IAssicurDBI

TECNOLOGIA BLOCKCHAIN E SMART CONTRACT

Nello scorso numero di gennaio, abbiamo fatto un piccolo passo all'interno del vasto mondo della tecnologia **blockchain** e delle sue applicazioni: il radicale incremento della potenza di calcolo a disposizione, l'aumento di intelligenza generale complessiva dei software, il cambio di paradigma culturale a cui stiamo assistendo (l'era digitale) e la possibilità da parte di tutti (o quasi) di utilizzare qualsiasi tipo di tecnologia (una sorta di democrazia tecnologica), stanno in qualche modo ridefinendo gli standard di progettazione di molti strumenti di lavoro. La tecnologia **blockchain** è figlia legittima della rivoluzione digitale dei primissimi anni '90 ed è stata implementata come oggi la conosciamo solo al compimento della maggiore età (18 anni dopo), da un tuttora sconosciuto programmatore, sotto lo pseudonimo di Satoshi Nakamoto.

Nè più nè meno di un registro digitale, seppur sufficientemente complesso da essere universalmente utilizzato e riconosciuto, la blockchain memorizza transazioni ed eventi in modo sicuro e verificabile: tale registro è infatti consultabile pubblicamente da tutti, vive come Napster o Emule in un network ***peer-to-peer*** (i dati non sono raccolti in un unico sistema centralizzato, ma sono distribuiti nella rete), ed è impossibile da alterare (nel senso che una volta scritti, i dati non possono essere retroattivamente cambiati senza che tutti i blocchi successivi si modifichino di conseguenza) grazie ai più intelligenti sistemi di crittografia disponibili. Nella pratica, la firma di ciascun blocco - una stringa alfanumerica calcolata da un algoritmo - dipende deterministicamente dal contenuto del blocco stesso ***più*** la firma del blocco precedente: alterare la firma di un blocco significa di fatto alterare tutte le successive e dare quindi origine ad una seconda blockchain, e così via.

Avere a disposizione una tecnologia di questo tipo, che garantisca fondamentalmente sicurezza, intelligenza e - perché no? - democrazia, apre tutta una serie di scenari possibili che fino a qualche tempo fa non erano (quasi) neanche pensabili realisticamente: dalle catene di fornitura globali, alle transazioni finanziarie, passando per i beni contabili e i social network distribuiti. Non è un caso, infatti, che la prima applicazione della allora nuova tecnologia fu "monetaria" a tutti gli effetti: un ***libro mastro*** per la nascente Bitcoin e l'obiettivo (chiaro a tutti) di eliminare le intermediazioni o i supervisori delle transazioni (Istituiti di Credito, Organi Statali, ecc.), regolare le interazioni tra soggetti e garantire alle persone di poter entrare in possesso di un fondo monetario affidabile e sicuro sia in termini di transazioni sia in termini di privacy, per monetizzare le proprie informazioni.

Proseguire in questa direzione diviene ormai quasi naturale e non fanno fatica ad emergere altre interessanti applicazioni della blockchain in varie aree del business. Tralasciando per un attimo gli ambiti finanziari ed economici diretti, uno dei settori più significativi in cui la blockchain attuale si sta indirizzando è la contrattualistica: gli **Smart Contract**, protocolli informatici che garantiscono la negoziazione o l'esecuzione di un contratto, permettendo l'automazione (parziale o totale) di molti tipi di clausole contrattuali, ne sono l'esempio più paradigmatico.

Se si pensa alla blockchain, in modo astratto, come ad un sistema per permettere transazioni ***in assenza di fiducia tra le parti e in assenza di ente controllore terzo a garanzia***, ci sono casi in cui è possibile utilizzarne le proprietà per eseguire automaticamente i contratti. Supponiamo di fare una **polizza assicurativa** da 10,00 euro per un ritardo aereo così definita: se l'aereo ha un ritardo maggiore di 15 minuti all'atterraggio, il passeggero che ha stipulato la polizza ha diritto a un risarcimento di 100,00 euro.

- Nel mondo senza smart contract (il nostro attuale, di fatto), il passeggero sarà decisamente scettico sul firmare questo tipo di polizza, perchè anche nel caso in cui avesse pienamente ragione (l'aereo ha un ritardo di ben 56 minuti!) sa già che dovrà perdere tempo e pazienza in un'infinita trafila di operazioni: aprire la segnalazione all'assicurazione, aspettare i tempi tecnici della pratica, seguirla passo passo e, infine, attendere il pagamento; anche l'assicurazione - dal canto suo - sa che dovrà eseguire diversi controlli per ciascuna segnalazione e che una discreta percentuale di passeggeri starà tentando di ottenere un rimborso anche se non dovuto. Nella pratica, la totale mancanza di fiducia reciproca (e nel sistema, come si dice) unita all'incertezza del pagamento (ridicolo, in questo caso) rende il contratto molto poco appetibile da entrambe le parti.

- Nel mondo ***smart*** (contract) che ci immaginiamo, l'utente e la compagnia stabiliscono assieme in modo preciso cosa si intende per "ritardo maggiore di 15 minuti all'atterraggio" - banalmente rispetto alla tabella ufficiale dell'aeroporto di Malpensa, ad esempio - e, tramite dei linguaggi specializzati, viene scritto lo smart contract relativo. In questo modo, quando arriva il giorno del volo, è lo smart contract stesso (consultando l'orario della tabella ufficiale di Malpensa e quello dell'effettivo atterraggio) a verificare la presenza o meno del ritardo in automatico e ad effettuare, se dovuto, il pagamento di 100,00 euro **senza alcun intervento dell'utente (che può mentire o sbagliarsi) o dell'assicurazione (che può prendere tempo e ritardare il pagamento)**.

Tramite lo smart contract, in pratica, il contratto viene eseguito senza assumere la "buona fede" delle parti e senza alcun bisogno di fare controlli incrociati successivi: è lo smart contract stesso, salvato ed eseguito tramite un sistema distribuito come la blockchain, ad eseguire automaticamente la transazione tra le parti. Il rivoluzionario approccio consente infatti di inserire nella blockchain sia la transazione economica nei due sensi (pagamento del premio ed eventuale liquidazione del sinistro), sia la traccia degli eventi accaduti (orari di arrivo effettivi, rispetto agli orari di arrivo previsti).