# La matematica dei minatori della blockchain

Jacopo De Tullio
Centro PRISTEM, Università commerciale L. Bocconi

Luglio 2018

**Sommario**

Blockchain e bitcoin sono termini che ormai sovente capita di leggere e sentire e spesso si fa confusione sul loro significato. In questo articolo ci soffermiamo sul funzionamento della tecnologia blockchain (che promettono essere rivoluzionaria) e in particolare il ruolo dei "minatori"che certificano le transazioni della catena attraverso un "problema matematico".

La blockchain, che possiamo tradurre brutalmente come catena di blocchi, è una tecnologia complessa e pervasiva, diventata famosa per il fenomeno finanziario legato ai bitcoin ma capace di andare ben oltre. Con la promessa di rivoluzionare qualunque ambito della nostra vita, dalla burocrazia alle relazioni interpersonali, dalla musica al settore energetico, in molti l'hanno definita "il nuovo internet" per la sua caratteristica di configurarsi come un registro di transazioni che le rende verificabili in ogni passaggio.

Le origini della "catena" risalgono al 2009 con la pubblicazione di un paper da parte di Satoshi Nakamoto, pseudonimo dietro cui si nascondono uno o più informatici la cui identità resta ancora segreta, che ha creato la criptomoneta bitcoin basandosi sulla tecnologia blockchain. Secondo le intenzioni di Satoshi "*una versione puramente peer-to-peer di denaro elettronico permetterebbe di spedire direttamente pagamenti online da un'entità a un'altra senza passare tramite un'istituzione finanziaria*". Insomma l'abolizione degli intermediari (le banche che certificano) che aumentano i costi di transazione, permettendo lo svolgimento di operazione criptate completamente anonime e archiviando tutte le transazioni in un registro pubblico distribuito in rete. Una visione forse un po' troppo idealista se si considera che tutte le grandi banche d'affari si sono unite in un progetto della svizzera UBS per creare una nuova forma di denaro digitale.

Se volessimo definire (informalmente) la blockchain, potremmo dire che è una sorta di libro mastro pubblico e decentralizzato che, sfruttando la

tecnologia *peer-to-peer*, valida le transazioni tra due parti in modo sicuro, verificabile e permanente. Le tecnologie alla base del funzionamento della blockchain sono tutte soluzioni informatiche già note e vanno dal *file sharing* alla crittografia, in particolare quelle *a chiave pubblica e privata* (in cui chiunque può cifrare un messaggio usando la chiave pubblica del destinatario, ma tale messaggio può essere decifrato solo con la chiave privata del destinatario) e *hash* (che data una stringa di una qualsiasi lunghezza ne produce una di una lunghezza definita da cui non è possibile risalire alla stringa originale), ma la rivoluzione è stata la loro unione nel formare quella che appunto viene chiamata "catena di blocchi".

Ma come funziona questo insieme di algoritmi matematici che lavorano su internet? La blockchain è un paradigma su cui si basano molti sofware scaricabili da internet e installabili sui propri computer. Una volta installati, si diventa un "nodo" collegato a tutti gli altri già in rete. Ciascun nodo è anonimo e univocamente identificato da un codice. Tra i diversi nodi possono avvenire transazioni e scambi di dati di diversa natura tramite i "blocchi" che registrano le operazioni. Quello che rende così particolare la blockchain sono due aspetti:

- una transazione non è certificata da un solo ente terzo ma, affinché abbia successo, deve essere approvata da almeno la maggioranza assoluta di tutti i nodi della rete;
- dopo che una transazione è avvenuta, lo storico e tutte le informazioni a essa collegate vengono salvate e conservate su ogni singolo blocco della catena che è pubblico e condiviso da tutti i nodi;
- quando c'è necessità di modificare un'informazione, occorre aprire un nuovo blocco, dichiararlo e questo deve essere approvato.

Come già detto per attivare un nuovo blocco alla catena è necessario il controllo delle transazioni contenute nel blocco stesso da parte dei nodi. Questo passaggio si risolve attraverso un complesso problema matematico che richiede un cospicuo impegno computazionale in termini di potenza e di capacità elaborativa.

