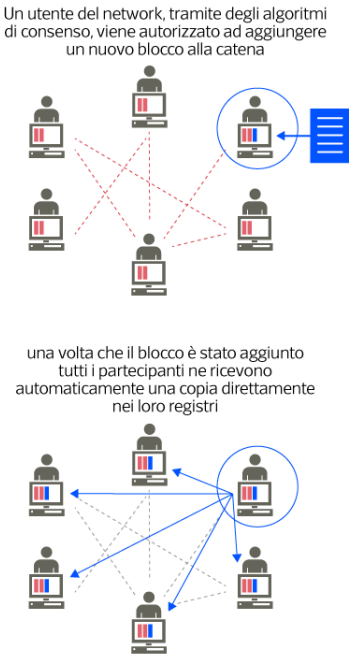
Corso di **Tecnologie per il cloud**

9. Blockchain

Si definisce **blockchain** una grande rete costituita da una serie di nodi, in cui per ciascuno viene distribuita una **catena di blocchi** contenente transazioni. Queste transazioni vengono approvate mediante un **meccanismo di consenso**.



Una blockchain può essere:

- **Pubblica:** il **meccanismo di consenso** è distribuito su **tutti** i nodi che ne fanno parte;
- **Privata:** il **meccanismo di consenso** è distribuito solo sui nodi **autorizzati**.

Solo le transazioni **autorizzate** vengono scritte nel registro e inoltre non può essere mutato. Il meccanismo è inoltre basato sulla **fiducia, responsabilità, comunità** e per ultimo, ma non per importanza, la **decentralizzazione**.

Componenti basilari della blockchain

I componenti basilari che costituiscono una blockchain sono i seguenti:

- **Nodo:** tutti i partecipanti alla blockchain;
- **Transazione:** i dati che rappresentano il tipo di scambio;
- **Blocco:** aggregatore di transazioni. Ciascun blocco che fa parte della blockchain è identificato univocamente (**collision resistance**) tramite un **hash**, calcolato tramite un'opportuna funzione. Il blocco corrente è collegato al precedente mediante un **hash pointer**;
- **Distributed Ledger:** registro pubblico in cui viene annotato lo storico delle transazioni in maniera immutabile, con la massima trasparenza. La registrazione avviene in modo ordinato, sequenziale e distribuito.

Le transazioni

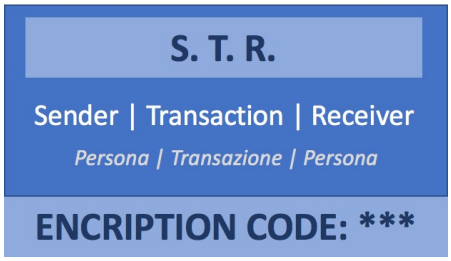
Le transazioni sono **immutabili**, ovvero, ciascuna transazione può essere modificata **solo** attraverso la **riproposizione** e la **riautorizzazione** delle stesse da parte dell'intera blockchain. Tale caratteristica garantisce e certifica la storia completa di tutti i dati e di tutte le operazioni collegate a ciascuna transazione.

La soluzione per tutte le transazioni della blockchain è affidata ai nodi che sono chiamati a vedere, controllare e approvare queste. Una volta che le transazioni vengono scritte nello storico possono essere viste da tutti i nodi.

IVAN SOLLAZZO - ANDREA PISCOPO - NICOLAS BRUNO
PROFESSORE PIERLUIGI GALLO - INGEGNERIA CIBERNETICA
UNIVERSITA' DEGLI STUDI DI PALERMO

