Blockchain per l'industria

NEGLI ULTIMI DUE O TRE ANNI, IL TEMA BLOCKCHAIN È STATO MOLTO ENFATIZZATO, CON ANALISI E RICERCHE DI VARIA NATURA, CON LE AZIENDE CHE INVESTONO, MA NON SI È ANCORA IN UNA FASE DI DIFFUSA APPLICAZIONE DELLA TECNOLOGIA

La tecnologia Blockchain, per quanto accreditata di poter apportare innovazioni rivoluzionarie anche nei processi produttivi (decentralizzazione, trasparenza, sicurezza, immutabilità dei dati) allo stato attuale pare essere più oggetto di attenzione e studio che non di iniziative concrete, e molto c'è ancora da verificare e comprendere. Dopo il nostro focus dello scorso anno su questo tema riprendiamo quindi l'argomento per indagare se vi sono cambiamenti e se iniziano a essere proposte soluzioni e applicazioni.

Alcune note teoriche

Per consentire una migliore comprensione dei concetti esposti da quanti hanno aderito a questo nostro focus, proponiamo alcune note "di base" sulla Blockchain, tecnologia che risale a 2008 quando un gruppo di informatici sviluppò un ecosistema per il trasferimento sicuro di valore senza l'intermediazione di una terza parte, quale può essere una banca, e da questo la nascita della criptovaluta Bitcoin. Il concetto di Blockchain (catena di blocchi) si basa su un'evoluzione del "libro mastro" (ledger), strumento per gestire contabilità, archiviazione dati e transazioni finanziarie. Se le modifiche di questo strumento vedono l'intervento, secondo specifiche linee guida di governance, dell'ente centrale che lo gestisce,

Ledger distribuito e consenso condiviso

Nel mondo Blockchain è decentralizzato secondo l'approccio DLT, Distributed Ledger Technology, cioè distribuito tra tutti i partecipanti, o nodi (computer), di un certo ecosistema Blockchain. Tutti ne possiedono una copia, da cui massima resilienza (la cancellazione di copie non danneggia il sistema né il suo storico), ed è l'intera comunità che può visionarlo, controllarlo, e modificarlo, aggiungendo blocchi di transazioni, ma solo dopo un consenso condiviso. Un certo numero di transazioni avvenute in un dato intervallo di tempo sono raggruppate in blocchi poi aggiunti alla catena. In dettaglio, un blocco contiene il block number, i dati memorizzati nel blocco riferentesi alle transazioni, l'hash del blocco precedente e l'hash di tutte queste informazioni, che sarà poi ripreso nel blocco seguente: a ogni blocco N si fa un hash dell'hash N-1, da cui la nozione di catena, e questa inclusione rende impossibile falsificare i dati rendendo la catena inalterabile in quanto una modifica di un blocco distruggerebbe l'integrità di tutta la catena. Per "hash" si intende un sistema matematico, o algoritmo, che converte un messaggio di lunghezza arbitraria in un codice alfanumerico di lunghezza fissa/prefissata, generandone l'impronta digitale: a partire da un dato in ingresso se ne calcola l'impronta, che poi serve a identificare il dato iniziale in modo univoco e irreversibile.

Elevati consumi energeti con il Proof of Work

Come detto, tutte le nuove transazioni devono essere validate prima di essere accettate, con i partecipanti di una Blockchain che devono poter valutare e concordare su tutte le aggiunte prima che siano permanentemente incluse nella catena di blocchi. Il processo di validazione prevede una fase di verifica basato su risorse di calcolo messe a disposizione dai partecipanti che si pongono tra loro in competizione, assumendo il ruolo di "miner", per risolvere problemi complessi o puzzle crittografici; il primo miner che risolve il problema validando la transazione riceve dall'ecosistema una remunerazione che nel caso Bitcoin consiste in Bitcoin appositamente creati o "mined", da cui, appunto, la denominazione di "miner". I meccanismi di consenso condiviso prevedono metodologie diverse basate su specifici algoritmi, tra cui Proof-of-Work (PoW, tipico del Bitcoin), Proof-of-Stake (PoS), Delegated Proof-of-Stake (DPoS) e PBFT (Practical Byzantine Fault Tolerance o tolleranza a errori arbitrari, o bizantini). La metodologia PoW consiste di base nel calcolare la hash del blocco che il miner vuole validare, a partire dai dati del blocco e da un "nonce" (number used only once), stringa casuale utilizzata nel processo di hashing di un blocco; viene usato un nonce diverso per ogni tentativo di hashing al fine di soddisfare il target richiesto nel processo di mining. Nel caso Bitcoin, per esempio, ogni due settimane la rete definisce un target minimo per l'hash, e tutti i valori al di sopra del target sono rigettati, quelli al di sotto accettati. La definizione del target si basa su un "aggregate computational power": più sono i miner, più basso il target e più difficile trovare l'hash adatto.

