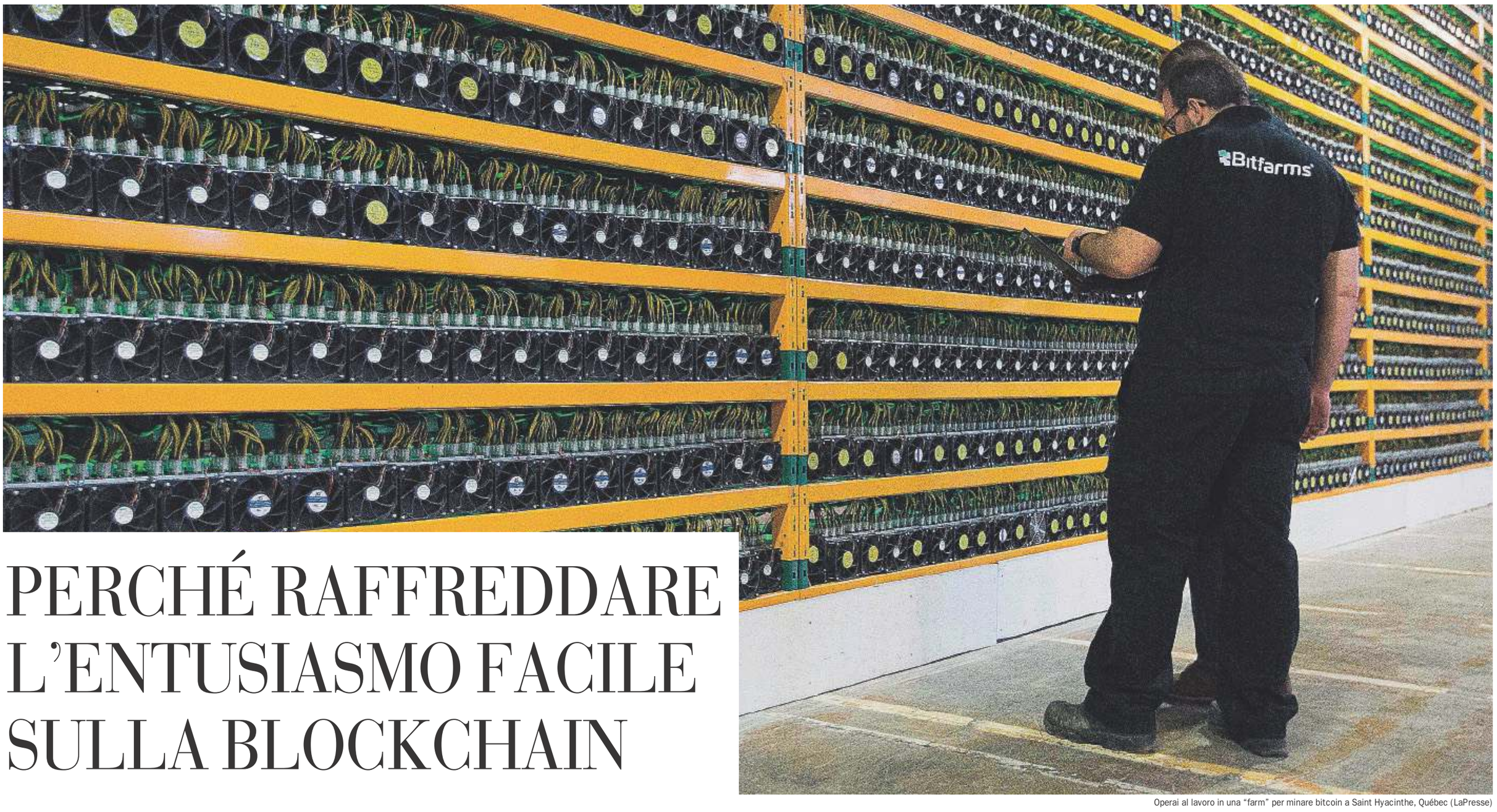
op-ed



Operai al lavoro in una "farm" per minare bitcoin a Saint Hyacinthe, Québec (LaPresse)

PERCHÉ RAFFREDDARE L'ENTUSIASMO FACILE SULLA BLOCKCHAIN

Se escludiamo Bitcoin, finora la tecnologia ha generato molto marketing e poca utilità, scrive ***Diego Piacentini****. Ci saranno sviluppi in futuro, ma per ora chi vuole usare la blockchain per tutto, specie nei servizi pubblici, si faccia delle domande*

Blockchain è una tecnologia dal potenziale dirompente ma è anche una parola di moda e abusata. Fatta eccezione per le criptovalute, non è oggi la scelta ottimale per molti dei possibili campi di utilizzo per problemi tecnologici e di efficienza. Il termine viene spesso sfruttato per scopi di marketing, come quelle aziende quotate in Borsa che hanno cambiato la ragione sociale aggiungendo blockchain al solo scopo di far salire il valore delle loro azioni o quelle catene di supermercati che vogliono usarla per tracciare "la filiera del pollo" al consumatore. Altre volte il termine viene usato commercialmente in maniera impropria per descrivere prodotti che in realtà sono basati su tecnologie simili ma più semplici.

