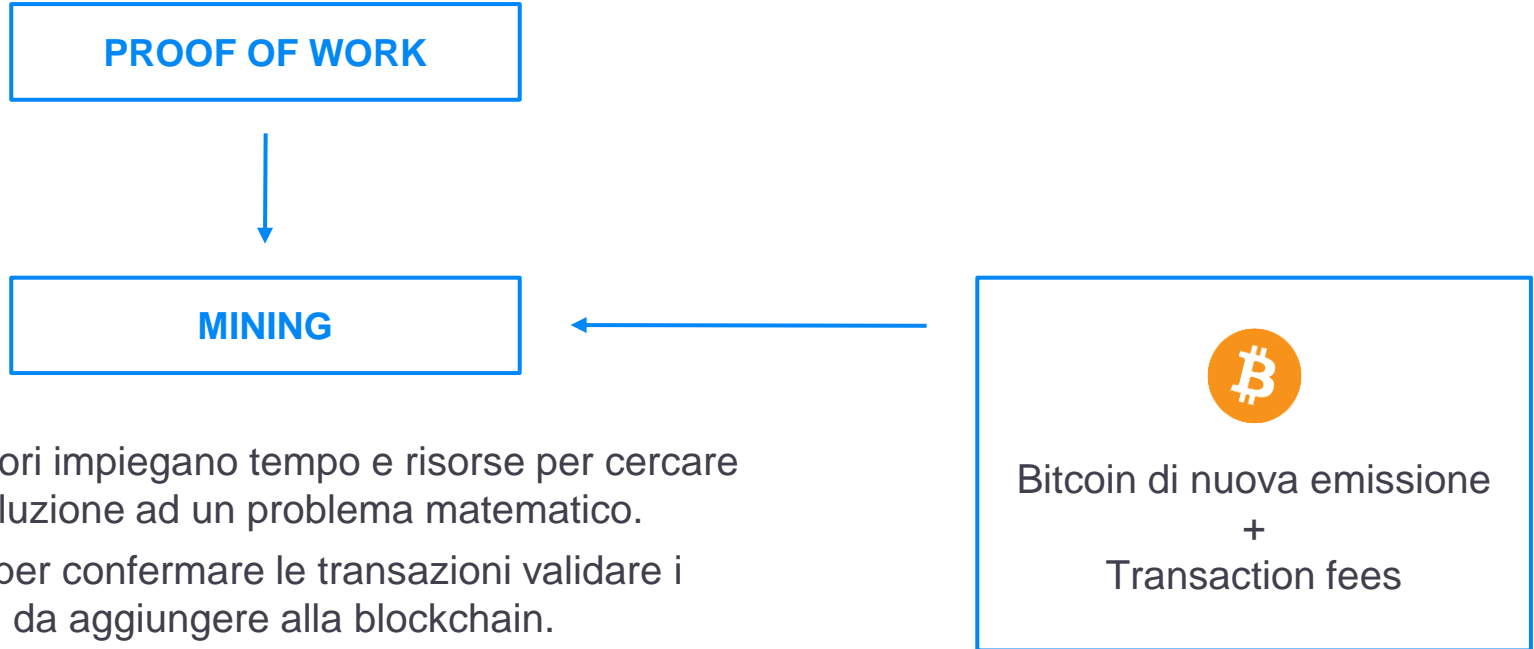
## 2 - Consenso



### ALTRI ALGORITMI DI CONSENSO

Proof of Importance (Pol)	Proof of Activity (PoA)	Delegated Proof of Stake (DPoS)
Proof of Capacity (PoC)	Simplified Byzantine Fault Tolerance (SBFT)	Leased Proof of Stake (LPoS)
Proof of Burn (PoB)	Delegated Byzantine Fault Tolerance (DBFT)	Proof of Elapsed Time (PoET)
Proof of Weight (PoWeight)	Directed Acyclic Graphs (DAG)	Practical Byzantine Fault Tolerance (PBFT)

## 3- Premio di convalida



- I minatori impiegano tempo e risorse per cercare una soluzione ad un problema matematico.
- Serve per confermare le transazioni validare i blocchi da aggiungere alla blockchain.

## Dall'oro al bitcoin



### **Klondike Gold Rush**

1896 - 1899



### **Bitcoin Rush?**

2009 - ?

## Offerta di moneta

**21 M**



**MINING**



**EXCHANGE**



**BUSINESS**

## Il mining al servizio del network



A cosa serve il mining?

