Misteriosamente Bitcoin

Qual è la vera identità di Satoshi Nakamoto? Quale ruolo svolge nel nuovo sistema di pagamento Gavin Andresen? Quali traguardi potrà conseguire la moneta virtuale?

Tom Simonite

Illustrazione: Tomi Um

In primavera, i giornalisti hanno incontrato Dorian Nakamoto, dinanzi alla sua casa a Temple City, in California. Il 64enne, all'apparenza stanco e disorientato, era stato indicato da "Newsweek" come la persona che aveva ideato Bitcoin. Come altri precedenti tentativi di capire chi si cela dietro lo pseudonimo dell'inventore, Satoshi Nakamoto, anche questo non ha avuto esito positivo. Allo stesso tempo, il vero protagonista del successo della moneta virtuale, che ha raggiunto il valore di 7,7 miliardi di dollari, si stava godendo il panorama all'altro lato della nazione, ad Amherst, in Massachusetts.

Questa persona è Gavin Andresen, un 48enne dall'aspetto mite, scelto come successore dal vero Satoshi Nakamoto, chiunque egli o ella sia, alla fine del 2010. Andresen, nella sua funzione di responsabile del software, si è occupato della manutenzione del codice open source che definisce le regole base di Bitcoin e fornisce il programma necessario al funzionamento del sistema. La combinazione del sostegno di Nakamoto e dell'assidua applicazione di Andresen al codice di Bitcoin hanno conferito a quest'ultimo un ruolo di primo piano nel mondo della moneta digitale. La CIA e i legislatori di Washington si sono rivolti a lui per farsi spiegare i meccanismi di circolazione dei Bitcoin ed è stato Andresen a fondare nel 2013 la Bitcoin Foundation, un'associazione senza scopo di lucro che svolge le funzioni di autorità centrale nella rete di pagamento con il nuovo tipo di denaro.

Alcuni convinti sostenitori di Bitcoin prevedono che con le transazioni a basso costo rese possibili dalla moneta virtuale, i consumatori americani potranno liberarsi delle pastoie burocratiche della Federal Reserve e le nazioni più povere potranno prosperare. Altri entusiasti supporter del sistema virtuale hanno l'aria di rappresentanti di commercio che snocciolano i diversi motivi per cui dovresti "comprare" il loro prodotto. Al contrario, Andresen sembra inseguire la soddisfazione personale, senza eccesso alcuno, come traspare dalla definizione che dà di sé: «Un *geek* interessato agli aspetti pratici delle cose».

Inoltre, Andresen ha avuto e mantiene più influenza di chiunque altro sul codice che determina il funzionamento di Bitcoin e in questo ultimo periodo anche sulla sua sopravvivenza. Come Andresen sfrutterà il suo potere, determinerà non solo il destino di Bitcoin, ma anche le sorti delle altre monete virtuali. Mentre le origini di Bitcoin sono avvolte nel mistero, si sa molto di più su Andresen e il suo passato. Andresen, alla nascita Gavin Bell, ha lavorato per sette anni come programmatore a Silicon Graphics, subito dopo il conseguimento della laurea in informatica a Princeton, nel 1988. Successivamente, ha collaborato con numerose start-up, passando dal software di progettazione 3D ai game on-line per fare sì che persone vedenti e non vedenti possano giocare insieme. Infine, nel 2010, è "incappato" in Bitcoin.

Allora, la moneta virtuale era senza valore e di non facile utilizzo. Ma Andresen intravide le potenzialità del design di Nakamoto e di una moneta al di fuori del controllo governativo. Invece di venire coniati da una banca centrale, i bitcoin vengono "estratti" da utenti dotati di un software per la soluzione di puzzle matematici. I bitcoin nuovi di zecca sono il premio, ma il meccanismo di estrazione, che serve anche a verificare le transazioni, viene sfruttato per dimezzarli periodicamente affinché il numero complessivo di bitcoin non superi mai i 21 milioni.

