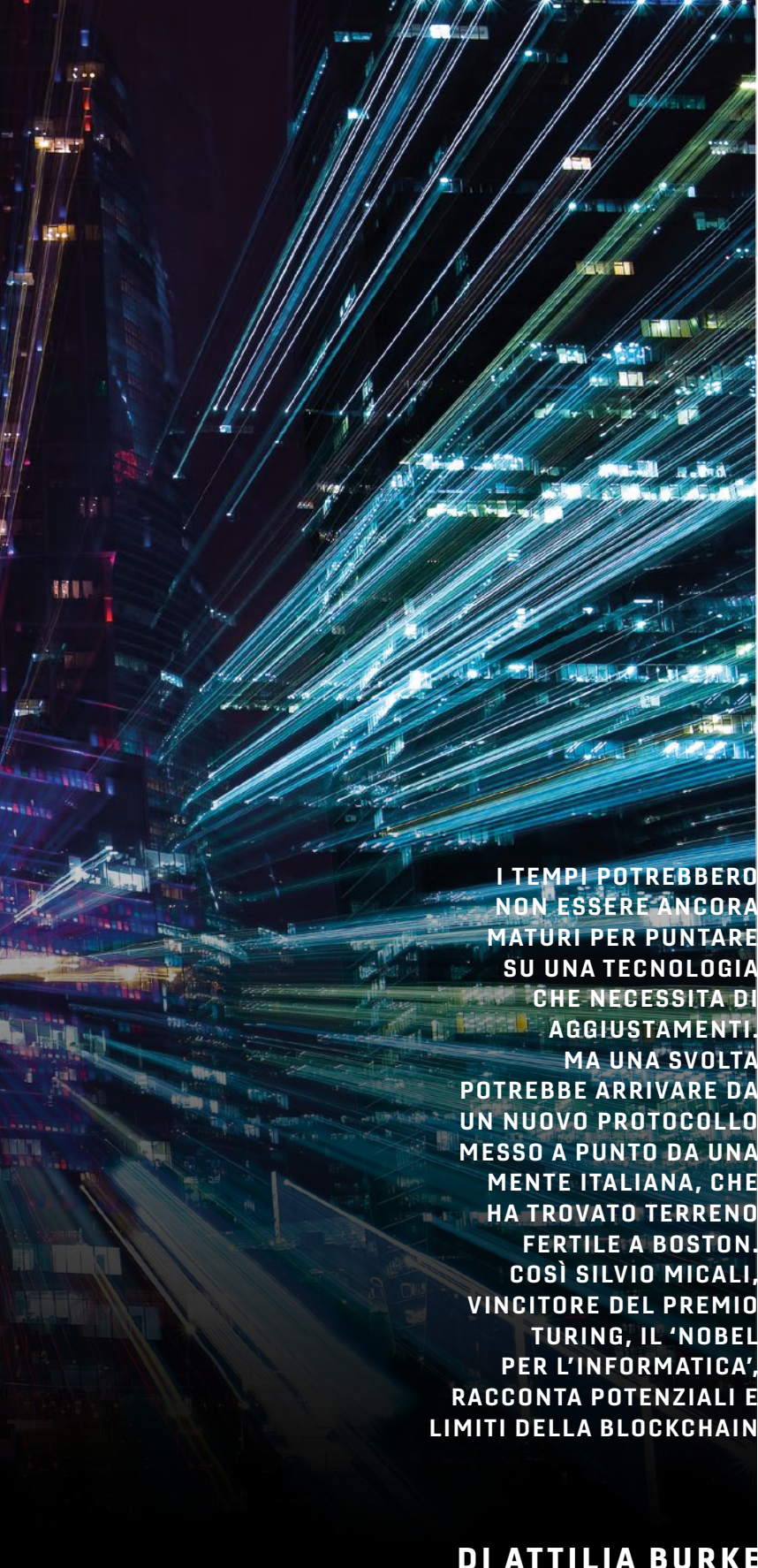




# BLOCKCHAIN (ANCORA) IMPERFETTE



**I TEMPI POTREBBERO  
NON ESSERE ANCORA  
MATURI PER PUNTARE  
SU UNA TECNOLOGIA  
CHE NECESSITA DI  
AGGIUSTAMENTI.  
MA UNA SVOLTA  
POTREBBE ARRIVARE DA  
UN NUOVO PROTOCOLLO  
MESSO A PUNTO DA UNA  
MENTE ITALIANA, CHE  
HA TROVATO TERRENO  
FERTILE A BOSTON.  
COSÌ SILVIO MICALI,  
VINCITORE DEL PREMIO  
TURING, IL 'NOBEL  
PER L'INFORMATICA',  
RACCONTA POTENZIALI E  
LIMITI DELLA BLOCKCHAIN**

