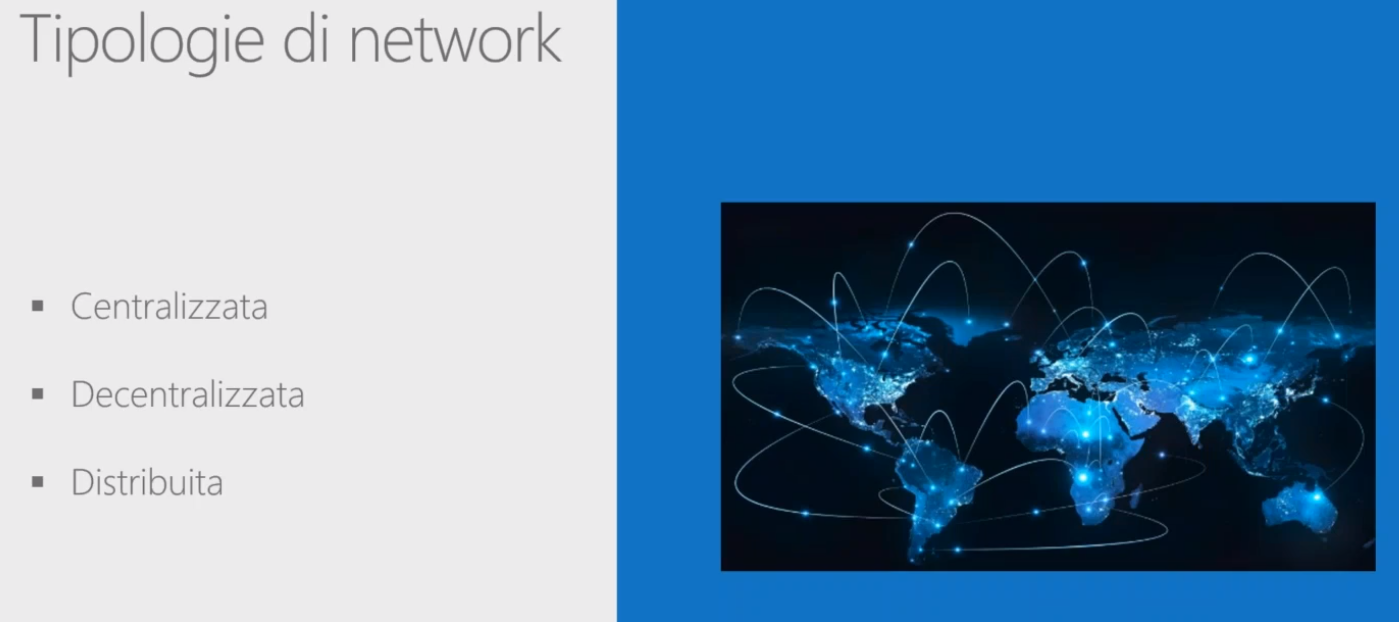
**Blockchain**



Centralizzata FIFO, un point of failure determina il down di tutto quanto.

Decentralizzata: non ho più un single point of failure, se abbiamo un failor su un hub si switcia verso quell’altro, ovviamente c’è la problematica della sincronizzazione.

Distribuita: tutti i nodi che entrano nella rete recepiscono il blocco di informazioni e rimangono aggiornati.



