quella "catena magica" *che cambierà il mondo*

di Giuseppe Fusto

Blockchain: una parola che ultimamente è sulla bocca di tutti, e campeggia sulle prime pagine dei giornali e sugli altri media. Ma di che cosa si tratta esattamente? E soprattutto, perché questa tecnologia/filosofia di "database distribuito" è destinata a rivoluzionare anche il settore dei servizi?

Non solo bitcoin. Certo, la più famosa delle criptovalute ha fatto un po' da "cavallo di Troia".

Una tecnologia? Meglio, una "filosofia"

Ma la vera rivoluzione non è tanto nelle monete virtuali, quanto nella tecnologia-filosofia di scambio e validazione dati che vi sta alla base: la cosiddetta blockchain, letteralmente "catena di blocchi". Ormai una parola diffusissima sui media, sulla rete e nel tam tam quotidiano: ma che cos'è esattamente? E soprattutto, perché potrebbe arrivare, in tempi brevissimi, a rivoluzionare anche il settore dei servizi?

Un esempio per cominciare

Partiamo da un esempio, uno dei più banali: quando accediamo al nostro conto in banca da pc o smartphone, vediamo dei dati: saldo, transazioni, bonifici, pagamenti, accrediti, ecc. Dati che, in un sistema tradizionale, sono in qualche modo in possesso dell'istituto di credito. Stessa cosa, che so, per i dati relativi alla nostra situazione sanitaria (pensiamo ai siti degli ospedali). O scolastica, o contributiva, pensionistica e così via. Tutte informazioni che, banalmente, stanno in un contenitore protetto, ma comunque in possesso di un soggetto "garante". Ma chi mi assicura che, in un giorno di ordinaria follia, qualcuno non acceda a modificare i dati? O ancora, quanto costa all'ente o all'impresa un sistema di sicurezza e protezione dati tanto rigido? In alternativa ci potrebbe essere il sistema dei cloud, tipo Drive per intenderci. Ma qui la soluzione sarebbe addirittura peggiore del problema: infatti in questo modo i dati sarebbero modificabili da chiunque, con i risultati che ben possiamo immaginare.

Impossibile bluffare

E qui entra in scena la blockchain, che altro non è che un database criptato e diffuso (distributed ledger) su talmente tanti computer distribuiti in tutto il mondo da creare una catena (chain, appunto) praticamente immodificabile. Anzi, è stato calcolato che è fisicamente impossibile intervenire su un solo dato, perché bisognerebbe intervenire su tutti i blocchi, insomma su tutti gli anelli della catena. Insomma, sarebbe come se due soggetti si scambiassero 10 euro davanti a milioni di persone che guardano: impossibile bluffare. In parole semplici stiamo parlando di un registro aperto e distribuito che può registrare le transazioni tra le parti in modo efficiente, verificabile e permanente. Per questo utilizzo, questo database sfrutta una rete peer-to-peer che si collega ad un protocollo per la convalida dei nuovi blocks.

I passaggi

Con l'aiuto del sito www.blockchain4innovation.it, uno dei siti più aggiornati e completi, davvero ricchissimo di informazioni sulla nuova tecnologia e sui suoi ambiti applicativi, cerchiamo di addentrarci nel funzionamento minuto del sistema. Anche in questo caso vale la pena avvalersi di un esempio concreto. Immaginiamo che due soggetti debbano effettuare una transazione: ad esempio Marco vende un immobile a Giovanni. A questo punto nasce la necessità di gestire una transazione commerciale tra due soggetti. Il primo passaggio è creare una transazione costituita da una serie di elementi come l'indirizzo pubblico del ricevente, le informazioni relative alla transazione e le Cryptographic Key. Nel no-

stro esempio la transazione comprende le informazioni sull'immobile, sul prezzo, sulla disponibilità economica dell'acquirente Giovanni, sull'effettiva proprietà dell'immobile da parte di Mario ed eventuali altre informazioni necessarie a completare il quadro di riferimento per la vendita e per l'acquisto. In preparazione vengono realizzate le Cryptographic Keys dei due soggetti coinvolti nella transazione. A questo punto la transazione entra a far parte di un Blocco di Transazioni: infatti allo scopo viene creato un nuovo Blocco con tutti i dati relativi alla transazione e con i dati relativi all'immobile e alla disponibilità economica del compratore.