1. Distribuisce la massa monetaria
2. Raccoglie le transazioni
3. Verifica le transazioni
4. Convalida i blocchi
5. Aggiunge i blocchi alla blockchain

L'attività di mining permette di verificare, confermare e registrare tutte le transazioni in bitcoin, ma al tempo stesso garantisce che la massa monetaria venga creata e distribuita sotto forma di incentivo.

## Definizione di mining



L'attività di mining di bitcoin è una competizione in cui ogni partecipante ha l'obiettivo di essere il primo minatore a trovare la risposta ad un problema matematico che risolve il blocco attuale.



### Esempio

- Si applica la funzione SHA-256 al messaggio “compra cento bitcoin”, ottenendo il seguente hash:

5335c303e0981e00317ec53582de99d9495df45cf7f2916d0e6931eee666849a

- Si aggiunge al messaggio un valore finale, che prende il nome di “nonce”, e si ricalcola la funzione SHA-256, ottenendo un nuovo hash.
- Vince chi per primo trova un nuovo hash inferiore o uguale ad un certo target, il quale deve avere come valore iniziale un certo numero di zeri. Nel nostro esempio il target è pari a un solo valore uguale a zero.

La strategia che adottiamo è quella di partire da un nonce pari a 1 che incrementeremo fino a quando non troveremo un hash che soddisfi il target.

In questo processo di calcolo è richiesta velocità, poiché vince solo il primo giocatore che riesce a trovare la soluzione.

Input	Nonce	Hash
compra cento bitcoin1	1	64dd594ceae0d5f...
compra cento bitcoin2	2	64dd594ceae0d5f...
...	...	...
compra cento bitcoin13	13	64dd594ceae0d5f...



- È bene precisare che la soluzione non è univoca, applicando infatti un nonce uguale a 1016 si ottiene comunque un hash che inizia con zero:

Input	Nonce	Hash
compra cento bitcoin1016	1015	0d1146506ce8132...

- È quindi evidente che la velocità nel ricercare una delle possibili soluzioni è l'aspetto peculiare dell'attività di mining.
- Questo perché il mining non è altro che un'operazione di forza bruta (brute force), in cui si procede per tentativi applicando tutte le possibili combinazioni, fino a quando un minatore non trova la soluzione.

## L'algoritmo di mining



- Il problema che deve risolvere il network Bitcoin è ovviamente più complesso, non tanto da un punto di vista logico ma quanto dalla mole di calcoli da svolgere.
- I passaggi svolti dall'algoritmo di mining sono sostanzialmente identici a quelli fissati nel nostro gioco:

Prende l'header(1) del blocco come input.

Cambia il Nonce.

Applica due volte la funzione Hash (SHA-256).

Verifica che l'Hash è inferiore al target ed in caso affermativo si riparte dal punto 1, altrimenti dal punto 2.

Il target è un numero estremamente grande, a 256 bit, che può rappresentare 2256 differenti informazioni ed è tipicamente espresso in scala esadecimale.

Ad esempio il 03/04/2014 il target era il seguente:

In scala esadecimale:

0000000000000000DB99000

In scala decimale:

5384518863803604621895699676581808210968416076987222720512

Il valore del Target si modifica in base alla differenza percentuale tra tempo effettivo e tempo teorico necessario per minare 2016 blocchi.

## Tempo teorico



Il protocollo Bitcoin prevede che il tempo teorico necessario per minare 1 blocco sia pari a 10 minuti, di conseguenza per minare 2016 blocchi sono teoricamente necessarie in teoria 2 settimane.

Tempo	N° Blocchi
10 minuti	1
1 ora	6
1 giorno	144
1 settimana	1008
2 settimane	2016

## Tempo effettivo



- I minatori sono stati veloci nel minare il blocco.
- Diminuisce il prossimo target, rendendo la successiva prova di lavoro più difficile.



