Capitolo 1

Introduzione alla blockchain

La parola "blockchain" è nata come un termine informatico per descrivere una struttura dati astratta. Col tempo la tecnologia è divenuta molto popolare e addirittura pervasiva, e così ha catturato l'immaginazione di molti. Oggi, la parola blockchain ha molti significati in molti ambiti.

In questo capitolo

- **La blockchain**
- **Il registro collaborativo**
- **Criptovalute**
- **Smart contract**
- **Una rete trustless**
- **Nuovi modi per collaborare**
- **Un protocollo "grasso"**
- **"In Code We Trust"**
- **Conclusioni**

La blockchain

Per chi lavora in campo informatico, la blockchain è costituita da una serie di blocchi di dati interconnessi. Ogni blocco di dati può memorizzare qualsiasi tipo di informazione, ma tipicamente conserva un insieme di "transazioni". L'informazione contenuta in un blocco è rappresentata da un codice "hash" univoco. Ogni blocco di dati contiene il codice hash del blocco (*block*) che lo precede nella catena (*chain*) (Figura 1.1).

NOTA

Un codice hash crittografico è una rappresentazione abbreviata di una grande quantità di dati ed è estremamente facile da calcolare. Ma se conoscete solo il codice hash, è estremamente difficile risalire ai dati originali che hanno prodotto questo codice hash.

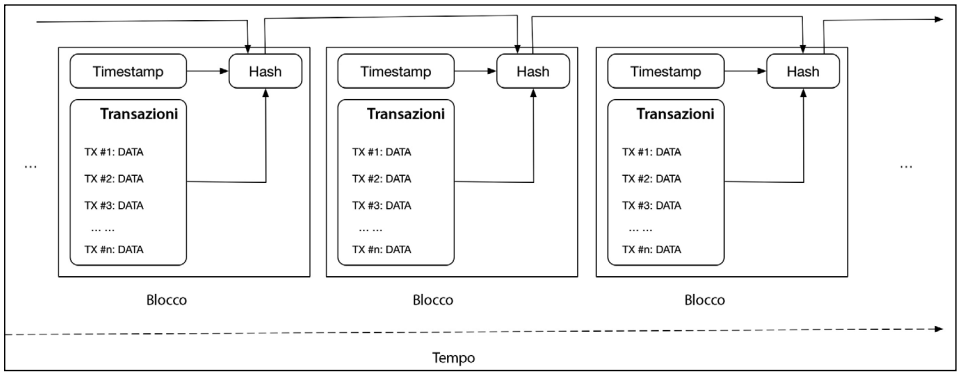

Figura 1.1 Una blockchain.

Perché vogliamo memorizzare dei dati in questa struttura blockchain? Perché non potremmo usare un database? Una funzionalità chiave della blockchain è che è difficile modificare i dati contenuti nella catena.

Immaginate di avere una blockchain con 1000 blocchi. Ora, qualcuno vorrebbe modificare il contenuto del blocco 10. Così questo qualcuno altera i dati, ma in questo modo cambia anche il codice hash del blocco 10. Poiché il blocco 11 contiene il codice hash del blocco 10, questo significa che deve cambiare anche il contenuto del blocco 11, il che a sua volta provoca un cambiamento nel codice hash del blocco 11. Questo processo si propaga lungo la blockchain. E così, per apportare una modifica in un blocco, occorre rigenerare tutti i blocchi che lo seguono. Questo prende il nome di *hard fork*: si tratta della creazione una nuova blockchain che è incompatibile con quella attuale, anche se entrambe usano lo stesso software. In questo senso, una blockchain è immutabile. È impossibile che qualcuno modifichi "silenziosamente" la cronologia di una blockchain. Come possiamo vedere, più è lunga la blockchain, più diviene stabile. Quando si effettuano transazioni sulla rete Bitcoin, spesso si legge che la vostra transazione è "confermata" dopo 6 o più blocchi (circa un'ora, in quanto la rete Bitcoin crea un blocco ogni 10 minuti). Dopo 6 blocchi, è improbabile che emerga una fork di una blockchain alternativa e venga accettata dalla comunità. E così, si è sostanzialmente certi che la vostra transazione è stata registrata come parte della cronologia permanente.