Dalla transazione al blocco, dal blocco alla catena

Il blocco, che comprende anche altre transazioni, viene preparato per essere sottoposto alla verifica e all'approvazione dei partecipanti alla blockchain. E qui sta il vantaggio del sistema di validazione: la transazione viene portata in rete per essere verificata da parte dei partecipanti alla blockchain, vale a dire che il Blocco che comprende la transazione in oggetto, unitamente ad altre transazioni, viene verificato e approvato dalla rete blockchain. Il modello si basa sulla combinazione tra firma digitale e marca temporale (Timestamp): la prima garantisce che mittente e destinatario di un qualsiasi tipo di messaggio siano identificati in modo certo, il secondo permette che un insieme di messaggi, validato con la marca temporale da parte di un nodo scelto casualmente da un robusto modello matematico, venga comunicato e scritto nel registro di tutti gli altri nodi della rete e reso irreversibile.

Il processo di validazione

Il processo di validazione prevede una fase di verifica e di approvazione basata su risorse di calcolo che vengono messe a disposizione dai partecipanti e che sono finalizzate alla risoluzione di problemi complessi o puzzle crittografici e che permettono di disporre di un consenso distribuito e non più di un consenso basato su un intermediario terzo o su un ente o istituzione centralizzata. Coloro che partecipano alla risoluzione del problema e che dunque concorrono alla validazione del processo e della transazione sono chiamati "miner" e il loro intervento viene remunerato attraverso l'emissione di una moneta virtuale o cryptocurrency. A ciò si deve aggiungere che i nodi non sono pubblici, ovvero non si conoscono fra loro e il Proof of Work rappresenta anche il modo per costruire un rapporto di fiducia basato sulla concreta collaborazione alla soluzione delle prove che devono essere validate.

Il blocco si aggiunge alla catena

Una volta verificato, il blocco si aggiunge alla catena, ed ecco che si crea la blockchain. Il nuovo blocco viene aggiunto alla catena di blocchi che forma la blockchain, è accessibile a tutti i partecipanti ed è nell'archivio di tutti. Diventa il riferimento permanente, immutabile e immodificabile di quella specifica transazione. La transazione è completata ed è archiviata su tutti i nodi della blockchain: se le informazioni sono considerate corrette la transazione viene autorizzata, validata ed effettuata. A quel punto la transazione entra a far parte di un nuovo blocco che viene creato e che comprende anche questa transazione.

Impossibile tornare indietro…

Niente di così fantascientifico, almeno in teoria: il segreto è che una volta registrati, i dati in un blocco non possono essere retroattivamente alterati senza che vengano modificati tutti i blocchi successivi ad esso, il che necessiterebbe il consenso della maggioranza della rete. Gli inizi, che risalgono esattamente a dieci anni or sono, hanno un'aura magica e leggendaria: il primo blockchain distribuito fu concettualmente idealizzato da una persona o un gruppo di persone identificate sotto lo pseudonimo di Satoshi Nakamoto nel 2008. Fu implementato l'anno successivo come componente fondamentale dei bitcoin dove viene applicato come libro contabile per tutte le transazioni, proprio perché questo modello consentiva di garantire l'infinita riproducibilità di un bene digitale.

Una filosofia trasversale

Ma, e qui viene il bello, la filosofia della blockchain (perché di questo, in effetti, si tratta) supera l'ambito della valuta digitale per estendersi a moltissime altre potenziali applicazioni praticamente in tutti i settori. Sì, perché in effetti la possibilità di scambiarsi dati in modo sicurissimo ed economico fa gola a tutti: finanza e istituti bancari possono avere la possibilità di transazioni sicure e decentralizzate, così come le assicurazioni, che potranno prevenire frodi e gestire meglio numerose operazioni; senza contare IoT e Industria 4.0, che di scambio di dati continuo vivono.