**DI ATTILIA BURKE**

# U

**UNA BANCA DATI INALTERABILE**, nella quale sono riposte informazioni indelebili e imm modificabili. Spogliandola di tutti i tecnicismi, questo è ciò che la tecnologia blockchain aspira ad essere, in un mondo ideale. Nell'era dei big data - dove le informazioni sono considerate uno dei beni più preziosi in circolazione, tanto da essere ribattezzate 'oro liquido' - la blockchain dovrebbe essere la 'cassaforte' ideale per contenere questi beni preziosi. Un sistema 'a prova di hacker'. La quinta essenza della sicurezza cibernetica. Ma nel mondo reale le cose non stanno esattamente così. Esiste un gap tra quello che la blockchain aspira ad essere, e quello che è la tecnologia implementata, almeno fino ad oggi. Ne è convinto Silvio Micali, professore al Massachusetts institute of technology (Mit) di Boston e vincitore del premio Turing, il 'premio Nobel per l'informatica'. "Faccio subito disclosure", afferma ironicamente mentre racconta a Fortune Italia come la sua blockchain, Algorand, riuscirebbe a superare i limiti di quanto messo a punto fino ad oggi. Laureato a Roma in matematica, prosegue gli studi a Berkeley. Inizialmente, lavora sugli algoritmi, ma seguendo un corso sulla teoria dei numeri incappa quasi accidentalmente nella crittografia e se ne innamora: "mancavano definizioni, quadri di riferimento, tecniche, e soluzioni. In compenso, c'era tanta passione, spregiudicatezza e spavalderia che mi hanno permesso di attaccare l'ignoto invece di evitarlo". Il coraggio di rischiare, e un percorso difficile costellato di traguardi. Parla di temi importanti, ma i toni rimangono pacati, quella modestia che è propria dei veri uomini di scienza: "ho avuto anche una buone dose di fortuna", sottolinea raccontando gli step che, nel giro di pochi anni lo hanno portato insieme alla collega Shafi Goldwasser, a fondare una teoria rigorosa sulla sicurezza dei dati, della pseudo-casualità, della conoscenza zero, della computazione allo stesso tempo segreta e corretta. "Insomma le tecniche alla base dell'e-commerce moderno. Ma anche della blockchain".

## SICUREZZA E PRIVACY

Ma facciamo un passo indietro. Perché la blockchain dovrebbe essere così sicura? “È un registro pubblico di dati che ha le seguenti tre proprietà: tutti possono leggere tutte le pagine del registro, nessuno può alterare i contenuti di una pagina del registro o l'ordine delle pagine del registro, tutti possono scrivere una riga in una pagina futura del registro - spiega Micali - In un database tradizionale, ad esempio quello di una banca, i dati della singola persona sono visibili solo alla banca. Se a un certo punto qualcuno volesse bloccare i miei conti - proprio come succede nei film - questo qualcuno potrebbe farlo senza lasciare traccia. Con la blockchain non può accadere perché nel momento in cui avviene una modifica, l'operazione è visibile a chiunque. Non ci sono carte nascoste, nessuno può essere buttato fuori dall'economia perché può continuare sempre a fare transazioni”. In un sistema visibile a tutti, a rendere possibile il matrimonio tra trasparenza e privacy è proprio la ‘magia’ della crittografia moderna. “La teoria della conoscenza zero e della computazione sicura sono alla base di questa riconciliazione. Per esempio, tali strumenti permettono di verificare che un portafoglio finanziario non sia sovra-esposto ad alcun asset (verifica necessaria per un Regolatore) senza rivelare qual è la composizione del portafoglio (tipicamente uno dei segreti del mestiere più gelosamente custodito dai gestori di fondi finanziari)”.

## UNA TECNOLOGIA DEMOCRATICA

Ma la blockchain, non aspira solo ad essere la Fort Knox dei dati. “Il personal computer ha portato la computazione alla portata di chiunque. Internet ha permesso a tutti di comunicare con tutti. E adesso la blockchain ha la potenzialità di andare oltre la semplice comunicazione, permettendo all'umanità di organizzarsi e funzionare senza poteri centrali”. Un missione ambiziosa davanti alla quale diviene chiara la spinta di Micali in questa direzione. Il crollo della disintermediazione è una delle rivoluzioni di questa nuova democrazia.

