



Stefano Bortolato

dsb005

Informatica Blockchain

Reti di alta sicurezza

Roma 25/6/2023

3



Criptomete

Nella 1° lezione abbiamo visto cosa sono le blockchain.

Nella 2° lezione abbiamo visto cosa sono le criptomonete.

Le due soluzioni sono un insieme di diverse tecnologie.
Possiamo quindi chiederci:

con queste tecnologie possiamo *creare* solo
criptomonte?

La risposta è semplice: **NO**.

A questo punto nasce una seconda domanda:

cosa, allora, possiamo creare che sia *utile* e
interessante?

Affrontiamo un piccolo excursus in cui presentiamo
alcuni prodotti nati dalle tecnologie che creano le
blockchain e le criptomonete.

Premesse





Blockchain



Le tecnologie che costituiscono le blockchain in realtà già esistevano da anni. Grazie all'aumento delle capacità dei computer, alla disponibilità di connessioni più veloci e all'intuito di qualche sviluppatore geniale sono state *assemblate* creando qualcosa di nuovo.

Semplificando il quadro le tecnologie di cui parliamo sono note come:

- registri distribuiti
- Timestamp
- HASH
- crittazione

Cosa sono



Blockchain

Cosa sono

Vediamo di capire cosa si nasconde dietro ai nomi sopra.

- **Registri distribuiti:** se pensiamo a un registro normalmente pensiamo ad un solo libro. Se è digitale pensiamo a un unico file. Una soluzione semplice, ma anche molto limitata. Con l'avvento di internet si è potenziata l'idea base spaccando l'unico file in molti parti. Ciascuna parte è duplicata. Ciascuna è in un posto diverso della rete. Ciascuna ha traccia delle altre. Ciascuna ha dei *codici* di verificare l'integrità delle altre. In questo modo si aumenta enormemente la sicurezza (nessuno ha tutto), si minimizza la probabilità di perdere le informazioni (tutto è duplicato), si rende impossibile la falsificazione e la copia (i codici di verifica rendono subito evidente la manomissione e se abbiamo una copia invece che un originale).

Cosa sono

- **Timestamp:** si tratta di una tecnica complessa con cui viene applicata una marca temporale. La tecnica è così precisa che non posso essere state fatte due copie di una stessa informazione nello stesso istante; una è un po' prima, l'altra un po' dopo.
- **Hash:** in italiano è sostanzialmente intraducibile, ma possiamo parafrasarlo come un codice che identifica un oggetto. Questo codice è fatto sul momento, tutti lo possono fare e verificare, ed è così preciso che se cambia anche un solo particolare minimo il codice cambia. Questa tecnologia è usata per creare i codici che tracciano tutte le informazioni del nostro registro distribuito. Così il timestamp permette di verificare se abbiamo una copia o un originale, e poi l'hash ci fa capire se è stato cambiato qualcosa, anche se fosse 1 solo bit creando, al tempo stesso, sia una verifica di interpolazione, ma anche una verifica di errore.



Cosa sono

- **Criptazione:** la parola, in questo caso, va collegata a 2 livelli diversi e va aggiunta un considerazione:
 - **crittografia della connessione:** significa che il collegamento via rete è cifrato e solo i 2 nodi interessati (trasmettitore e ricevente) sono in grado di decifrare la comunicazione;
 - **crittografia dei dati:** significa che i dati dei file che vengono letti o scritti sono criptati;
 - **criptazione:** la parte innovativa è nell'adozione di una chiave doppia asimmetrica. Significa che metà della chiave è in internet, accessibile a tutti, ma l'altra metà è solo in mano a chi trasmette o riceve l'informazione. Per spiegarmi è la tecnica diventata obbligatoria con tutti i siti web in questi ultimi anni. E' il motivo per cui pochi siti che non hanno la criptazione SSL (crittografia asimmetrica) vengono resi quasi inaccessibili dai computer. Questo ci racconta della robustezza di questo sistema ora adottato da tutto il mondo.



Cosa sono

- **TLS o SSL:** attraverso una tecnica asimmetrica (metà della password è pubblica, metà è personale) permette di avere i tre requisiti basi di crittografia nella rete: autenticazione, integrità dei dati e confidenzialità; in sintesi: funziona bene ed è veramente sicuro.

**A cosa server tutto
questo**



Blockchain

A cosa serve tutto questo

È difficile spiegarlo con 2 parole a tutti, ma è la base del funzionamento di quasi tutto (l'accesso a un sito web, l'uso dell'email, il funzionamento di WhatsApp, ecc...) ed è l'inizio della sicurezza informatica.

Quindi la vera domanda è "chi non usa queste cose?"

Se abbiamo appreso i concetti sopra, allora possiamo proseguire. Quanto sopra è il mantra delle blockchain, dell'email, di WhatsApp, di TikTok e di molti altri servizi.

