



Stefano Bortolato

dsb005

Informatica Blockchain

DB speciali e di sciurezza

Roma 3/8/2023

4



Nella 1° lezione abbiamo visto cosa sono le blockchain.

Nella 2° lezione abbiamo visto cosa sono le criptomonete.

Nella 3° lezione abbiamo visto le reti ad alta sicurezza.

Le blockchain sono un insieme di tecnologie che possiamo trovare impiegate in altri settori come nel caso delle reti sicure.

Una delle tecnologie impiegate sono i database. A differenza di quelli di pubblico dominio i database delle blockchain sono *particolari*.

Vediamo cosa hanno di particolare e unico e se possiamo impiegarlo anche fuori delle blockchain.

Utilità del database nelle blockchain



Le tecnologie delle blockchain necessitano di tener traccia di tutte le operazioni.

Tutte queste informazioni vengono scritte in un database.

Questa soluzione permette uno stoccaggio efficiente delle informazioni e un reperimento delle stesse in modo molto efficace.

Questa soluzione è adottata da diverse applicazioni, ma le blockchain hanno aggiunto dei particolari innovativi:

- il database è distribuito
- i database sono reciprocamente trustati
- le scritture sono firmate.

vediamo cosa significano queste specificità partendo da una panoramica che ci permetta di capire l'innovazione nel suo complesso.

Panoramica



Panoramica

Immaginiamo che in una blockchain viene, a un certo punto, assegnato 1 criptovaluta al signor Mario Rossi.

L'operazione viene scritta nel database del nodo dove avviene l'assegnazione. L'informazione, successivamente, viene propagata a tutti i database dei nodi della rete della blockchain. Ogni singola scrittura viene *firmata* in modo che sia unica e verificata.

Immaginiamo ora che un ladro provi ad assegnare a se stesso la criptovaluta data al signor Mari Rossi. Il ladro è un esperto informatico che conosce molto bene il funzionamento delle blockchain e pensa di poter assegnare a se stesso la criptovaluta semplicemente scrivendo nel database il suo nome al posto di quello di Mario Rossi.

Panoramica

In primo luogo interviene la firma della scrittura nel database: sarà subito evidente (ai computer) che la scrittura è stata manomessa.

In secondo luogo intervengono le copie negli altri database presenti nei vari nodi della blockchain che diranno che è falsa la scrittura manomessa e diranno che il proprietario di quella criptovaluta è il signor Mario Rossi.

In fine (in realtà è il primissimo passo) per poter accedere, scrivere, leggere, modificare bisogna avere un "trust", ovvero un *accreditamento di fiducia* presso tutti i nodi della blockchain.

Panoramica

In conclusione per poter *imbrogliare* il sistema bisogna cambiare le scritture in tutti i nodi della blockchain, creare delle firme valide per ogni nodo della rete e avere un accreditamento di fiducia verso ogni singolo nodo della rete.

In pratica è impossibile riuscire a fare un'alterazione anche in un solo dato di un database della blockchain.

Database distribuito



Database distribuito

Dalla panoramica si può capire che un aspetto fondamentale della tecnologia sta nel fatto che il database è distribuito.

Cosa vuol dire che è distribuito? Quali caratteristiche lo contraddistinguono?

Possiamo individuarle in:

- molti nodi
- copia dei dati
- autoconsistenza del singolo nodo
- verifica incrociata
- metadati di validazione
 - della rete
 - di ciascun nodo
 - del singolo dato
- resilienza.

Database distribuito

Procediamo scoprendo cosa sono queste caratteristiche.

- 1) **Molti nodi:** il database della blockchain è in realtà molti database, uno per ciascun nodo, in prima approssimazione;
- 2) **Copia dei dati:** le informazioni sono duplicati su tutti i database;
- 3) **Autoconsistenza del singolo nodo:** ciascun database è consistente in se stesso. Questo significa che funziona ed è *usabile* anche se scollegato dalla blockchain;
- 4) **Verifica incrociata:** l'attendibilità e la veridicità di ogni dato contenuto in un database è data dalla verifica incrociata sugli altri database;

Database distribuito

- 5) **Metadati di validazione:** ogni scrittura è completata da dati che sono usati dalla blockchain e, normalmente, non sono accessibili dagli utenti. Questi metadati sono:
- 1) **della rete:** ciascun nodo conosce la *posizione* in rete degli altri nodi. Ogni nodo diffida di connessioni non mappate;
 - 2) **di ciascun nodo:** ogni nodo ha delle chiavi segrete con cui dimostra ai nodi con cui si connette di essere se stesso. Questi metadati vengono anche usati per criptare le connessioni;
 - 3) **del singolo dato:** altri metadati vengono usati per meccanismi di verifica interna nel singolo nodo. Questo permette il funzionamento anche se sconnesso dalla rete e permette di dimostrare la coerenza dei dati;
- 6) **Resilienza:** gli accorgimenti sopra descritti, insieme ad alcuni altri, permette al database della blockchain di funzionare anche in situazioni particolarmente penalizzate.

Trust



Trust

Il database presente in un nodo della blockchain non accetta in modo acritico ogni connessione, ogni dato.

Come sopra accennato ci sono dei meccanismi di verifica e protezione:

- in primo luogo, normalmente, ogni database diffida delle richieste di connessione;
- l'insieme dei metadati, delle chiavi di connessione e la tecnica di mappatura degli altri nodi permette al singolo database-nodo di verificare identità e permessi.