I nodi delegati e il Proof of Stake

Concretamente si devono calcolare molti hash facendo variare il nonce per trovarne uno compatibile con le esigenze, e questo non significa risolvere un puzzle, ma far uso di vera e proprio "forza bruta", perchè un puzzle fa intuire l'esistenza di riferimenti, mentre qui serve solo grande potenza di calcolo, da cui enormi consumi di energia e anche rallentamento nella creazione dei blocchi. Nel Proof-of-Stake partecipano al consenso quanti hanno una particolare presenza nella Blockchain, per esempio chi ha più investito. Nel Delegate PoS vi sono dei nodi delegati a rappresentare gli altri partecipanti: i delegati sono eletti dalla rete con un sistema di "democrazia rappresentativa" dei consensi, che hanno un peso che è funzionale alla quantità di criptomoneta o più in generale di "token" posseduti dai votanti.

Necessità di meccanismi di consenso più agili

Il caso PBFT è per certi versi bizzarro, almeno in prima lettura, anche se tecnicamente il riferimento è al problema informatico su come raggiungere consenso in situazioni in cui è possibile la presenza di errori. Come esempio concettuale al di fuori del contesto Blockchain si potrebbe considerare l'ambientazione Cloud Computing, dove i server messi a disposizione degli utenti potrebbero episodicamente dover far fronte a errori arbitrari, quali cadute temporanee di rete, trattamento di messaggi corrotti o arresti inopinabili, e occorre che fornitori e utenti possano accordarsi su una qualità di servizio attesa. La denominazione "errori bizantini" nasce poi da una scelta informale dalla comunità informatica che rimanda al caso di generali bizantini che devono decidere se attaccare o ritirarsi come ordinato da un comandante superiore, ma un generale potrebbe essere un traditore e confondere gli altri comunicando ordini discordanti da quello impartito dal co-

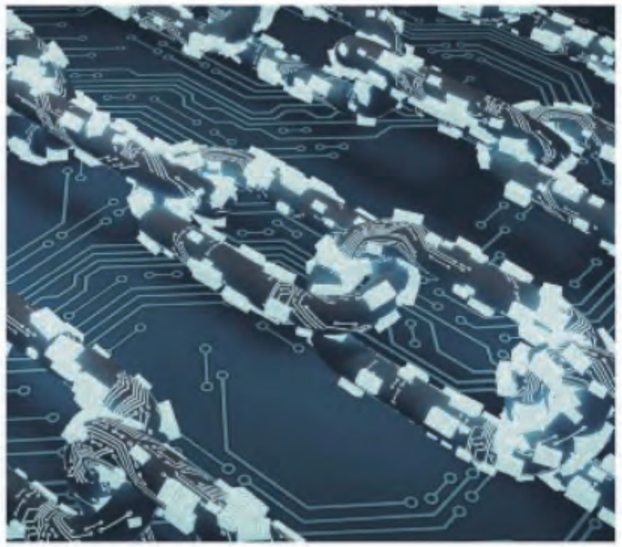
mandante. Da aggiungere il Closed Consensus, che non prevede mining ma dove ad alcuni nodi è chiesto un certo deposito a garanzia per partecipare all'aggiornamento della Blockchain, e questo meccanismo sta crescendo in popolarità nei segmenti bancari e assicurativi. E' prevedibile che con la diffusione di Blockchain molte complessità legate al consenso saranno semplificate, senza escludere anche l'uso di una semplice votazione di base.

