

Stefano Bortolato

dsb005

Informatica Blockchain

Cosa sono le Blockchain

Roma 19/6/2023

1





Premessa

Cosa sono le Blockchain? A cosa servono? Dove sono impiegate? Sono collegate con le Criptomonete?

Vediamo di rispondere a queste domande e di dare una panoramica esauriente senza scendere negli aspetti tecnologici.

Cosa sono le Blockchain?





Blockchain



Se traduciamo letteralmente il nome si tratta di una "catena di blocchi".

Il nome rende molto bene l'identità di questa tecnologia, ma non ci spiega cos'è.

Per prima cosa le blockchain sono una tecnologia costruita usando diverse tecnologie.



Blockchain



Obiettivi di questa tecnologia è la sicurezza, l'integrità dei dati e la disponibilità dei dati.

Ciascun blocco è collegato ad un altro (o a più blocchi) attraverso connessioni criptati.

Scopo della catena è di far passare i dati da un blocco all'altro fino a giungere a destinazione. Il trasferimento dei dati ha delle caratteristiche molto precise:



Blockchain



- "time-stamp": ogni movimento, quando passa in un blocco viene segnato con una marca temporale. In questo modo non sarà possibile falsificare il passaggio di una transazione a meno che non si modifichi tutta la catena
- "tracciamento": ogni singolo blocco contiene l'informazione di tutte le transazioni. In questo modo non è possibile falsificare le transazioni a meno che non si modifichino tutti i blocchi della Blockchain
- "trasparenza": le informazioni di tutti i nodi sono leggibili a chiunque rendendo evidente a tutti la verità.

Cosa fanno le Blockchain?





Blockchain



I principi di funzionamento sopra esposti rendono le blockchain molto resistenti e particolarmente utili su diversi fronti.

Immaginiamo la distribuzione delle affermazioni del presidente del Fondo Monetario Internazionale affidate ad una blockchain: diventano una verità evidente, accessibile e infalsificabile.

Pensiamo anche al caso di un pagamento-incasso: il tracciamento e il pagamento diventano visibili a tutti, trasparenti e infalsificabili.

I benefici sono notevoli, ma ci sono alcuni aspetti pro e contro sono da tener presenti.

Pro

Elementi a favore
Delle Blockchain





Blockchain



- La catena garantisce sicurezza integrità, trasparenza e non falsificabilità
- vengono usate tecnologie note e solide
- le tecnologie impiegate funzionano su (quasi) ogni hardware rendendole (quasi) universali
- la neutralità tecnologia di fondo le rende usabili per ogni ambito: dalla distribuzione delle news delle agenzie, alle transazioni delle borse.

Contro

Elementi a detrimento Delle Blockchain





Blockchain



I contro sono di più, ma sono più *sottili*:

- rete: il buon funzionamento dipende dalla connessione di rete (chi non è connesso è fuori) e dalla velocità di connessione
- capacità: le tecnologie di marche temporali, crittografia, ecc... richiedono molto calcolo. Gli hardware datati sono esclusi dal buon funzionamento e quelli recenti devono essere performanti
- quantità di dati: la sistematica duplicazione dei dati richiede grande spazio come somma di tutti i nodi, ma anche il singolo nodo deve dedicare molto spazio all'archiviazione

