COME LA BLOCKCHAIN PUO' DIVENTARE LA CHIAVE DI VOLTA DELLECONOMIA DIGITALE (E DEL MONDO REALE)

Nel 2014, Ibm stimava che gli esseri umani stessero creando ogni giorno 2,5 exabyte di dati, ovvero 2,5 quintilioni di byte di dati, che per la maggior parte venivano archiviati in modo permanente, grazie alle risorse di un'era di Cloud computing in cui l'archiviazione è diventata così economica che distruggere i dati non ha molto senso. Secondo Ibm, questo numero significava che gli esseri umani avevano creato il 90% di tutti i dati accumulati nel corso della storia in solo due anni, e la maggior parte di questi dati era archiviata sui server dei fornitori di servizi Cloud. Oggi, a pochi anni di distanza, il volume di dati, collegati a ogni genere di attività digitale, e non, è ancora più colossale, e lo sarà sempre di più in futuro. Come la loro archiviazione, analisi, applicazione. L'unico modo per proteggere tutti questi dati, e ridurre l'impeto, i danni e le conseguenze degli attacchi che li colpiscono, (attacchi definiti "Cyber", ma dagli effetti molto reali), "è toglierli dai server centralizzati e creare una struttura di archiviazione più distribuita. Il controllo dei dati deve essere rimesso nelle mani di coloro ai quali i dati appartengono, ovvero dei clienti e degli utenti finali dei servizi di Internet", sostengono Michael Casey e Paul Vigna, nel loro libro " La macchina della verità ", ovvero "La Blockchain e il futuro di ogni cosa", come indica il sottotitolo, pubblicato in Italia da FrancoAngeli. E rimarcano: "se gli hacker vogliono i nostri dati, dovranno inseguirci tutti, uno per uno: una prova molto più ardua del semplice compito di trovare un punto vulnerabile in un deposito gigantesco che raccolga tutti i nostri dati, comodamente, in un unico luogo". Per raggiungere questo obiettivo, "dobbiamo adottare il modello della fiducia distribuita", ovvero il meccanismo alla base della Blockchain. La protezione dei dati è cruciale Non si tratta solo di soldi, o di Business e aziende. Che sono già aspetti essenziali. C'è un legame intrinseco tra la sfida di tutelare la Privacy e la sicurezza dei dati. Quando la tutela della Privacy viene meno, come accade spesso, le conseguenze possono essere molto gravi: le persone, oltre che le società e organizzazioni, subiscono furti di denaro e altre risorse, ma anche il sequestro della propria identità e reputazione, sono esposte a ricatti ed estorsioni. "Il furto di identità online è stato correlato con la depressione e perfino con il suicidio", sottolineano Casey e Vigna, "e gli esperti sono convinti che presto conosceremo il cyber-omicidio, quando automobili connesse a Internet e altri dispositivi potenzialmente letali diventeranno gli obiettivi di hacker sicari. I primi omicidi potrebbero addirittura essere già stati commessi: l'ipotesi che la misteriosa scomparsa, nel 2014, del volo Mh370 della Malaysian Airlines sia il risultato di un attacco di hacker contro il computer di bordo del velivolo non è più solo una teoria del complotto". Gli attacchi con richiesta di riscatto del malware noto come WannaCry, durante i quali i dati sanitari dei pazienti di diversi ospedali del mondo sono stati criptati da hacker che chiedevano dei pagamenti in Bitcoin per rilasciarli, hanno colpito un grande numero di strutture sanitarie e altri contesti in cui i dati sono una questione vitale. Sul fronte dell'attività economica, gli attacchi informatici colpiscono molte aziende che pagano un alto prezzo in termini di danni e spese legali, rimborsi agli utenti e investimenti in nuovi sistemi di sicurezza. Spendono sempre di più per costruire Firewall sempre più alti, scoprendo che i loro avversari intanto lavorano a "scale" sempre più alte. "Nodi" individuali, non grandi gruppi "Abbiamo bisogno di un'architettura Hi-Tech adeguata per la nostra sicurezza. E le idee alla base della tecnologia Blockchain possono aiutarci a svilupparla", rilevano i due esperti. Che osservano: "nella struttura distribuita di un ambiente di tipo Blockchain, i partecipanti non dipendono da alcuna istituzione centrale che mantenga delle infrastrutture per la sicurezza informatica, come i Firewall, per proteggere grandi gruppi di utenti. Gli individui, invece che degli "intermediari di fiducia", sono responsabili della conservazione dei propri dati

più sensibili, mentre qualsiasi informazione che venga effettivamente condivisa è soggetta a un processo di elaborazione comune del consenso che ne assicuri la veridicità". È questo il meccanismo che potrebbe rappresentare la chiave di volta per l'economia digitale, e anche per molti aspetti concreti della società e della vita delle persone in futuro.