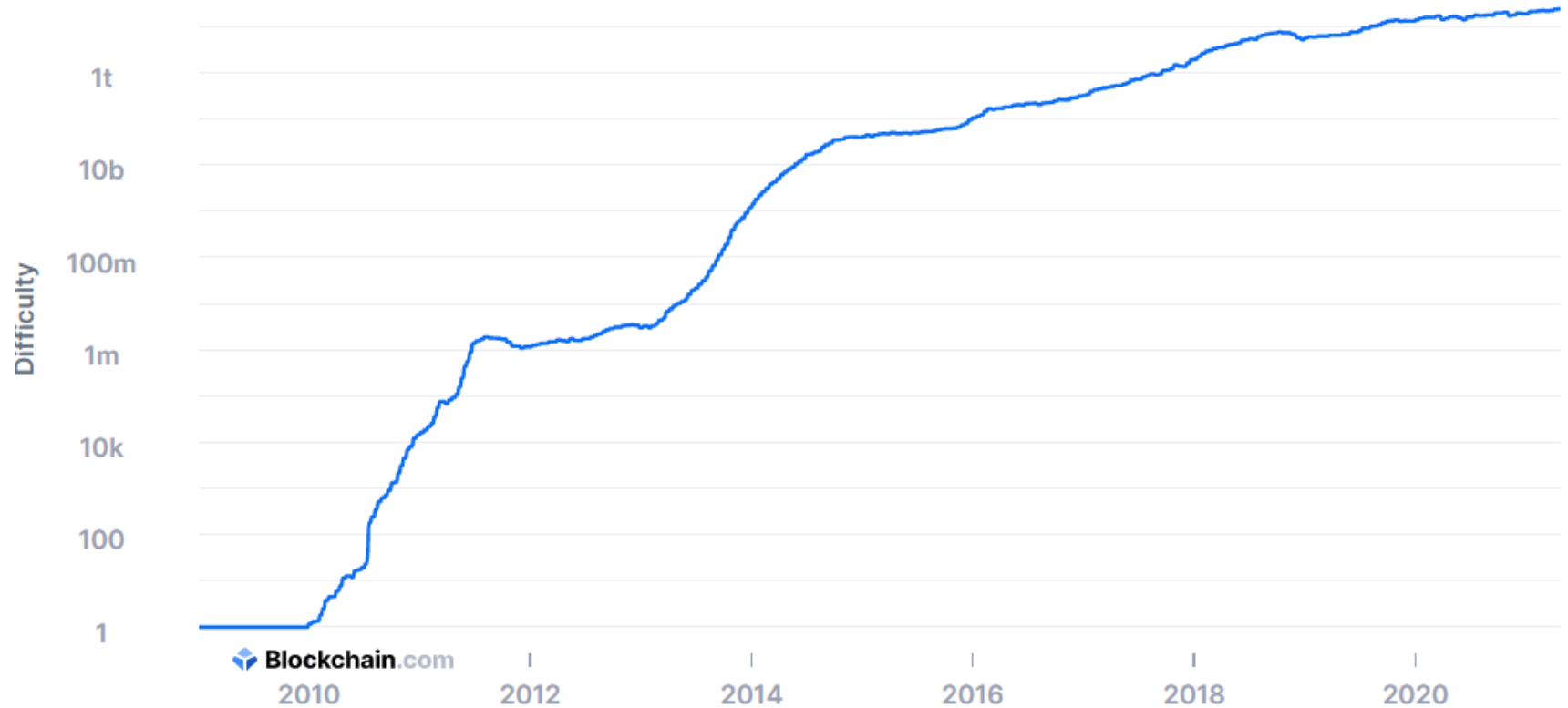
- I minatori sono stati lenti nel minare il blocco.
- Aumenta il prossimo target, rendendo la successiva prova di lavoro più facile.

- Più il target è piccolo e più è difficile ricercare una soluzione che lo possa soddisfare.
- L'incremento o il decremento del nuovo target non può essere superiore o inferiore di un fattore 4 rispetto al target attuale.

La difficoltà è la misura di quanto sia difficile trovare un hash inferiore al target.

- Il valore iniziale è stato fissato uguale a 1.
- Non ha un valore massimo.
- Non può mai essere inferiore a 1.
- Si aggiusta ogni 2016 blocchi ovvero ogni 2 settimane circa.
- È inversamente correlata con il Target.
- È positivamente correlata con l'Hash rate.