Nel 2010, Andresen ha creato un sito Web chiamato Bitcoin Faucet, che offriva gratuitamente cinque bitcoin a ogni visitatore (il valore del bitcoin era allora di pochi centesimi di dollaro, rispetto ai 600 dollari attuali; Andresen ridusse la quantità di bitcoin circolanti a causa della crescita di valore e chiuse successivamente il sito nel 2012). Nel frattempo aveva cominciato a spedire proposte di modifiche del codice a Nakamoto. Il fondatore di Bitcoin apprezzò il lavoro di Andresen al punto da lasciare solo il suo indirizzo e-mail sulla homepage del progetto. Andresen fece la sua comparsa ufficiale in un post del 2010 sul forum di Bitcoin. Da allora ha lavorato a tempo pieno alla moneta virtuale e, nel 2013, la Bitcoin Foundation gli ha versato come pagamento 209.648 bitcoin.

La sua irresistibile ascesa ha alimentato le ricorrenti voci che Andresen e Nakamoto siano la stessa persona e che abbia abbandonato lo pseudonimo quando la moneta ha iniziato ad avere successo. Andresen ha sempre negato con decisione: «Io non sono Satoshi Nakamoto. Non l'ho mai incontrato. Ho solo avuto un serrato scambio di e-mail con lui». Se le sue sono bugie, Andresen è un imbroglione di grande classe. In centinaia di post sui forum, nei messaggi e-mail e nelle linee di codice, il suo stile è sempre stato distinto da quello di Nakamoto. Non si sa bene quanti bitcoin Andresen possieda, ma, secondo le sue dichiarazioni, abbastanza da potersi tranquillamente ritirare a vita privata.

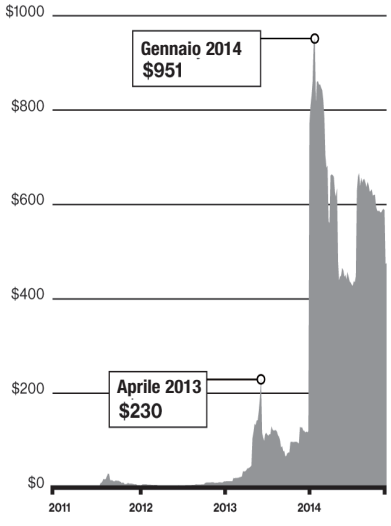
Quando iniziò la sua collaborazione con Nakamoto, Andresen si impegnò a portare avanti il progetto, affidandosi alla sua esperienza organizzativa per produrre software. Venne creato un gruppo di cinque programmatori, con a capo Andresen. Solo loro avevano il potere di cambiare il codice di Bitcoin e di accettare le proposte degli altri utenti.

Il prezzo dei bitcoin è salito anno dopo anno grazie al lavoro del gruppo di Andresen, che ha elaborato il software necessario a rendere possibile questo risultato. Il gruppo ha garantito alti livelli di sicurezza e di affidabilità del software, migliorando allo stesso tempo la qualità dell'interfaccia utente.

Un compito per nulla semplice, perché il tipo di software lasciato da Nakamoto non era adatto a realizzare un prodotto vincente, sostiene Mike Hearn, ingegnere informatico proveniente da Google, che ha contribuito alla scrittura del codice. «Nakamoto ha creato Bitcoin per dimostrare che la sua idea poteva funzionare, ma non lo ha progettato per diventare un prodotto sostenibile nel lungo periodo», spiega Hearn.

Questo lavoro è stato prevalentemente svolto da Andresen e Wladimir van der Laan, il programmatore di Amsterdam prescelto da Andresen come responsabile del codice. Alla fine dell'opera di riscrittura, era rimasto in vita meno di un terzo del codice inizialmente scritto da Nakamoto. «È stato senza dubbio un ottimo programmatore, ma a volte "stravagante"», dice Andresen.

Valore di un bitcoin



Fonte: Coindesk.