Quei nodi che procedono alla ricerca della soluzione sono detti "minatori" e il primo che riesce a risolvere il problema viene premiato con una quota di bitcoin generati proprio grazie a questo processo. Inizialmente la ricompensa era di 50 bitcoin per blocco, ma se tale ricompensa rimanesse sempre la stessa, la moneta in circolazione aumenterebbe infinitamente nel tempo e si verificherebbe una continua inflazione. Per evitare questo problema il sistema è programmato per generare moneta secondo una serie geometrica fino a che il

numero totale di bitcoin non giunge a 21 milioni. Il sistema bitcoin dimezza la ricompensa ogni 210000 blocchi minati (ovvero ogni 4 anni circa); così facendo si ottiene:

$$210000 \cdot 50 \cdot \sum_{n=0}^{+\infty} \left(\frac{1}{2}\right)^n = 21000000$$

Il quesito matematico che i minatori devono risolvere viene chiamato *Proof of Work* e non si risolve ricorrendo alla logica, bensì è un problema crittografico che richiede un enorme numero di tentativi e si risolve con il metodo di forza bruta (ovvero un algoritmo che consiste nel provare tutte le soluzioni teoricamente possibili fino a trovare quella adatta) che rende impossibile prevedere quale utente troverà la soluzione prima degli altri a meno di non disporre di una potenza computazionale rilevante.

Ogni blocco è diviso in due parti: l'header (di lunghezza predefinita) e i dati delle transazioni. Uno dei campi all'interno dell'header è detto "nonce" (acronimo di *number used once*) rappresentato da una sequenza di 32 bit che devono essere riempiti in maniera casuale proprio dai minatori: se la stringa output è inferiore a un valore soglia stabilito (detto *target*), allora il blocco è valido.
Più piccolo è tale valore e più difficile e costosa è l'operazione di generazione di un nuovo blocco.
Formalmente, data una funzione hash crittografica $H$, la soluzione del problema si ottiene trovando un valore $x$ tale che $H(x) \leq T$ dove $T$ è il target.
Questo valore è stabilito dal sistema per regolare automaticamente la velocità di creazione di un blocco, viene modificato ogni 2016 blocchi creati (circa due settimane) in modo che occorra una media di 10 minuti per incatenarne uno nuovo.

Per capire meglio facciamo un esempio pratico. Il sistema bitcoin sfrutta la funzione $H$ hash SHA-256 che, data una stringa di lunghezza qualsiasi, restituisce una stringa di 64 caratteri esadecimali (Fig. 1).

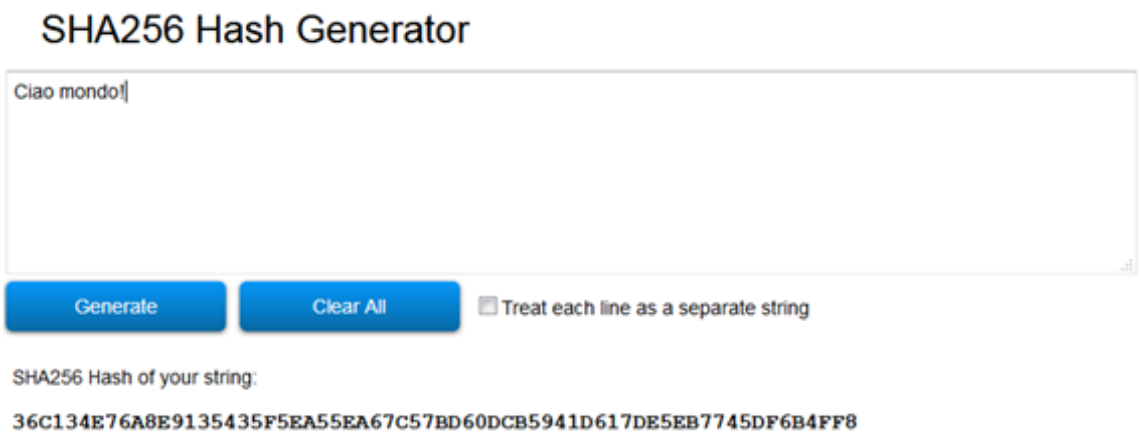


Fig. 1 Stringa generata dal messaggio "Ciao mondo!" con un generatore SHA256

Bastano anche piccole modifiche al messaggio di partenza per ottenere una stringa completamente diversa (Fig. 2).