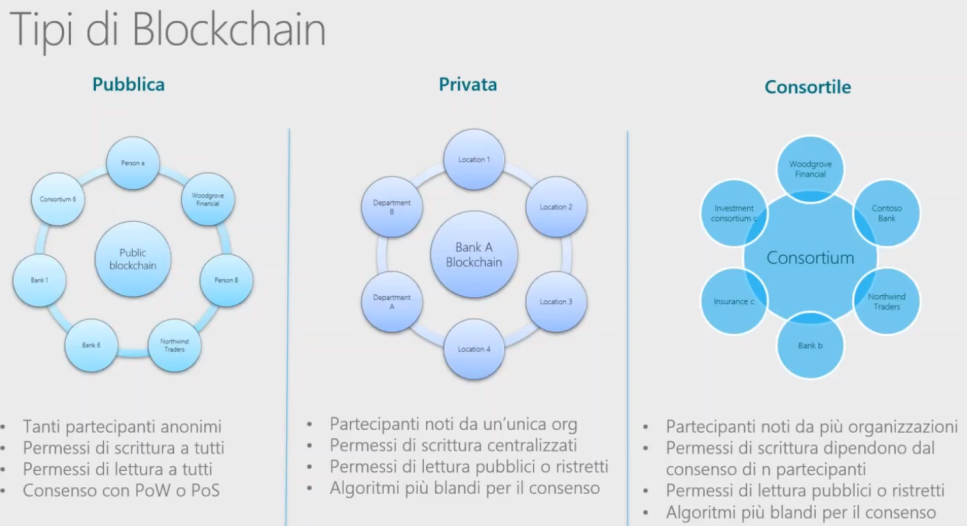
Fondamentale   
condivisione.

l’immutabilità della informazione.

Sicurezza.

Distribuzione delle informazioni.

Esistono declinazioni differenti di blockchain:

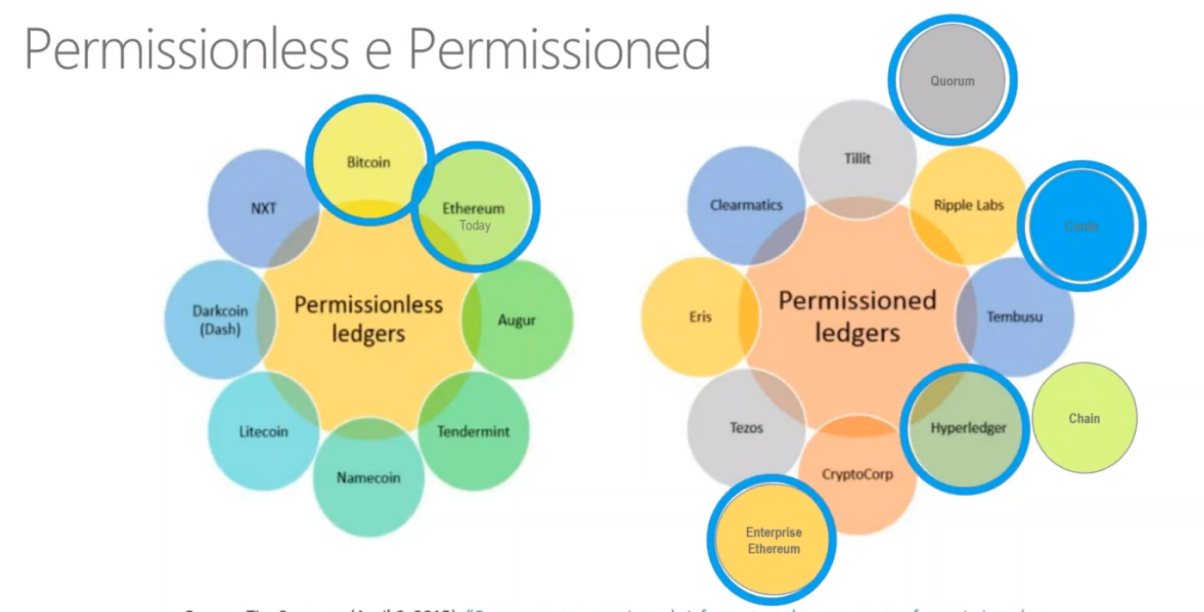


Pubblica: partecipanti anonimi, cio che ci identifica è una copia di chiavi (pubblica e privata), da permessi di lettura e scrittura da parte di tutti i partecipanti. Vi sono meccanismi di consenso per validare i dati della blockchain che possono essere PoW o PoS, l’esigenza di una validazione strong nasce dal fatto che tutti possono scrivere.

