

Blockchain e Smart Contracts: i contratti intelligenti del futuro

di F. dalle Nogare – Capire come funziona la tecnologia sottostante la blockchain è compito arduo che lasciamo agli esperti di algoritmi.

Tuffarsi nel futuro ed immaginare quali applicazioni beneficeranno di questa tecnologia è invece più semplice e anche più divertente.

Prima però va compreso che la blockchain aggiunge una dimensione ulteriore all'internet che conosciamo.

Internet è la rete delle reti all'interno della quale scambiamo dati e informazioni, compriamo e vendiamo beni e servizi, effettuiamo pagamenti e trasferimenti di titoli e denaro ecc. Tutto questo avviene sempre all'interno di piattaforme proprietarie riconducibili ad un soggetto che svolge un ruolo (spesso remunerato) di intermediario e di garanzia.

Può trattarsi di Amazon per i beni che compriamo, di Facebook per i dati che scambiamo, delle banche presso le quali abbiamo aperto i nostri conti per le transazioni economiche che svolgiamo. Insomma un intermediario c'è sempre.

La tecnologia rivoluzionaria della blockchain scardina questi paradigmi. Se compro o vendo o scambio dati e informazioni, lo faccio direttamente con il mio interlocutore perché il data base che contiene le mie interazioni – criptate – è distribuito tra un numero elevatissimo ed imprecisato di partecipanti.

E' come scaricare i file con Torrent. Se lo facciamo (ma non

andrebbe fatto...è solo un esempio!) entriamo a far parte di una community che utilizza una rete peer-to-peer nella quale non ci sono intermediari ed è retta da un modello di consenso distribuito.

Soltanto che qui stiamo parlando non di singoli bit di film da scaricare, ma di transazioni in piena regola che vengono effettuate all'interno di community sempre più vaste.

Ma cosa succede se vendo/acquisto una macchina usando la blockchain?

Immaginiamo che una casa automobilistica metta in vendita un'auto nuova. Immaginiamo anche che il venditore faccia parte di una community in rete di migliaia e migliaia di persone. Il venditore crea un "blocco" di informazioni, nel quale sono inserite tutte le caratteristiche tecniche dell'auto e i dati amministrativi e lo "immette" nella rete, nell'ambito della community di appartenenza.

Immediatamente tutti i partecipanti ricevono il blocco di informazioni. Questo blocco, e le informazioni che esso contiene, sono riconosciuti/approvati dalla maggioranza della community (con automatismi resi possibili da sistemi di algoritmi e tecnologie assai complessi) e diventano "contenitori" di informazioni accessibili in qualsiasi momento e luogo da parte di tutti i membri della community.

Questi blocchi, una volta creati, sono anche immutabili e quindi possono essere sempre recuperabili per ogni fine utile (attestazione, prova processuale, ricostruzioni fattuali ecc.).

Inoltre, la loro modifica fraudolenta risulta pressoché impossibile, visto che si dovrebbe raggiungere il consenso della maggioranza dei nodi, ovvero di migliaia (o anche milioni) di persone. Infine, i dati personali inseriti sono crittografati e nessuno può accedervi senza il consenso del titolare di tali dati.

Questo è solo un esempio, ma varrebbe lo stesso per l'acquisto o vendita di una casa o di qualsiasi altro bene o servizio.

Ma torniamo alla nostra storia.

Nel contesto sopra descritto, un membro della community si fa avanti per acquistare l'auto, e mette in rete nella community, un nuovo blocco di informazioni contenente i suoi dati anagrafici, la sua disponibilità economica ecc. Anche in questo caso il contenuto del blocco è riconosciuto/approvato dalla maggioranza della community e si aggiunge, con le stesse caratteristiche di cui sopra, al blocco iniziale (la catena inizia a formarsi).

Il venditore può controllare i dati e decidere di procedere. A questo punto succede qualcosa di nuovo. Utilizzerà un format contrattuale assolutamente inedito. Parliamo degli Smart Contracts.

Gli Smart Contracts sono codici e/o protocolli di programmi predefiniti e adattati alle transazioni più diverse, in grado di adeguarsi da soli "strada facendo" a seconda dei dati dei contraenti, dell'oggetto contrattuale, delle prestazioni previste, delle clausole di rescissione, annullamento e capaci altresì di gestire l'enforcement contrattuale.

É un passo avanti incredibile.

Facciamo un esempio: supponiamo che l'automobile sia pagata a rate. Se l'acquirente dovesse "bucare" una rata, grazie alla tecnologia blockchain il contratto "intelligente" non consentirebbe più l'uso dell'auto, la quale verrebbe bloccata a distanza, fino alla regolarizzazione dei pagamenti.

E più apparecchi e beni saranno tra loro collegati tra loro con la blockchain, più gli smart contracts svilupperanno potenzialità maggiori nell'eseguire e gestire a distanza le transazioni commerciali.

Questo apre la strada a tutta una serie di possibilità e innovazioni. Lavori che conosciamo da secoli scompariranno e altri faranno il loro ingresso. E questo è davvero solo l'inizio. Perché la tecnologia blockchain è solo all'inizio del suo percorso.