Blockchain: la cassaforte di cristallo

Author : Marco Crotta

Date : 8 Marzo 2019

Una delle prime caratteristiche che vengono tipicamente associate alla blockchain è la sicurezza. Questo non dovrebbe sorprendere, data la dimostrazione pratica che questa tecnologia ci sta dando ogni giorno in ormai 10 anni di diffusione. Vediamo infatti che, per la prima volta, una tecnologia informatica ci permette di avere dati che vengono resi praticamente immutabili una volta scritti, protetti in modo esemplare da funzioni crittografiche di comprovata affidabilità.

È proprio grazie a queste sue esclusive peculiarità che la blockchain è in grado di gestire addirittura una moneta elettronica ad alto valore, come bitcoin e molte altre. Va ricordato che la blockchain di fatto è nata per rendere possibile il bitcoin, il cui nome compare fin dal titolo del famoso paper di **Satoshi Nakamoto**, mentre il termine blockchain arriverà solo successivamente, come contrazione di “chain of blocks”, man mano che la criptomoneta si diffondeva.

La blockchain non solo permette di gestire e spostare bitcoin, ma soprattutto è il suo habitat. Non bisogna farsi trarre in inganno su questo punto: i bitcoin “nascono” nella blockchain e non escono mai da essa: esistono solo al suo interno, sotto forma di transazioni. I wallet non contengono bitcoin, ma solo le chiavi crittografiche che permettono di muoverli e disporne.

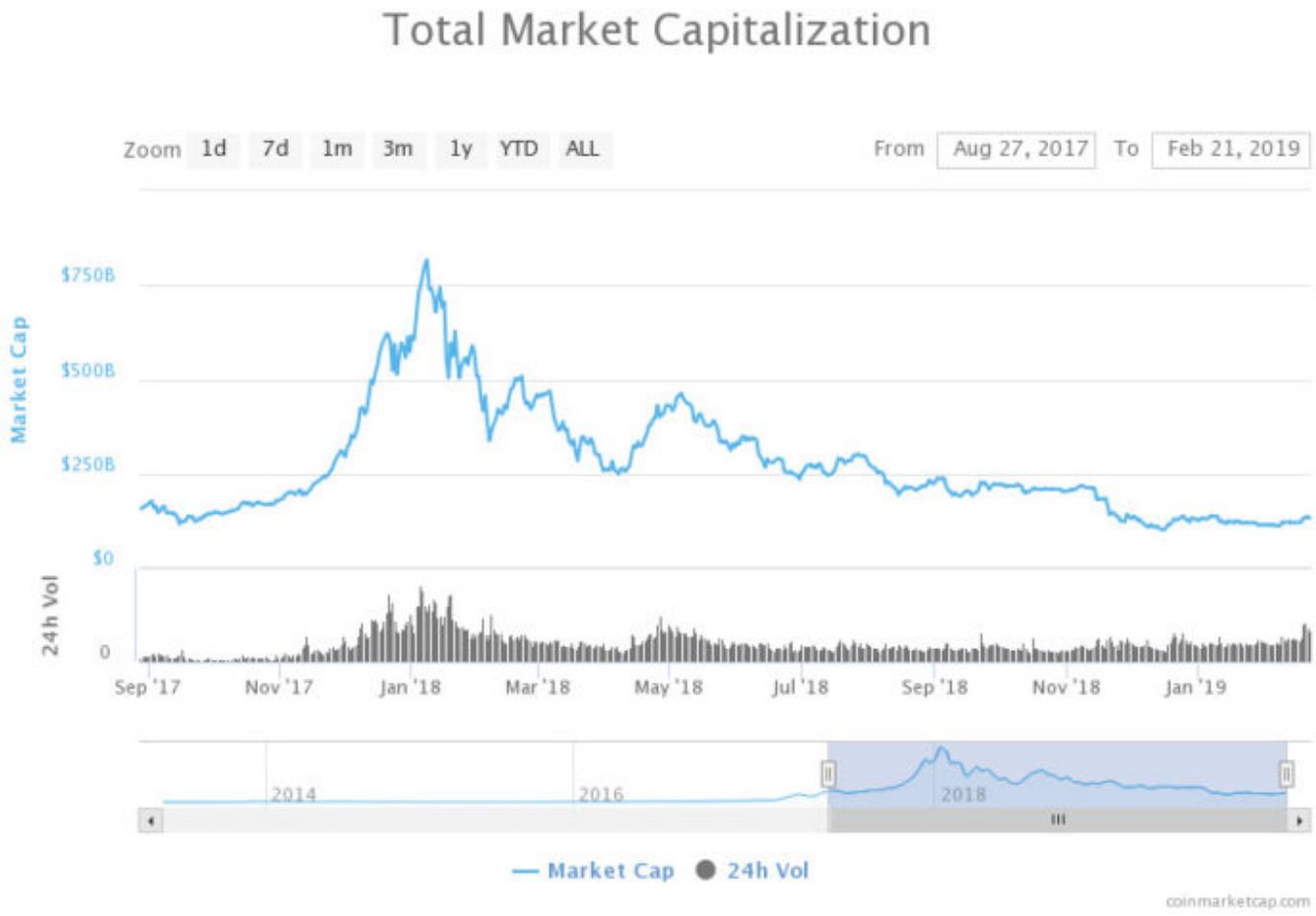
Ma se la blockchain è la “casa” dei bitcoin, **quanto è sicura?** Non è facile dare una risposta a questa domanda dato che non esiste un’unità di misura o paragone, ma possiamo dare un’idea della sua sicurezza attraverso un’immagine.
La blockchain è come una cassaforte di cristallo: da una parte è completamente trasparente, dato che chiunque ha la possibilità di averne una copia, studiarla, esaminarla e conoscere ogni spostamento, da indirizzo a indirizzo, di ogni frazione di bitcoin in essa contenuto. Dall’altra, le strutture scelte per immagazzinare i dati, le modalità utilizzate per legare tra loro transazioni e blocchi, e la crittografia asimmetrica usata per autorizzare le operazioni fanno sì che nessuno abbia modo di interferire col funzionamento di questa cassaforte, asportare il valore in essa contenuto o impossessarsene.