Prendiamo ad esempio un contratto di compravendita di un appartamento, dove il venditore è in America e il compratore in Italia. Tradizionalmente c'è bisogno di almeno un mediatore che riceve il contratto firmato dal compratore, unitamente al denaro necessario all'acquisto. Una volta ricevuto il contratto controfirmato dal venditore, in doppia copia, il mediatore rilascia il denaro al venditore e una copia del contratto doppiamente firmato al compratore. Questa operazione mediata naturalmente richiede molto tempo ed è necessariamente costosa perché il mediatore, notaio o legale che sia, vuole essere pagato per i suoi servizi. Con una blockchain efficiente la compravendita può essere completata senza mediazione, con un'unica transazione che contemporaneamente trasferisce la proprietà e il denaro, senza che ci sia possibilità per uno dei contraenti di imbrogliare l'altro. “Tra l'altro una banca dati inalterabile e trasparente è la forma più semplice ed efficiente di catasto”, sottolinea l'esperto.

## BLOCKCHAIN IMPERFETTE

Questo è un modello ideale caratterizzato da tre pilastri: sicurezza, decentralizzazione e scalabilità. Ma “nella realtà accade che le blockchain implementate ad oggi non riescano a cogliere tutte e tre queste proprietà”, spiega l'esperto. Il punto è: chi costruisce queste cassaforti trasparenti? Nel Bitcoin, e più in generale nelle blockchain basate sul ‘proof of work’,

per costruire nuovi blocchi è necessario risolvere indovinelli crittografici difficilissimi. E per farlo è necessario consumare energia elettrica. Chi risolve questi indovinelli sono i cosiddetti ‘minatori’. Più il numero dei minatori aumenta più difficili diventano gli indovinelli. E più energia si consuma. I minatori oggi comperano ed operano su migliaia e migliaia di computer super-specializzati, progettati soltanto per risolvere questi speciali indovinelli. Inoltre, per meglio operare, i minatori si consociano, così che il potere finisce per concentrarsi in poche mani, fino alla perdita di una delle peculiarità chiave della blockchain: la decentralizzazione. Delle duemila blockchain implementate ad oggi, la maggioranza sono di questo tipo. Le altre utilizzano sistemi diversi per aggiungere altri blocchi ma ugualmente inefficaci: “la ‘delegated proof of stake’ e la ‘bonded proof of stake’ presentano altri limiti”, spiega Micali. Il fondatore di Ethereum, Vitalik Buterin, ha pubblicato quello che è conosciuto come ‘il trilemma della blockchain’ secondo il quale una blockchain non può essere simultaneamente sicura, scalabile, e decentralizzata. Buterin ha raggiunto questa conclusione “basandosi sull'esempio di oltre duemila blockchain, nessuna delle quali è riuscita a mantenere queste tre proprietà”, spiega Micali.

Lo stesso Bitcoin è controllato da soli tre consorzi di minatori. Significa che ci sono solo tre poteri decisionali. Ethereum, invece, è gestita da due soli consorzi di minatori. E tutti questi consorzi si trovano in Cina, dove l'energia costa meno, spiega Micali. “Ma un sistema che è controllato da tre enti, è considerabile decentralizzato?”. Una semplice domanda che scioglie ogni dubbio sulla fallacia del sistema. “Ma se lei avesse una banca con miliardi di euro di valore, li trasferirebbe in una blockchain dove non glieli possono rubare ma il permesso di spenderli deve chiederlo a queste tre persone? Accordandosi, queste tre entità potrebbero riscrivere la storia della blockchain che, invece di essere incorruttibile, diventerebbe alterabilissima”.

Cosa succederebbe se la società si appoggiasse a una tecnologia con il presupposto di aver adottato un sistema incorruttibile, ma poi così non fosse? Il rischio è di portare al collasso interi sistemi: organizzazioni, aziende e istituzioni. Ma Micali, con la serenità e la naturalezza di chi la vita la vive come una fonte inesauribile di opportunità, offre la sua versione della storia: “non è esattamente una deduzione matematica dire che una cosa non si può fare perché in duemila non sono ancora riusciti a farla. In realtà nella vita ci sono cose impossibili,



Silvio Micali,  
studioso vincitore  
del premio  
Turing, il 'Nobel'  
dell'informatica

ma fortunatamente sono molto poche". Non è un'osservazione casuale la sua. Lui, che di una nuova tecnologia blockchain è l'ideatore. Non si trova casualmente a Roma quel giorno. Da Boston, dove vive e forma le menti degli scienziati di un domani, è arrivato in Italia per spiegare anche ai giovani conterranei il suo lavoro. Non in una sede qualsiasi, ma proprio in quello che in Italia è il dipartimento di eccellenza sul tema della cybersecurity, il Diag (dipartimento di Ingegneria informatica automatica e gestionale Antonio Ruberti) della Sapienza Università di Roma.

