

Blockchain : Gli Smart Contract

Febbraio 14, 2018 · admin



Continua la rubrica dedicata ad uno dei temi più caldi del momento: la Blockchain.

Contrastanti sono i pareri sull'argomento. C'è chi sostiene che il mondo dei Bitcoin sia un enorme bolla speculativa che presto richiederà una regolamentazione da parte degli organi competenti, altri, invece, considerano il fenomeno come grossa opportunità di guadagno.

Intanto noi di RuralHack, continuiamo il nostro viaggio alla scoperta di questa rivoluzionaria tecnologia e di tutti i suoi possibili ambiti applicativi.



Blockchain in 5 punti

Brevemente possiamo ricapitolare e sintetizzare la blockchain e il suo funzionamento in cinque macro punti :

1. E' una rete *peer-to-peer* (una rete tra pari) di computer, al cui interno avviene uno scambio di dati e di informazioni. Il bitcoin è un'informazione, che ha un valore economico e permette di effettuare scambi nel network. Il numero di bitcoin riproducibili è limitato, stimato intorno ai 21 milioni, e gli scambi avvengono con quei bitcoin, il cui prezzo dovrebbe tendere a salire.
2. I blocchi che formano la catena sono degli attori della rete che mettono in circolo i nuovi bitcoin, vengono chiamati miner (minatori). Ad oggi, occorrono dispositivi con una potenza di calcolo sempre maggiore, per rispondere all'esigenza di protezione verso i blocchi. Il timing, ovvero l'algoritmo alla base della blockchain, viene garantito dal fatto che più aumentano i player e la loro potenza di calcolo, più la catena diventa sicura garantendo l'equilibrio nel sistema.
3. I nodi garantiscono l'efficacia delle transazioni, gli utenti stessi sono garanti degli scambi. Sono registri che contengono tutti i passaggi di monete da un capo all'altro della rete, in un sistema aperto e controllabile da chiunque.

4. La sicurezza è il valore centrale dei bitcoin, è una rete sicura di pagamento in grado di garantire la validità nelle transazioni e l'anonimato nella protezione dei propri dati. Sono i nodi e i miner a garantire la sicurezza di tutto il sistema, considerando che il bitcoin non può essere contraffatto o riutilizzato.
5. Fonte di guadagni sempre maggiore, ogni nodo e miner riceve una percentuale di bitcoin, definita fee, ogni volta che controlla una transazione diventando così sempre più redditizio controllare gli scambi nel sistema di blocchi. Ogni transazione deve risultare accettata per il 51% dei nodi della rete, altrimenti verrà annullata. Ogni utente investe un grande quantitativo di soldi per diventare un nodo di controllo, quindi non gli converrebbe che la catena saltasse a causa di un'anomalia.

Il vero potenziale dei bitcoin, come già sottolineato resta la blockchain, un protocollo che permette di annientare gli intermediari, le terze parti, tutto viene gestito da rete di blocchi che validano le operazioni. Lo scopo è quello di generare una rete orizzontale, aperta a tutti.



Gli Smart Contract

Importante è parlare di smart contract quando parliamo di blockchain. Se questa tecnologia consente di eliminare gli intermediari, consentendo agli utenti di effettuare le proprie transazioni in modo diretto, lo stesso vale per la stipulazione dei contratti. Gli smart contract sono l'evoluzione dei contratti classici, dove il patto viene sancito in un sistema reticolare, reso possibile da:

- Un blocco per permettere di escludere terze parti;
- Una "porta sul retro" per autorizzare solo le parti del contratto;
- Alla sicurezza della transazione. Le due parti hanno accesso alla stessa solo se non è ancora terminata. Quando la transazione risulterà conclusa entrambe le parti saranno escluse dal blocco, questo verrà sigillato e risulterà impossibile accedervi o apportare

delle modifiche di alcun tipo, grazie alla tecnologia degli hash.

Quindi, gli smart contract sono un insieme di clausole contrattuali che si rafforzano attraverso l'uso di codice di programmazione, *Ethereum*, uno degli esempi più efficaci della realizzazione dei contratti tramite la tecnologia blockchain. Il contratto viene creato come parte di una transazione e gestito da ogni singolo nodo. Uno smart contract, non è necessariamente un contratto in senso strettamente legale, ma comunque può diventarlo, dipende dal tipo di transazione e dagli obiettivi degli attori coinvolti. Nei contratti classici, figura di un intermediario risulta cruciale per garantire la buona riuscita dello scambio, negli smart contract, invece, l'intermediario non è necessario, lo scambio viene garantito dal codice.

Come funziona ?

Ogni utente deve iscriversi nella rete del sito per inserirsi all'interno dei nodi. Il potenziale acquirente crea il contratto attraverso una web app e lo invia all'indirizzo del venditore collocata in Ethereum, attraverso gli ether, una valuta elettronica simile ai bitcoin, può creare una prima tipologia di scambio. Quando si decide di intraprendere la realizzazione di un contratto intelligente, a ogni utente viene fornita una chiave pubblica e una privata, la prima serve come firma digitale, l'altra per accedere al proprio wallet, in cui sono collocati i propri soldi digitali; il server non è centralizzato, quindi la logica base è quella p2p, dove gli scambi avvengono direttamente tra gli utenti

La particolarità degli smart contract risiede, soprattutto nella *disintermediazione*; non serve un ente che tuteli la transazione perché è garantita dal sistema della blockchain. Un contratto in senso classico è *“un accordo avente finalità lecite sottoscritto volontariamente da due o più parti, ciascuna delle quali si propone di creare uno o più obblighi legali tra di loro”*. Lo smart contract non può legarsi a questa definizione, perché non gestisce nessun tipo di accettazione, è uno scambio che non prevede agenti, ma si basa principalmente sulla fiducia, tra due o più parti, garantita da un algoritmo. Lo scopo è quello di ridurre i costi associati alla transazione e incrementare la sicurezza alla contrattualistica esistente.

La blockchain compensa il problema della validità dell'utente, circa la definizione della propria identità, l'identità diventa una garanzia ed anche i canali di pagamento negli smart contract, grazie al libro mastro e alla proof of work.

Quando sono utili ?

Questi possono essere usati per:

- Smart Property, i beni immobili possono essere venduti, affittati o scambiati attraverso la catena di blocco;
- Transferable virtual property, sono oggetti digitali che possono essere negoziati, ma non duplicati.
- Agent, sono programmi autonomi che vengono usati per mantenere il proprio wallet. Il denaro si ottiene dai servizi agente di distribuzione.
- Distributed markets sono un modo per implementare legami p2p, tra pari e compravendita di azioni, permettendo alle monete digitali di entrare nei mercati azionari globali.

I contratti intelligenti consentono di automatizzare le interazioni tra le parti, non solo per gli scambi tra privati, ma anche per una moltitudine di operazioni, e quasi tutte richiedono la figura di un terzo ente che faccia da garante, sostituito dalla blockchain.

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

Smart Contract: http://szabo.best.vwh.net/smart_contracts_idea.html

Ethereum: <https://www.ethereum.org/>

Blockchain, Bitcoin storia e spiegazione: <http://www.chefuturo.it/2015/10/blockchain-bitcoin-storia-spiegazione/>

Pepe S., *Investire Bitcoin*, Flaccovio Dario .

Fonte: <https://www.ruralhack.org/blockchain-gli-smart-contract/>