## Difficoltà





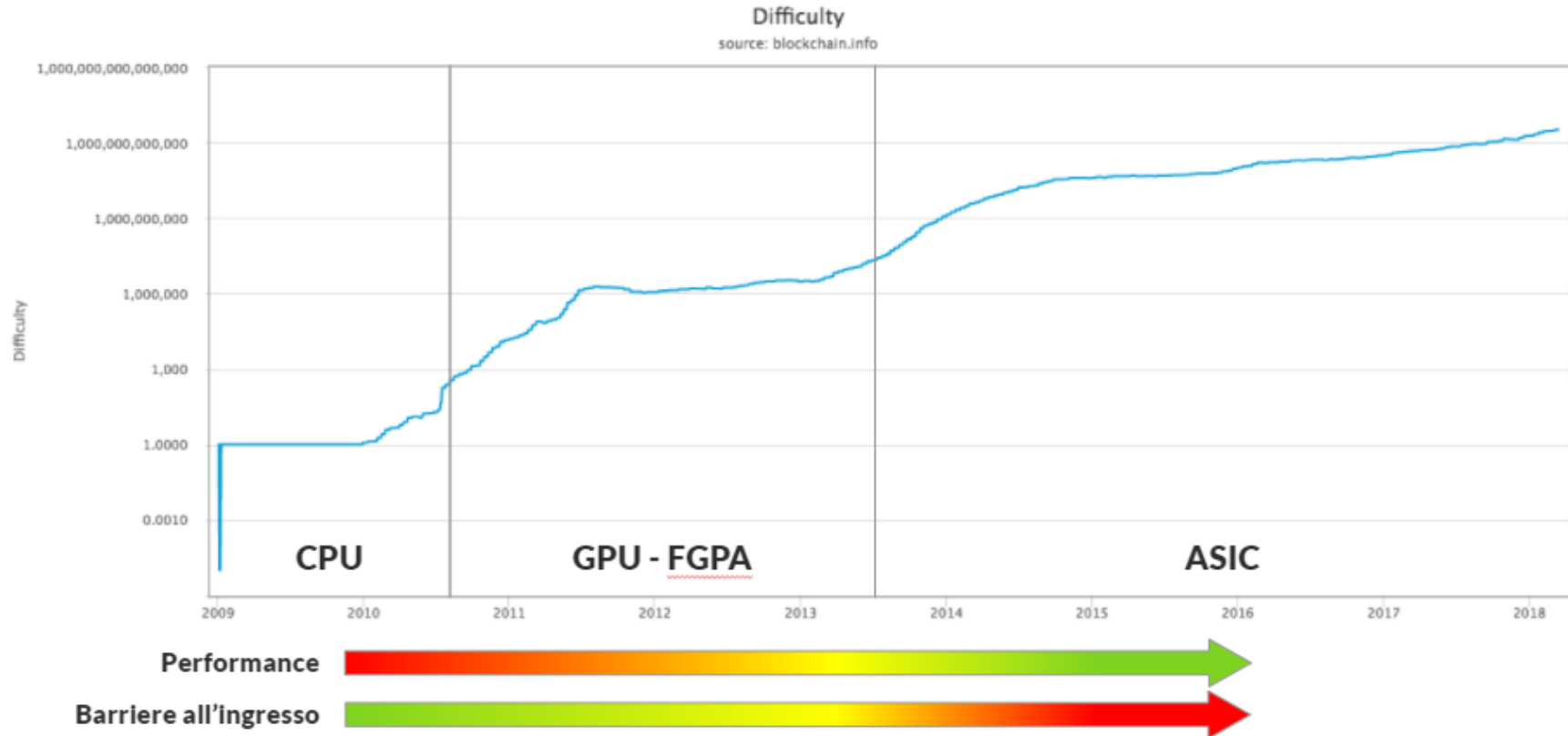
## 2 Strumenti di lavoro del minatore



## Evoluzione dell'hardware



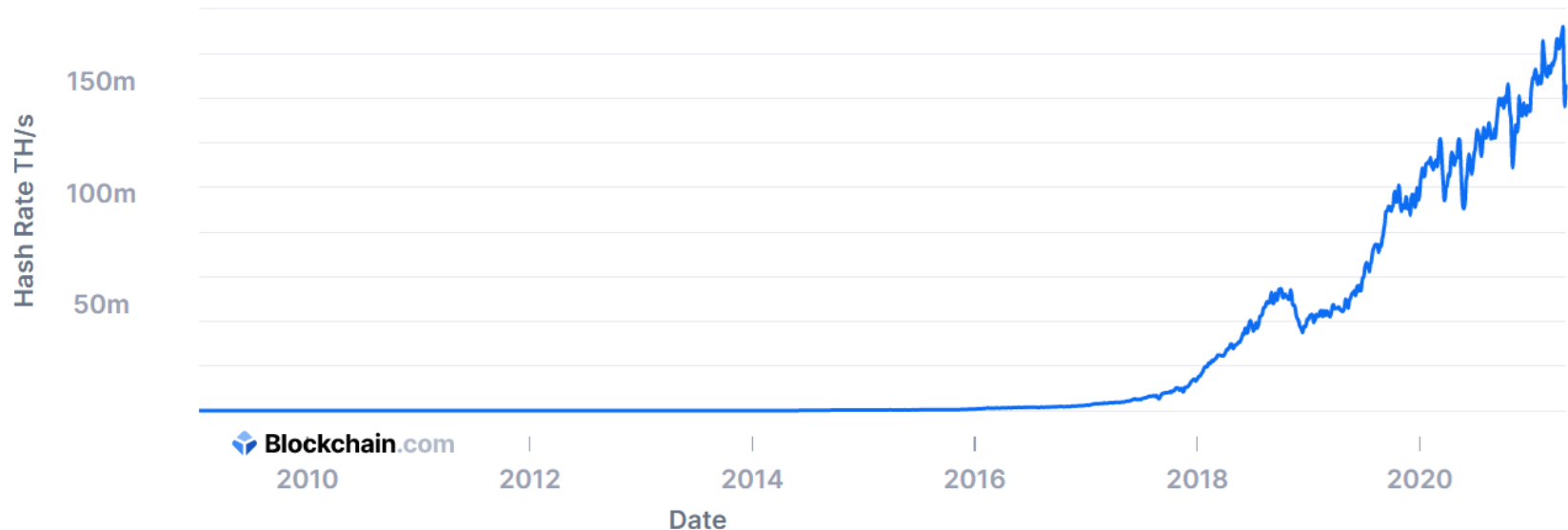