La blockchain è un tipo molto particolare di database append-only, ovvero un database nel quale è possibile aggiungere nuove informazioni in coda alle precedenti ma in cui è vietato modificare, cancellare o cambiare ordine alle informazioni inserite in precedenza conservando una storia cronologica e immutabile di transazioni.

La conservazione viene eseguita in maniera distribuita su un numero sufficientemente grande di nodi di computazione gestiti da entità tra loro indipendenti, senza un coordinamento centrale o una terza parte fidata; i partecipanti raggiungono periodicamente quello che viene definito il consenso sul contenuto ufficiale del database attraverso meccanismi crittografici: in un database distribuito ogni nodo della rete detiene una copia indipendente delle informazioni e, per garantire che tutte le copie siano identiche, serve un meccanismo di allineamento e convergenza che possa dirimere, in caso di conflitto tra due copie diverse, quale sia quella valida. Questi processi sono noti come *meccanismi di raggiungimento del consenso*.

Come dimostrato dal position paper *On Scaling Decentralized Blockchains* di IC3, un'iniziativa congiunta di membri di diverse università internazionali per lo studio delle criptovalute, il funzionamento della blockchain è, a oggi, complesso, lento e computazionalmente costoso; si stima ad esempio che sulla rete Bitcoin mondiale sia possibile eseguire meno di dieci transazioni a secondo e mediamente per ogni transazione si devono attendere decine di minuti per il completamento dell'operazione. Oltre che in termini di hardware necessario per sostenere l'infrastruttura, il costo è misurato anche e soprattutto in termini di elevato impatto energetico.

Complessità e inefficienza di queste tecnologia possono essere giustificate in alcuni contesti di nicchia nei quali si vuole che le transazioni siano certificate senza l'intervento di un'organizzazione gerarchica con un decisore ultimo. Nel caso di Bitcoin, nato subito dopo il fallimento di Lehman Brothers nel 2008 e l'inizio della crisi finanziaria mondiale, si voleva realizzare un sistema monetario senza fare affidamento sulle banche e sugli stati.

I sistemi di voto digitale hanno già notevoli criticità, la blockchain è semplicemente troppo immatura

Negli ultimi dieci anni il Bitcoin e le criptovalute hanno acquisito velocemente popolarità, attirando ingenti finanziamenti in ricerca e sperimentazioni, alimentando fenomeni speculativi e generando altissime aspettative. Complici anche innumerevoli articoli e studi autorevoli, la blockchain è stata presentata come una innovazione in grado di rivoluzionare molti settori economici, anche non connessi alle transazioni economiche.

Più recentemente, tuttavia, c'è stata una inversione di rotta, che ha visto la pubblicazione da parte di illustri esperti di studi più critici e consapevoli verso l'abuso di comunicazione sulla blockchain. Ne è un esempio quello di Ferdinando Ametrano, professore dell'Università Bicocca e del Politecnico di Milano, secondo cui la blockchain è utile solo in relazione a Bitcoin. Addirittura, c'è chi, come John Burg dell'US Agency for International Development (USAID), fa notare che, nonostante ingentissimi investimenti, non ci siano ancora oggi applicazioni di successo, o chi, come Peter Alexander, Chief Digital Officer della Digital Transformation Agency del governo australiano, in uno studio giunge a una conclusione ancora più netta per quanto riguarda l'uso della blockchain nei servizi pubblici digitali: "Per ogni uso della blockchain che potresti prendere in considerazione, oggi c'è una tecnologia migliore".

Nelle notizie che leggiamo ogni giorno sulla blockchain, vengono solitamente utilizzate due accezioni del termine, che si rifanno a due possibili campi di applicazione.

Il primo, quello delle blockchain pubbliche (*aperte*), a cui chiunque può partecipare creando un nodo della rete peer-to-peer, ricevendo una copia intera del database e potendo agire sui dati in maniera paritaria rispetto a tutti gli altri partecipanti. Questo è il caso di Bitcoin e di Ethereum. Il secondo, quello delle blockchain private (*permissioned*), nelle quali la partecipazione alla rete è riservata a un insieme controllato di attori, ai quali vengono assegnati anche vincoli sulle modalità di lettura e scrittura dei dati. Questa tipologia richiede un'organizzazione superiore o un coordinamento tra un numero ristretto di enti che definiscono le regole di partecipazione.

Oggi le blockchain pubbliche si reggono solo se c'è un incentivo economico per i gestori dei nodi che devono essere remunerati per i costi. Ne consegue, quindi, che solo il caso monetario (come per i Bitcoin) ha un senso dal punto di vista della sostenibilità economica. Esse, come dimostra l'interessante articolo *Blockchains don't scale. Not today, at least. But there's hope*. di Preethi Kasireddy su Hacker Noon hanno inoltre un problema di scalabilità, ovvero vanno in crisi all'aumentare del volume dei dati scambiati, obbligatoriamente anche memorizzati. Un altro problema è che complicano la coordinazione degli aggiornamenti al software, che occorre applicare periodicamente a tutti i nodi per correggere i bug e stare al passo dell'evoluzione tecnologica, come evidenziato da Adam Frisby, CEO di Sinespace, in un suo articolo per VentureBeat.

