

Che cos'è la blockchain e come funziona questa tecnologia?

Febbraio 5, 2018 · admin

Per un certo periodo la blockchain è stata confusa, o meglio identificata, con la bitcoin una criptomoneta che è semplicemente una declinazione della rivoluzionaria tecnologia definita blockchain. Si tratta di una piattaforma che consente la gestione di transazioni e scambi d'informazioni e dati anche in settori completamente diversi e lontani dal finance e dal payment. Per comprendere la blockchain occorre fare riferimento ad alcuni concetti apparentemente lontani tra loro: il concetto di "trust", di comunità, crittografia, trasparenza, condivisione, aggiungendo l'immutabilità nel tempo dei dati e la decentralizzazione. L'insieme di questi concetti e caratteristiche consentono di creare un'innovazione potente e complessa, ma anche democratica e potenzialmente solidale.



La blockchain è stata definita come la nuova generazione di Internet o, con maggior precisione, una sorta di Internet delle Transazioni e ancor di più, l'Internet del Valore. Potremmo addirittura azzardare che la blockchain possa assumere anche un valore "politico", come piattaforma che consente lo sviluppo e la concretizzazione di una nuova forma di democrazia, decentralizzata e in grado di garantire a tutti la possibilità di disporre di una totale trasparenza, di dare vita ad archivi immutabili e condivisi e per questo inalterabili, imm modificabili e dunque immuni da corruzione.

Come funziona la blockchain?

Nel panorama attuale la blockchain deve la sua implementazione alla necessità, da parte degli utenti, di una maggiore sicurezza riguardo agli scambi in rete. I blocchi che compongono la catena sono immutabili e ogni transazione si lega a quella precedente, formando una catena sicura, efficace e soprattutto trasparente, aperta per chiunque voglia verificare la veridicità degli scambi in atto tra i nodi. La blockchain permette ad utenti, organizzazioni, enti pubblici e privati di stipulare un accordo senza il bisogno di parti terze o

intermediari di alcun tipo, stravolgendo le logiche su cui si basa ogni tipologia contrattuale. Riprendendo l'idea proposta da Satoshi Nakamoto, ideatore della tecnologia p2p su cui si fonda la teoria bitcoin, questo è un sistema che non si basa solo sulla fiducia, ma anche sul controllo delle transazioni, grazie all'uso delle firme digitali, che ne impediscono le alterazioni. Il problema risiede sempre nell'esigenza di avere degli intermediari, come istituti di pagamento che attraverso carte di credito o prepagate, consentono la possibilità di effettuare delle transazioni. Per Nakamoto, la soluzione per disintermediare completamente le transazioni tra due utenti diversi è la creazione di un network totalmente p2p, che utilizza una nuova moneta digitale, appunto i bitcoin. Il network proposto dal programmatore esegue una marcatura temporale sulle transazioni, sottoponendole ad hash, ovvero un algoritmo matematico che trasforma ogni blocco di dati in una nuova stringa formata da nuovi caratteri di dimensione fissa. Gli *hash* rappresentano uno strumento fondamentale per proteggere i file e le transazioni, sottoponendo ogni dato ad una conversione criptografica. Le funzioni criptografiche di un hash sono usate, principalmente, per proteggere l'integrità di un messaggio o di una transazione. In altre parole, esaminando l'output di un hash generato sia prima che dopo la trasmissione di dati, si assicura che i file o i dati non siano stati soggetti ad alcuna manipolazione. Se i risultati del prima e del dopo coincidono, la trasmissione si considera autentica. Gli hash vengono inseriti, nell'algoritmo di Nakamoto, in una catena di prove continua, riproducendo un risultato imm modificabile e generando, così, una transazione sicura ma allo stesso tempo molto lenta. I messaggi e le transazioni che avvengono all'interno della blockchain, quindi questa catena di blocchi che si susseguono, sono trasparenti e accessibili a tutti in qualsiasi momento.