## Barriere all'entrata



## Hash rate

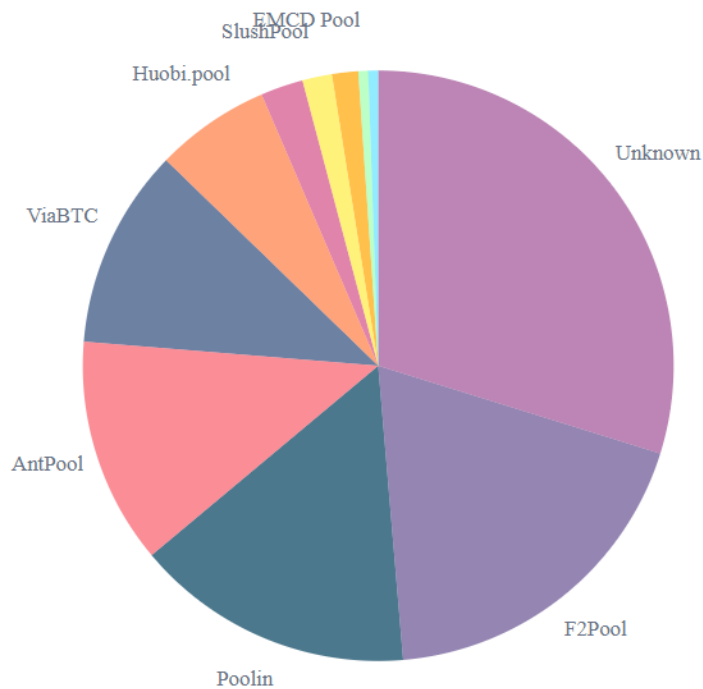


L'hash rate è la potenza computazionale complessiva in Tera-Hash al secondo (TH/s), che il network sta eseguendo.



