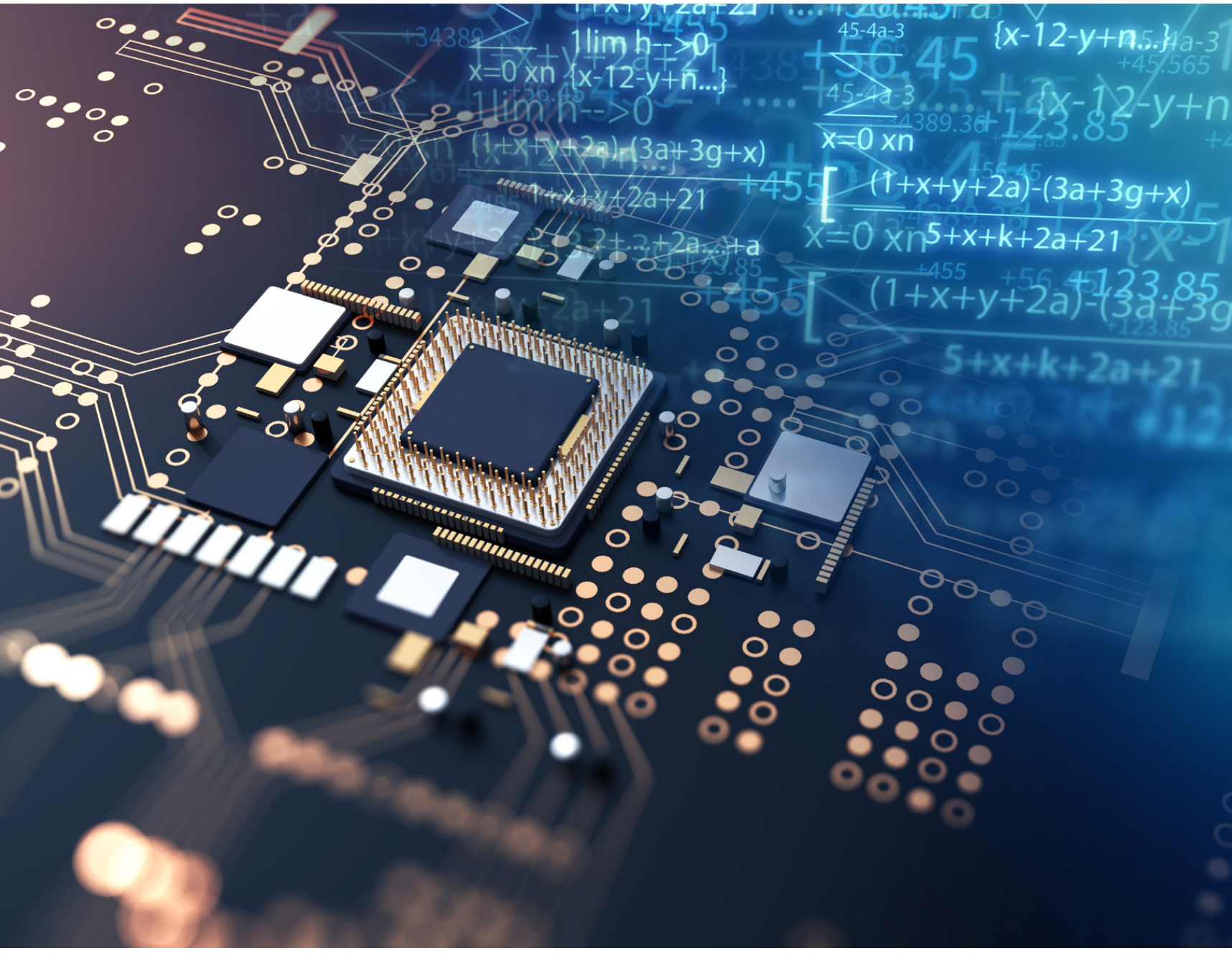
Blockchain per l'industria

…ovvero, come utilizzare al meglio una delle tecnologie informatiche più coinvolgenti e più alla moda degli ultimi anni, applicabile anche al mondo dell'industria elettronica

a cura di DM Management & Consulting



La blockchain è una tecnologia sempre più al centro dell'attenzione e, sebbene non sia più una novità, rimangono ancora molti dubbi e domande a cui dare una risposta. Come alcuni sapranno, la prima blockchain decentralizzata è stata concettualizzata nel 2008 da una persona (o più probabilmente da un gruppo di persone) nota come Satoshi Nakamoto. Questa tecnologia, quindi, esiste già da parecchio tempo sebbene il boom lo stia vivendo soltanto in questi ultimi tempi. Coloro che non sono "addetti ai lavori" spesso ne sanno poco, non sono a conoscenza dei suoi vantaggi e quali possono essere le criticità di questa tecnologia. Spesso la parola Blockchain viene associata alle criptovalute, tuttavia non è propriamente così e il perché verrà analizzato in questo articolo.