Blockchain permissionless e permissioned

Da sottolineare che esistono diverse tipologie di Blockchain: pubblica, privata e ibrida. La prima tipologia è una rete completamente decentralizzata senza permessi di accesso (Permissionless, Bitcoin come esempio), dove chiunque può partecipare al processo di consenso e diventare "miner". Una Blockchain pubblica prevede meccanismi di consensom lenti ma comunque è più veloce degli attuali meccanismi di controllo delle transazioni finanziarie. Le Blockchain private (Permissioned, per ambientazioni business tradizionali), sono attivate da singole imprese o gruppi di aziende per creare un contesto comune per scambi confidenziali e in sicurezza, con il ruolo di verificatore svolto, in funzione del tipo di governance, dall'autorità che ha attivato quella Blockchain; è l'azienda stessa che scrive e verifica le transazioni, da cui una maggiore velocità rispetto allle catene pubbliche, con la possibilità di poter anche definire chi può avere accesso in lettura alle transazioni, innalzando il livello di privacy. La tipologia ibrida, in parte pubblica e in parte privata, è riferibile per esempio a un consorzio, con il processo di consenso controllato da un numero fisso di nodi, operando quindi sotto la leadership di un gruppo, non di una singola entità.

Una diffidenza verso Blockchain legata alla rapidità del suo sviluppo

Simone Milli, Consulente Europeo i marchi, disegni e modelli, di Bugnion.



Indispensabile cautela nel lanciare progetti

In conclusione di queste note, alcune considerazioni di prospettiva rese recentemente disponibili dalla società di consulenza e analisi di mercato Gartner, in cui si afferma che per quanto Blockchain continui a essere una "parola d'ordine" forte, con aziende che continuano a investire, da qui al 2023 la maggior parte (quasi il 90%) delle iniziative dedicate specificatamente alla gestione della supply chain rallenteranno a causa di una carenza di risultati apprezzabili. Attualmente molti progetti hanno come focus il potenziamento di tracciabilità, visibilità dei flussi e verifica di autenticità, ma non si sono completamente sviluppati per mancanza di riferimenti standard. Inoltre le aziende non sono in grado di identificare specifici casi d'uso ad alto valore su cui puntare, da cui il lancio di più trial per poter trovare un'applicazione in grado di garantire valore. Questo non nega certo il valore che Blockchain può apportare ai processi, ma suggerisce una cautela sottolineando anche che probabilmente la tecnologia non ha il carattere pervasivo che le si attribuisce, e va valutata con attenzione a seconda del contesto. Lasciamo ora la parola a chi ha aderito al nostro focus.

Un'opinione su Blockchain

La nostra prima domanda lascia senz'altro spazio ad ampie considerazioni: Cosa ne pensate di Blockchain?

La prima opinione su Blockchain ci è stata sottoposta da Simone Milli, Consulente Europeo in brevetti, marchi, disegni e modelli, oltre che professore a contratto nel corso di Laurea del Design Industriale dell'Università di Bologna, della società Bugnion, tra le prime società in Europa per consulenza in proprietà industriale e intellettuale. "Blockchain è sicuramente una tecnologia molto interessante", premette Milli, "in questo momento già matura per importanti utilizzi industriali e per poter lavorare anche con elevate quantità di dati e tempi di attesa di scrittura e lettura dati ridotti".

Competizione tra soluzioni Blockchain diverse

Il contesto iniziale di utilizzo, principalmente legato al mondo delle criptovalute (laddove la tecnologia è nata), si è infatti ora allargato ed esteso al mondo dei processi industriali. In questo momento, l'ecosistema del settore Blockchain è piuttosto ampio, e non pare ancora emersa una specifica tecnologia Blockchain, fra le numerose esistenti, che abbia preso il sopravvento, per caratteristiche tecniche e/o dimensioni raggiunte della comunità di supporto. "Il modello che si è imposto nel settore", conclude Milli, "è quello della convivenza, naturalmente competitiva, fra differenti soluzioni tecnologiche di Blockchain, le une anche estremamente differenti dalle altre per caratteristiche tecniche. Il livello di conoscenza di base della tecnologia fra i non addetti ai lavori in questo momento è piuttosto buono: segno che la tecnologia ha avuto una risonanza e una diffusione importante in questi ultimi anni".

(CONTINUA A PAGINA 36)

Serve tempo per la Blockchain nei processi produttivi

Paolo Moro, Amministratore unico di Business Research, azienda che si occupa di tecnologie innovative al servizio delle imprese, considera Blockchain come un nuovo strato tecnologico che si aggiunge al complesso mondo già esistente. "Si tratta di una tecnologia interamente costruita dal basso e quindi ci vorrà del tempo perché sia compresa e perché possa essere implementata nei sistemi in produzione. Più o meno come internet negli anni ottanta. Quel nuovo che avanza e non si conosce deve prima essere digerito, sperimentato, capito e integrato".