I componenti di una transazione

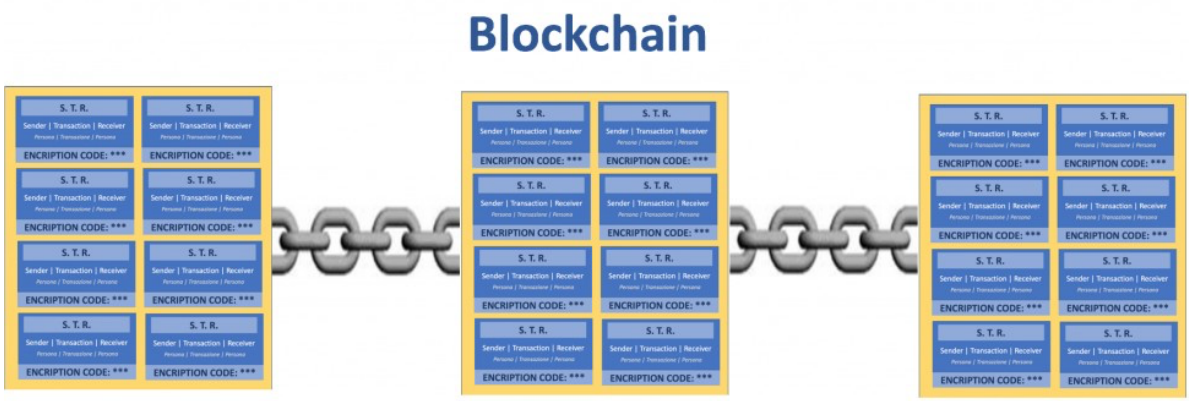
I componenti della Transazione



Lo storico di una transazione all'interno di un blocco contiene i seguenti dati:

- Il **mittente**;
- Il **destinatario**;
- Le **info sulla transazione**;
- La **firma crittografica**.

Un **blocco** avrà dunque un **insieme** di tutte queste **transazioni** e l'unione di più blocchi costituisce la blockchain.



Esempio

Supponendo di avere due persone chiamate Paolo e Anna, per cui nasce l'idea di acquistare un immobile. La transazione conterrà dunque informazioni sull'immobile, il prezzo, la disponibilità economica di Anna, ecc. Il quadro di riferimento è scritto tutto nella transazione, così come le chiavi di crittografia dei due utenti.

1. Entrambi gli utenti generano una coppia di chiavi crittografiche, composta da una chiave privata e una chiave pubblica. La chiave privata è segreta e deve essere mantenuta riservata, mentre la chiave pubblica viene condivisa con l'altra parte.

2. Firma digitale: Paolo utilizza la sua chiave privata per firmare digitalmente la transazione. La firma digitale è un'operazione crittografica che garantisce l'autenticità e l'integrità della transazione. In pratica, la firma digitale crea un'impronta unica dei dati della transazione utilizzando la chiave privata di Paolo.

3. Verifica della firma: Anna riceve la transazione firmata digitalmente da Paolo insieme alla sua chiave pubblica. Utilizzando la chiave pubblica di Paolo, Anna può verificare la firma digitale per assicurarsi che la transazione sia stata effettivamente firmata da Paolo e che i dati non siano stati modificati.

4. La transazione entra dunque a far parte **di un blocco di transazioni**, messo in attesa, pronto per la verifica e l'approvazione (vedi dopo) di tutti i partecipanti della blockchain;

5. L'intero blocco viene verificato dall'intera blockchain

6. Il blocco viene aggiunto alla catena, entrando a far parte della catena di blocchi

7. La transazione viene pubblicata sulla blockchain, archiviata nello storico di tutti i nodi e risulterà d'ora in poi accessibile a tutti i partecipanti. Tale transazione risulterà dunque immutabile e permanente.

Il bitcoin

Il principio delle blockchain è sfruttato dalle criptovalute come il **Bitcoin** e l'**Ethereum** (maledetti). La rete è appunto formata da nodi, ovvero, computer in comunicazione tra loro grazie al software open source di Bitcoin, e possono avere diverse funzioni: ci sono nodi che validano solo la **regolarità delle transazioni**, nodi che **inoltrano le transazioni** verso altri nodi, ecc.

Il bitcoin mining

Tra i vari nodi del bitcoin esiste una categoria detta **miners**, i quali hanno il compito di **creare la blockchain**, dove viene conservato lo storico delle transazioni. I minatori investono ingenti risorse per risolvere dei complessissimi calcoli matematici per essere ricompensati con della criptovaluta.

Come già accennato, il mining richiede un impiego di risorse molto ingente: energia elettrica, hardware in grado di eseguire calcoli nel minor tempo possibile, e così via. Attualmente, lo strumento più utilizzato dai miner sono le **schede video**, ma esistono i cosiddetti **ASICs** ottimizzati per queste operazioni. Oltre all'energia elettrica è opportuno investire in costosissimi e efficientissimi sistemi di raffreddamento, al fine di mantenere l'integrità fisica dei calcolatori da mining. Ciascuna squadra di miner opera per competere con altri miner, poiché solo i vincitori di un dato esercizio otterranno la ricompensa proposta.