### ALGORAND, LA BLOCKCHAIN DEL FUTURO

"Quando ho sentito per la prima volta come funziona Bitcoin, ho trovato il problema entusiasmante, ma la soluzione poco elegante. Siccome criticare soltanto non basta, mi sono chiesto come avrei architettato io il sistema. Mi sono chiuso a chiave per alcuni mesi e gettato le basi di Algorand. Ho quindi messo online il progetto per ottenere commenti. Il commento più significativo è venuto proprio dai miei colleghi del Mit: 'il sistema sembra troppo bello per essere vero'. Così abbiamo condotto una simulazione del sistema su larga scala. L'esito di questo esperimento è stato positivo. Ho quindi deciso di fondare una società. Dei primi 11 impiegati, 8 provenivano dal Mit. Abbiamo raccolto 66 mln di

dollari (in equity financing) da investitori da tutto il mondo, e abbiamo costruito e stiamo finendo di testare il network". Micali racconta così quale sia la leva che lo ha condotto verso la stesura del protocollo che "dimostra che il trilemma è falso". Una blockchain alternativa che non utilizza minatori e indovinelli crittografici.

La catena Algorand cresce tramite una serie di 'comitati' di utenti sempre diversi. Ogni comitato consiste di un migliaio di utenti scelti a caso e in modo indipendente. Ogni membro del comitato diffonde in rete un singolo messaggio corto e facile da computare. Dopodiché viene eletto un altro comitato attraverso una lotteria crittografica individuale e sicura. Neanche un utente che disponesse della capacità computazionale di un'intera nazione riuscirebbe ad aumentare la propria possibilità di vincita. Così i comitati cambiano a caso ogni volta: "Algorand è veramente distribuito, perché ogni comitato è responsabile di diffondere una sola onda di messaggi; è scalabile perché ogni utente conduce la propria micro lotteria nel proprio laptop, senza dovere attendere il risultato della lotteria degli altri; è veramente sicuro", sottolinea Micali spiegando il perché: "supponiamo che nel mondo ci sia un 'nemico' capace di corrompere istantaneamente ogni utente. Tale avversario vorrebbe naturalmente corrompere il nuovo comitato. Ma ha un serio problema: non sa chi corrompere. Infatti i membri del comitato sono i vincitori di lotterie private giocate sui propri computer. Possono essere 'scoperti' solo quando i loro messaggi si stanno propagando sulla rete in modo virale, e l'avversario non può più fermarli, così come un governo non può fermare un messaggio propagato viralmente da Wikileaks. All'inizio, un avversario non saprebbe chi attaccare, e dopo ogni attacco sarebbe inutile". Sul fronte finanziario, ora Algorand è pronta per dare i natali ad Algo: "a breve, la Fondazione Algorand lancerà la criptomoneta, l'Algo, da Singapore - racconta Micali - sarà una criptomoneta veramente decentralizzata, un vero mezzo di scambio, utilizzabile per comperare anche una fetta di pizza. Le criptomonete attuali non hanno simultaneamente la scalabilità, la sicurezza, e la decentralizzazione necessaria per un mezzo di scambio". Uno degli scopi di Algorand è la democratizzazione della finanza. "Attualmente i mezzi finanziari sofisticati sono a disposizione di pochi eletti. Tutti gli altri si devono accontentare delle briciole dei loro banchetti". Ma un altro scopo fondamentale di questa tecnologia sarà fornire il supporto tecnico necessario per permettere l'autogoverno efficiente di comunità trasversali sempre più ampie. "Stiamo approntando già le tecnologie successive: scambi di beni sulla blockchain in pochi secondi, mediate un'unica (e quindi veramente 'atomica') transazione; contratti (veramente) smart, e così via". D'altra parte "il lavoro e il divertimento non mancano di certo", conclude. ■

## ► DIAG E CYBERSECURITY

Selezionato dal Miur come centro d'eccellenza per la cybersecurity, il dipartimento di Ingegneria informatica automatica e gestionale Antonio Ruberti (Diag) della Sapienza collabora da molti anni con il dipartimento per la sicurezza (Dis). "Il Diag

è cardine della cybersecurity in Italia", afferma la direttrice Tiziana Catarci, raccontando il fitto intreccio tra Diag e Dis, non solo didattico ma anche operativo. "Il vice direttore del Dis, Roberto Baldoni, è un nostro professore e ha fondato sia un

centro per la cybersecurity qui alla Sapienza, sia uno a livello nazionale ospitato dal Consorzio interuniversitario nazionale per l'informatica". Esempio virtuoso e "non top secret" di attività è "il Framework nazionale per la cybersecurity e la data protection:

un prodotto per aziende e Pa che serve a tutelarsi", spiega Leonardo Querzoni, ricercatore e professore associato del Diag. Sin dall'inizio "una delle missioni che il Dis ci affidò era quella di contribuire alla cultura della sicurezza".