Crescono le minacce informatiche per la Blockchain

Per Morten Lehn, General Manager Italy di Kaspersky Lab, il business delle tecnologie Blockchain ha avuto un rapido sviluppo negli ultimi anni: basta pensare al mercato delle criptovalute che costituisce oggi una quota significativa dell'economia globale. "Anche se in origine la Blockchain è stata considerata come una tecnologia pretamente sicura, ora abbiamo diverse testimonianze di minacce e di vari rischi per la sicurezza informatica. Negli ultimi due anni, gli esperti di Kaspersky Lab si sono imbattuti in fenomeni di phishing, come l'individuazione di copie di un popolare sito web per ICO, Initial Coin Offering, in attacchi mirati a società di scambio di criptovalute, in adware progettati per il furto di criptomoneta e in altri vettori di attacco".

Una tecnologia da digerire, sperimentare, capire e integrare

Paolo Moro, Amministratore unico di Business Research.

Le prospettive di Blockchain per l'industria

La tecnologia Blockchain è sempre più accreditata di poter apportare innovazioni rivoluzionarie anche nei processi produttivi. E' realistico ipotizzare un trasferimento delle logiche delle transazioni finanziarie, da cui sono nati gli ecosistemi Blockchain, al mondo dei processi di produzione o quantomento, dato che molto se ne parla, alle applicazioni Internet of Things?

Milli (Bugnion) ritiene che Blockchain sia oggi, ancora più di ieri, un termine di grande attualità, sia nel mondo industriale che in quello accademico. Se è vero che in questo momento ci sono molti progetti in studio e anche progetti implementati (si pensi alla filiera della tracciabilità delle merci e dell'anticontraffazione laddove, appunto, esistono numerosi progetti Blockchain-based), è altrettanto vero che c'è ancora una naturale diffidenza verso l'investimento in questo settore, soprattutto da parte di aziende il cui "core business" è di tipo tradizionale. "La naturale diffidenza verso questa tecnologia che ho riscontrato non è tanto legata all'affidabilità di questa tecnologia, che non è più in discussione, ma è invece più legata alla rapidità del suo sviluppo, e alle numerose varianti di "distributed ledger" in circolazione".

Per gli investimanti manca uno scenario ben definito

Infatti, prosegue Milli, le sorti di ciascuna Blockchain, per esempio Ethereum, Corda, Ripple, e altre ancora, sono inscindibilmente legate all'adozione e al mantenimento nel tempo da parte di una rete di computer distribuita del software necessario al funzionamento dei nodi. In altre parole, le sorti di ciascuna specifica Blockchain, cioè la sua sopravvivenza nel tempo, sono legate alla crescita e allo sviluppo della sua comunità di supporto, che è costituita da sviluppatori, miner e utenti. Lo scenario di estrema mutevolezza di queste comunità pone l'imprenditore dell'azienda tradizionale in una situazione di incertezza, in cui si rimandano gli investimenti in attesa di uno scenario più definito. In altre parole, il rischio che vedono alcuni imprenditori è quello di investire oggi in una specifica Blockchain che potrebbe non esistere più nei prossimi anni, fagocitata da una Blockchain differente e più performante. "Lo scenario attuale in cui si trova la Blockchain nel mondo industriale è quindi quello della forte selettività: l'euforia e l'entusiasmo iniziale è oramai esaurito e si portano avanti progetti industriali in cui la tecnologia ha in effetti un forte e percepito valore nel contesto in cui viene implementata, e per cui il rapporto rischi/benefici è certamente a favore di questi ultimi".

Nel Fintech il vero business della Blockchain

Moro (Business Research) ci ricorda che la Blockchain nasce per transazioni economiche: vi sono sono molti progetti che ne potenziano le funzionalità ma non ci si deve dimenticare che il vero motivo per cui è nata riguarda soprattutto lo scambio economico. Di fatto tutti i progetti oggi decollati che fanno vero business (in Italia e nel mon-

(CONTINUA A PAGINA 38)

Nuovi servizi per le aziende che implementano tecnologie Blockchain

Morten Lehn, General Manager Italy di Kaspersky Lab.

do) con la tecnologia Blockchain sono progetti Fintech, termine che, stando all'Osservatorio Fintech & Insurtech del Politecnico di Milano, si riferisce a tutte le innovazioni digitali in ambito finanziario, a prescindere dall'attore che eroga il servizio, quindi attori tradizionali come banche e istituti di credito ma anche attori emergenti come Startup e Big Tech, cioè i big del mondo tech quali Google, Apple, Microsoft, Facebook.

