

Bitcoin e Blockchain: verso un nuovo sistema monetario?

di Alessandra Caputo – Action Institute

A oggi i Bitcoin sono usati da 360.404 utenti, con un prezzo di mercato di 639\$. L'ammontare in circolazione è di 15.705.900 e arriverà a 21 milioni entro il 2030. Action Institute mette in luce come la nuova moneta digitale sta rivoluzionando il sistema finanziario e, probabilmente, il modo stesso con cui si concepisce la moneta.

Cosa rende i Bitcoin così innovativi? Una risposta a questa domanda si può dare ricostruendo il momento storico in cui sono apparsi per la prima volta sul mercato e la ragione sottostante la loro creazione. Nel novembre 2008, l'annus horribilis del sistema finanziario globale, Satoshi Nakamoto pubblica il protocollo di Bitcoin. La creazione non è casuale e anzi mira a costituire una contante digitale utilizzabili per fare pagamenti a distanza, in modo istantaneo, senza costi per le parti e di qualsiasi entità. Transazioni tendenzialmente cost free. I costi sono dell'1% del valore della transazione, rispetto al 2-4% dei sistemi di pagamento elettronici e all'8-9% dei servizi di rimessa che non si appoggiano al sistema bancario. Data l'assenza di una banca centrale che decida l'aumento o meno di bitcoin in circolazione, il protocollo stabilisce a priori che l'ammontare massimo sarà pari a 21 milioni e che questo sarà raggiunto attraverso aumenti decrescenti nel tempo.

La tecnologia blockchain è stata definita dal responsabile della ricerca presso R3CEV, Tim Swanson, come il glutine: tutti ne parlano ma nessuno sa effettivamente cosa sia. Si compone di una serie concatenata di blocchi dove sono registrati i dettagli di ogni transazione. Questa costituisce la vera rivoluzione innovativa. Il libro contabile, distributed ledger, non è più infatti tenuto dalla singola banca ma da ciascun utente, cui è affidato il controllo dell'intero sistema. Costituisce quindi una rappresentazione coerente e veritiera dell'economia Bitcoin, che permette di conoscere la successione temporale delle singole transazioni. Tuttavia, le operazioni non sono rintracciabili del tutto, poiché, nonostante l'apparente trasparenza, gli utenti sono identificati non con i dati anagrafici ma attraverso codici. Nello specifico, ciascuno genera una coppia di chiavi, una pubblica ed una privata, con cui viene poi identificato in rete. Dal momento che ciascuno può creare più coppie di chiavi, un corretto matching tra utente e transazioni effettuate può risultare complesso, rendendo più facile l'abuso della tecnologia e l'adozione di comportamenti illeciti. D'altro canto, sebbene potenzialmente difficile, un efficace controllo non è impossibile; controprova è il caso di Ross Ulbricht (fondatore della Silk Road) che aveva intravisto nei Bitcoin la possibilità di guadagnare ingenti somme attraverso la gestione di un mercato di beni e servizi illegali, stupefacenti compresi, ma che è stato arrestato e condannato all'ergastolo nel 2013.

Bitcoin è quindi un sistema di pagamento enormemente innovativo, caratterizzato, in potenza, da un efficace trade-off tra trasparenza per il pubblico e privacy per i privati. Alta trasparenza del sistema dei pagamenti garantita dalla distribuzione della tenuta dei conti. Adeguata privacy garantita dal rintracciamento esclusivamente attraverso i codici. Bitcoin è un sistema di pagamento e una valuta al tempo stesso, trasferisce e genera potere d'acquisto. Ma se i contanti digitali sono così innovativi e potenzialmente efficaci, quale sarà il loro destino? Prenderanno il sopravvento sulla carta-moneta e sulla moneta digitale così come questi hanno fatto con oro e argento? Una moneta per essere adottata e utilizzata deve avere potere d'acquisto; è necessario che il suo valore sia stabile e che ci sia un mercato. In altre parole, è necessario che all'offerta corrisponda la domanda. Quale l'utilità di avere bitcoin, se poi non possono essere utilizzati a causa della mancanza di controparti negli scambi? La tecnologia Bitcoin, trasferisce e crea potere d'acquisto, la cui garanzia risiede nella scarsità generata artificialmente fissando l'ammontare massimo e l'algoritmo per la creazione di nuove monete. Il valore di bitcoin come moneta non dipende dalle decisioni dei banchieri come per le classiche valute, poiché tutto è già deciso e stabilito dal protocollo.

Impossibile non pensare però anche ai possibili rischi e ostacoli. Un sistema di pagamento completamente digitale, che non prevede l'esistenza di un ente controllore, ingloba il rischio di attacchi da parte di [hacker](#), il che costituisce una minaccia non solo alla sicurezza dei consumatori, ma all'intero sistema. Come ha affermato il Comitato per i pagamenti e le infrastrutture di mercato della Bank for International Settlements, la decentralizzazione del sistema e la sua struttura aperta e flessibile implica che può essere difficile anticipare simili complicazioni. Nondimeno, perché il sistema regga è necessario che esso si basi sulla fiducia. Fiducia delle e tra le parti, nel sistema e nel valore della valuta. Chi effettuerebbe una transazione senza la certezza che la controparte effettivamente possiede l'oggetto di scambio? Come essere certi che lo stesso bitcoin non sia oggetto di scambio due volte? Nel sistema di pagamento tradizionale, le banche assicurano la correttezza e la validità dei trasferimenti. Nella frenesia di liberarsi delle parti terze, non si è pensato sufficientemente ai vantaggi di queste, comprovato dalla loro mancata sostituzione. Con la nuova struttura ci si affida ai ledger, coloro che validano le transazioni, persone fisiche e non di cui non si conosce che un codice. È quindi necessario un atto di fede, non così automatico. La sfida è la necessità di avere una perpetua fiducia negli utenti e nei ledger; la stabilità del sistema sarà intaccata non appena gli utenti giudicheranno opinabile l'affidabilità, l'onestà e, più in generale, l'operato dei ledger.

Laddove il sistema finanziario è più antiquato, la blockchain risulta più interessante e può guadagnare maggior terreno. Molteplici start-up stanno utilizzando la nuova tecnologia con [fini alquanto diversi](#): dal voler agevolare le banche a spostare moneta in modo più efficace (Ripple), a voler proteggere beni di lusso (Everledger). Il distributed ledger potrebbe rivoluzionare la società grazie ai plurimi usi possibili. I bassi costi di transazione potrebbero portare alla nascita di nuovi modi di fare business.

In definitiva, Bitcoin e blockchain nascono in risposta ad un sistema monetario sempre più propenso a dare sostegno alle banche e poco capace

di sostenere gli scambi e gli investimenti reali. Nascono affinché non sia più necessario richiedere aiuti esterni per correggere gli errori degli intermediari finanziari, consuetudine ormai al giorno d'oggi. Svincolano i pagamenti elettronici dalla necessità di passare attraverso un sistema bancario, consentendo transazioni fra utenti (peer-to-peer) senza ritardi e senza oneri, utenti così liberi dal giogo delle banche. Dunque, una forte pressione quella che i bitcoin potrebbero esercitare sulle banche, se la loro adozione si diffonderà in maniera capillare. Alla domanda quale sarà il futuro del sistema monetario e bancario, potranno rispondere solo i posteri.

Autore: [Alessandra Caputo](#)

Action Institute
Valore. Indipendenza. Dialogo. Impatto.