1. Deve essere raggiunto un certo **obiettivo**, che consiste nel calcolo di un numero esadecimale SHA-256 con k zeri iniziali. Questo numero è associato a un determinato blocco di transazioni candidato ad essere aggiunto alla blockchain, e la presenza degli zeri iniziali non è un caso. Inoltre, più sono gli zeri, maggiore è la difficoltà di centrare l'obiettivo finale;

2. Partita l'operazione, i calcolatori da mining procedono col calcolo dell'obiettivo, usando:
    a. L'**hash** di riferimento del blocco transazioni associato (***ogni miner ha il suo, infatti i blocchi sono formati da transazioni scelte a piacere dai singoli miner*** - vedi dopo per chiarimenti);
    b. L'**hash** di riferimento del blocco transazioni precedente;
    c. Un numero **casuale.**

3. La procedura è interamente a **tentativi**;

4. Al primo tentativo la macchina che mina inserisce nel risultato il numero 1 e controlla quanti zero ci sono davanti a tale numero. Al secondo tentativo ricalcola lo SHA-256 con lo stesso set di transazioni e aggiunge il numero 2, al terzo il numero 3 e così via, fintantoché non ottiene un numero che inizia con lo zero davanti. Tra l'altro, gli zero devono soddisfare quelli richiesti dal protocollo e sono numeri grandissimi, tant'è che solo circa ogni dieci minuti uno dei calcolatori in giro per il mondo riesce a soddisfare le richieste del protocollo. Una volta che si trova l'hash con k zeri, il lavoro è terminato.

5. Quando un minatore ha trovato la soluzione valida, espone a tutta la blockchain di essere riuscito di essere giunto alla soluzione, il blocco di transazioni viene approvato e aggiunto alla blockchain. Il premio chiaramente se lo aggiudica chi è arrivato per primo alla soluzione (la medaglia la prende il vincitore della corsa).

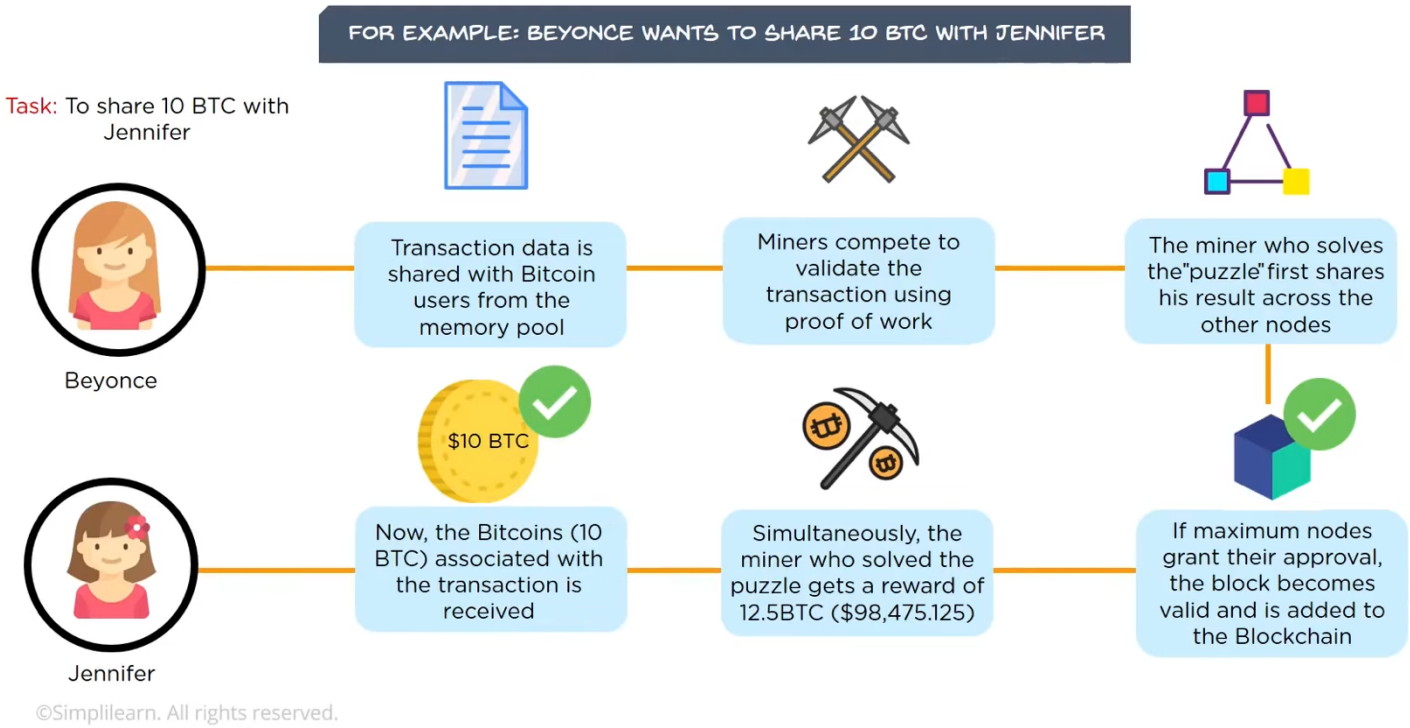
Questo particolare meccanismo che prevede una coordinazione del sistema in maniera decentralizzata è detto **proof of work** (prova di lavoro).