"Portare la possibilità di effettuare una transazione economica all'interno di un dispositivo IoT significa dargli la possibilità di completare il percorso di automazione anche amministravo/economico. Pensiamo per esempio a un robot che applica tappi di plastica nelle bottiglie, Quando stanno per finire i tappi potrà comprarne direttamente di nuovi approvvigionandosi automaticamente. Diamo alle macchine il compito di ordinare attraverso un wallet personale che potrà essere ricaricato a distanza come un centro di costo. In questo caso la chiave privata che permette di creare la transazione potrà essere applicata direttamente al robot che diventa padrone della scelta di comprarsi la materia prima per funzionare. Il prossimo passo della macchine per l'industria sarà questo: gestire il processo finanziario per poter funzionare autonomamente. Pagheranno la bolletta elettrica in base ai consumi, i ricambi in caso di manutenzione, etc. La macchina sarà venduta con un wallet ricaricabile che le permetterà di continuare a vivere".

Lavori in corso

Avete iniziative di studio o di valutazione della tecnologia Blockchain, se non addirittura applicazioni implementate nelle vostre soluzioni?

Secondo Milli (Bugnion) il mondo della proprietà industriale, che è del resto l'ambito in cui il nostro interlocutore opera, è storicamente tradizionalista, ovvero è un settore in cui la tecnologia entra con un certo ritardo rispetto ad altri settori.

Tutelare i progetti in ambito Blockchain

Di questo mondo fanno parte numerosi attori, che collaborano necessariamente per permettere la tutela della proprietà industriale: gli studi privati, gli avvocati, gli Uffici Brevetti e Marchi nazionali e regionali, e i loro fornitori. Quello che sta recentemente accadendo è che gli Uffici Brevetti regionali, principalmente l'EPO, European Patent Office, che si rivolge a cittadini e imprese per fornire procedure di applicazione uniformi in materia di protezione dei brevetti in 38 Paesi europei, e l'EUIPO, European Union Intellectual Property Office, che gestisce i diritti sui marchi, disegni e modelli europei, stanno svolgendo numerose attività formative, tra cui convegni e congressi in tema di Blockchain, sintomo di un forte interesse su questa tematica spinto principalmente dagli utenti finali cioè dalle aziende che sviluppano progetti Blockchain-based. "Il fatto che gli Uffici Brevetti si stiano muovendo nella direzione di formare internamente gli Esaminatori e di diffondere cultura a livello di sistema la dice lunga: certamente la tecnologia Blockchain fa già parte del mondo della proprietà intellettuale industriale. Certamente il nostro ruolo di professionisti del settore IP ci impone di essere al passo con i tempi e di essere informati in materia per poter seguire i nostri clienti anche su questo fronte. In questo senso, anche la nostra società ha da tempo avviato iniziative interne di formazione e sensibilizzazione in materia dei propri professionisti, affinché gli stessi siano pronti per tutelare i progetti dei clienti anche in ambito Blockchain".

Sicurezza per le aziende con la Blockchain

Moro precisa che la sua azienda, Business Research, sta lavorando su Lightning Network, il secondo layer del protocollo Bitcoin per poter effettuare transazioni in millisecondi senza fee di spesa, sempre garantendo la disponibilità attraverso i canali nelle Blockchain principali. "Di fatto il prossimo step è rendere la tecnologia plug & play per permettere la distribuzione veloce e facile". Kaspersky Lab, sempre impegnata a sviluppare innovative soluzioni di sicurezza, ha sviluppato, come sottolinea Lehn, alcuni nuovi pacchetti di servizi progettati per le aziende che operano implementando tecnologie Blockchain e nell'ambito dell'economia delle criptovalute. Il pacchetto su misura per le aziende comprende Application Security Assessment (per aiutare i proprietari di scambi di criptovalute a rilevare bug critici e ad affrontarli prima che causino danni), Penetration Testing (per l'individuazione di eventuali punti deboli all'interno dei sistemi), User Account Takeover Prevention (rilevamento di eventuali accessi ai portafogli degli utenti da parte di malintenzionati), protezione dal phishing, funzionalità di Incident Response e Cybersecurity Awareness Training. "Oltre a questi servizi, Kaspersky Lab fornisce anche la protezione dalle frodi e dal riciclaggio di denaro per quanto riguarda scambi di criptovalute e per il rilevamento degli attacchi mirati". ■