Bitcoin, blindato e inviolato da 10 anni Le potenzialità di questa idea trovano un primo esempio nel sistema Bitcoin. La sua specifica Blockchain potrebbe anche non essere la soluzione definitiva a questi problemi, ma vale la pena ricordare che, senza ricorrere a nessuno dei classici strumenti di sicurezza informatica centralizzata, come i Firewall, e sebbene in palio ci sia un bottino tentatore pari a centinaia di miliardi di dollari, in valore di mercato della prima e più nota criptovaluta, il registro di funzionamento e sicurezza condivisa che sta al cuore del sistema Bitcoin si è dimostrato, fino a ora, inattaccabile. Essendo fondata sulla solidità del proprio registro, la resistenza del sistema Bitcoin, che dal gennaio 2009 del suo esordio proprio in questi giorni compie 10 anni, fornisce una prova convincente della capacità del suo componente fondamentale di garantire una fiducia distribuita fra gli utenti. E suggerisce che una delle applicazioni più importanti della Blockchain, al di là delle valute digitali, potrebbe essere proprio la sicurezza. Fiducia e sicurezza distribuite Una delle ragioni per cui il Bitcoin è sopravvissuto è il fatto che non lasci agli hacker niente da violare. Il registro pubblico non contiene alcuna informazione identificante sugli utenti del sistema. Cosa ancora più importante, nessuno possiede o controlla il registro. Non c'è una copia "originale". Ogni volta che, dagli utenti stessi, un nuovo gruppo di transazioni in rete viene confermato – i cosiddetti "blocchi" della Blockchain –, viene creata una nuova versione aggiornata dell'intero registro, che quindi viene installata su ogni nodo. Di conseguenza, non c'è nessun vettore centrale da attaccare. Se un qualsiasi nodo della rete viene attaccato con successo, e qualcuno cerca di annullare o riscrivere le transazioni sulla versione del registro di quel nodo "hackerato", i nodi che controllano le altre centinaia di versioni accettate rifiuteranno di includere nei propri aggiornamenti qualsiasi dato proveniente dal nodo violato. Il conflitto tra le molte versioni intatte e l'unica versione manomessa porterà automaticamente a etichettare come inattendibile il nodo "disonesto". La macchina della verità Le diverse tecnologie Blockchain esistenti e applicate a contesti differenti, dalla tracciabilità degli scambi alla verifica delle operazioni, per esempio finanziarie e di pagamenti, hanno gradi diversi di sicurezza, e alcune di esse, note come "private" o "autorizzate", fanno affidamento su autorità centrali, incaricate di decidere dei partecipanti. Il sistema Bitcoin, invece, è basato su un modello distribuito che non prevede approvazioni centralizzate, ma conta sul fatto che i partecipanti siano abbastanza interessati al denaro che possiedono all'interno del sistema per preoccuparsi di proteggerlo. In tutte le versioni della tecnologia Blockchain, a ogni modo, la natura essenzialmente condivisa e reduplicativa dei registri, che fa sì che la memoria comune della " verità " risieda in una molteplicità di luoghi, fonda questa idea decisiva di sicurezza distribuita, per cui il rischio di un collasso è scongiurato dalla "ridondanza". "Non c'è dubbio che convincere delle istituzioni che fino a oggi hanno avuto il mandato di garantire la sicurezza dei nostri dati a cedere il controllo e delegare questo compito a una qualche rete distribuita, priva di qualsiasi autorità riconoscibile e alla quale si possa fare causa se le cose vanno male, sarà una grande sfida", prevedono gli autori di "La macchina della verità". Ma "proprio questo potrebbe rivelarsi il passo più importante da compiere per una maggiore sicurezza dei dati. Certo sarà necessario che queste organizzazioni concepiscano la sicurezza come il prodotto non di complessi sistemi crittografici o di altre protezioni esterne, ma dell'economia, e cioè del rendere gli attacchi così costosi che per nessuno valga più la pena provarci". Casey e Vigna rimarcano: "è evidente che l'economia digitale trarrebbe grandi benefici dalla decisione di abbracciare l'architettura a fiducia distribuita consentita dalle Blockchain, che si tratti semplicemente del Backup dei dati offerto da

un sistema distribuito, o dell'idea più radicale di un sistema aperto, protetto da un rapporto tra costi e benefici molto elevato. Una volta che siamo entrati in questo ordine di idee, emergono nuovi modelli di gestione dei dati, modelli liberatori in quanto sono capaci di restituire il controllo dei dati agli individui che li producono, e di garantire per quei dati una protezione molto maggiore". IoT sì, ma nell'interesse di tutti Anche l' IoT, l'Internet delle cose, è importante non tanto per il fatto che abbiamo abilitato miliardi di dispositivi a eseguire dei calcoli autonomamente, quanto per il fatto che questi dispositivi vengano via via connessi tra loro, così da creare un colosso computazionale infinitamente più grande della somma delle sue singole parti. "Per la società, è un momento non da poco", fanno notare Casey e Vigna: "resta da vedere se questo potenziale sarà sfruttato per il bene delle persone o a loro danno. Se però in queste nuove reti si inscrivesse una macchina della verità robusta, ben congegnata e distribuita, avremmo fatto un grande passo per assicurarci che queste nuove e grandiose macchine virtuali lavorino per l' interesse collettivo ". 0 Shares