17/01/2018

LA STAMPA

Pagina 28

EAV: € 41.279
Lettori: 533.243

Università degli Studi di Perugia: Si parla di Noi

Nella rete "blockchain" non soltanto i bitcoin

STEFANO MASSARELLI


28 TuttoScienze

SCIENZE

Lettera aperta dei ricercatori su «Nature»: «Cambiamo la legge dell'Ue contro gli Ogm»

L'appello

TECNOLOGIA?

Nick Bostrom Filosofo

"Insegniamo un po' di etica alle macchine o l'Intelligenza Artificiale ci sterminerà"

Esce in Italia il saggio "Superintelligenza", monito sui rischi dell'hi-tech senza controllo

Esperimento a Kyoto

I neuroni sintetici leggono nel pensiero

Nella rete "blockchain" non soltanto i bitcoin

Il database potrà sopravvivere alla criptovaluta, con applicazioni dall'Industria alla sanità

Tecnologia2

Più del loro valore di mercato, sempre più oscillante, a rendere grandi i bitcoin è la tecnologia che ne regola l' utilizzo. Ogni transazione di questa criptovaluta viene gestita e registrata in una mastodontica rete organizzata in una catena di «blocchi» - detta «blockchain» - che contiene il database di tutti gli scambi avvenuti in bitcoin, opportunamente protetti da sistemi crittografici. Questo registro completo e inviolabile, democraticamente condiviso, chiamato «distributed ledger», rappresenta una delle più grandi idee informatiche degli ultimi decenni e potrebbe rivoluzionare il settore della finanza, dell' industria e perfino della sanità. Il «distributed ledger» è infatti il libro mastro che tutti attendevano, la cassaforte digitale che non può essere rubata e non ha bisogno di terze parti per essere custodita. «Essendo un registro pubblico distribuito e affidabile può essere utilizzato per molte attività, ad esempio nell' erogazione di servizi pubblici, nella gestione della filiera produttiva o nel tracciare gli scambi d' oro e diamanti», racconta Stefano Bistarelli, direttore del nodo dell' Università di Perugia del Laboratorio Nazionale «Cini» di Cybersecurity, tra i protagonisti delle ricerche sui «distributed ledger». Questa tecnologia rende possibile registrare qualsiasi atto notarile o protocollo oppure tenere traccia di qualsiasi prodotto manifatturiero o alimentare, senza bisogno di strutture centralizzate in cui stoccare le informazioni e con notevoli risparmi. Nei sistemi sanitari, per esempio, la catena di blocchi potrebbe regolare le cartelle elettroniche e le spese sanitarie di ogni assistito, veicolando le informazioni nel rispetto della privacy. «Con il mio gruppo studiamo i potenziali utilizzi della tecnologia di "distributed ledger" per servizi innovativi, che mostreremo in un workshop il prossimo 1° febbraio a Perugia: abbiamo dimostrato che la "blockchain" potrebbe essere utilizzata per implementare un servizio di votazione elettronica sicuro», prosegue Bistarelli. In questo ambito le tecnologie sviluppate dal gruppo italiano prevedono la possibilità di affidare ai votanti dei

«satoshi», le più piccole unità scambiabili di bitcoin, per veicolare le preferenze in forma anonima durante un' elezione. Ma il sistema della «blockchain», basato sul semi-anonimato, può rappresentare anche una copertura per finanziamenti illeciti, riciclaggi di denaro e attività criminali, come dimostrano i mercati illegali che spopolano nel dark web e che prevedono pagamenti con la più nota delle criptovalute. «Le nostre ricerche in questo ambito si concentrano sulle attività del traffico in bitcoin attraverso l' analisi dei Big Data», sottolinea Bistarelli. Se, per esempio, l' utente x acquista un' arma dall' utente y, e quest' ultimo ha eseguito in passato una transazione in una comune attività commerciale che accetta bitcoin, è possibile identificare una cerchia di utenti su cui avviare un' indagine. Inoltre, chi è dedito ad attività illecite tende a ricorrere a sistemi di anonimato, i «mixnet». «Abbiamo avviato un' attività di de-anonimazione delle "mixnet", che rappresentano spesso la base logistica dei commerci illegali», prosegue il ricercatore. A fianco di una febbre da transazioni, quindi, i bitcoin hanno aperto il vaso di Pandora di tante possibile innovazioni, portando, in un triennio, a depositare 2400 brevetti basati sulla tecnologia «blockchain», con circa 1,4 miliardi di dollari investiti. Nel frattempo le banche centrali discutono sulla possibilità di adottare i «cubi» della «blockchain» per creare piattaforme regolate («permissioned»), in cui permettere transazioni in una forma più controllata. Una scelta a favore della sicurezza e contro l' illegalità, che tuttavia manderebbe in fumo il sogno di una moneta libera, nata dalla mente di un informatico ancora sconosciuto all' indomani della grande crisi finanziaria.