Anche se in una blockchain potete memorizzare qualsiasi tipo di dato, l'utilizzo più frequente della blockchain consiste nel memorizzare i record delle transazioni. Questo è perfettamente logico, in quanto l'accuratezza cronologica e la validità delle transazioni monetarie sono critiche. In pratica, le blockchain vengono usate come registri digitali per memorizzare le transazioni.

Il registro collaborativo

Ora, anche un database può memorizzare cronologie. Noi tutti abbiamo usato spreadsheet o database come registri di transazioni fin dall'invenzione del personal computer. Il registro stesso non complica né offre un significativo valore aggiunto.

Rimane la domanda: perché abbiamo bisogno di usare una nuova struttura dati, pesante dal punto di vista computazionale, come la blockchain? La risposta sta nella seconda funzionalità chiave della blockchain: è facile organizzare una rete collaborativa basata su blockchain.
Dal momento che ogni blocco viene aggiunto alla catena singolarmente, possiamo progettare una rete in cui una o più parti propongono il blocco successivo e poi tutti i nodi della rete (ovvero i computer che costituiscono la rete) possono convalidare il blocco proposto e raggiungere un consenso sul fatto che debba essere aggiunto alla blockchain. Se un blocco proposto è considerato non valido dalla maggior parte dei partecipanti alla rete, la blockchain può annullarlo e perfino punire i suoi proponenti. Per ulteriori dettagli tecnici sul consenso e la blockchain, consultate il prossimo capitolo.
La regola di convalida dipende dalla specifica blockchain. Per esempio, i miner della blockchain Bitcoin esaminano le firme crittografiche e i saldi dei conti per ogni transazione registrata nel blocco per assicurarsi della sua validità.
Facendo questo, la blockchain diviene un registro collaborativo.

Criptovalute

Il registro può, appunto, registrare i movimenti di una qualche valuta. Una grande innovazione è stata rappresentata dal fatto di aver immaginato che la blockchain può anche definire una propria "valuta" e conservarne le transazioni. È chiamata criptovaluta perché la validità di tale valuta è garantita dalla crittografia impiegata nelle reti blockchain. Per esempio, ogni transazione in tale valuta è firmata digitalmente per garantire che sia autentica e unica. Quando si parla di una criptovaluta si usano anche i termini "criptotoken" o anche solo "token". In questo libro impiegheremo questi termini come sinonimi.
Le regole di convalida di una transazione consentono a una blockchain di creare una propria "politica monetaria" che governa la sua criptovaluta. Per esempio, la blockchain Bitcoin definisce le seguenti regole per la creazione e il consumo della sua criptovaluta (per esempio, i bitcoin).

- I proponenti di un nuovo blocco riceveranno nuove unità appena create della valuta bitcoin.
- Vi saranno solo 21 milioni di bitcoin in totale e pertanto la ricompensa per il blocco si riduce nel corso del tempo.
- Ogni bitcoin può essere diviso in cento milioni di satoshi, da usare nelle transazioni.
- I miner di bitcoin riceveranno bitcoin per la convalida delle transazioni in un nuovo blocco.

L'aspetto interessante, qui, è che tali politiche monetarie sono codificate nel software della blockchain Bitcoin. Nessuno può modificarlo senza creare una nuova blockchain (come nel caso di una *hard fork*).
La criptovaluta creata dalla blockchain ha una funzione cruciale. Fornisce un meccanismo tecnico, tramite una struttura a incentivi (una tecnica economica), per ottenere qualcosa che la tecnica software, da sola, non può ottenere: creare fiducia.
Mettendo insieme la tecnologia blockchain e l'idea della criptovaluta possiamo realizzare reti trustless (non fidate) ma tuttavia collaborative.