Riepilogo sul funzionamento del bitcoin mining

Quando un nodo invia una transazione, quelli più vicini verificano la disponibilità effettiva dei fondi e, se questa verifica viene approvata, la transazione è messa in coda (memory pool) per essere processata dai minatori.

Il termine "memory pool" o "mempool" si riferisce a una parte della rete Bitcoin in cui le transazioni valide sono temporaneamente memorizzate in attesa di essere confermate e inserite in un blocco nella blockchain.Quando un utente invia una transazione Bitcoin, questa viene trasmessa alla rete e viene inserita nel mempool dei nodi completi o dei "nodi miner" che compongono la rete Bitcoin. **Le transazioni vengono generalmente selezionate prima che il problema crittografico venga risolto.** I nodi completi sono i nodi che verificano e validano le transazioni e i blocchi. Il mempool funziona come una sorta di coda di transazioni in sospeso. Le transazioni nel mempool sono ordinate in base alla priorità dei loro fee, ossia le commissioni pagate per l'inclusione nella blockchain. Durante il processo di mining, i miner prendono le transazioni dal mempool e cercano di costruire un blocco valido che includa un insieme di transazioni. Il blocco viene creato con le transazioni selezionate e quindi viene eseguito il processo di hashing per risolvere il problema crittografico. Ogni miner ha la libertà di selezionare un insieme diverso di transazioni da includere nel blocco che sta cercando di confermare. Le transazioni possono rimanere nel mempool per un certo periodo di tempo, a seconda del traffico di rete e della priorità dei fee pagati. Quando un miner crea un nuovo blocco, seleziona un insieme di transazioni dal mempool, le verifica e le include nel blocco. Una volta che una transazione viene inclusa in un blocco, viene considerata confermata e aggiunta alla blockchain. Le transazioni non confermate rimangono nel mempool fino a quando non vengono confermate o supera un determinato periodo di tempo senza essere confermate, momento in cui vengono eliminati dal mempool.In sintesi, il memory pool Bitcoin (mempool) è una coda di transazioni in sospeso all'interno della rete Bitcoin, dove le transazioni valide sono temporaneamente memorizzate in attesa di essere confermate e inserite nella blockchain.

A questo punto i miner calcoleranno lo SHA-256 per poter vincere la “gara”. Terminato il processo il minatore vincente pone il suo blocco (e quindi le tutte relative transazioni) nella blockchain. Il minatore viene ricompensato con dei bitcoin e le transazioni vengono scritte su tutti i nodi.



L'hash power e hash rate

L'hash power è un indicatore della sicurezza del sistema, misurato dal numero di minatori che non riescono a vincere la competizione per l'aggiudicazione dei bitcoin sull'ultimo blocco di transazioni. La veridicità delle transazioni è un aspetto cruciale, poiché se tutti potessero vincere i bitcoin, sarebbe possibile approvare transazioni fasulle. L'hash power funge da muro difensivo, proteggendo la blockchain dal cosiddetto "double spending" e da potenziali malintenzionati che cerchino di corrompere l'integrità del sistema. **L'hash power rappresenta anche la potenza complessiva della rete e, indirettamente, il numero di nodi che la compongono. Un valore di hash power elevato riduce le possibilità che un gruppo di nodi si accordi per validare transazioni illecite, in un attacco noto come "attacco del 51%". Infatti, per avere un'alta capacità di calcolo sono necessari numerosi computer potenti, che non potrebbero essere controllati da un'unica organizzazione.**

L'**hash rate** (n tentativi di hash/secondo) misura invece la capacità del calcolatore nel determinare il più velocemente possibile la soluzione del blocco di transazioni.