Privata: agli antipodi della pubblica, io decido di creare una blockchain per salvare delle info aziendali e do io quindi il permesso a determinati utenti. Le info contenute nella blockchain possono essere rese pubbliche o mantenute private.

Consortile: a meta tra pubblica e privata c’è la consortile: partecipanti noti che fanno parte anche di organizzazioni diverse dalla mia azienda.

Esistono quindi due tipologie a seconda che il permesso sia dato da un attore o che nessuno dia permessi ad altri:



Password Hash

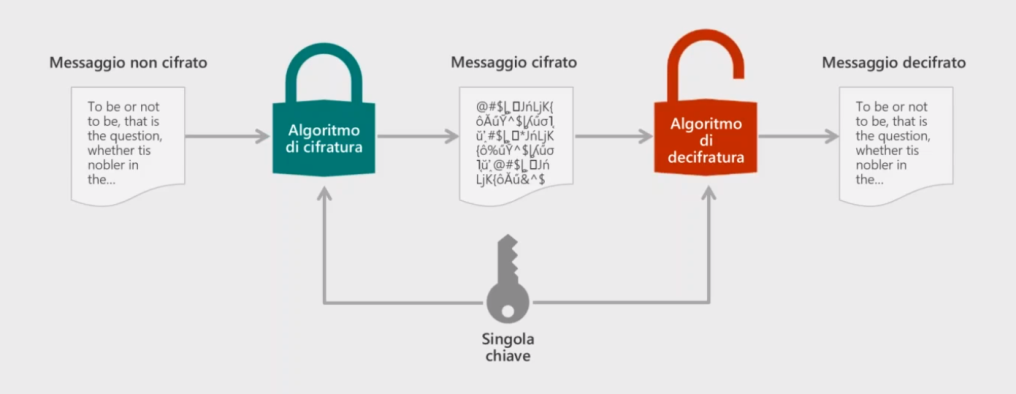
Hash crittografico: algoritmo che rappresenta delle informazioni in modo sintetico, producendo un digest (sommario), che deve coprire le tematiche della sessione completa e se io cambio qualcosa ci si deve accorgere.

Il digest ha sempre la stessa lunghezza, molto diverso anche se l’input è leggermente differente.Dato l’input è facile calcolare il digest viceversa è quasi impossibile propriò perché anche se ci si avvicina il digest è molto diverso anche se il contenuto da cui è stato prodotto è molto simile.:



Crittografia simmetrica ed asimmetrica.

Simmetrica: genero una chiave privata che scambio con chi voglio comunicare attraverso un canale sicuro, prendo il messaggio cifrato, ci applico la chiave privata e lo cripto, la persona con cui comunico attraverso la chiave privata lo decripta e lo legge.



Questo tipo di criptografia è critico dal punto di vista sicurezza (se qualcuno frega la chiave…)

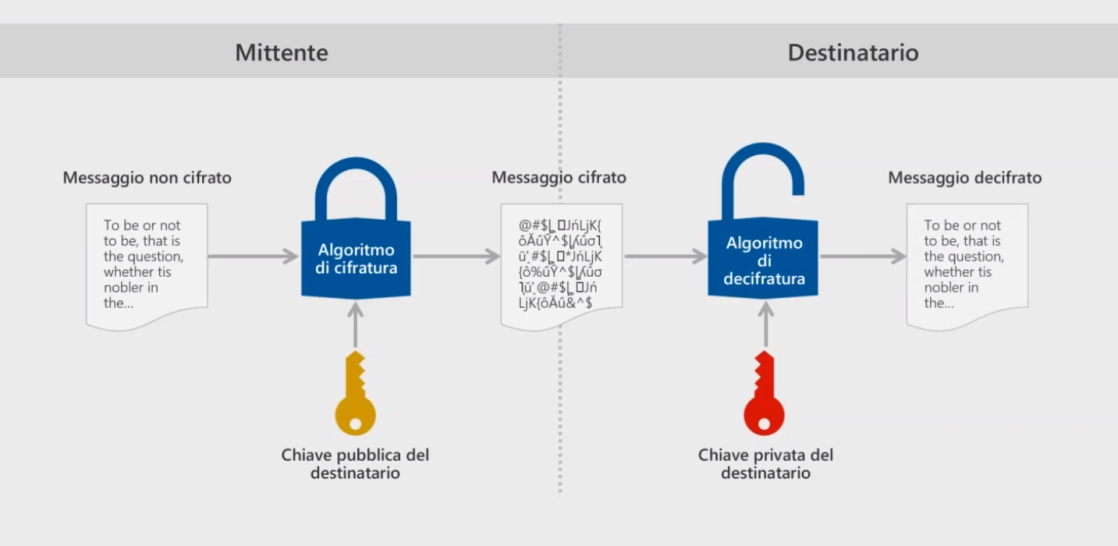
Asimmetrica.