Non solo; il codice sorgente della blockchain è completamente aperto, chiunque lo può studiare

per trovare falle o bug. Chiunque può realizzare, con poca spesa, un nodo di questa rete ed entrare a farne parte, eventualmente provare a interferire, senza dover chiedere alcuna autorizzazione. Chiunque può scrivere programmi per interfacciarsi alla blockchain e - potenzialmente - mandare transazioni errate o malevole, ma senza sortire effetto. Infatti, tentativi di questo tipo vengono fatti costantemente e ininterrottamente. Eppure **la blockchain non ha mai perso un solo satoshi** (la centomilionesima parte di un bitcoin) e ha continuamente dimostrato, nei 10 anni passati, la sua totale sicurezza e affidabilità.

Inoltre, la Blockchain è sostenuta da una rete di nodi diffusi sul pianeta, interconnessi tra loro in una modalità nota come “peer-to-peer” (da pari a pari) per cui, anche in caso di pesanti menomazioni di questa rete (c’è chi si spinge a dire anche in caso di disastro nucleare), essa non ne soffrirebbe in alcun modo.

Quindi, per rispondere alla nostra domanda, potremmo dire che la blockchain è stata finora in grado di resistere ad ogni attacco di cui sia stata oggetto mantenendo in totale sicurezza al suo interno un controvalore che ora ammonta a **133 miliardi di dollari** (market cap a marzo 2019, mentre a dicembre 2017 ammontava a **813 miliardi**). Un bottino di tutto rispetto, di certo più che sufficiente a motivare molti hacker a fare del loro meglio per impossessarsene, ma senza successo. Non sono molti i sistemi in grado di reggere un confronto e di fornire altrettante garanzie all’utente.



Ma come è possibile tutto questo? Innanzitutto va precisato che **quando si parla di "blockchain" si intende il modello pubblico, aperto, decentralizzato, *trustless* e *permissionless*** che possiamo trovare in molte blockchain, quali quelle di bitcoin, ethereum e molte altre. Sono solo queste, infatti, le blockchain che possono fornire livelli superiori di sicurezza in grado di proteggere i dati anche in condizioni di totale apertura ed esposizione. Per tutti gli altri modelli *permissioned*, privati, *trust based*, contrariamente a quanto si potrebbe pensare, non si possono né si devono fare le stesse considerazioni, né dare per scontato di avere le stesse garanzie, dal momento che questi funzionano sotto assunti diversi e in differenti condizioni.