## Mining pool

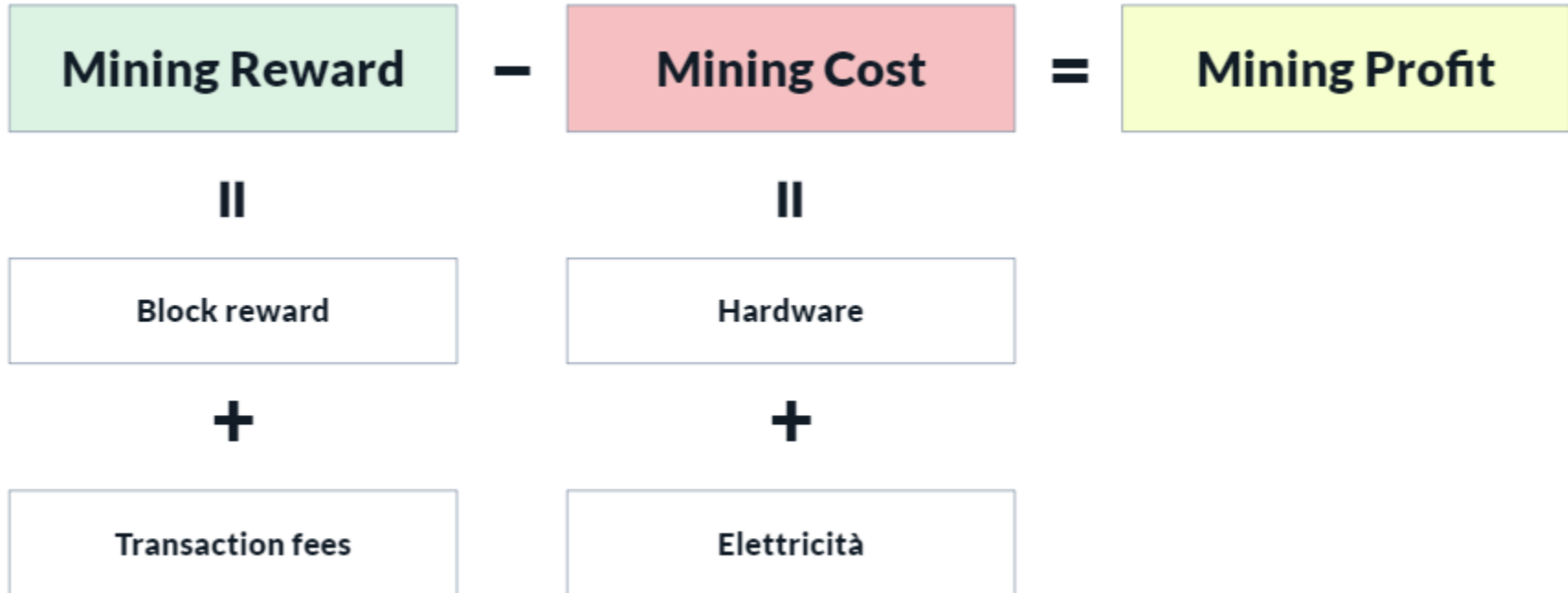
**Cos'è un pool?**





### 3 L'equazione del minatore

## Ricavi e costi





## 4 Il mining è profittevole?

## Miners Revenue (USD)



Total value of coinbase block rewards and transaction fees paid to miners.

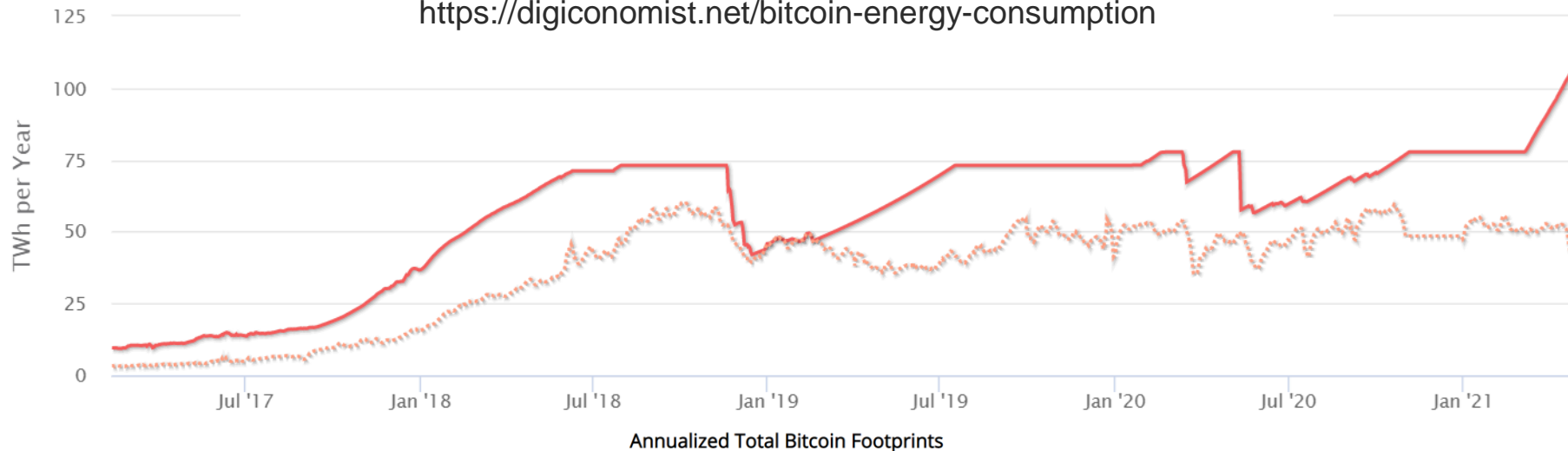




## Bitcoin Energy Consumption Index



<https://digiconomist.net/bitcoin-energy-consumption>



Carbon Footprint	Electrical Energy	Electronic Waste
50.31 Mt CO2	105.92 TWh	8.78 kt
Comparable to the carbon footprint of Hungary.	Comparable to the power consumption of Kazakhstan.	Comparable to the e-waste generation of Luxembourg.