L'e-commerce attuale si appoggia quasi esclusivamente su istituzioni finanziarie che fanno da garanti nel processo di pagamento elettronico. Nel caso delle transazioni non è possibile ovviare in modo efficace a problemi di mancate spedizioni, dispute, frodi e atteggiamenti scorretti. Grazie alla tecnologia blockchain, nel caso specifico dell'e-commerce, le transazioni diventano sicure, svincolate da possibili intermediari, su un server p2p, generando una prova computazionale dell'ordine cronologico delle transazioni. Ogni bitcoin è una catena di firme digitali, ogni utente lo trasferisce al successivo, in maniera criptografica insieme all'hash della transazione precedente e alla chiave di decifratura al futuro proprietario. Il ricevente può verificare le firme e quindi l'intera catena dei blocchi, quindi delle transazioni, qui ha un ruolo cruciale il server di marcatura temporale. Questo funziona sottoponendo ad un hash un blocco di dati, il quale viene sottoposto a verifica e solo poi trasmesso all'hash

successivo. Ogni marcatura include anche quella precedente nel proprio hash, formando dunque una catena, sempre più valida. Per implementare un server di marcatura temporale su base p2p è fondamentale un sistema di prova (*Proof of work*), che consiste nel cercare un valore tale che, quando sottoposto ad hash ne generi un altro con un certo numero di bit a zero. Per il network di marcatura temporale, si implementa la prova del lavoro aumentando un apposito parametro detto *nonce* nel blocco, e l'hash deve risultare con un numero di bit a zero funzionale alla sua validità. Una volta che la proof of work è terminata, il blocco non può essere cambiato senza rifare tutto il lavoro. Visto che i blocchi successivi sono legati al primo, il lavoro necessario per cambiare il blocco dovrebbe includere il rifacimento di tutti i blocchi. Ogni bitcoin, seguendo Nakamoto, è unico ed imm modificabile, questo grazie alla struttura che lo forma, quindi non può essere duplicato, ne esisterà sempre uno, con un solo codice identificativo.

Ogni utente riceve la notifica delle diverse transazioni, le quali attendono la loro conferma, e inizia la verifica sulla validità, circa la catena che si sta generando. In questo modo, visto che ogni utente è a conoscenza di ogni transazione, si evita per esempio che uno stesso utente possa spendere due volte lo stesso bitcoin, nel caso si tratti di uno scambio monetario. La catena non è contigua, può subire delle variazioni, ad esempio se un utente effettua un cambio nella transizione, e questo cambio viene accettato da tutti i nodi, si formerà un nuovo blocco, aggiornato, da cui inizieranno le nuove decisioni. Il sistema di prova del lavoro risolve anche il problema di determinare la maggioranza nel processo decisionale, ogni processore equivale ad un voto, questo va a eliminare la possibilità, da parte di chiunque, di falsificare il sistema. Se la maggioranza si basasse su un sistema di voto seguendo gli IP, il risultato potrebbe essere falsificato da chi ha la possibilità di accedere a più IP contemporaneamente. La decisione della maggioranza è legata alla lunghezza della catena, che ha richiesto l'investimento di sforzo maggiore nella prova del lavoro. Per modificare un blocco passato, sarebbe necessario rifare la prova del lavoro del blocco stesso e di tutti quelli seguenti, e poi raggiungere e superare il lavoro dei nodi onesti.

Gli step che individua Nakamoto per far funzionare il network di nodi nella catena sono:

1. le nuove transazioni devono essere rese pubbliche a tutti i nodi della rete;
2. ogni nodo raccoglie le nuove transazioni in un blocco;
3. ogni nodo lavora per trovare una prova del lavoro per il proprio blocco;

4. quando un nodo trova una prova del lavoro, rende il blocco pubblico per tutti gli altri nodi;
5. i nodi accettano il blocco solo se tutte le transazioni in esso sono valide e non sono già state usate una volta;
6. i nodi esprimono la loro accettazione del blocco lavorando per creare il blocco seguente nella catena, utilizzando l'hash del blocco accettato.

Gli utenti, quindi i nodi, lavorano per espandere la stessa catena, inserendo blocchi sempre nuovi. La struttura legata alla logica delle transazioni e della catena di blocchi, di contenuti, verificati è vantaggiosa, soprattutto per garantire la trasparenza nelle transazioni.

L'esigenza di concretizzare il rapporto fiduciario tra cittadini e governo è sempre più una realtà. Un sistema di governance e di operazioni, nel settore pubblico, basato sulla blockchain e quindi sulla trasparenza e la verifica di tutte le transazioni avvenute, consente lo spostamento del potere decisionale, completamente nelle mani dei cittadini, che diventano i principali gestori della governance. Inoltre, la potenzialità nella tecnologia della catena di blocchi risiede anche nella sua sicurezza, un attacco esterno dovrebbe radunare una capacità di calcolo tale da poter cryptare tutti i nodi facenti parte della catena, anche se dovesse riuscirci potrebbe riprendere solo i propri pagamenti, quindi otterrebbe di più restando nel gioco degli scambi.