Le blockchain pubbliche traggono la loro sicurezza dal proprio protocollo, che è sicuro *"by design"* in quanto concepito per dare delle forti garanzie in tal senso, tenendo conto che ogni singola operazione sarà certamente oggetto di un attacco. Non solo: il protocollo tiene conto del fatto che più attori all'interno della blockchain potranno avere comportamenti scorretti e, quindi, l'intero sistema di regole dovrà essere affidabile sia in presenza di nemici interni al sistema sia di nemici esterni.

Il concetto di base di questo protocollo è che tutte le informazioni che veicola possono e devono essere controllate in modo autonomo da ogni nodo della rete che le riceve. Si fa leva sulla trasparenza e sulla **verifica costante e distribuita**. Su questo si innesta un articolato sistema di pesi e contrappesi basato sulla teoria dei giochi: le regole infatti incoraggiano ogni partecipante ad applicare le regole su sé stesso e sugli altri, essendo questa la condotta che gli darà i risultati migliori sia a breve che a lungo termine. Barare non conviene mai: è molto difficile, si viene facilmente scoperti, ci si trova a competere contro tutti gli altri nodi onesti e costa moltissimo lavoro che, se fosse impiegato in modo consono alle regole, avrebbe una resa molto più promettente.

Il sistema degli indirizzi si basa sulla crittografia a chiave pubblica. Le criptovalute di quella blockchain sono associate a un indirizzo (concettualmente simile a un IBAN). Questo indirizzo deriva dalla chiave di cifratura pubblica dell'utente. Solo dimostrando di possedere la chiave privata corrispondente, con lo stesso meccanismo alla base della firma digitale, si può disporre un movimento delle monete associate a quell'indirizzo. Va ricordato che stiamo parlando di un tipo di crittografia tra le più sicure al mondo.

I dati sono resi immutabili da un complesso sistema di validazione distribuita chiamato *mining*. I blocchi che contengono le informazioni devono prima essere validati controllando la validità di ogni informazione, e successivamente "chiusi". La chiusura, nota anche col termine *"Proof of Work"*, richiede che il blocco presenti delle caratteristiche ben precise. Questa operazione richiede moltissimi calcoli e l'utilizzo di moltissima energia. Successivamente, una volta che il blocco è chiuso, chiunque avrà la possibilità di verificare autonomamente la correttezza e la validità dello stesso in tempi infinitesimali. Questa complessa procedura, tra le altre cose, **rende i dati contenuti nella blockchain virtualmente immodificabili**: riscrivere un blocco richiederebbe di ripetere tutto il lavoro di chiusura e validazione spendendo di nuovo tutta l'energia, mentre il resto della catena di blocchi continua a crescere avendo quindi una situazione in cui, una volta tanto, è la tartaruga ad inseguire (senza possibilità alcuna) Achille.

Su questa caratteristica di “immutabilità pratica” si innesta il concetto di data certa. Questa caratteristica, accoppiata alla data inserita nel blocco che contiene le informazioni, consente di legare indissolubilmente l’esistenza di quelle informazioni a quella data.

Ma questa non è l’unica trovata all’interno del protocollo delle blockchain: vi sono molti altri dettagli che rivelano tratti di genialità. Ad esempio, uno dei grossi limiti di tutte le altre monete digitali antecedenti la blockchain è stata la possibilità di inflazionare la moneta a piacere, facendo un semplice copia-incolla della moneta virtuale. Bitcoin ha **trasformato questo punto debole in un punto di forza** utilizzando un approccio diverso, per cui non viene digitalizzata la moneta, ma il suo spostamento. Le transazioni infatti non registrano l’informazione *“+10€”* e neppure che *“Mario ha 10€”* ma che *“Luigi ha dato 10€ a Mario”*. Questa informazione non è alterabile in quanto richiede l’utilizzo della chiave privata di Luigi, e solo lui può fare questa operazione. Contemporaneamente, se duplichiamo più volte questa informazione, non facciamo che renderla più sicura. Inoltre, restiamo sempre in grado di conoscere il saldo di Luigi e Mario ripercorrendo la storia di tutte le transazioni. Stesso risultato, massima sicurezza.

Dal punto di vista accademico, va poi ricordato che la blockchain concepita da Nakamoto è “Bizantine Fault Tollerant” (BFT) ovvero è in grado di risolvere il cosiddetto “dilemma dei generali bizantini”: un problema sottostante alle reti distribuite in cui si cerca un modo sicuro per raggiungere il consesso, ovvero fare sì che tutti i nodi della rete distribuita, comunicando fra loro, possano raggiungere l’accordo su una data informazione, anche in presenza di nodi che potrebbero non funzionare o alterare volutamente la sincronizzazione.