NOTA

Per molto tempo, la comunità tecnologica ha ritenuto che un uso "enterprise" della tecnologia blockchain consistesse nel realizzare un registro distribuito all'interno di un'azienda o di un gruppo di aziende che già intrattenevano relazioni fidate. I sistemi di convalida di reti fidate e i nodi semplificano lo sviluppo di protocolli di consenso ad alte prestazioni. Aziende come IBM e Microsoft hanno promosso l'uso di tali blockchain a permesso o fidate. Tuttavia, dopo molti anni di sperimentazione, è chiaro che tale uso "enterprise" delle blockchain in un ambiente fidato/interno/centralizzato ha un impatto molto limitato sulle pratiche aziendali. La blockchain fidata è solo un'altra soluzione software di gestione dei dati a disposizione dei dipartimenti IT di un'azienda. Tale uso delle blockchain non crea alcun effetto in rete.

Smart contract

Quando i miner della blockchain Bitcoin convalidano le transazioni, controllano solo le più semplici regole contabili. Per esempio, il mittente della transazione deve avere fondi sufficienti nel proprio conto e deve firmare la transazione con la propria chiave privata. È facile per i miner di bitcoin verificare queste transazioni e raggiungere un consenso. Ora, invece di controllare le semplici regole contabili, i miner della blockchain possono lanciare ogni genere di programma e poi raggiungere un consenso sulla correttezza dei risultati del calcolo eseguito. I risultati in termini di consenso possono poi essere salvati sulla blockchain per la registrazione permanente. Questa è l'idea sulla quale si basa lo smart contract. Il meccanismo di consenso sviluppato per i bitcoin può essere impiegato per garantire la sicurezza per ogni tipo di calcolo.

La blockchain Ethereum è fra le prime blockchain pubbliche a supportare gli smart contract. Offre una macchina virtuale Turing completa, chiamata EVM (*Ethereum Virtual Machine*). La EVM opera su tutti i nodi per convalidare la correttezza di attività di calcolo di natura arbitraria. I programmi scritti per la EVM cono conservati all'interno di conti nella blockchain. Ogni transazione che coinvolge il conto verrà convalidata dal programma stesso tramite i miner Ethereum e solo a questo punto la transazione potrà essere registrata nella blockchain. Gli smart contract sono diventati fra le più importanti applicazioni blockchain.

L'idea davvero rivoluzionaria della blockchain è la possibilità di ottenere risultati fidati di calcoli generati da partecipanti non cooperativi su reti trustless.

Una rete trustless

L'applicazione originale e più nota di una blockchain è la rete Bitcoin, creata e gestita interamente su una rete trustless. Chiunque può accedere alla rete Bitcoin per convalidare transazioni, proporre nuovi blocchi e ricevere ricompense in bitcoin se il blocco viene accettato da parte del sistema di consenso. Coloro che partecipano alla rete Bitcoin non si conoscono fra loro e non si fidano gli uni degli altri. Tuttavia, il sistema è concepito in modo da impedire che uno dei partecipanti possa applicare modifiche truffaldine alla blockchain.

L'esatto meccanismo impiegato dalla rete Bitcoin per ottenere il consenso è chiamato *Proof-of-Work* (PoW). Presenteremo i dettagli tecnici di PoW nel prossimo capitolo. Per il momento basti sapere che vi sono meccanismi mediante i quali i partecipanti a questa rete trustless si accordano su quali transazioni sono valide e devono essere registrate nella blockchain. Centrale per il meccanismo di consenso è l'uso delle criptovalute, che incentivano i partecipanti a comportarsi secondo le regole (ovvero a non convalidare transazioni non valide). Questo uso delle criptovalute come incentivi è alla base della cripto-economia.

La possibilità di raggiungere un consenso senza un'autorità fidata centrale è davvero potente. Oggi tutte le più grandi aziende che operano su Internet si fondano sull'effetto rete. Aziende come Uber e Airbnb operano come autorità centrali per le reti che hanno costruito. Sono le aziende a definire le regole, specialmente quelle regole che riguardano le transazioni di denaro sulla rete. Si assicurano che ognuno segua le regole e da questo processo traggono grandi profitti. Ma queste autorità sono davvero necessarie? Le loro reti non potrebbero funzionare anche senza che la società funga da "creatore delle regole" e "arbitro"? Perché non possono essere gli stessi partecipanti della rete a possedere la rete e a trarne i profitti?

Tuttavia, tutti gli sforzi di sostituire Uber e di realizzare una "rete cooperativa" di trasporto non-profit sono ampiamente falliti. I motivi sono vari.

