ALESSANDRO VALERIO

IL BITCOIN E LA BLOCKCHAIN

Cos'è il Bitcoin

Bitcoin è una moneta informatica o matematica. Risultato di un progetto di cryptocurrency concluso da Satoshi Nakamoto nel 2009, indica un tipo di valuta che viene scambiata elettronicamente su reti digitali. E nessuno sa chi si nasconda dietro lo pseudonimo di Satoshi Nakamoto. Il progetto viene caricato su SourceForge nel novembre del 2008, se ne cominciò a parlare nelle mailing list cypherpunk.

Il nome Bitcoin si riferisce sia alla moneta (con la b minuscola) che al software open source (con la B maiuscola) progettato per implementare il protocollo di comunicazione e la rete peer-to-peer che ne consente lo scambio e rende concreta la possibilità di evitare il ricorso a un ente centrale grazie a un database distribuito tra i nodi della rete che tengono traccia di tutte le transazioni.

Ogni importo bitcoin è legato a una coppia di codici, le chiavi crittografiche, una privata nota solo al proprietario, che gli permette di spenderlo, una pubblica, e cioè l'indirizzo bitcoin, che permette di riceverlo.

Bitcoin quindi non viene "coniato" da banche o enti centrali, ma grazie a un algoritmo residente su computer attraverso il mining. Tanto più ampia è la rete dei miners, tanta più moneta verrà controllata e generata attraverso l'algoritmo del software bitcoin. La rete bitcoin crea un blocco casuale di monete che deve essere verificato dai miners per poterle utilizzare. Oggi esistono numerosi servizi (Exchange) su Internet che vendono bitcoin accettando come controvalore anche le monete nazionali.

La rete bitcoin che memorizza la produzione di tale moneta digitale ha un limite dato dall'algoritmo di produzione del bitcoin, che è di 21 milioni di bitcoin, suddivisi da 8 decimali, l'unità ultima è chiamata Satoshi. Si raggiunge la fine della produzione nell'anno 2140.

Cos'è la Blockchain

L'intero sistema monetario bitcoin risiede in un database replicato (chiamato Blockchain) in tutti i nodi della rete bitcoin e questo semplice fatto rende superfluo l'intervento di un'autorità centrale (banca). Per creare il proprio portafoglio digitale è sufficiente scaricare il client (una App) bitcoin su qualsiasi piattaforma software divenendo subito parte della rete che ne garantisce stabilità e affidabilità anche contro il double spending (ovvero spendere due molte gli stessi soldi).

Le transazioni in bitcoin sono pseudoanonime (è ipertracciato ma non chi sia il possessore) tra chi possiede un indirizzo bitcoin (se ne può creare uno anche per ciascuna transazione), e ogni possessore può tenerle in un portafoglio digitale sul proprio computer o presso terze parti come gli Exchange. Il numero di bitcoin circolanti stabilito a priori algoritmicamente in 21 milioni di unità rende praticamente impossibile manipolare il numero dei bitcoin. Tuttavia il controvalore del bitcoin è variabile in relazione al numero di bitcoin circolanti, alle transazioni, agli acquisti effettuati e all'importanza che ci dà l'essere umano, segue appunto le leggi della domanda e dell'offerta.

Perché è nata questa tecnologia

Premetto che non è proprio una tecnologia ma un insieme di più tecnologie già inventate, il sig. Satoshi le ha solo messe insieme e trovato un metodo per farle funzionare con questo scopo descritto nel suo whitepaper (descrizione del progetto).

Poiché da molto tempo la produzione di moneta usata come controvalore per l'acquisto di beni e servizi non è più vincolata alle riserve auree, ma segue criteri flessibili decisi da organi istituzionali (che si dovrebbero ritenere etici e non comandati da banche provate), è sufficiente che un adeguato numero di soggetti decidano di usarla stabilendone il valore. È inoltre da considerare che ogni oggetto, ogni dato, ogni informazione può essere scambiato con qualcos'altro come pagamento.

Tuttavia affinché funzioni è necessario creare un sistema fiduciario che assicuri di poter continuare a spendere il controvalore del bene venduto. Nel sistema bitcoin ciò si ottiene diventando la propria banca e uno dei nodi della rete in grado di replicare tutte le informazioni necessarie a mantenere il sistema sicuro ed efficiente in una logica di peering, da punto a punto con i computer legati dal consenso decentralizzato (autocontrollato da chi li usa).

Come studioso della Evoluzione mi domando sempre perché nasce qualcosa di così importante nel mondo e mi rispondo nella più semplice: Serviva questo cambiamento agli esseri umani. Abbiamo inventato la moneta con un proposito e deve avere delle caratteristiche: unità di conto, strumento di pagamento, riserva di valore. In seguito gli abbiamo dato forme diverse fino al passaggio da materiale a digitale. Stanchi di un sistema bancario che usa a sproposito il signoraggio (diritti di tassa sullo scambio della moneta) abbiamo inventato la decentralizzazione della autorità sulle transazioni della moneta. Ed è nato il Bitcoin.

Come può essere utile al NM

Nel corso di questi anni dal 2011 ho sentito parlare molto del come utilizzare questa tecnologia nei Network Marketing, essendo un appassionato di questo "strumento marketing" molto utile per le aziende innovative che vogliono entrare nei mercati virali. Seguo e condivido fin dal 2000 quando iniziai con Amway ed Herbalife.

Alcune aziende mi hanno chiesto come inserire le cryptovalute o come utilizzare la blockchain. Spesso ho dovuto fare una lezione introduttiva di cosa è questa tecnologia prima di far comprendere che è inutile usarla se si fa credere di possedere una moneta nella maniera tradizionale, il valore è dato dale persone che commerciano.

Le Crypto e il NM sono solo strumenti, devono essere collegati a un marketplace con degli utenti che comprano e vendono. Non puoi usare un martello per avvitare una vite. Non puoi vendere una Crypto tramite un NM, o viceversa, non ha senso. La blockchain ha più utilizzi, se la vediamo come tracciatura di transazioni non modificabili può essere utile per un controllo sicuro dei processi. Se la vediamo come eliminazione di ente di controllo può essere utile per evitare il lavoro di consensi del Network. Se la vediamo come trasporto di valore può certamente essere utile per i compensi della rete.

Ma ne vale la pena? Qui bisogna capire i costi e il tempo di sviluppo. Ci sono soluzioni semplici con blockchain già in funzione da tempo, come l'Ethereum molto utilizzato, che ha dei costi relativamente contenuti, oppure la creazione di una propria blockchain e una propria moneta che consiglio solo a chi ne ha realmente bisogno, con minimo centomila utenti e fatturati sopra il milione di euro. Non dimentichiamoci degli sviluppatori che già di per se hanno giustamente un loro costo, figuriamoci se esperti della blockchain.

In conclusione si può utilizzare questo strumento con il NM? Assolutamente si! I due strumenti non sono incompatibili, anzi. Ma come tutti gli strumenti vanno adoperati eticamente e bene e non dare illusioni di facili guadagni. Nel contempo far capire che le opportunità sono innumerevoli, un mondo nuovo si sta aprendo per le attività imprenditoriali e i business men!

Alessandro Valerio

www.alessandrovalerio.com
cocioale@gmail.com skype: cocioale telegram: @cocioale

Seguimi su: facebook

Consigliere Bitcoin Foundation Italia **www.bitcoin-italia.org** a cura di Roberto Carboni