4 # Il mining è profittevole?

[Cryptocompare.com](https://cryptocompare.com)



CryptoCompare

Coin ListTop Lists ▾Research ▾News

Q Search

Currency

BTCETHETCXMRZECDASHLTC

Calculated for  
1 BTC = \$ 53,668.67

Hashing Power

40TH/s ▾

Power consumption (w)

1500

Cost per KWh (\$)

0.12

PROFIT RATIO PER DAY

164%

PROFIT PER MONTH

\$ 213.39

Profit per day	Mined/day	Power cost/Day
<b>\$ 7.11</b> Pool Fee \$ 0.1155	<b>฿ 0.0002152</b>	<b>\$ 4.32</b>
Day		
Profit per week	Mined/week	Power cost/Week
<b>\$ 49.79</b> Pool Fee \$ 0.8084	<b>฿ 0.001506</b>	<b>\$ 30.24</b>
Week		
Profit per month	Mined/month	Power cost/Month
<b>\$ 213.39</b> Pool Fee \$ 3.46	<b>฿ 0.006455</b>	<b>\$ 129.60</b>
Month		
Profit per year	Mined/year	Power cost/Year
<b>\$ 2,596.20</b> Pool Fee \$ 42.15	<b>฿ 0.07854</b>	<b>\$ 1,576.80</b>
Year		

L'offerta di Bitcoin dipende da tre elementi:

**EMISSIONE  
LIMITATA**

**21 milioni**

**HALVING**

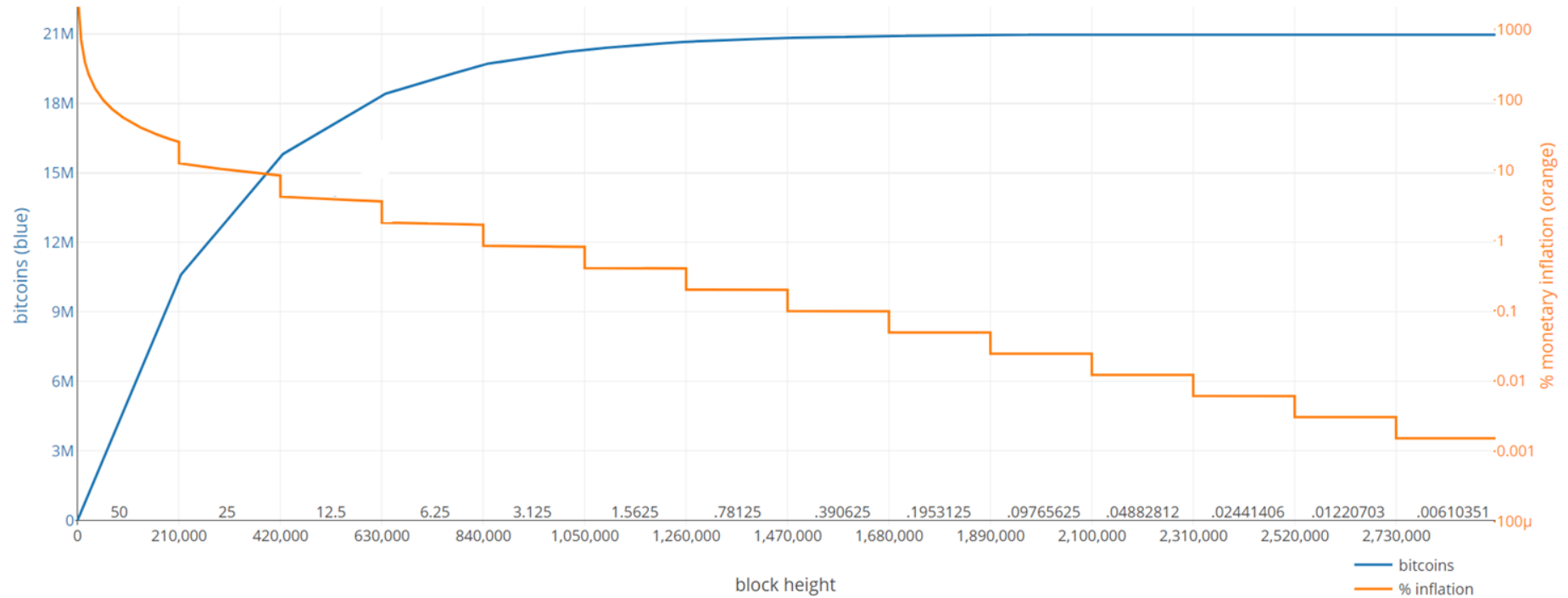
**Dimezzamento della  
remunerazione ogni 210.000  
blocchi generati**

**DIFFICOLTÀ  
MINING**

**Aumento o diminuzione ogni  
2016 blocchi generati**

4 # Il mining è profittevole?