La definizione di Blockchain

La parola blockchain nasce dall'unione di due parole "block" e "chain", che in italiano si possono tradurre come "catena di blocchi", ed è il termine stesso che definisce la tecnologia. Quindi questa catena di blocchi che cos'è?

I block sono anche conosciuti come nodi, i quali sono collegati tra loro e formano una rete peer-to-peer, più o meno come la rete internet che ci risulta molto più familiare. La differenza con il web è rappresentata dal legame che c'è tra questi nodi, poiché non sono "centralizzati" non essendoci è un nodo centrale che gestisce e trasferisce le informazioni. In sostanza questi nodi sono "decentralizzati" e sono in grado di comunicare senza la necessità di avere un nodo centrale. Un'altra caratteristica principale è che i nodi sono crittografati e questo permette loro di comunicare in modo sicuro. Essi vengono utilizzati per registrare le transazioni o i dati su molti computer in modo tale che qualunque blocco fra quelli coinvolti nell'operazione non possa essere modificato retroattivamente. Di conseguenza, nel caso si volesse effettuare una modifica retroattiva, verrebbero alterati tutti i blocchi successivi. Inoltre, la catena di blocchi sfrutta le caratteristiche di una classica rete informatica e ciò permette di gestire e aggiornare in modo sicuro un registro comune. Il registro comune contiene dati, transazioni e informazioni e questo spiega il perché non è necessario un nodo centrale per il controllo e la verifica delle operazioni.

Per meglio comprendere il concetto di rete e operazionalità in riferimento alla blockchain possiamo suddividere la tipologia di rete in tre parole e successivamente fare un esempio pratico:

Rete aperta: la rete si definisce aperta quando i nodi che ne fanno parte sono in grado comunicare tra loro e verificare in qualunque momento lo stato del registro. Rete aperta significa anche che chi è esterno alla rete può consultare, ma non modificare, il registro delle operazioni.

Rete condivisa: in questo caso sono i nodi a condividere lo stesso registro e ne comunicano i propri movimenti all'interno della rete. Come per la rete aperta, tutti coloro che sono esterni alla rete possono visionare il registro.

Rete distribuita: i nodi non sono controllati da un'entità centrale con la differenza sostanziale che possono essere distribuiti in qualsiasi parte (del mondo).

Una volta identificate le tipologie di rete, immaginiamo ad esempio il caso di una persona (che chiameremo A) la quale vuole inviare un documento a una persona chiamata B. Riguardo al funzionamento della Blockchain, A non manderà il file originale del documento; tuttavia, B riceverà

La blockchain non è ormai più nel periodo sensazionalistico condito da annunci, news e iniziative di progettazione in quanto è entrata nel quotidiano. Questo significa che è iniziata la fase applicativa

comunque una copia documento. La copia del documento è passata attraverso un nodo centrale che lo ha codificato e smistato inviandolo da A a B. A trasmissione avvenuta, A e B avranno un file contenente il documento e ciò significa che il documento è stato duplicato. Se si parla di file o informazioni da trasmettere questa modalità è perfetta, tuttavia, cosa succede se A dovesse inviare a B una somma di denaro? Per ovvi motivi B non potrà mai ricevere una "copia" del denaro, bensì dovrà ricevere ciò che viene chiamato valore. La blockchain viene indicata anche come internet del valore, il che implica un trasferimento vero e proprio e non una duplicazione come avviene per i documenti o i file. A questo punto A ha una sua chiave di accesso privata, e attraverso essa entra nel registro e inserisce il movimento di denaro da mandare a B. Per convalidare il trasferimento, i nodi presenti nella rete devono accettare l'inserimento di A nel registro affinché B possa ricevere il denaro. I nodi che validano l'operazione sono i nodi della rete ad esclusione di A e B e svolgono il compito che dovrebbe eseguire un nodo centrale: confermano che quel movimento è valido e autentico. In questa fase del processo si applica il tema della tecnologia "decentralizzata" e il registro comune viene aggiornato secondo regole e criteri stabiliti dall'intera rete.