Per le blockchain private, invece, i problemi sono soprattutto legati alle inefficienze e ai costi del loro utilizzo come soluzione database, oltre che all'insufficiente stabilità dal punto di vista della cybersecurity. Il vantaggio per eccellenza della blockchain, l'impossibilità di modificare i dati memorizzati, viene reso vano quando si usa questo strumento in un contesto dove uno o pochi attori hanno il controllo sull'intera rete e la gestiscono per tutti gli altri partecipanti.

Problema comune a tutte le tipologie di blockchain, come per tutti i database, è che non viene data alcuna garanzia sulla qualità dei dati contenuti. Garantiscono sì che i dati inseriti siano integri rispetto a ciò che è stato inserito all'origine, ma non che siano anche corretti: se il dato è stato inserito sbagliato alla fonte rimarrà tale. Mano a mano che le difficoltà emergono, molti dei progetti di ricerca su blockchain vengono abbandonati o riconvertiti su tecnologie tradizionali, ma tendono a non perdere il nome "blockchain"!

A mio avviso le soluzioni della blockchain non sono ancora mature a sufficienza per essere adottate su larga scala in sistemi critici come quelli che le Pubbliche amministrazioni usano per trattare i dati dei cittadini.

La funzione principale di ogni stato è fatta di poteri costituiti che creano le regole, le aggiornano e ne garantiscono l'applicazione. Non sembra quindi ottimale, per i servizi pubblici, usare uno strumento che ha come principale vantaggio la rimozione di un controllo superiore e di fatto la negazione delle istituzioni. Sulla scia di questo recente entusiasmo verso la blockchain, si sta incoraggiando l'utilizzo di questa tecnologia in riferimento al sistema di voto. Il voto elettronico presenta dei rischi di sicurezza elevatissimi già con tecnologie ordinarie e consolidate, come hanno dimostrato gruppi hacker *white hat* come il Chaos Computer Club, esponendo delle vulnerabilità. Utilizzare sistemi immaturi e ancora in fase di studio approfondito come la blockchain potrebbe moltiplicare i problemi di sicurezza e creare un target naturale sia per hacker individuali sia per unità di cyberwar organizzate.

I problemi tecnologici, legati a scalabilità e cybersecurity, saranno risolti anche grazie a stati e istituzioni

Questi problemi, legati soprattutto a scalabilità e cybersecurity e figli spesso di una immaturità tecnologica, sicuramente avranno soluzioni future, anche grazie agli interessamenti da parte di stati e istituzioni, come l'Unione europea, che di recente ha allocato 340 milioni di euro, o l'Italia, che ha creato un fondo con una dotazione di 15 milioni e assoldato un gruppo di esperti presso il ministero dello Sviluppo economico.

Prendendo spunto da un accurato articolo di Gideon Greenspan per Coin Center, *Do you really need a blockchain for that?*, si possono elaborare semplici criteri da seguire per decidere se l'opzione blockchain possa essere davvero utile in un progetto:

1. Si vuole creare un database condiviso con altri attori e organizzazioni, e mettere in comune le informazioni che si sta raccogliendo nel database?
2. Si richiede che gli attori del sistema possano scrivere in parallelo sul database?
3. Si ritiene necessario registrare in maniera immutabile tutta la storia delle modifiche impedendo a chiunque (incluso se stessi) di aggiustare o cancellare i valori passati?
4. Si vuole evitare a tutti i costi un intermediario fidato che operi sul database eseguendo comandi per nostro conto?
5. Le transazioni eseguite dai vari attori interagiscono tra loro, creando interdipendenze tra i dati?

Se almeno una delle cinque domande ha ricevuto risposta negativa allora sicuramente si può risolvere il problema con una tecnologia più semplice e con migliori performance rispetto alla blockchain. Se, invece, tutte e cinque le domande hanno ricevuto risposta positiva, la blockchain potrebbe essere una soluzione sensata.

Sono ottimista sulla potenziale estensione della blockchain a nuovi settori, anche perché molti dei problemi esposti verranno probabilmente risolti nel tempo. Ma raffreddiamo gli entusiasmi di chi la vuole usare correntemente ovunque, soprattutto nella Pubblica amministrazione.

(alla stesura di questo articolo ha contribuito Simone Piunno)

Diego Piacentini è stato Commissario Straordinario per l'attuazione dell'Agenda Digitale per la Presidenza del Consiglio dei Ministri pro bono dall'agosto 2016 a ottobre 2018, fondando il Team per la Trasformazione Digitale. Dal 2000 ha ricoperto il ruolo di Senior Vice President International per Amazon per 16 anni. In precedenza ha lavorato per 12 anni in Apple, concludendo come General Manager Europe. Oggi è investitore in numerose startup, membro del CdA e Comitato Esecutivo dell'Università Bocconi, mentor di Endeavor Global, oltre che cofondatore e componente del Board di Endeavor Italia

(Credits foto: PAOLO TRE/A3/CONTRASTO/laif)