## Inflation Rate



Dati aggiornati al 16 Aprile 2021

## Post halving

### Bitcoin After The 3<sup>rd</sup> Halving

March 30, 2021

Source: original ohlc data from Coinmarketcap

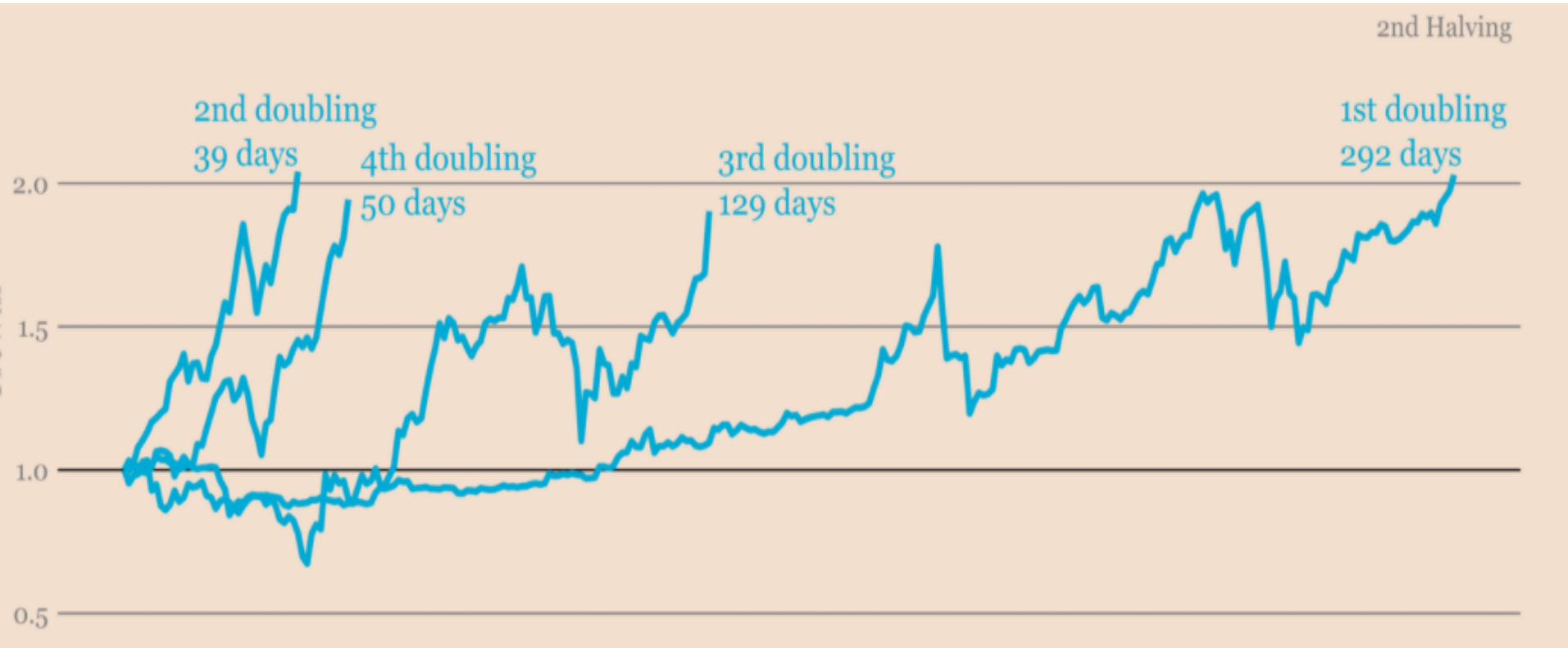
By: @ecoinometrics, ecoinometrics.substack.com



## Post halving



## Post halving



## Post halving





## Post halving





**Disponibili su Amazon, Hoepli e nelle principali librerie**



QUANT-OI

***Grazie... e buon trading***

**QUANT01.AI@GMAIL.COM**