- La sostituzione dell'azienda centralizzata con un'organizzazione non-profit altrettanto centralizzata non risolve il problema della fiducia. Molte organizzazioni non-profit sono corrotte e perlopiù arricchiscono i loro ideatori. I *driver* e i *rider* continuerebbero a non avere alcuna reale "proprietà" della rete.
- Un'organizzazione non-profit centralizzata non è dotata dei mezzi per ricompensare i primi adottatori del sistema e quindi per lanciare la rete. Uber, al contrario, può raccogliere denaro dagli investitori e trasformarli in grandi incentivi, fino a che l'effetto rete non cominci a funzionare da sé.

Una rete blockchain basata su cripto-token può risolvere entrambi questi problemi. La rete opera da entità trustless e pertanto non può essere corrotta. La rete può emettere dei token per ricompensare i primi adottatori tramite un processo come l'*Initial Coin Offering* (ICO). Inoltre, trasformando i partecipanti alla rete (i *driver* e i *rider* nell'esempio di Uber) in proprietari di token, si può stabilire una rete monetaria e creare quella fedeltà alla rete che Uber non è mai stata in grado di conseguire.

Nuovi modi per collaborare

Questa rete trustless dà origine a nuovissimi metodi di collaborazione. Per esempio, immaginate che vi sia un prezioso insieme di dati, ma che nessuno possieda tutti quei dati. Ogni partecipante alla rete possiede una parte di tale insieme, ma è riluttante a condividere la propria parte, in quanto colui che condividerà la propria parte per ultimo trarrà il massimo dei vantaggi da tale condivisione. In questo scenario, è l'intero sistema a non poter far uso di tale insieme di dati.

NOTA

Un caso molto concreto è rappresentato dai dati medici in possesso degli ospedali in un assetto di sanità privata: anche se, collettivamente, tali dati sono estremamente preziosi, nessun ospedale è incentivato a condividere la propria parte di dati.

Ora, immaginiamo una rete in cui tutte le parti possono contribuire con i loro dati. Quando l'uso di tali dati genera un profitto, la rete distribuirà la ricompensa alle parti in base agli accordi preventivi e ogni distribuzione viene convalidata in modo indipendente dai partecipanti alla rete, in modo che non vi sia alcuna possibilità di frodi.
Tale rete dati collaborativa è possibile anche senza blockchain, ma richiede un'autorità centrale che tutti considerano fidata per determinare e distribuire i profitti. L'autorità centrale fidata ha sia gli incentivi sia l'opportunità di "barare" e questo complica la realizzazione di tali reti fidate.

Un protocollo "grasso"

La caratteristica peculiare di una rete blockchain è che permette di creare valore senza avere alle spalle una corporation. Il valore della rete non dipende da un'azienda, ma dal protocollo della rete e si riflette nel valore dei token della rete. Questa teoria è chiamata *Fat Protocol* (protocollo "grasso"), ed è stata originariamente proposta da Joel Monegro di Union Square Ventures. Per esempio, sulle reti Bitcoin o Ethereum di oggi, non esiste una società che abbia raggiunto una valutazione oggettiva significativa, ma ciononostante tali reti fanno circolare e "valgono" decine di miliardi di dollari. La Figura 1.2 mostra come i protocolli Internet siano *thin*, "magri" e pertanto come siano le applicazioni a catturare la maggior parte del valore; al contrario i protocolli blockchain sono *fat*, "grassi" e sono in grado loro stessi di catturare il valore.