Dalla sanità al retail

Ma ci sono anche altri ambiti meno evidenti e tuttavia altrettanto centrali nella vita di tutti i giorni. Pensiamo alla sanità: gestire i dati medici dei pazienti attraverso un sistema condiviso permetterebbe ai medici di condividere informazioni sui pazienti in maniera sicura e veloce, e quindi aiuterebbe molto la medicina e la sanità a migliorare il servizio fatto ai pazienti, con la possibilità di avere sotto controllo l'intera cartella clinica di un paziente, e quindi di conoscere in anticipo la storia del paziente, in modo da somministrare cure migliori e in tempi più rapidi. E si tratta, come è facile immaginare, di dati sensibili da proteggere con la massima sicurezza. Un discorso analogo si potrebbe fare per la PA in generale: la tecnologia blockchain potrebbe infatti aiutare la Pubblica Amministrazione e i cittadini ad avere una vera identità digitale, condivisa e implementata in questo sistema, con diversi vantaggi tra cui: rendere più difficile l'evasione fiscale, avere un controllo maggiore dei cittadini e quindi combattere la criminalità, servizi semplificati in tutti i settori della Pubblica Amministrazione (invio di dati semplificato), e molto altro. E che dire del settore retail? Proprio mentre stanno aprendo i primi super e ipermercati senza cassa, gli attuali metodi di pagamento in negozio potrebbero usufruire della potenzialità delle catene di blocchi, assicurando operazioni ancora più rapide, sicure ed economiche.

Trasparenza fra produttore e consumatore

A proposito, già che ci siamo: la blockchain aumenterà la trasparenza nei rapporti tra produttore, distributore e consumatore sui prodotti stessi (e non solo sulle transazioni commerciali), perché grazie alla tecnologia della catena di blocchi sarà possibile conoscere la storia, lo stato e le prestazioni di un prodotto: informazioni sulle modalità di produzione, su come è stato trasportato, come è stato conservato e lo stato di qualità in qualsiasi momento. E qui ci avviciniamo a un ambito che ci è più familiare, perché di fatto l'idea della tracciabilità dei dati, della loro sicurezza, immediatezza e immodificabilità non lascia fuori nemmeno i servizi di pulizia, manutenzione e, più in generale, facility management.

Anche nel Facility management

Non è un caso che, recentemente, fra i sette "top trends" 2018 individuati da QSI Facilities per il FM ci sia proprio, accanto a IoT e Vr, la tecnologia blockchain che, come dice testualmente la società americana: "Quest'anno rivoluzionerà il settore del facility management dando la possibilità di realizzare anche i sogni più selvaggi (sì, c'è scritto proprio wildest!)". Il perché è presto spiegato: i manager del facility sapranno in tempo reale cosa è successo, quando è successo, perché e cosa bisogna fare per aggiustare il tiro e risolvere i problemi, oltre a prevenire che accadano nuovamente. E ancora, si potrà sapere chi ha scoperto il problema, come l'hanno riportato e che cosa è accaduto da allora. Come si vede, si va ben al di là dell'aspetto delle transazioni economiche. In realtà tutto ciò che accade, e che può essere condiviso sotto forma di dato, può essere impacchettato in un blocco, validato, trasmesso e reso così immodificabile. Del resto, non è forse vero che oggi le informazioni (e la rapidità e la sicurezza con cui vengono recapitate e scambiate) sono un valore? E così la blockchain si potrà integrare all'internet delle cose per creare una sinergia potentissima capace di ridurre drasticamente i tempi di scambio di informazioni e aumentare l'efficienza e l'operatività anche nel nostro settore. Le imprese sono avvisate.

La blockchain per il commercio globale

Per fornire al mercato globale metodi più sicuri ed efficienti grazie anche all'utilizzo della blockchain, Maersk e Ibm, hanno deciso di dare vita, lo scorso gennaio, a una joint venture. In pratica si impegnano a mettere a punto una piattaforma per ridurre le barriere nella filiera internazionale: questo grazie all'utilizzo della blockchain e di altre tecnologie cloud su open standard, dall'intelligenza artificiale all'Internet of Things fino agli analytics, fornite da Ibm Services, per aiutare le società a muovere e tracciare digitalmente le merci a livello globale.