Fig. 2 Stringa generata dal messaggio "Ciao Mondo!" con un generatore SHA256

Per risolvere il *Proof of Work* i minatori devono completare il messaggio in maniera tale che la stringa risultante riporti come prime cifre un valore minore del target $T$ dunque, essendo $T$ un numero molto piccolo, i primi caratteri del codice devono essere una (lunga) sequenza di zeri.
Affinché il valore target rispetti il tempo di ricerca di 10 minuti circa è necessario ricorrere a qualche calcolo. Poiché ogni valore hash è un numero di 256 bit, ci sono $2^{256}$ possibili valori hash e la probabilità di trovare un valore hash minore di $T$ risulta $p(T) = \frac{T}{2^{256}}$ e il numero di prove necessarie a trovarlo $N(T) = \frac{1}{p(T)} = \frac{2^{256}}{T}$.

Sia $t_m$ il tempo di generazione degli ultimi 2016 blocchi, allora i minatori hanno lavorato a una velocità $v_m = \frac{N(T)}{t_m}$. Il nuovo valore target $T'$ deve essere regolato affinché il tempo di creazione di un blocco sia pari a 600 secondi, quindi $600s = \frac{N(T')}{v_m} = t_m \cdot \frac{T}{T'}$, da cui $T' = T \cdot \frac{t_m}{600s}$.
Questo processo rende anche impossibili tentativi di corruzione, truffa o furto. Infatti se si volesse "truccare" la blockchain non basta intervenire su un singolo blocco per rendere questa modifica valida, bisogna intervenire su tutti i blocchi della catena e per farlo si stima che sarebbe necessaria la potenza di un computer 6000 volte più potente dei 500 super computer più veloci al mondo.

Ma le applicazioni della blockchain non si limitano ai bitcoin e negli ultimi anni sono stati avviati circa 80mila progetti basati su questa tecnologia (anche se il 92% di questi è fallito nei primi dodici mesi) che stanno sperimentando banche, imprese e governi; al momento la capitalizzazione di tutte le blockchain esistenti al mondo è di 250 miliardi di dollari ed è in continua crescita.
Bitnation sta progettando una carta d'identità virtuale d'emergenza per migranti che potrebbe provare crittograficamente l'esistenza di una persona e le sue relazioni familiari registrate su una blockchain pubblica. Il World Food Programme delle Nazioni Unite ne ha riconosciuto il potenziale per aiutare le popolazioni che soffrono la fame, meno costi di transazioni consentirebbero che le offerte arrivassero non decurtate dai costi di commissione. La compagna marittima danese Maersk la sta sperimentando con IBM per migliorare efficienza e sicurezza del trasporto mercantile velocizzando la trasmissione delle innumerevoli autorizzazioni necessarie per trasportare la merce da un porto all'altro. Nell'agroalimentare permette di conoscere la storia di ogni prodotto, dalla nascita al consumatore finale. Le cartelle cliniche potrebbero essere condivise fra i medici in qualunque parte del mondo, attraverso un database che consente di conoscere l'intera storia clinica di un paziente. E, infine, la blockchain permetterebbe agli artisti di controllare la distribuzione della propria opera e il relativo pagamento dei diritti di riproduzione.

# Riferimenti bibliografici


[1] B. Bertani, "La crittografia nel sistema di moneta digitale Bitcoin", Tesi di Laurea in Crittografia, Università di Bologna, a.a. 2013/2014.

[2] "Blockchain a Technical Primer for 2018", *tranquilityhalo.com* (consultato 10/7/2018).