

OPEN INNOVATION



Le caratteristiche principali delle blockchain

Dalla trasparenza alla resilienza sino all'affidabilità



DI VINCENZO GERMANO*

Facendo seguito al precedente articolo (si veda *Il Giornale dell'Ingegnere* n. 1/2024, ndr.), l'avvento delle *blockchain* segna una svolta significativa nell'evoluzione tecnologica: ne abbiamo visto brevemente alcune fasi quando dal 1991 alcuni ricercatori svilupparono un metodo per contrassegnare dei *record* digitali in modo che le persone non potessero più manometterli, fino ai giorni nostri, in cui la nascita delle criptovalute ha permesso l'evoluzione odierna della tecnologia delle *blockchain*. Per quanto il termine è diventato un sinonimo di criptovaluta, in realtà i due non sono la stessa cosa; sono sicuramente strettamente correlati ma la storia delle *blockchain* ha radici ed evoluzioni che si estendono oltre le criptovalute, permettendo una continua espansione delle sue applicazioni. Oltre alle due caratteristiche fondamentali analizzate, ovvero la decentralizzazione e la sicurezza, ne possiamo approfondire ulteriori come la trasparenza, la resilienza e l'affidabilità.

LE CARATTERISTICHE PRINCIPALI

Riprendendone brevemente il concetto chiave, una *blockchain* possiamo vederla come una forma di registro digitale distribuito e decentralizzato che registra transazioni in modo sicuro e trasparente attraverso una rete di nodi interconnessi, con una struttura di base composta da blocchi di dati collegati tra loro in modo crittografico, a formare

una catena immutabile. Perciò, semplificando, è un *database* digitale immutabile, trasparente e decentralizzato, con il quale vengono registrate transazioni in modo che chiunque possa vederle ma nessuno può modificarle. Sulla base di tale concetto esemplificato, com'è facile immaginare, la **resilienza e l'affidabilità** rappresentano due pilastri fondamentali di tale tecnologia, dovendone garantire la sicurezza e l'integrità (ad esempio di transazioni) in un ambiente digitale sempre più complesso e soggetto a minacce. Il primo dei due concetti deriva dalla loro struttura distribuita e decentralizzata; infatti, a differenza dei sistemi centralizzati, dove un singolo punto di fallimento può compromettere l'intero sistema, le *blockchain* sono progettate per essere robuste e resistere a guasti e attacchi malevoli. Questo presuppone che ogni nodo della rete ha una copia del registro completo, rendendo difficile per gli aggressori manipolare i dati senza il consenso della maggioranza dei nodi. In aggiunta, la distribuzione dei dati su molti nodi aumenta la resistenza agli attacchi informatici: infatti, anche se alcuni di essi vengono compromessi, la rete nel suo complesso continua a funzionare in modo affidabile, garantendo che le transazioni possano essere validate e registrate in modo sicuro.

Inoltre, esistono protocolli *software* specifici che richiedono ai nodi della rete di raggiungere un accordo sulla validità delle transazioni prima che possano essere aggiunte alla catena. Ciò impedisce a un singolo parteci-

pante di imporre transazioni fraudolente o dannose alla rete, proteggendo l'integrità del sistema nel suo complesso.

Dal punto di vista dell'affidabilità, questa viene garantita attraverso il concetto di immutabilità dei dati. Una volta che una transazione è stata registrata in un blocco e aggiunta alla catena, diventa permanentemente parte del registro e non può essere modificata o cancellata. Questo assicura che la cronologia delle transazioni rimanga intatta nel tempo, consentendo agli utenti di verificare l'autenticità e l'integrità dei dati. La comunità che orbita attorno alle *blockchain* continua a sviluppare nuove tecniche e soluzioni per mitigare questi rischi e rafforzare la sicurezza del sistema.

Passando oltre e considerando la **trasparenza** delle *blockchain*, essa consente agli utenti di accedere e verificare in modo aperto e affidabile le informazioni registrate sulla rete. Questa caratteristica distintiva contribuisce a promuovere la fiducia e la responsabilità tra gli attori coinvolti, garantendo che le transazioni e i dati siano visibili e accessibili a tutti i partecipanti d'interesse. Tutto ciò deriva dalla loro struttura decentralizzata e distribuita: infatti, ogni nodo della rete ha accesso a una copia completa del registro delle transazioni, consentendo agli utenti di verificare l'autenticità e l'integrità dei dati in qualsiasi momento. Questo modello elimina la dipendenza da intermediari centralizzati e offre una visione completa e imparziale delle attività sulla rete. Inoltre, la trasparenza è supportata dalla natura immutabile dei dati registrati, questo perché

una volta che una transazione è stata aggiunta alla catena, diventa permanentemente registrata e non può essere modificata o cancellata retroattivamente. Tale aspetto assicura che la cronologia delle transazioni rimanga pubblicamente accessibile e verificabile nel tempo.

L'aspetto della trasparenza delle *blockchain* ha molteplici vantaggi, primo tra tutti in ambito finanziario: ad esempio, consente agli investitori di monitorare e tracciare le transazioni finanziarie in modo trasparente e in tempo reale. Nel settore della catena di approvvigionamento, offre una visibilità completa sul percorso e sull'origine dei prodotti, consentendo di identificare eventuali problemi o irregolarità lungo il processo di produzione e distribuzione.

Inoltre, la trasparenza promuove la responsabilità e l'equità. Tutti i partecipanti alla rete hanno accesso alle stesse informazioni, eliminando la possibilità di manipolazione o discriminazione da parte di terze parti, favorendo una maggiore trasparenza e responsabilità nell'esecuzione di transazioni e contratti digitali. Tuttavia, è importante notare che la trasparenza può anche sollevare questioni legate alla *privacy* e alla riservatezza dei dati. Mentre le transazioni stesse sono pubblicamente visibili, le identità degli utenti possono essere protette attraverso l'uso di pseudonimi o indirizzi crittografici. Gli sviluppatori di *blockchain* stanno continuamente esplorando nuove soluzioni per bilanciare la trasparenza con la protezione della *privacy* degli utenti. Un

esempio applicativo potrebbe essere il garantire la trasparenza e l'integrità delle elezioni utilizzando una *blockchain* pubblica e trasparente. Ogni voto verrebbe registrato come una transazione, consentendo ai cittadini di verificare autonomamente i risultati e garantendo che nessuna manipolazione possa avvenire senza il consenso della maggioranza dei nodi della rete.

Un altro esempio potrebbe essere la *privacy* nei sistemi sanitari digitali: infatti, utilizzando una *blockchain* privata e sicura, è possibile gestire in modo riservato le informazioni sanitarie dei pazienti. Ogni paziente potrebbe avere il controllo completo delle proprie informazioni, consentendo loro di condividere selettivamente dati con fornitori di assistenza sanitaria autorizzati senza compromettere la *privacy* o la sicurezza delle informazioni.

CONCLUSIONI

In conclusione, tra le altre caratteristiche, la trasparenza, la resilienza e l'affidabilità sono elementi chiave che definiscono il potenziale e l'impatto delle *blockchain* nell'ambito digitale, promuovendo la fiducia, la responsabilità e l'equità. Tali fondamentali caratteristiche svolgono un ruolo cruciale nel plasmare un futuro digitale più sicuro, trasparente e innovativo per tutti gli utenti.

***INGEGNERE ELETTRONICO E VICECOORDINATORE COMMISSIONE INNOVATION & PROJECT MANAGEMENT DELL'ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI TORINO**