A questo protocollo **lavorano alcuni tra i migliori crittografi e programmatori al mondo**. Il tutto è costantemente sottoposto a review, ad analisi, ad *adversarial thinking*, ed è sottoposto ad un costante lavoro di correzione e miglioramento. Basta pensare che spesso, contrariamente a quanto succede con molti software proprietari, nelle blockchain le correzioni agli errori sono pubblicate e applicate prima che queste vengano scoperte e sfruttate per scopi fraudolenti.

Un capitolo a parte andrebbe dedicato agli ***smart contract***. Contrariamente a quanto suggerisce il nome, questi sono programmi che nulla hanno a che vedere col concetto legale di contratto e hanno molteplici ambiti di applicazione che non hanno alcuna attinenza con i contratti. Questi software, sviluppati in proprio da privati e aziende, sono stati spesso messi in crisi da errori nel codice che hanno portato alla perdita di ingenti somme di denaro. Per questo motivo, molto lavoro viene fatto proprio sul versante della sicurezza del codice, spingendo verso l’adozione di librerie, standard implementativi e revisione del codice da parte di enti terzi. Ma tutte le volte che uno *smart contract* ben scritto viene messo in azione, abbiamo la garanzia di un programma che verrà eseguito all’unisono da centinaia di nodi, che dovranno pervenire deterministicamente allo stesso risultato. Avremo cioè un codice inarrestabile.

Tuttavia, nonostante la sicurezza implicita nella blockchain, esistono dei rischi per l’utenza dovuti agli **errori** che si possono commettere o all’inesperienza. La blockchain non perdona: l’utente infatti è responsabile della corretta conservazione delle proprie chiavi crittografiche e di come dispone le transazioni. Molti furti di bitcoin sono stati fatti agendo su vulnerabilità dei wallet, rubando le chiavi o agendo in diversi modi sull’elemento più fragile: l’utente. Ma va ribadito che mai si è stati in grado di scalfire la sicurezza della blockchain stessa.

Esiste un’unica possibilità, nota e costantemente monitorata, di sovvertire il funzionamento di una blockchain, che consiste nel possedere e controllare almeno il 51% dei nodi che la compongono, imponendo a tutti questi di comportarsi in modo sleale e barare. Tuttavia questo rischio, legato alla centralizzazione delle risorse, è fortemente tenuto sotto controllo dalla comunità. Al momento attacchi di questo tipo si sono dimostrati possibili solo sulle blockchain di più piccole dimensioni e a costi molto alti.

Tutte queste caratteristiche fanno sì che, ad oggi, la blockchain sia uno dei sistemi più sicuri mai esistiti, in grado di dare totale controllo all’utente degli asset in suo possesso, garantendo una “pseudo-privacy”, rendendo impossibili intromissioni, espropri o ingerenze esterne. Molti dei sistemi che usiamo tutti i giorni e di cui ci fidiamo non danno le stesse garanzie. Diversamente la blockchain è **trustless by design**, ovvero non richiede fiducia: al suo interno tutto viene verificato, controllato e dimostrato. Uno dei motti della sua community è infatti *“don’t trust, verify”*.

La sicurezza della blockchain, accoppiata da tutte le caratteristiche che abbiamo visto fin qui, ha giustamente stimolato in molti la volontà di utilizzare la blockchain per scopi diversi dal trasferimento di valore. Sono da qui nate le ricerche relative alla notarizzazione dei documenti, *supply chain management*, tokenizzazione degli asset e molte altre. Tutte queste applicazioni distribuite (DApp) godono immediatamente di livelli di sicurezza molto alti. Per questo, c’è da aspettarsi che nel prossimo futuro sempre più applicazioni che necessitano di alte garanzie dal punto di vista della sicurezza saranno sviluppate sulle blockchain pubbliche, decentralizzate e *permissionless*.

Bibliografia:

- https://bitcoin.org/bitcoin.pdf**.**
- https://github.com/bitcoin/bitcoin**.**
- **Andreas M. Antonopoulos, *Mastering Bitcoin.***
- **Francesco De Collibus-Raffaele Mauro, *Hacking finance.***

Articolo a cura di Marco Crotta