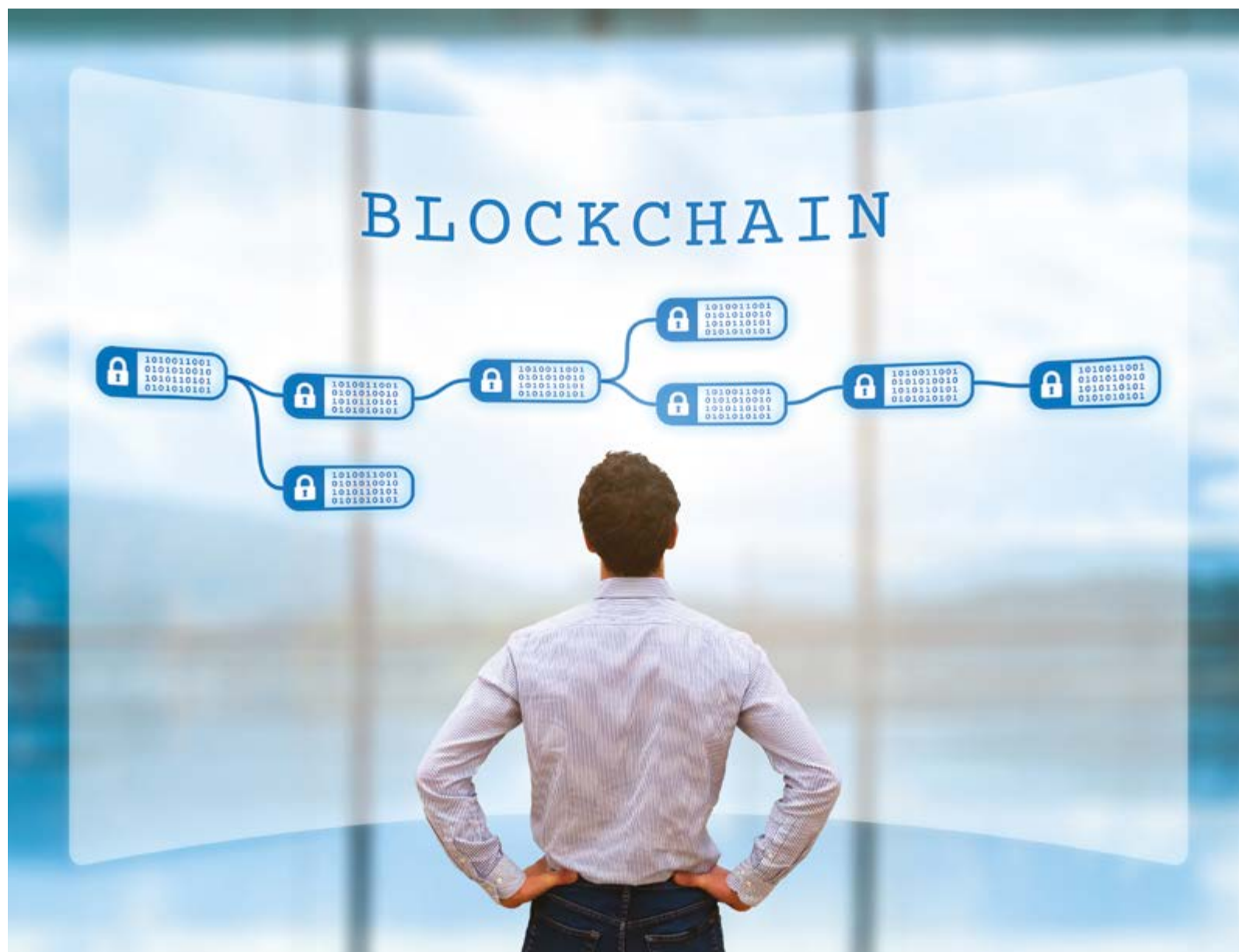


OPEN INNOVATION



La rivoluzione digitale delle blockchain

Storia, caratteristiche e applicazioni, con uno sguardo al futuro



DI VINCENZO GERMANO*

L'avvento delle *blockchain* segna una svolta significativa nell'evoluzione tecnologica e, per quanto siano nel pieno della loro evoluzione digitale, la loro storia ha radici lontane. Un primo esempio di tecnologia rudimentale che gettò le basi per esse nacque nel 1991 dai ricercatori Stuart Haber e W. Scott Stornetta, che svilupparono un metodo per contrassegnare dei *record* digitali in modo che le persone non potessero più manometterli. A tale scopo vennero archiviati i documenti a formare "un blocco in una catena protetta grazie alla crittografia". Successivamente, nel 1992, riuscirono ad aggiungere la funzionalità di traccia temporale che gli permise di archiviare più documenti in un blocco. Tuttavia questo sistema non venne mai utilizzato e il brevetto passò inosservato fino a scadere nel 2004; tutto ciò fin alla nascita delle criptovalute, che hanno poi permesso l'evoluzione odierna della tecnologia delle blockchain.

Di sicuro il momento più significativo nella storia delle blockchain risale al 2008, quando, sotto lo pseudonimo di Satoshi Nakamoto (un individuo o un gruppo di persone), venne presentato al mondo il concetto di *bitcoin*, os-

sia una valuta digitale basata su una tecnologia innovativa chiamata *blockchain*, con l'obiettivo di creare un sistema di pagamento *peer-to-peer* (da punto a punto) senza la necessità di intermediari. Questa idea ha dato il via a una rivoluzione che ha superato i confini delle criptovalute per influenzare diversi settori.