La struttura di Merkle tree

Per tutelare sempre la validità delle transazioni, queste vengono sottoposte, anche durante l'eliminazione, a controllo secondo la struttura di Merkle, ovvero quella della maggior parte delle funzioni di hash. Qualunque tentativo di modificare qualsiasi parte del Merkle tree porterà ad un'incongruenza da qualche parte nella catena. Nello specifico un Merkle tree è un tipo di struttura binaria, composto da un set di nodi, con un grande numero di nodi dipendenti alla base della struttura, che contengono dati sottostanti, un insieme di nodi intermedi dove ogni nodo è l'hash. La finalità del Merkle tree è quello di consentire che i dati in un blocco siano consegnati in maniera frammentaria: un nodo può scaricare solo l'intersezione di un blocco da una sorgente, la piccola parte della struttura di loro interesse da un'altra sorgente, per assicurarsi che tutti i dati siano correnti. Il protocollo Merkle tree è, senza dubbio, essenziale per la sostenibilità della transazione sul lungo periodo, perché individua i blocchi non validi e li elimina.

La privacy è un'altra caratteristica importante della blockchain, nonostante le transazioni siano tutte pubbliche, è possibile mantenere la privacy, le informazioni non vengono legate ad un utente particolare, ma il transito delle stesse è visibile, per consolidare la validità della catena. Nel caso della creazione di una catena alternativa non valida, diversa da quella originale, i nodi non accetteranno mai una transazione invalida, o un blocco che la contenga. I bitcoin, quindi, seguendo la logica della tecnologia che li rende possibili (la blockchain), si auto-regolano, eliminando, non solo i rischi insiti in qualsiasi transazione tra le parti, ma anche la necessità di leggi regolamentari tradizionali, che hanno dimostrato di essere inefficaci in occasioni come, ad esempio, il riciclaggio di denaro. Il nuovo modello legato al bitcoin promuove, comunque, un modo di lavorare e di agire, onesto e corretto, svincolato da possibili forme di egoismo, tutti gli users hanno lo stesso potere decisionale.

I cittadini hanno bisogno di trasparenza e della possibilità di partecipare in modo continuo al processo decisionale. A differenza dei modelli rappresentativi tradizionali di governance, in cui vengono esercitati sistemi di controllo e di equilibrio attraverso rappresentanti delegati tramite elezioni, nell'ambito del modello di consenso dei bitcoin, la responsabilità è distribuita direttamente ed esercitata da tutti. Viene a crearsi una nuova forma di responsabilità sociale condivisa, garantita dal sistema trasparente e legittimato dalla tecnologia blockchain.

Le innovazioni derivanti dall'uso della blockchain, in sintesi, sono:

- scambio rapido di dati tra attori diversi;
- verifica automatica dell'identità dei nodi;
- integrità ed autenticità dei dati scambiati.

La vera rivoluzione, come spiegato dalla rivista The Economist, risiede nella tecnologia descritta fin ora, ovvero la blockchain che tutela le transazioni tra gli utenti, ma allo stesso tempo genera un modo nuovo, disintermediato, p2p, per gli utenti, che contempla una comunicazione diretta tra gli stakeholder, garantita dagli hash. Il sistema bitcoin, è il modello più conosciuto di uso della blockchain, alla luce di quanto evidenziato da Nakamoto, è un sistema sicuro, grazie all'impossibilità di aggirarne i meccanismi, ed economico, perché elimina le commissioni e gli intermediari. Secondo The Economist si potrebbe utilizzare la stessa logica in ambiti diversi, oltre a quelli dei bitcoin e la governance per poter rendere gli scambi più efficienti. Il meccanismo della blockchain può essere applicato a tutti quei campi

che richiedono un intermediario, oltre a quello bancario, quindi per incentivare l'attuazione del p2p, della sharing economy e della tutela dei commons.

Il potere decisionale nelle mani esclusivo degli utenti, tutelati dalla tecnologia blockchain, potrebbe generare, alla luce di quanto emerso, una maggiore responsabilità e commons equamente distribuiti, consentendo la creazione di nuovi modi di produzione.

Nakamoto S., *Bitcoin: A Peer-to-Peer Electronic Cash System*.

Arlyn Culwick *MayorsChain: a blockchain-based public expenditure management system*.

Libro Bianco delle applicazioni alternative della Blockchain.

The Economist, *The next big thing*.

La Digital Strategy nell'innovazione rurale. Il ruolo svolto da Blockchain e Open Data. Daniela Sparano

Fonte: <https://www.ruralhack.org/che-cose-la-blockchain-e-come-funziona/>