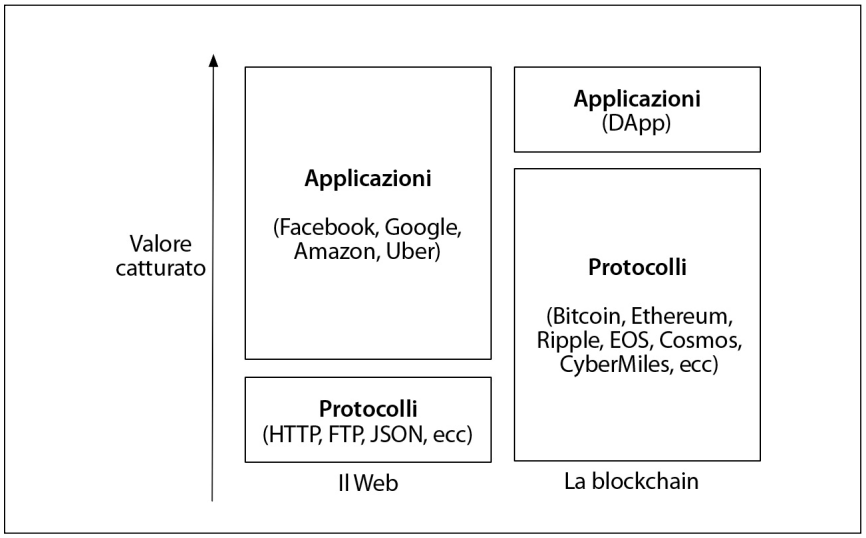

Figura 1.2 Protocolli "magri" (thin) e protocolli "grassi" (fat).
Figura adattata da https://www.usv.com/blog/fat-protocols.

L'essenza stessa delle grandi corporation si basa sul fatto che i costi delle transazioni esterne fra la corporation e i suoi partner sono molto più elevati dei costi delle transazioni fra i dipartimenti interni all'azienda. Questo è dovuto alla struttura di comando e controllo che le corporation possono imporre ai dipartimenti interni. Tuttavia, nell'economia attuale, dove i costi di comunicazione calano continuamente, il costo delle transazioni esterne precipita al punto in cui le aziende ricorrono sempre di più all'*outsourcing* e al lavoro a contratto (è esattamente il caso degli esempi di Uber e Airbnb).
Le reti blockchain trustless riducono ulteriormente i costi delle transazioni esterne. Queste reti snelliscono le transazioni non solo delle informazioni ma anche del denaro. La rete blockchain pubblica, insieme ai cripto-token, permette di attuare nuovi modelli commerciali che hanno le potenzialità di sostituire le attuali corporation o di creare nuove opportunità che non possono essere risolte dalle corporation.
Le regole della collaborazione e del consenso di una rete blockchain sono incorporate e applicate nello stesso protocollo di rete. Questo assetto è naturalmente molto differente rispetto alle regole "a natura umana" applicate dalle corporation. La regole di collaborazione basate su blockchain sono algoritmiche, automatiche, veloci, eque e coerenti. Per sfruttare appieno le reti blockchain, occorre codificare il più possibile le regole di collaborazione nel protocollo di rete.

"In Code We Trust"

Gli smart contract spesso somigliano ai classici contratti del mondo reale. Per esempio, le due parti di una transazione si possono impegnare sul fatto che i fondi verranno pagati solo se si sono verificate determinate condizioni. Ora, è compito dei validatori e dei gestori della rete stabilire se tali condizioni si sono verificate e in quale modo la transazione debba essere eseguita quando i nuovi blocchi verranno aggiunti alla blockchain.
Tuttavia, a differenza dei contratti "fisici", che sono garantiti dalla forza del governo e della legge, gli smart contract possono applicare automaticamente le regole di collaborazione della blockchain. Le regole sono scritte nel codice e verificate dai partecipanti non fidati della rete, per prevenire ogni corruzione o collusione. Per questo motivo, consideriamo il codice degli smart contract la "legge" nelle reti blockchain. Il codice viene eseguito così come è stato scritto. Anche se il codice contiene bug o effetti collaterali non previsti dal suo autore, è comunque considerato la "fonte della verità" e applicato come una "legge".

Conclusioni

In questo capitolo abbiamo trattato i concetti chiave delle reti blockchain. Tramite le criptovalute, la rete blockchain combina il software e la tecnica economica per generare fiducia in una rete di partecipanti non cooperanti. Questo meccanismo ha le potenzialità per sovvertire le aziende che oggi operano sulla base di Internet, in quanto gli effetti rete non vengono più gestiti dalle grandi aziende situate al centro di tali reti. La rete, al contrario, viene gestita dal software, condiviso da ogni partecipante. Tutta la fiducia si basa sul codice: "In Code We Trust".