Per quanto il termine *blockchain* sia 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. Le blockchain hanno attraversato diverse fasi di evoluzione, a partire dal debutto con i *bitcoin* fino alle molteplici applicazioni e raffinamenti tecnologici che caratterizzano il suo panorama attuale. Infatti, inizialmente si focalizzavano principalmente sulla gestione delle transazioni finanziarie, tuttavia la comunità tecnologica ne ha rapidamente compreso il potenziale al di là delle criptovalute, spingendo gli sviluppatori a esplorare nuove possibilità. Uno tra gli esempi chiave che può essere citato è stata l'introduzione dei "contratti intelligenti", ossia codici *software* autonomi che eseguono automaticamente e applicano le clausole di un contratto quando

vengono soddisfatte determinate condizioni. *Ethereum*, lanciato nel 2015, è stato il pioniere di questa innovazione, aprendo la strada a una vasta gamma di applicazioni decentralizzate (*DApps*) e contratti intelligenti. Prima di ulteriori esempi o applicazioni, approfondiamone il concetto.

CARATTERISTICHE E APPLICAZIONI

Partendo dal concetto, possiamo considerare la *blockchain* 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.

Una delle caratteristiche fondamentali è la **decentralizzazione**, che, a differenza dei sistemi centralizzati dipendenti da "un'autorità centrale", consente alla blockchain di operare su una rete di nodi indipendenti, con un "potere decisionale" e gestione dei dati distribuiti tra numerosi nodi partecipanti alla rete anziché concentrati in un'unica posizione.

Infatti, ogni nodo ha una copia del registro completo e partecipa al processo di consenso per validare nuove transazioni (grazie all'implementazione del consenso distribuito, dove i nodi della rete devono concordare sulla validità delle transazioni). Questo rappresenta un cambio di paradigma cruciale, trasformando il modo in cui concepiamo l'autorità, la sicurezza e la fiducia nelle transazioni digitali. La sua adozione continua a plasmare il panorama tecnologico, aprendo la strada a nuove opportunità e modelli di *business* innovativi.

Un altro aspetto rilevante è la **sicurezza**, che viene garantita attraverso l'uso di algoritmi crittografici. Questo è uno degli aspetti più critici poiché deve garantire la protezione dei dati e delle transazioni in un ambiente distribuito e decentralizzato. In prima istanza sia le transazioni che i dati immagazzinati nei blocchi sono crittografati, rendendo estremamente difficile per chiunque manipolarli senza la chiave crittografica corretta. Ciò contribuisce a garantire l'integrità e la confidenzialità dei dati. Una volta che una transazione (o dati) è registrata in un blocco e aggiunta alla catena, diventa praticamente impossibile modificarla retroattivamente. Questo concetto di immutabilità è essenziale per garantire l'integrità della crono-

logia. Alcuni protocolli software specifici di consenso distribuito sono progettati per garantire che la maggioranza dei nodi nella rete sia d'accordo sulla validità delle transazioni. In tal modo si riescono a prevenire attacchi malevoli in cui un singolo partecipante cerca di introdurre dati falsi nella catena. La natura distribuita delle blockchain rende più difficile attuare attacchi come avviene in un sistema centralizzato, perché gli attaccanti devono compromettere la maggioranza della rete per avere successo.

Oltre alle criptovalute, la blockchain ha dimostrato il suo valore in svariati settori: alcuni esempi sono la gestione della catena di approvvigionamento, per offrire una tracciabilità completa e la possibilità di verificare l'autenticità di prodotti; nel settore finanziario, per facilitare trasferimenti di denaro internazionali più rapidi ed economici, eliminando gli intermediari grazie a contratti intelligenti (utilizzati per automatizzare accordi legali); nel campo della sanità, per migliorare la sicurezza dei dati e semplificare la condivisione di informazioni tra gli attori coinvolti.

IL FUTURO

Il futuro delle blockchain è molto promettente e intrinsecamente collegato all'innovazione tecnologica continua, soprattutto in un contesto di scalabilità e consumo energetico. Esse stanno stimolando la ricerca di soluzioni più efficienti mediante nuovi algoritmi che richiedono meno risorse. Non solo, l'integrazione con altre tecnologie emergenti, come l'intelligenza artificiale e l'internet delle cose (*IoT*, *Internet of Things*), è destinata a creare sinergie importanti. Basti pensare alla possibilità che le blockchain vadano a facilitare la condivisione sicura e l'analisi dei dati tra dispositivi *IoT*, garantendo al contempo la *privacy* e la sicurezza.

CONCLUSIONI

La blockchain è una tecnologia che partendo dai *bitcoin* si è evoluta in una forza catalizzatrice per l'innovazione in svariati settori. Grazie alla sua capacità di fornire sicurezza, trasparenza e decentralizzazione sta aprendo la strada a una vasta gamma di applicazioni, alcune delle quali stiamo appena iniziando a esplorare. Mentre affronta sfide e cresce in complessità, continua a plasmare il panorama tecnologico, promettendo di essere un elemento chiave nella trasformazione digitale globale.

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