Reti *particolari*





Blockchain



Questo concetto è usato da molte tipi di reti che usano internet per raggiungere i PC.

Di seguito alcuni casi dove vengono usate le tecnologie viste in precedenza.

Si tratta di un'esposizione non esaustiva. Lo scopo è di dare consapevolezza della trasversalità di molte parti delle tecnologie delle blockchain e delle criptomonete.

Reti Scientifiche





Reti Scientifiche

In molti casi le reti scinetifiche usano vaste reti di computer, anche PC dei singoli utenti-ricercatori per i loro scopi. In questo specifito caso d'uso abbiamo 2 aspetti da getire:

- dati dello stesso esperimento o dello stesso evento distribuiti a molti per essere elaborati. I risultati devono seguire rigorosamente l'ordine temporale della rilevazione dello stesso evento;
- dati dello stesso evento, ma rilevati da osservatori diversi in momenti diversi. E' il caso tipico dell'osservazione astronomica dove telescopi diversi osservano lo stesso evento in orari diversi sulla terra (es: una supernova vista dai satelliti, poi dall'osservatorio in Messico e dall'osservatorio in Cina).

Reti di Supercalcolo





Reti di Supercalcolo

Una costola specifica dell'ambito scientifico è il supercalcolo.

In questi casi è necessario che i singoli nodi ed i singoli computer non solo condividano le loro capacità, ma servono alcune funzionalità specifiche delle blockchain come le firme temporali, identificatori univoci, verifica di integrità dei dati, ecc...

Reti Bancarie





Reti Bancarie

Le stesse tecnologie servono alle reti bancarie per gli ordini che emettono, che ricevono, per la quotazione nell'istante dell'ordine, per la riservatezza assoluta della disposizione, per l'ordine, la totale riservatezza dello stesso e per un log delle attività a *prova di manomissione*.

Reti delle Borse





Reti delle Borse

Quanto sopra descritto riguarda anche le piazze di scambio come le borse, dove è particolarmente critico il time stamp, la sicurezza delle informazioni ed il numero di operazioni. Infatti una Borsa produce e riceve centinaia o migliaia di ordini al secondo.

Reti P2P



Blockchain

Reti P2P

Nate come declinazione di una tecnologia di riservatezza, hanno avuto grande notorietà per l'attività illecita che le contraddistinse: trasmissione-ricezione di file illeciti.

Come si immaginerà le componenti tecnologiche adottate permettono la criptazione totale dei dati, la certezza dei nodi di partenza e quello di destinazione, la duplicazione sicura dei dati nei nodi, la disponibilità asincrona dei dati e la totale confidenzialità e anonimicità delle connessioni.

Reti Dark Web





Reti Dark Web

Queste tecnologie sono note ai più per le finalità illecite che perseguono (es. vendite proibite).

A onor del vero a volte permettono attività lecite, ma proibite per motivi ideologici o politici (cf. libertà d'informazione in Cina o in Afghanistan) permettono di riprendere la libera aggregazione e la libera discussione.

Opportunità e Problemi



Opportunità e Problemi

A conclusione di questo excursus vediamo alcune caratteristiche che creano valore aggiunto o disvalore.

- 1.** In primo luogo sono tecnologie molto più presenti nell'ordinario di quanto si pensi
- 2.** I benefici riguardano svariati aspetti dell'ordinario a iniziare dalla sicurezza e il contrasto della perdita d'informazione
- 3.** Queste tecnologie possono essere una buona scelta per potenziare, securizzare e sistemare le reti di controllo di sistemi strategici come centrali elettriche, dighe, sistemi di pompaggio acque, ecc...



Opportunità e Problemi

- 4.** Un primo aspetto negativo, però, riguarda la grande quantità di dati *aggiuntivi* che vengono generati e che occupano molta parte della rete e molto spazio sulle memorie
- 5.** Altro aspetto (purtroppo non ancora adeguatamente affrontato) sono tecnologie molto energivore: consumano tanta corrente!
- 6.** sono reti LENTE

Opportunità e Problemi

7. Infine dobbiamo dire che sono tecnologie complesse, soprattutto se assemblate come nel caso delle blockchain. Ciò significa che non sono per tutti, servono tecnici e ingegneri qualificati, serve avere aziende capaci di costruire l'hardware, il software e capaci di garantire il mantenimento, la ricambistica e lo sviluppo.

Conclusione





Conclusione

Tutti abbiamo di fatto in mano uno o più pezzi delle tecnologie che costruiscono le blockchain e le criptomonete.

Danno diversi benefici, ma compensano adeguatamente il fatto che sono molto energivore e di elevata complessità?

Vedremo, nella prossima lezione, in quali altre soluzioni troviamo queste tecnologie e se riescono a compensare i problemi energetici e la complessità o se li amplificano.

Domande?

Questions?

Stefano Bortolato

dsb005

Informatica Blockchain

Reti di alta sicurezza

Roma 25/6/2023

3



