

L'informatico: previsti tre requisiti indispensabili e sono sicurezza, scalabilità e decentralizzazione

“Blockchain sì, ma democratica”

Micali, star del Premio Turing: “Così rivoluzionerò le criptovalute”

PERSONAGGIO / 2

STEFANO MASSARELLI

Internet come lo conosciamo oggi non sarebbe lo stesso senza le geniali innovazioni di Silvio Micali, l'informatico italiano inserito nell'Olimpo della crittografia mondiale e unico rappresentante del nostro Paese ad

essersi aggiudicato, in 53 anni di storia, il Premio Turing, vale a dire il «Nobel dell'informatica».

A Silvio Micali si devono i sistemi crittografici che regolano le autenticazioni online, le transazioni economiche e i sistemi di firma digitale. Traguardi che hanno cambiato il volto della società e raggiunti «per gioco», come ama ricor-

dare. Erano gli Anni 80, quando lo scienziato di origine siciliana, oggi docente al Mit di Boston, decise di trasferirsi a Berkeley per un dottorato in informatica, dopo una laurea in matematica all'Università La Sapienza di Roma. Una volta in California, conobbe la ricercatrice israelo-americana Shafi Goldwasser, con cui era solito giocare a poker per

telefono. Fu proprio questo gioco «telefonico» a liberare la loro creatività. «Era necessario un nuovo metodo per crittografare le carte, evitando allo stesso tempo che uno dei due imbrogliasse», ha spiegato al convegno organizzato a Roma dal dipartimento di ingegneria informatica di La Sapienza.

Con il tempo i due ricerca-

tori misero a punto un modello di «crittografia probabilistica», una teoria matematica che ha rivoluzionato il mondo dell'informatica e spianato la strada a un futuro inimmaginabile, oltre che al loro premio Turing. «Fino a quel momento la crittografia era considerata un'arte più che una scienza. Da quell'istante in poi, invece, i sistemi critto-

stro distribuito, organizzato in blocchi - la blockchain appunto - sia potenzialmente in grado di democratizzare moltissimi settori della società, da quello immobiliare a quello finanziario, questa tecnologia necessita di miglioramenti. «La blockchain ha bisogno di tre requisiti: sicurezza, scalabilità e decentralizzazione. Al mondo esistono oltre 2 mila blockchain, ma nessuna soddisfa queste tre caratteristiche assieme». Tra le blockchain imperfette Micali annovera quella della criptovaluta più nota al mondo, i bitcoin, in cui la conferma delle transazioni è regolata da sistemi di calcolo molto complessi, i quali necessitano di enormi risorse computazionali ed energetiche. Questo limite ha fatto sì che l'intero controllo dei bitcoin ricadesse nelle mani di tre grandi consorzi di «minatori» - i «miners» - i quali controllano l'intero mercato.

Da qui l'idea di Micali di creare Algorand, una piattaforma di blockchain alternativa, democratica ed efficiente, capace di consentire transazioni immediate e in completa sicurezza. «Siamo partiti da principi totalmente nuovi per non incorrere negli stessi errori commessi dalle altre blockchain, creando così la prima piattaforma digitale di pagamenti realmente scalabile, sicura e decentralizzata». Algorand, infatti, non prevede alcuna distinzione tra classi di utenti e l'approvazione delle transazioni richiede calcoli semplici ed eseguibili da tutti con un semplice laptop. Per questa ragione la figura del «giurista» che approva le transazioni sono approvate dagli stessi utenti, i quali vengono eletti casualmente in «comitati», a cui spetta il compito di approvare le transazioni.

«La giuria popolare è differente per ogni blocco», dice Micali. Inoltre il sistema è a prova di corruzione, dato che nessuno conosce l'identità della giuria prima che la transazione venga approvata. Forte di queste caratteristiche e di un finanziamento di 66 milioni di dollari ottenuto da venture capital statunitensi, Algorand è pronta a fare il debutto in società con un proprio sistema di criptovaluta e nuovi strumenti volti a eliminare la necessità di intermediari, soprattutto nel settore finanziario. «Uno dei nostri obiettivi è la democratizzazione della finanza. Non ci può essere democrazia senza una finanza realmente democratica». —

© STEFANO MASSARELLI



SILVIO MICALI
È PROFESSORE DI INFORMATICA
NEL LABORATORIO D'INFORMATICA
E INTELLIGENZA ARTIFICIALE (CSAIL)
DEL MIT DI BOSTON

“Ho creato Algorand: si tratta di una piattaforma alternativa, capace di transazioni economiche molto efficienti”

grafici hanno cominciato a far uso di nozioni matematiche sempre più complesse, che persistono anche oggi», spiega. A quel successo Silvio Micali e Shafi Goldwasser aggiunsero l'elaborazione della cosiddetta teoria delle «prove a conoscenza zero», la quale ha fornito la base del linguaggio dei moderni sistemi crittografici che regolano molte attività sul web, dalla prenotazione dei treni fino all'archiviazione delle foto sulla nuvola.

Tuttavia, questi traguardi non hanno alterato la sete di innovazione dello scienziato italiano, oggi impegnato a rendere migliore una delle tecnologie più avveniristiche e allo stesso tempo incomplete: la blockchain. Secondo Micali, sebbene l'idea di un regi-