Il numero di persone che lavorano al software di Bitcoin rimane limitato, ma i problemi sono aumentati in modo esponenziale. Quando il valore della moneta digitale era arrivato a circa 8 miliardi di dollari, l'utenza si è allargata dai primi entusiasti sostenitori agli investitori di Wall Street e Silicon Valley. I legislatori e le autorità regolatrici hanno espresso giudizi positivi su Bitcoin e si sono impegnati a definire una cornice legale.

Il rischio di falle nella sicurezza è una preoccupazione costante per Andresen. Sorride quando racconta di come, nel 2010, qualcuno abbia riferito a Nakamoto di un bug che permetteva di spendere i bitcoin degli altri utenti: «Satoshi si limitò a cambiare il codice e a dire a tutti di adottare il nuovo codice senza chiedersi perché».

Ma anche se molti bug del software attuale hanno una pericolosità limitata, non è escluso che quel problema si presenti di nuovo. «Per questa ragione dico sempre che Bitcoin è in fase sperimentale e non si devono investire i risparmi di una vita», spiega Andresen.

Sfortunatamente, la migliore difesa contro le falle della sicurezza, vale a dire avere persone che passano in rassegna il codice di altri utenti, è di difficile adozione da parte di Bitcoin.

I volontari non pagati preferiscono scrivere il proprio codice più che vagliare accuratamente quello degli altri. Il valore attuale della moneta digitale è determinato quasi esclusivamente dalla speculazione, quindi qualsiasi indizio di vulnerabilità del sistema può provocarne una caduta verticale.

Allo stesso tempo, Andresen sta fronteggiando un serio problema strutturale ereditato da Nakamoto.

La rete di Bitcoin non è in grado di processare più di sette transazioni al secondo, un volume trascurabile per una tecnologia con ambizioni globali Ancora oggi su Bitcoin viene eseguita una sola transazione al secondo. Visa ne esegue 480 al secondo e può arrivare fino a 47mila. «Sono preoccupato da questa situazione e spero che il dibattito in corso nella comunità di Bitcoin porti a qualche risultato concreto», afferma Andresen.

La sua soluzione è di incrementare le dimensioni dei "blocchi" di transazioni che vengono confermati dalla rete di *miners* (server e nodi anonimi gestiti da individui altrettanto anonimi) ogni 10 minuti.

Non tutti concordano con questa proposta perché ritengono che si verrebbe a creare un eccesso di centralizzazione. Andresen si appoggia agli scritti di Satoshi per dare forza alla sua tesi: «Se si leggono con attenzione le sue parole, Satoshi intendeva il sistema come una rete di transazioni giornaliere aperta a tutti».

In un modo o nell'altro, alla fine si farà quello che vuole Andresen. Ma egli ribadisce che il gruppo fondamentale di programmatori ascolterà sempre le opinioni degli altri prima di qualsiasi intervento sul codice. «Ogni ritocco dovrà essere concordato», spiega Andresen e ricorda che il software è open source e chiunque sia in disaccordo può crearne una sua versione.

Ma gli altri sviluppatori e utenti hanno poco interesse a mettere in discussione lo *status quo* e Andersen gioca su questo. In definitiva, il valore di una moneta virtuale si poggia sull'accettazione condivisa. Nel caso di Bitcoin, la fiducia è legata non solo al codice di Nakamoto, ma a chi lo utilizza.

Andresen ha una spiegazione alternativa in merito alle ragioni per cui non ci saranno grandi cambiamenti nel modo di funzionare di Bitcoin. Dopo che il problema delle transazioni verrà risolto, il compito di "sorvegliare" il codice sarà affidato a chi si occupa della manutenzione e non ai responsabili della programmazione, sostiene Andresen anticipando la sua intenzione di dedicare sempre meno tempo al funzionamento del sistema per dedicarne sempre di più allo studio della economia delle monete virtuali e dei saggi accademici inerenti l'argomento. «Sono molto ottimista sul futuro e spero che nei prossimi dieci anni si andrà oltre Bitcoin», conclude Andresen. ■

Tom Simonite è redattore capo di MIT Technology Review USA.