Questo tipo di tecnologia può essere usato in due declinazioni:

Cifratura:

Con la chiave pubblica si cripta il messaggio, solo chi ha la chiave privata decripta e legge.



L’unico aspetto legato alla sicurezza è che io tenga la chiave privata in modo consono.

Un altro tipo di implementazione della criptografia asimmetrica è la firma.

Chi firma ha la chiave privata, chi verifica ha una chiave pubblica

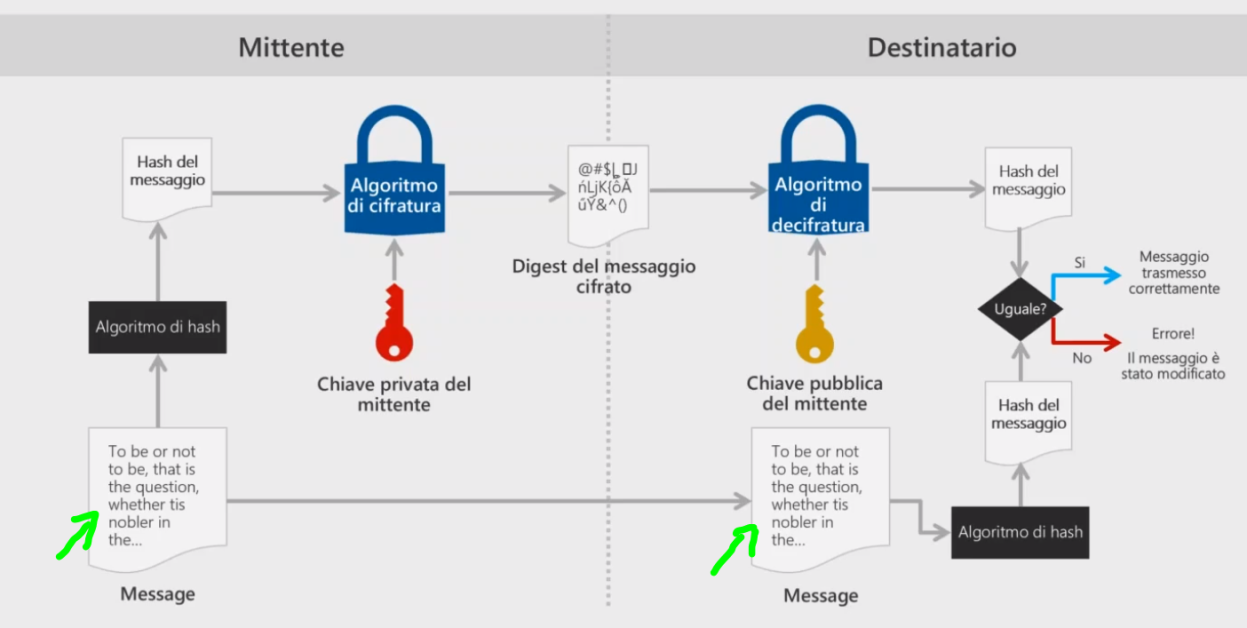




Se un mittente volesse scambiare un messaggio certificando il fatto che sia stato mandato in modo corretto

