NEW ECONOMY

La sfida bitcoin
Un'arma segreta
contro il sistema

Antonio Maria Costa A PAGINA 9

Il bitcoin potrebbe diventare l'arma segreta dell'antipolitica

Una tecnologia in grado di riuscire dove i sistemi tradizionali falliscono

ANTONIO MARIA COSTA

L'anti-politica afferma di rappresentare la gente comune, contro il sistema. Le anti-valute sono definite (dalla Bce) monete accettate dalla gente comune, non emesse dal sistema. Due sfide convergenti, oppure due raggiri? Bitcoin, l'anti-valuta più nota, è l'arma segreta dell'anti-politica, oppure uno strumento di speculazione?

Per giudicare, partiamo da lontano nel tempo e nello spazio - dalla Mesopotamia (odierno Iraq), cinquemila anni fa. Usando tavolette e simboli cuneiformi, i Sumeri creano la contabilità a partita semplice: Erishki mi deve 2 shekel, io devo 3 shekel a Enki. La prima rivoluzione avviene nel Rinascimento, quando mercanti genovesi e banchieri fiorentini introducono la contabilità a partita doppia: dare/avere, costi/ricavi sono registrati congiuntamente, poi certificati da notai, revisori, catasto, agenzie delle entrate. Un sistema oggi complesso e costoso, soprattutto per le istituzioni finanziarie che gestiscono milioni di transazioni quotidiane.

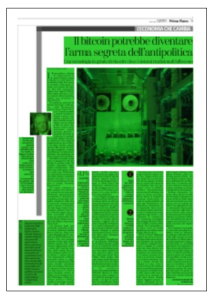
Nel 1989 la seconda rivoluzione. Il giapponese Yuji Ijiri inventa la partita tripla che combina contabilità, criptografia e certificazione – tutto nelle mani della gente comune, a costo zero. Un'alternativa a intermediari parassitari? Una sfida al potere costituito? Questo e ben altro: è una minaccia al capitalismo tecnologico di Google, Facebook, Amazon & Co.

Per capire, risaliamo al 1989, quando Tim Berners-Lee inventa la rete (internet). Sfruttando sperimentazioni accademiche e finanziamento pubblico, fa interagire molteplici calcolatori sulla base di protocolli computerizzati aperti: nessuno è proprietario della lingua franca che le macchine parlano l'una l'altra. Nascono lingue informatiche accessibili gratuitamente per gestire posta elettronica (Pop e Smtp), accesso alla rete (Htpp), e la geo-posizione (Gps).

Col passare degli anni «l'umanità commette un grave errore» (afferma l'analista Steven Johnson). Dopo avere creato linguaggi aperti (=gratuiti) per posta elettronica, internet e Gps, non protegge l'identità sociale degli utenti: indirizzi, agenda, foto, video, canzoni, viaggi, letture, studi - e anche dati riservati come Iban, codice fiscale, Dna, genoma, diagnosi medica, ecc. In un attimo, il settore privato vede l'opportunità. Sviluppa procedure chiuse (=a pagamento) per appropriarsi della nostra identità individuale nella sua totalità e funzionalità. Amazon ed eBay accumulano dati bancari e criteri di spesa; Facebook conosce famiglia e amici; Instagram ha le foto; WhatsApp e Skype possiedono indirizzi e telefoni; Google sa cosa leggi, acquisti, bevi, regali, studi, ricerchi; Spotify e Netflix marcano i tuoi divertimenti; Apple offre applicazioni conformi alla tua persona. Quando accedi ai servizi di questi giganti tecnologici, in effetti chiedi l'uso temporaneo dell'informazione che estraggono da te a costo zero, per rivenderla a caro prezzo (a te come tariffa, a terzi come pubblicità).

Come sfuggire al cappio che le multinazionali dell'informatica hanno stretto al collo dell'umanità? Risponde alla sfida Satoshi Nakamoto (un ignoto lui? lei? loro?) che nel 2008 costruisce sul concetto contabile sviluppato da Yuji Ijiri vent'anni prima: propone un meccanismo per generare la prima anti-valuta al mondo, bitcoin. Successo o raggiro? Non importa. L'intuizione di Nakamoto si rivela rivoluzionaria anche se bitcoin risultasse un fallimento. Vediamo in pratica come questo funziona, e in termini logici come interagisce con l'anti-politica.

Primo passo. Un'applicazione specializzata (MetaMask, ma ne esistono dozzine) sceglie per me 12 vocaboli nel dizionario. Eccoli: mela nulla pace polemica vaso cotone minestra fusione cameriera galera vento auto. Roba senza senso? Nient'affatto. Nella parlata delle cripto valute, questa filastrocca è la mia frase seme, che MetaMask istantaneamente trasfor-



ma in un codice alfa-numerico di 32 caratteri: 2d0ope7ehx6sllk6ms6698kam300ksol23. Questa è la chiave elettronica, unica, criptata e irreversibile che protegge la mia identità e mi apre al mondo. Non c'è contraddizione: rimango ignoto e interagisco con tutti.

