## Analisi tecnologia blockchain

## Abstract

Una blockchain è essenzialmente un database decentralizzato, distribuito pubblicamente contiene tutte le transazioni o eventi digitali che sono stati eseguiti e condivisi tra le sue parti partecipanti. Ogni pacchetto di dati al suo interno viene definito blocco.

La rete blockchain si occupa di certificare l’integrità e la sicurezza del sistema complessivo tramite differenti tecniche di crittografiche, per esempio effettuare un hash sul blocco stesso ed inserire una referenza al suo precedente.

I vari blocchi possono essere salvati in differenti catene, oltre alla principale è infatti possibile creare dei rami esterni e parzialmente indipendenti; la catena più lunga è definita determinante in quanto possiede la maggior parte di nodi attivi. Finché quest’ultima non viene attaccata non esistono virtualmente metodi per prendere controllo della rete, inoltre, i nodi possono unirsi e abbandonare la rete a proprio piacimento, a patto che al loro rientro rispettino la catena più lunga creatasi durante la loro mancanza.

Ogni transazione nel registro pubblico è verificata dal consenso di una maggioranza dei partecipanti al sistema, per la precisione 50%+1, ed una volta confermata le informazioni non possono mai essere cancellate o modificate.

Per usare un'analogia di base, è facile rubare una caramella all’interno di un contenitore tenuto in un armadio ma risulta molto difficile se esposto in un mercato osservato da migliaia di persone.

## Introduzione

L'attuale economia digitale si basa sulla dipendenza da una certa autorità attendibile.

Le nostre transazioni online si basano sulla fiducia di qualcuno/qualcosa, può essere la banca che ci offre il servizio di e-banking o il nostro ISP che ci offre un servizio internet per casa e/o telefono.  
In entrambi i casi ci affidiamo ad una terza entità per la sicurezza e la privacy delle nostre informazioni digitali, queste fonti di terze parti possono essere violate, manipolate o compromesse.

La tecnologia blockchain è nata per prevenire questi problemi legati alle terze persone.

## Algoritmi di consenso, POW (Proof of Work) vs POS (Proof of Stake)

Questi sono i 2 principali algoritmi tramite i quali blockchain opera e sono tra i fattori decisivi da considerare al momento di decidere se investire in un progetto di criptovaluta o meno, alcuni degli aspetti critici da considerare in questa scelta includono la velocità, le applicazioni, nonché gli algoritmi di consenso.

POW

Proof of Work è l’algoritmo più utilizzato e riconosciuto, molti dei capisaldi del settore lo adoperano come Bitcoin (BTC), Ethereum (ETH) e Dash (DASH).

Come minatore di criptovalute che utilizzano POW è necessario risolvere complessi problemi matematici alla ricerca della valuta virtuale, questo rende l’azione nel tempo esponenzialmente sempre più difficile. Dopo aver risolto con successo diversi calcoli per varie transazioni, le transazioni verificate vengono infine messe insieme e memorizzate in un nuovo blocco sul registro pubblico.

Punti a favore di POW

• Qui la maggior parte dei voti sono da sviluppatori, minatori e altri importanti membri della comunità, scelte congiunte.

Punti a sfavore di POW

• Spreco sia di potenza di calcolo che di elettricità nella generazione dei presupposti casuali.

POS

In seguito al fatto che l'estrazione in POW sia diventata lenta e costosa nel tempo, l’algoritmo POS è entrato in gioco. A differenza di POW che utilizza la potenza del computer, POS capitalizza sulla carenza della moneta. Si concentra di più sulla proprietà degli utenti, invece di una soluzione ad un calcolo.

L’utente deve dimostrare di essere il proprietario di un certo valore in criptovaluta, come tale ottiene dei benefici e crescite nel tempo del suo bene.

Punti a favore di POS

• Non c'è bisogno di computer avanzati a livello hardware

* L'intero processo è a basso costo elettrico

Punti a sfavore di POS

• POS offre una piattaforma che contraddice uno dei principi della tecnologia blockchain, quello di non avere un'autorità centrale, consentendo a coloro che possiedono più monete per dettare le modifiche da attuare sulla piattaforma.

• I possessori di ingenti somme di criptovaluta subiscono un aumento maggiore rispetto a chi ne possiede in quantità minore.

POA (Extra)

In questo algoritmo, gli amministratori di una rete blockchain convalidano e approvano le transazioni.  
Si tratta di una soluzione altamente centralizzata, ma anche molto efficiente, potrebbe funzionare per reti private dove i membri conoscono e si fidano uno dell'altro.

## Funzionamento

In seguito viene dimostrato insieme ad alcune immagini significative il funzionamento di una rete blockchain, per la spiegazione viene utilizzato l’algoritmo di consenso POW (Proof of Work).

 Indirizzo

Ogni utente all’interno della rete possiede un indirizzo univoco, questo viene usato per effettuare versamenti verso il proprietario.

Si tratta di una stringa alfanumerica, solitamente lunga 32 caratteri.

Chiave privata

Una chiava privata univoca viene accoppiata con ogni account utente, viene utilizzata per effettuare pagamenti verso altri indirizzi e **deve** rimanere confidenziale.