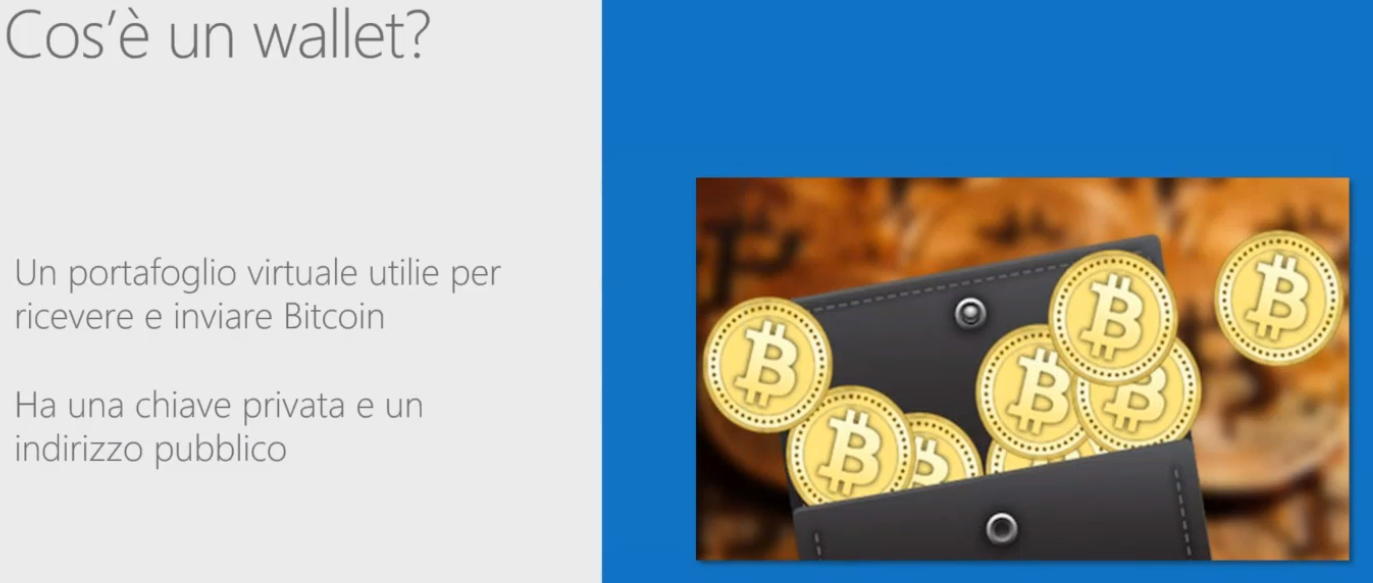


Mando il messaggio a Simone in chiaro e poi lo firmo criptandolo con la chiave privata così simone sa che sono Io il mittente, il messaggio viaggia criptato sul canale non sicuro per poi arrivare da simone che lo decripta con la chiave pubblica confronta l’hash del messaggio da lui generato con l’hash che gli è arrivato per vedere che siano uguali mentre se è diverso vuol dire che è stato modificato.