Tipologie di Blockchain

La Blockchain si divide in pubblica, privata e ibrida. Va considerato che il mantenimento economico della blockchain dipende dal sistema che è in essa integrato e da come sono impostate e regolamentate le commissioni per ogni operazione.
La Blockchain pubblica è la tipologia più utilizzata poiché risulta quella più sicura da un punto di vista legato alla privacy. Le reti sono aperte e chiunque può farne parte gestendo un nodo della rete. Non vi è alcuna restrizione, anche se ciò, a seconda dell'ambito in cui la blockchain opera, potrebbe rappresentare una lama a doppio taglio. Chiunque può visionare e modificare il registro e ha a disposizione in modo trasparente tutti i dati. La blockchain pubblica è una rete decentralizzata, pertanto non esiste una entità centrale che gestisce e regola i movimenti, bensì sono i nodi-validatori che confermano e validano i movimenti del registro.
La Blockchain privata è un ecosistema in cui è presente un centro di controllo, che nella maggior parte delle volte coincide con il fornitore della blockchain, e rispetto a quella pubblica ha un accesso limitato da autorizzazione degli altri nodi che compongono la rete e l'accesso al registro è privato.
La Blockchain ibrida è unmix tra pubblica e privata ed è caratterizzata proprio dalla differenza relativa alle due precedenti tipologie. La blockchain ibrida è nata successivamente allo scopo di risolvere i limiti e le criticità di pubblica e privata. Anche in questo caso l'accesso è consentito previa autorizzazione dei nodi presenti nella rete, il registro è pubblico, quindi chiunque può vedere le informazioni registrate. È parzialmente decentralizzato, al fine di garantire maggiore trasparenza e privacy.

Blockchain in azienda

È innegabile che la Blockchain è entrata a far parte dei processi di numerose aziende, le quali la utilizzano per effettuare operazioni di invio documenti, file, come anche lo scambio di denaro. Sono infatti le proprietà di immutabilità e trasparenza della Blockchain che permettono alle aziende di registrare dati, documenti e operazioni in modo tale che per visione e verifica siano a disposizione di altri attori dell'ecosistema o di attori terzi. Ad esempio, il timestamping di un documento viene effettuato attraverso la blockchain per verificare l'autenticità della data di creazione e rendere immodificabile il documento nel tempo. La maggiore trasparenza viene quindi assicurata da registri consultabili e dati immodificabili.

Criticità

Le criticità della blockchain sono sostanzialmente la scalabilità, la privacy, l'autoreferenzialità e naturalmente l'aspetto energetico. Vi è un problema di scalabilità poiché la quantità di movimenti, transazioni e operazioni varie che la blockchain è in grado di gestire sono inferiori ai sistemi in vigore. Per quanto riguarda la privacy, sebbene sia vero che ogni identità è assicurata da codici alfanumerici, nelle reti aperte chiunque può consultare i registri pubblici e può venire a conoscenza che quel dato codice alfanumerico ha eseguito varie operazioni e verso quali nodi. L'autoreferenzialità è un'altra criticità della blockchain, poiché essa può funzionare soltanto come un ecosistema dove sono presenti diversi attori. Nell'ambito aziendale, si può utilizzare la blockchain per garantire che il proprio prodotto sia autentico e creato a regola d'arte, tuttavia, se i validatori sono attori dell'azienda stessa, la validazione diventa autoreferenziale e quindi il concetto di decentralizzazione viene meno. Ultimo e non meno importante è l'aspetto energetico; è oramai noto che i data center hanno la caratteristica di essere sistemi energivori. Ogni transazione eseguita attraverso la blockchain richiede un elevato consumo di energia elettrica, richiesta che con il proliferare delle reti non può far altro che crescere esponenzialmente.

La prima blockchain decentralizzata è stata concettualizzata nel 2008 da una persona (o più probabilmente da un gruppo di persone) nota come Satoshi Nakamoto

Conclusioni

La blockchain è una tecnologia oramai applicata a più ambiti e settori; rispetto a qualche anno fa abbiamo potuto notare che la blockchain non è più nel periodo sensazionalistico condito da annunci, news e iniziative di progettazione in quanto è entrata nel quotidiano. Questo sta a significare che è iniziata la fase applicativa. •••