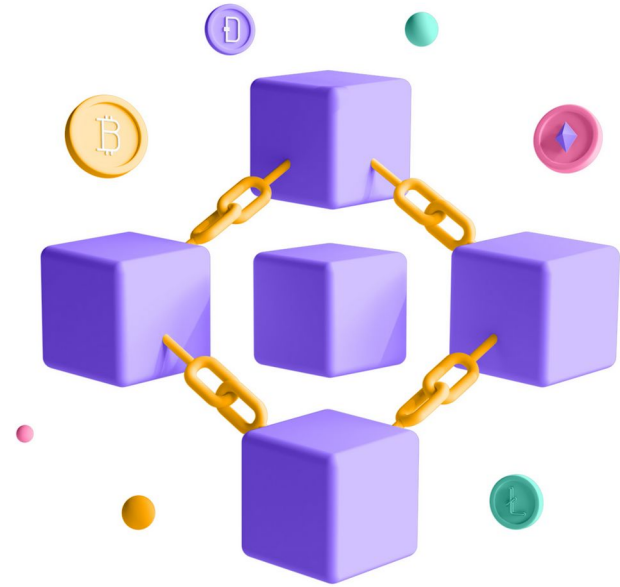


Blockchain



- energivoro: la catena consuma tanta, tanta corrente. Quindi è costosa e difficile da mantenere
- molte varianti possibili: non accennato, ma possiamo introdurre molte varianti sui principi di funzionamento dando luogo a molti *tipi* di catene che potrebbe non parlare tra loro o creare antipodi aberranti (es. una blockchain totalmente criptata, impossibile da ispezionare e dedicate a sole attività illecite)
- non manipolabile: questo beneficio potrebbe essere negativo ad esempio nell'economia reale dove a volte è necessario alterare i processi solamente *automatici* per mantenere sostenibilità e vivibilità delle regole di mercato.

A cosa servono le Blockchain?





Blockchain



In primo approccio potremmo impiegarle per (quasi) ogni cosa a partire dalla rubrica dei contatti degli amici.

Gli aspetti prima accennati di rete, numero di noti, firme temporali, crittografia, ecc... rendono immediatamente evidente l'esagerazione della scelta tecnica rispetto al fine e al contenuto dell'agenda dei contatti personale.

Se creiamo una blockchain per gestire le transazioni bancarie da quella della carta di credito per pagare un gelato a quelle del mutuo è facile capire che si tratta di una tecnologia costosa, ma adeguata.



Blockchain



Le scelte di impiego non sempre sono state *onorevoli*.
Comunque, come la fama racconta, l'impiego principe
è stato nelle **criptomonete**.

Alcune, purtroppo, sono state impiegati per scopi
delittuosi (come per acquisti illeciti).

Molte altre con scopi leciti, distinte da specifiche
qualità (alcune hanno accentuato gli aspetti di
inalterabilità, altre la possibilità di correttivi umani, altre
la trasparenza dei dati, ecc...).

Da riporta che ancor prima di creare l'etichetta
"blockchain" il core questo insieme di tecnologie era
già usato nelle reti di ricerca mondiale per lo scambio
di dati astronomici, piuttosto che nello scambio-
elaborazione di dati di esperimenti come quelli del
CERN di Ginevra.

Blockchain: quale rete?





Blockchain



È lecito chiedersi quale rete usano le blockchain.

Nel pensiero comune rete è sinonimo di internet e non distinguiamo tra dati, voce, tempo, ecc...

Se riflettiamo per qualche istante è evidente che un cellulare usa una rete voce e una dati. L'internet del computer non è la stessa usata dal controller di domotica di casa. Anche il circuito dei bonifici bancari non è lo stesso delle email...



Blockchain



Le blockchain partono dalla considerazione base che su internet possiamo far viaggiare ogni cosa. Se a questo principiamo aggiungiamo accorgimenti⁹ come la crittografia, le firme temporali, la ridondanza dell'informazione, ecc... possiamo considerare, in ultima analisi, che è sufficiente una connessione internet.

A seconda delle qualità della nostra connessione varia il tempo necessario per l'elaborazione-trasferimento. Inoltre a seconda della capacità di calcolo del singolo blocco è necessaria una diversa quantità di tempo.



Blockchain



Costante, invece, che in ogni caso è sempre necessaria molta energia.

In conclusione è sufficiente una connessione internet (qualsiasi essa sia), ma se piccola il tempo necessario per l'elaborazione può essere così tanto da non essere sufficiente la connessione in se.

Conclusione





Conclusione



Se le blockchain sono alla base del funzionamento delle criptomonete, queste ultime cosa sono?

Nella prossima lezione rispondiamo a questa domanda dando una panoramica a queste nuove monete.

Domande?

Questions?