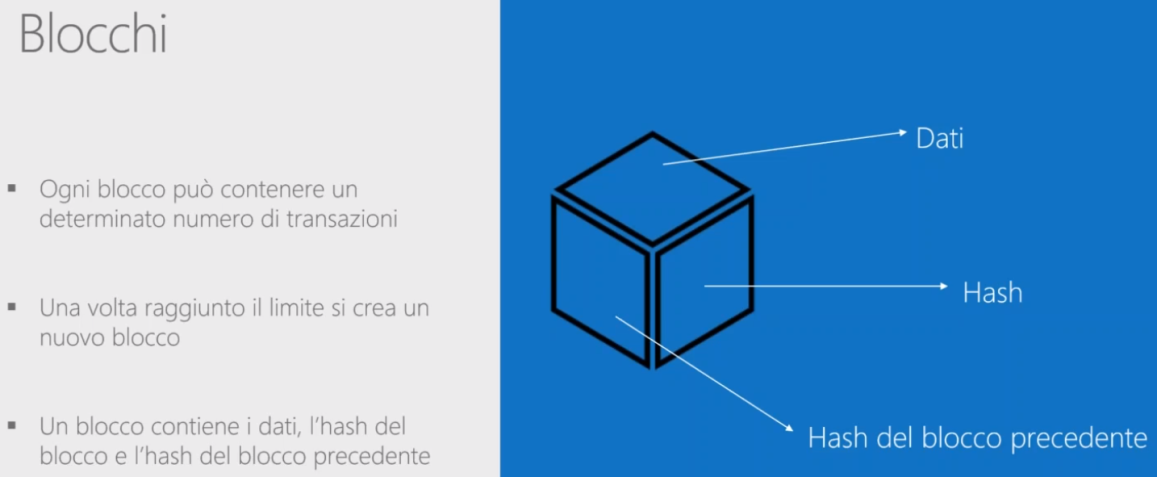


Un soggetto della blockchain viene identificato da una coppia di chiavi (publica e privata).

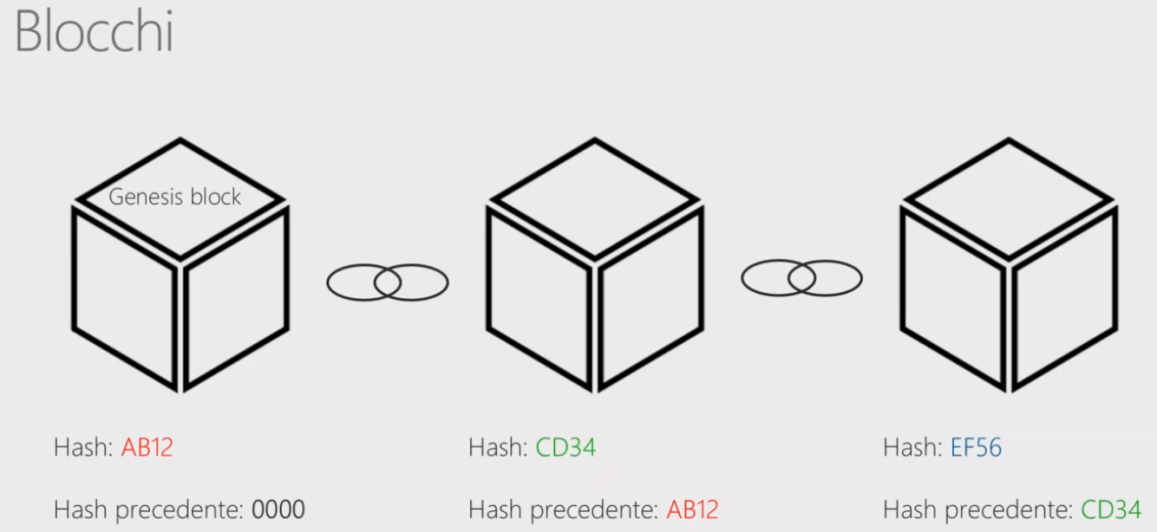
La privata va custodita severamente e non bisogna perderla!!. La chiave privata permette di accedere ai bitcoin o alle informazioni in generale salvate a cui noi abbiamo accesso.



La blockchain è formata da una catena di blocchi. Le transazioni vengono salvate all’interno dei blocchi. Un blocco ha una capienza massima determinata dall’algoritmo di blockchain e raggiunta la capienza massima ne genera uno nuovo. Il blocco numero 2 avrà il richiamo al blocco numero 1.



La catena di blocchi



Il blocco di partenza è il genesis block.