Trust

La relazione di trust (ovvero la "relazione di fiducia") tra i nodi è il meccanismo che autorizza la connessione e lo scambio di dati.

Il trust è una relazione complessa costruita da diverse informazioni.

Il trust non avviene anche quando un solo dato non collima.

Trust

Da aggiungere, per completezza, che il sistema di resilienza del database non *rompe* il trust.

A seconda del livello di sicurezza e confidenzialità che viene adottato:

- Il singolo database sconnesso dalla rete della blockchain mantiene consistenza ed usabilità
- Accesso e manipolazione delle informazione è possibili se i metadati di sicurezza vengono confermati.

Pertanto se uno sconnette un database dalla sua blockchain, normalmente non può leggere e/o manipolare le informazioni.

Firma



Firma

Il concetto "firma" è equivoco anche nel campo informatico. In questo caso non è la firma digitale che conosciamo, ma usa le tecnologie adottate dalla firma digitale.

Quando viene scritta un'informazione (o modificata, o cancellata) viene applicato un procedimento matematico che da, come risultato, un'informazione che è la *firma* prodotta da quell'informazione.

In qualsiasi situazione applicando questo processo matematica sulla firma ci darà come risultato una conferma o una smentita circa l'autenticità dell'informazione. Anche l'alterazione di un solo bit darà un risultato di falsità. Nelle situazioni di implementazione forte anche il cambio delle marche temporali e/o la presenza di un timestamp di copia darà un risultato di falsità se anche un solo bit non collima.

Firma

Quindi ogni azione sui dati e ogni duplicazione o spostamento deve essere ri-firmato per essere valido.

Come accennato precedentemente esistono molte diverse blockchain.

Anche i database dei nodi delle blockchain possono implementare tutte le potenzialità o solo alcune.

Questa discrezionalità è guidata da diverse ragioni, tra cui il costo (banda di rete necessaria, tempo di calcolo, RAM necessaria, tempo necessario, corrente necessaria, ecc...).

Dove usare i database delle blockchain



Dove usare i database delle blockchain

Questi particolari database impiegati dalle blockchain offrono svariate opportunità, insieme a limiti da tener ben presenti.

Caratteristica comune a tutti i database delle blockchain è un elevatissimo livello di sicurezza a tutto campo.

Questa caratteristica è la motivazione principale per casi d'uso esterni alle blockchain. Anche le altre caratteristiche entrano nel bilancio di scelta per impieghi esterni alle blockchain.

Dove usare i database delle blockchain

Dove vengono usati? Alcuni esempi:

- database bancari
- database delle borse di scambio
- database delle finanziarie
- database forensi
- alcuni database scientifici.

L'elenco è solamente esemplificativo per dare consapevolezza che troviamo impiegate queste tecnologie delle blockchain anche in servizi *ordinari*.

Limiti e Difficoltà



Limiti e Difficoltà

Prima abbiamo visto gli aspetti affascinanti di queste tecnologie, ma abbiamo fatto anche qualche insinuazione circa limiti e difficoltà.

Per riflettere: se ci sono tutti i benefici prima narrati, come mai non c'è un uso diffuso e capillare?

Vediamo le principali criticità che affliggono queste tecnologie:

Limiti e Difficoltà

- 1) **Lentezza:** già esposto l'applicazione di queste tecnologie rende lento il sistema a tal punto che non è adatto ad impieghi diffusi e capillari come, ad esempio, il denaro elettronico;
- 2) **Calcolo:** queste tecnologie sono molto esose in termini di calcolo. L'avanzamento delle capacità dei microprocessori non compensa la grande richiesta di calcolo fino a rendere insignificanti i ritardi introdotti;
- 3) **Energivoro:** la richiesta di molto calcolo, RAM, spostamenti dei dati significa corrente. Allo stato attuale queste tecnologie consumano tanta corrente e messe in rete nella loro fisionomia completa diventano tra i primi consumatori mondiali di corrente elettrica;

Limiti e Difficoltà

- 4) Grandi quantità di dati:** la duplicazione delle informazione, la costante aggiunta di metadati, ecc... da, come risultato finito, un'enorme quantità di informazione. I dispositivi di memoria di massa sono diventati molto capienti ed i costi si sono contratti. Resta il problema della dimensione totale (da moltiplicare per tutti i casi d'uso) e il problema della conservazione a lungo termine di tutti i dati;
- 5) Grande traffico di rete:** direttamente connesso al punto precedente è l'enorme quantità di traffico che viene generato sulla rete. Questo significa un problema di saturazione della capacità di rete ed un progressivo rallentamento della ricezione dei dati.

Conclusione



Conclusione

I database li usiamo tutti quotidianamente, ma non né abbiamo consapevolezza.

Anche l'uso della rete non ci restituisce una consapevolezza del livello di saturazione della sua capacità.

Pertanto questa lezione porta un sapore dominante di teoria perché ha esposto elementi che non restituiscono subito una percezione consapevole.

Quanto abbiamo visto in questa lezione racconta di una tecnologia molto potente, che offre altissimi livelli di sicurezza e molti casi d'uso possono essere interessati a impiegarla.

Conclusione

Dall'altra parte ha delle limitazioni molto importanti per essere impiegata in modo diffuso e capillare.

Ultimo, ma non ultimo, consuma grandi quantità di corrente.

Nella prossima lezione vedremo gli impieghi delle blockchain.

Domande?

Questions?

Stefano Bortolato

dsb005

Informatica Blockchain

DB speciali e di sciurezza

Roma 3/8/2023

4