Secondo passo: uso la chiave ogni volta che compro, vendo, voto, viaggio, scarico musica, studio, ecc. La mia identità rimane segreta, protetta dal mio codice alfa-numerico incorruttibile. Ogni mia operazione invece è pubblica, condivisa istantaneamente con una rete di calcolatori che usano la stessa procedura. Questo blocco di computers incatenati (block-chain) diventa un registro pubblico nel quale ogni falsificazione, manipolazione o distruzione sono impossibili. Altro beneficio: questo registro informatico non è di proprietà privata, appartiene agli utenti. I suoi sostenitori lo considerano una rivoluzione tecnologica che protegge dal furto d'identità e annulla i costi di certificazione. Per l'anti-politica è un passo verso un mondo ugualitario, una difesa contro Google, Amazon & Co.

Chi fa il lavoro? Nakamoto propone una prova di lavoro: chiunque dedica parte del proprio calcolatore per mantenere il sistema e impedire interferenze, è pagato. È a questo punto che nasce bitcoin, concepito come remunerazione - un gettone, non un'anti-moneta. La stessa creazione di bitcoins è un processo complesso: si chiama estrazione, analogo a quanto succede per esempio col rame. Come il prezzo del rame è il risultato di sforzi crescenti di prospezione ed estrazione in località remote nelle viscere della terra, la creazione di un minerale virtuale come bitcoin richiede sempre maggiore potenza di calcolo, alimentata da crescenti quantità di energia in località remote in Europa e Asia. Questa difficoltà, anche ambientale, genera critiche – che non riducono il potere dirompente dell'intuizione di Nakamoto. Non è la specifica anti-moneta (bitcoin) a minacciare il potere costituito, ma la logica (l'algoritmo) che la genera.

Esistono alternative. Secondo Silvio Micali del Mit, uno dei migliori criptografi, alla base di tutte le cripto-valute (che sono associative per definizione, cioè non imposte dall'alto) c'è un algoritmo di natura consensuale. Bitcoin gestisce il consenso sulla base di prova di lavoro. Altre monete preferiscono la prova di partecipazione al processo costitutivo. Concetti diversi, che convergono nel riconoscere la capacità innovativa del registro pubblico.

Per concludere, l'anti-politica vede nelle anti-valute la ribellione contro le istituzioni, un modo per rafforzare il controllo sulla moneta da parte del cittadino. In effetti, qualcosa di più importante è in gioco. Accantonando le inevitabili speculazioni che altalenano il valore di mercato di bitcoin, ritengo che la partita tripla e la catena di blocchi potrebbero riuscire proprio nei comparti dove la politica, vecchia e nuova, fallisce: ridurre il divario sociale, moderare la demarcazione tra investitori e utenti, abbassare i costi di gestione, contenere il potere dei monopoli informatici. Se questo accade, l'umanità avrà un grosso debito verso Yuji Ijiri e Satoshi Nakamoto.

autore@scaccomatto-all-occidente.com

-3,1%

La perdita
La criptovaluta ha perso ieri il 3,1% a 8.559 dollari Pesanti anche i future sul Bictoin: quello del Cme cede il 3,9% a 8.515 dollari mentre il Cboe arretra del 3,2% a 8.548,57 punti Fra le altre criptovalute perde terreno il Ripple, in calo del 5,8% a 98 centesimi sulla piattaforma di scambio Bitstamp

1

Tripla
Nel 1989 il giapponese Yuji Ijiri inventa la partita tripla che combina contabilità, criptografia e certificazione, a costo zero

2

Bitcoin
Satoshi Nakamoto nel 2008 propone un meccanismo per generare la prima anti-valuta al mondo, bitcoin. Una intuizione rivoluzionaria

Economista
Per due volte vicesegretario generale dell'Onu, capo dell'ufficio contro il traffico di droga e il crimine internazionale, Antonio Maria Costa è stato anche direttore generale alla Commissione europea e capo della Banca per la ricostruzione e lo sviluppo. Nel 2015 ha pubblicato il romanzo «Scaccomatto all'Occidente» per Mondadori.

BITCOIN

Bitcoin è la prima e la più nota delle criptovalute. Queste "monete virtuali" hanno in comune il fatto di non avere alle spalle alcuna banca centrale né uno Stato, ma di basarsi solo su un meccanismo di condivisione di un libro mastro che tiene traccia delle transazioni tra gli utenti della rete. Il libro mastro è pubblico, ma non si sa però a chi appartengano i singoli nomi utente.