Approfondimento ricevimento

Definiamo Hash Rate il numero delle funzioni di hash che posso calcolare nell'unità di tempo. Invece Hash Power che è comunque legato all' Hash Rate è la potenza che uso per calcolare gli hash. Esempio: se uso un "ASIC" piuttosto che un "FPGA" ho più Hash Power, quindi di conseguenza avrò maggior Hash Rate

Autoregolazione della difficoltà

I nodi si accordano su quale sia l'ultimo blocco valido, dopodiché riparte la gara per trovare lo SHA-256 del blocco accordato. Inoltre, il sistema si autoregola sulla base della potenza di calcolo immessa nel sistema.

- Quando l'hash rate complessivo è talmente grande da determinare soluzioni valide in meno di dieci minuti, la difficoltà **aumenta** aggiungendo ulteriori zeri allo SHA-256;

- Se invece l'hash rate complessivo è molto basso, tale da non determinare soluzioni valide entro ogni 15 minuti, la difficoltà **diminuisce** e quindi viene abbassato il numero di zeri dello SHA-256.

Ci si può quindi rendere conto che:

- Più potenza di calcolo non significa più Bitcoin, al contrario, l'hash power ha la tendenza ad aumentare man mano che aumenta il prezzo del Bitcoin;
- **Più potenza di calcolo implica più sicurezza**, poiché maggiore è l'hash power, meno persone vincono Bitcoin.

Smart contracts

Gli **smart contracts** sono un insieme di clausole contrattuali codificate in linguaggio di programmazione, le quali vengono impiegate per concludere dei rapporti di natura contrattuale, conferendo autonoma esecuzione ai termini programmati al verificarsi di determinate condizioni. Si basa sul costrutto *if then*.

Non vengono utilizzati al di fuori di ambiti giuridici, per via del fatto che si tratta di uno strumento che da esecuzione ad una volontà che è stata **precedentemente** elaborata dalle parti.

In virtù di tale scenario, si può dire che lo smart contract:

- Possa essere **accessorio** rispetto a un accordo più ampio. Le parti perfezionano degli accordi al di fuori della blockchain e poi ricorrono a uno smart contract, solo dopo aver firmato un contratto più ampio;

- Sia in grado di stabilire gli obblighi e i vincoli di ambo le parti;

- **Automatizzi** obblighi contrattuali visibili a tutti i partecipanti della blockchain e non solo alle parti coinvolte;

- Sia **trasparente** e **immutabile**. Il contratto è sempre in chiaro e non può essere annullato/modificato.

- **Impedisca** la volontaria **inadempienza** di ambo le parti, dato che si affida a un meccanismo automatizzato, intelligente e trasparente all'interno di una rete in cui tutti possono vedere.

Alcune blockchain, come l'**Ethereum** (maledetti ancora), permettono di creare smart contract con un meccanismo di **autodistruzione**, attivabile dal nodo che ha inizializzato per primo il contratto. Tale caratteristica serve più che altro a ottimizzare le prestazioni della blockchain.

Non tutte le blockchain supportano gli smart contract e le caratteristiche variano in base alla piattaforma.

Un esempio di uno smart contract potrebbe essere un accordo per la vendita di una casa (come già visto nell'esempio poche pagine prima). Le condizioni dell'accordo, come il prezzo di vendita e le date di pagamento, verrebbero inserite nello smart contract. Una volta che queste condizioni sono state soddisfatte, il contratto si eseguirà automaticamente, trasferendo la proprietà della casa all'acquirente e il pagamento al venditore.

Fork

Si definisce **fork** un "cambiamento" del codice originario (o precedente) della valuta virtuale, che permette di definire una nuova versione della blockchain, conservando lo storico della precedente valuta.

Un esempio di fork potrebbe essere la nascita del **Bitcoin Cash**, derivato dal codice sorgente del **Bitcoin**.

I fork si distinguono in:

- **Hard fork:** rompe la compatibilità tra il vecchio e il nuovo codice. Ad esempio, gli scambi monetari tra Bitcoin Cash e Bitcoin non possono avvenire;

- **Soft fork:** mantiene la retrocompatibilità col vecchio codice e consente pertanto gli scambi monetari tra vecchia e nuova valuta.

Un fork influenza la validità delle regole e sono tipicamente realizzati per aggiungere nuove funzionalità alla blockchain oppure sistemare bug catastrofici. Alcuni cambiamenti sono così importanti che, in particolare negli hard fork, richiedono il cambio del **client**.

Mappa Capitolo