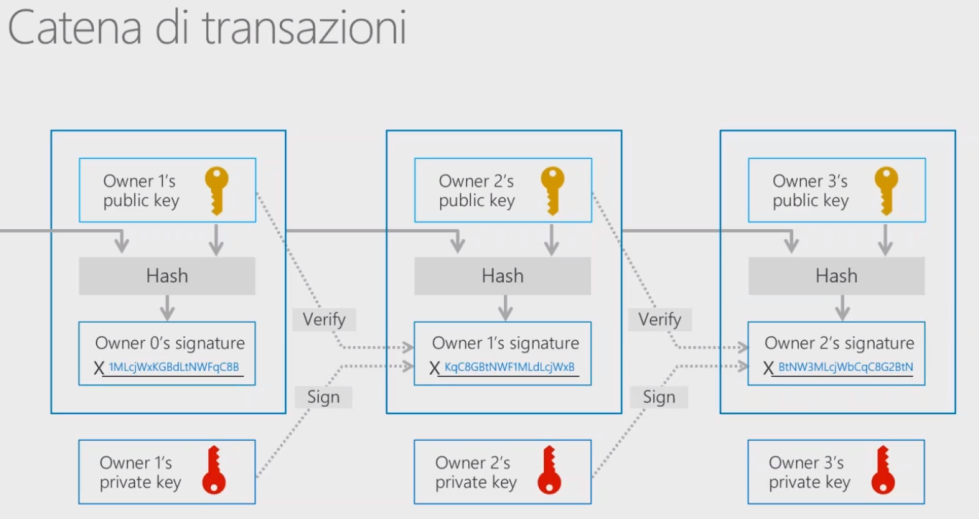
Per calcolare l’hash corrente prendo l’hash di tutte le transazioni e l’hash del blocco precedente.

Se comprometto un blocco comprometto tutti gli altri in quanto cambia l’hash a catena di tutto.

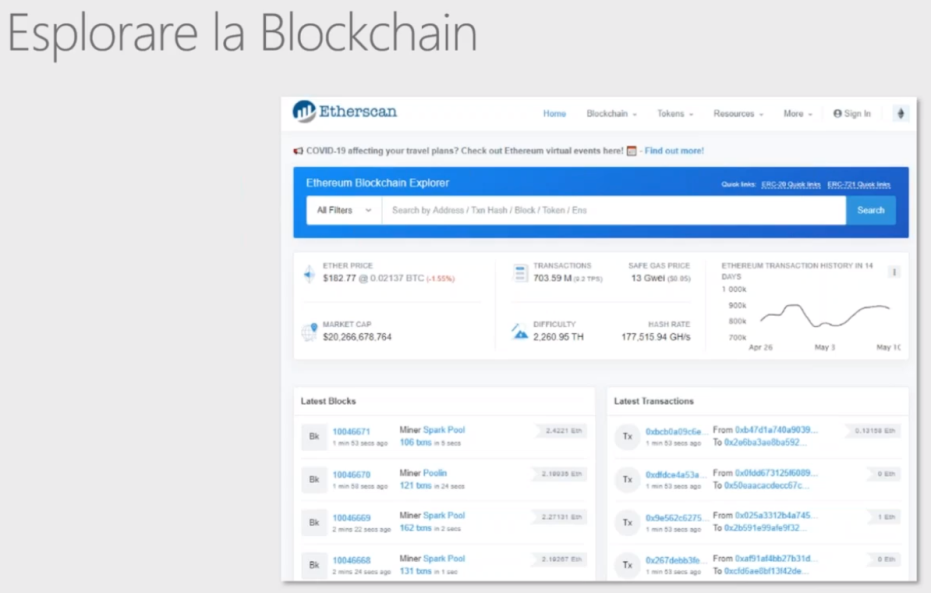
Se voglio rappresentare una transazione che Bob invia ad Alice di 10 bitcoin vado a prendere l’id della transazione precedente in cui Bob ha ricevuto almeno 10 bitcoin, Bob prende la chiave pubblica di Alice che usa per criptare l’informazione e poi prende la sua chiave privata per firmare l’informazione.



Alice riceverà il messaggio usando la chiave pubblica di Bob, verificherà che è stato Bob a mandare e con la sua chiave privata ruiscirà ad aprire il messaggio e ricevere i 10 bitcoin.



Esistono blockchain pubbliche per vedere quello che succede in una blockchain pubblica:



Mining:



