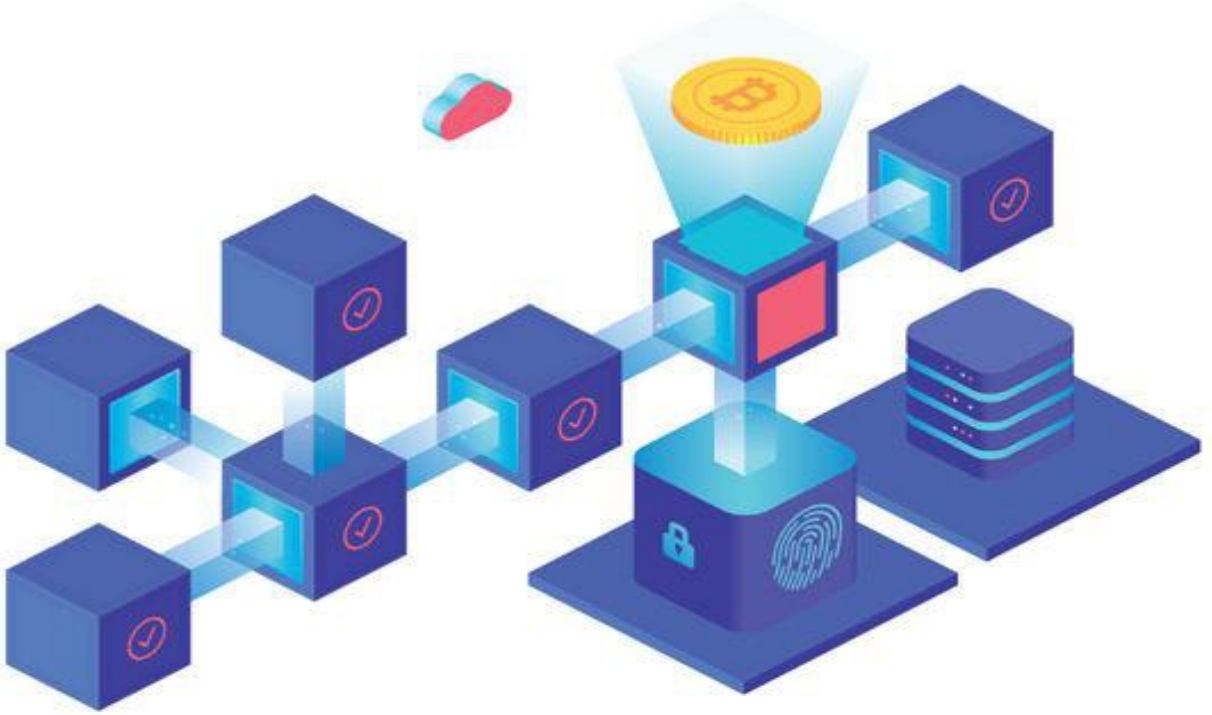
Gianluca Chiap Jacopo Ranalli Raffaele Bianchi

BLOCKCHAIN

TECNOLOGIA E APPLICAZIONI PER IL BUSINESS



Tutto ciò che serve per entrare nella nuova rivoluzione digitale

HOEPLI

Blockchain

Gianluca Chiap
Jacopo Ranalli
Raffaele Bianchi

Blockchain

Tecnologia e applicazioni per il business

EDITORE ULRICO HOEPLI
MILANO

via Hoepli 5, 20121 Milano (Italy)
tel. +39 02 864871 – fax +39 02 8052886
e-mail hoepli@hoepli.it

www.hoepli.it

Seguici su Twitter: @Hoepli_1870

ISBN EBOOK 978-88-203-9007-5

Progetto e realizzazione editoriale:
Maurizio Vedovati – Servizi editoriali (info@iltrio.it)

Copertina:
Sara Taglialegne

Realizzazione digitale:
Promedia, Torino

Indice

- PoW mining
- PoW: pro e contro

- Proof of Stake (PoS)
  - PoS mining (staking)
  - PoW vs PoS

- Fork
  - Fork regolare
  - Soft fork
  - Hard fork

6. Aspetti della decentralizzazione

- Immutabilità
- Rischio
- Fiducia
- Cripto-economia

- Scalabilità
  - Transazioni off-chain
- Distributed Ledger Technologies
  - Tangle (IOTA)

7. Criptovalute

- Blockchain e criptovalute
  - Internet del valore
  - Il denaro come linguaggio
- Evoluzione del denaro
  - Baratto
  - Denaro commodity
  - Denaro commodity-backed (paper money)
  - Denaro fiat
  - Denaro digitale

- Panoramica sulle criptovalute
  - Caratteristiche delle criptovalute
  - Politiche monetarie
  - Modello di distribuzione

8. Bitcoin

- Overview tecnica e politica monetaria
  - Blockchain e Bitcoin
  - Scarsità
  - Mining
  - Indirizzi e privacy
- Scalabilità
  - SegWit
  - Lightning network
  - Rete di pagamenti
  - Micro-pagamenti e pagamenti

- streaming

9. Smart contract

- Che cos'è uno smart contract
- Esempi di smart contract
  - Crowdfunding
  - Consegna a domicilio
- Token
- ICO
  - Struttura di una ICO
  - Perché avviare una ICO
- Ethereum
  - Overview tecnica e politica monetaria
  - Gas
  - Account e indirizzi

10. Altcoin

11. Exchange

Mercato

- Order book e order matching
- Ordini parziali
- Bid-ask Spread
- Profondità di un mercato (market depth)
- Volume
- Volatilità

Posizioni

- Long position
- Short position
- Margin trading e leva finanziaria

Tipologie di ordine

- Market order
- Limit order
- Stop loss

Manipolazione del mercato

- Pump and dump

- Organization
- La rivoluzione del web
  - Web 1.0
  - Web 2.0
  - Web 3.0
- Le blockchain private nell'industria
  - Blockchain private vs blockchain pubbliche
  - Blockchain private vs database distribuiti
  - Perché le aziende stanno scommettendo sulle blockchain private
  - Hyperledger
- Interledger, il protocollo per l'Internet del valore

13. Le applicazioni blockchain

- Servizi finanziari
  - Transazioni e pagamenti
  - Verifica dell'identità
  - Trading e finanza
- Industria 4.0
  - Supply chain
  - Anti-contraffazione
- IoT
  - Smart home
  - IOTA
  - Self driving car
- Energia
  - Power Ledger
- Le applicazioni in ambito governativo

- Identità digitale
- Il voto digitale
- Sanità
- Istruzione

Il retail

No-profit

Le Nazioni Unite

Digital advertising

BAT (Basic Attention Token) e browser Brave

Smart property

Il progetto Svezia

Le applicazioni del cloud

- Cloud storage
- Cloud computing

Prefazione

La blockchain è una tecnologia che viene spesso definita “l’Internet del futuro”, dal momento che rappresenta un vero e proprio stravolgimento infrastrutturale con possibili ripercussioni in innumerevoli settori. La sua componente innovativa è legata alla possibilità di sviluppare applicazioni decentralizzate, effettuare transazioni immutabili e rimuovere la presenza di intermediari. Grazie a queste e ad altre caratteristiche, la blockchain è destinata a cambiare molti aspetti della società moderna, e si ritrova ora al centro di

discussioni tecnologiche e monetarie.

Sebbene l'interesse mediatico su questi temi sia relativamente recente, è dal 2008, anno di nascita del Bitcoin, che si è iniziato a parlare di blockchain, e col passare del tempo il numero di persone a essersi incuriosite è cresciuto sempre più. Tra questi ci siamo anche noi, un gruppo di amici che, dopo aver approfondito e sperimentato con la tecnologia, ha deciso di mettere la propria esperienza a disposizione di imprese e startup intenzionate a implementare la blockchain nei loro progetti.

Tuttavia ci siamo subito resi conto che in questo ambiente esistono ancora molti pregiudizi e una sensazione di

diffidenza generale che ne ostacolano la diffusione, specialmente in Italia, dovuti in primo luogo alla disinformazione e alla scarsa disponibilità di materiale informativo in italiano sul tema. Ed è per questa ragione che abbiamo deciso di scrivere questo libro, per dare a chiunque gli strumenti per comprendere il funzionamento della blockchain e consentirgli di capire il reale potenziale che si cela dietro questa tecnologia – che va ben oltre le criptovalute.

Nel corso di questi anni la blockchain – come, più in generale, le Distributed Ledger Technologies (DLT) – sta iniziando a prendere piede in quasi ogni settore, andando a fornire delle

soluzioni prima irrealizzabili: dalla finanza all'IoT, dal governo all'industria, dalle valute alla creazione di veri e propri contratti digitali. La maggior parte delle grandi imprese sta infatti iniziando a utilizzare queste tecnologie in vari ambiti – supply chain, smart city, pagamenti internazionali istantanei ecc.

Siamo ormai entrati in una nuova era informatica – proprio come era successo negli anni '90 con Internet – e quelli che ne trarranno maggiore vantaggio sono senz'altro coloro che se ne renderanno conto per primi.

Teniamo a precisare sin da subito che per comprendere il potenziale e le implicazioni della blockchain è

necessario innanzitutto conoscere nel dettaglio le caratteristiche della tecnologia. La causa principale della disinformazione sul tema, infatti, non è altro che la scarsa conoscenza di basi tecniche da parte di chi divulga le informazioni. La nostra intenzione è risolvere il problema alla radice.

Nel tentativo di accelerare l'adozione di queste tecnologie e favorire la nascita di nuove applicazioni, abbiamo cercato di raccogliere nel modo più semplice e compatto possibile tutte le informazioni che permettessero di ottenere una conoscenza esaustiva dell'argomento, e di avere quindi i mezzi per approfondire

autonomamente ogni aspetto di questo tema apparentemente complesso.

Questo libro offre tutto ciò che serve per entrare nella nuova era digitale, è un percorso a 360 gradi a partire da una visione sul panorama globale a una guida sulla tecnologia, e non richiede alcuna conoscenza specifica. Concluderemo con numerosi esempi di come la blockchain venga oggi applicata, mettendo in luce benefici e rischi di un mondo decentralizzato che, inevitabilmente, sembra destinato a essere sempre più reale.

Nella speranza di trasmettervi anche solo una piccola parte della nostra passione per questo tema, vi auguriamo una buona lettura.

Gli autori

Introduzione

Nate formalmente nel 2009 con la creazione del Bitcoin grazie alla geniale intuizione di Satoshi Nakamoto, le criptovalute sono passate in poco tempo da materia per pochi appassionati ad argomento capace di catturare l'attenzione del pubblico mondiale, complici anche le variazioni esponenziali (in positivo e in negativo) del prezzo di queste valute.

In un mercato a oggi composto da più di 2.000 criptovalute e con un valore stimato pari a oltre 200 miliardi di dollari, il Bitcoin ne rappresenta una

parte enorme (54% dell'intero mercato a ottobre 2018)[1].

Ciò che accomuna le criptovalute è la tecnologia su cui sono basate: la blockchain.

Tuttavia, le applicazioni della blockchain non si limitano alle criptovalute. Infatti già oggi la blockchain è considerata una delle tecnologie più innovative a disposizione delle imprese.

Per comprendere in che modo si possa trarre vantaggio dalla tecnologia blockchain è però indispensabile conoscere nel dettaglio i principi del suo funzionamento.

D'altronde la novità e la complessità

dell'argomento, l'immensa mole di contenuti a disposizione, la mancanza di un testo unico ove consultarli e il fatto che la gran parte del materiale informativo sia in lingua inglese, rendono l'accesso a questa tecnologia non alla portata di tutti, o comunque fanno sì che acquisire le competenze necessarie per approfondire autonomamente questi temi sia estremamente impegnativo.

Per contribuire alla divulgazione di queste tecnologie, abbiamo cercato di raggruppare tutti i concetti fondamentali, esponendoli nella maniera più chiara e semplice possibile per chiunque, anche per chi non possiede conoscenze in ambito informatico.

Perché allora conoscere la tecnologia è così importante?

In realtà la stessa Internet e ancor prima i computer hanno passato un periodo simile negli anni ’80-’90, quando solamente chi era in possesso di competenze molto specifiche era effettivamente in grado di coglierne il potenziale o di contribuire al loro sviluppo. Questo fenomeno è infatti tipico di tutte quelle tecnologie nuove e ancora in via di sviluppo – specialmente quelle innovative e infrastrutturali – non ancora pronte per essere utilizzate poiché si trovano in “fase di prototipazione”.

Il che ci porta ad affrontare la stessa

domanda da una diversa prospettiva: perché approfondire l'argomento se la tecnologia non è ancora pronta?

La blockchain sarà fondamentale per le imprese

Ogni giorno nascono infatti nuovi progetti con l'intento di sfruttare questa tecnologia per sviluppare soluzioni innovative e/o ridurre enormemente costi e inefficienze.

Per esempio, uno dei campi di applicazione è nella supply chain (la catena di distribuzione), dove un prodotto tipicamente deve superare numerosi passaggi prima di arrivare al

consumatore, e richiede la collaborazione di molti esercizi commerciali. Tra coloro che già la implementano c'è Carrefour, che la usa per identificare e tracciare alcuni prodotti, così come semplificare enormemente la condivisione delle informazioni con le numerose parti coinvolte nel processo di distribuzione.

Ma le prospettive sono sempre più rosee, a questo proposito: di recente è stata istituita la European Blockchain Partnership per la creazione di un'infrastruttura digitale europea nel settore pubblico[2] (iniziativa di cui fa parte anche l'Italia), e anche nel resto mondo la blockchain è già ritenuta una

delle tecnologie più interessanti su cui puntare.

Riteniamo dunque che la blockchain acquisirà inevitabilmente sempre più rilevanza nel corso dei prossimi anni e che questo sia il momento più adatto per approfondire in che modo questa tecnologia può essere applicata alle imprese per rivoluzionare il modo in cui operano.

Investire in criptovalute o in progetti basati su blockchain

Le maggiori opportunità di investimento riguardano mercati in forte crescita e

con un grande potenziale innovativo, come per esempio il mercato delle criptovalute. Per questa ragione si parla di una vera e propria "corsa all'oro", e molti investitori per paura di perdere l'opportunità (in gergo FOMO, fear of missing out) si affrettano a entrare nel mercato senza prima conoscerne i dettagli – e le insidie.

Il mercato stesso è intrinsecamente rischioso per via della sua estrema volatilità, e il pericolo aumenta ulteriormente quando si investe in monete da poco introdotte sul mercato o addirittura in fase di ICO.

Infatti, se per chiunque è possibile documentarsi su Internet avendo accesso

a ogni tipo di informazione, allo stesso tempo è diventato anche estremamente facile comprare le criptovalute da parte di chi non ha ancora ben chiaro a cosa va incontro. Questa situazione, unita a una regolamentazione in molti Paesi non ancora ben definita, ha contribuito alla nascita di molti progetti-truffa con l'intenzione di fare leva su questa vasta categoria di investitori abbagliata da false promesse e alti guadagni, per poi sparire con i loro soldi.

Sebbene il mercato attuale sia molto più controllato rispetto agli scorsi anni e i rischi siano diminuiti, il pericolo è sempre in agguato.

Conoscere la tecnologia permette non solo di cogliere i punti di forza e

l'innovazione di un progetto basato su di essa, ma rende anche immediato il riconoscimento di potenziali frodi.

La blockchain è destinata a cambiare il mondo come lo conosciamo

Considerando le problematiche relative alla gestione dei dati personali, è ormai noto a tutti come i nostri dati siano nelle mani di pochi, di quanto poco controllo ne abbiamo e del pericolo che corriamo quando non vengono gestiti correttamente. Questa è solo una delle conseguenze dei tanti sistemi

centralizzati che costituiscono la società in cui viviamo oggi.

Proviamo a immaginare come sarebbe un mondo in cui si possa mantenere il controllo dei propri dati, in cui l'autorità passi dall'essere concentrata su poche entità centrali a essere equamente distribuita, in cui la presenza di intermediari e garanti venga sostituita da un sistema incorruttibile nel quale poter avere fiducia.

Questa visione sta lentamente prendendo forma grazie alla tecnologia blockchain.

Conoscere la tecnologia ti permetterà di andare oltre i luoghi comuni e di prendere parte alle discussioni sul tema. Capirai in cosa

consiste l'unicità di questa tecnologia e perché la sua implementazione ed evoluzione è ritenuta da molti ormai inesorabile.

Basata sui concetti di open source e di decentralizzazione, la blockchain è una tecnologia che si rafforza al crescere della community e del numero di persone che la utilizzano. Anche tu avrai l'opportunità di far parte di questa rivoluzione. Senza dilungarci ulteriormente, proseguiamo con le differenze – e le strane somiglianze – tra la blockchain e le altre tecnologie dei giorni nostri e del passato.

1. Il dato corrente si può trovare su https://coinmarketcap.com/currencies/bitcoin.
2. Maggiori dettagli su https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership.

Glossario breve

Architettura (di rete)

Identifica l'architettura di una rete: solitamente si fa distinzione tra architettura client/server e architettura peer-to-peer (vedi **Peer-to-peer**).

Bitcoin

"Bitcoin", con la B maiuscola, si riferisce all'intero ecosistema Bitcoin, mentre "bitcoin" con la b minuscola fa riferimento alla criptovaluta identificata dal simbolo BTC.

Peer-to-peer (p2p)

Un modello di architettura logica di rete informatica in cui i nodi sono equivalenti, o ‘paritari’ (peer), potendo fungere al contempo da client e server verso gli altri nodi terminali (host) della rete.

Criptovaluta (token)

Un asset digitale sviluppato su una tecnologia blockchain.

Denaro fiat

In italiano, “moneta legale”. È una valuta che acquisisce valore poiché riconosciuta da uno Stato. Sono le tipologie di valute correntemente utilizzate, di cui fanno parte l’euro, il dollaro e la sterlina.

Network

Insieme di due o più sistemi informatici interconnessi tra loro.

1

Una panoramica sulla tecnologia

Una tecnologia in fase di prototipazione

Un mondo in cui non è facile entrare

Negli anni in cui i primi computer

diventavano accessibili al pubblico, il loro utilizzo era molto complesso per un utente con poche conoscenze di linguaggi informatici, dal momento che l'interazione avveniva esclusivamente mediante la digitazione di stringhe di testo sul terminale di comando. È solo in seguito alla creazione di interfacce grafiche e applicazioni che i computer sono diventati mainstream, riuscendo a nascondere la complessità della tecnologia e permettendo così anche a utenti meno esperti di utilizzare e apprezzare questi nuovi dispositivi.

Ciò che ostacolava la diffusione dei computer a quel tempo era una vera e propria barriera conoscitiva nei confronti dell'utilizzatore, la quale, il

più delle volte, limitava persino le potenzialità della tecnologia e i modi in cui poteva essere utilizzata. Mancava quindi un'interfaccia semplice e intuitiva che eliminasse la necessità di apprendere competenze specifiche.

La tecnologia blockchain e le criptovalute stanno attualmente attraversando un periodo simile: essendo la tecnologia ancora in fase di definizione e sottoposta a continui aggiornamenti, l'interazione da parte dell'utente avviene tramite procedure macchinose e non banali che spesso richiedono l'apprendimento di nuove competenze specifiche – analogamente a come il terminale di comando

ostacolava l'ingresso nel settore a gran parte dei suoi potenziali utilizzatori.

Se vi è capitato di provare ad approfondire l'argomento in passato, vi sarete resi conto che anche per compiere le operazioni più basilari come comprare o vendere una criptovaluta, si devono affrontare concetti mai incontrati prima (la registrazione a un crypto-exchange, la scelta del wallet, dove custodire la chiave privata ecc.), i quali spesso lasciano un utente poco esperto con il dubbio di aver sbagliato qualcosa.

Coinbase

Tra le piattaforme di trading di criptovalute, una di quelle che ha ottenuto più successo è indubbiamente Coinbase, che ha reso estremamente semplice e intuitivo l'acquisto e la vendita di alcune criptovalute. Si può quindi considerare come uno dei primi casi riusciti di applicazione in grado di eliminare la barriera di accesso al mondo delle criptovalute.

Il life-cycle della blockchain

Per continuare l'analogia con il settore dei software, si può provare a identificare i diversi stadi dello sviluppo della tecnologia blockchain

facendo riferimento alle fasi che accompagnano lo sviluppo di un software (Figura 1.1).

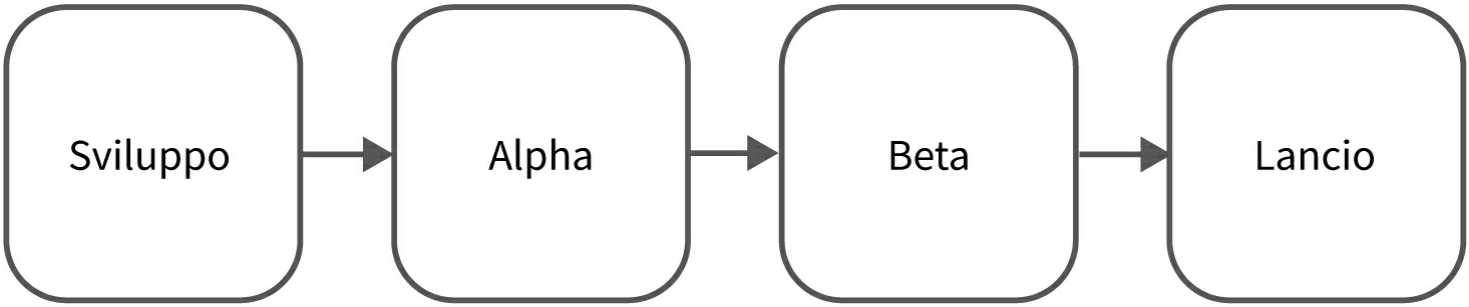


Figura 1.1 – Le fasi che compongono il ciclo di vita di un software.

Fase Alfa: si intende lo stadio di sviluppo successivo al completamento di un software o piattaforma, quando gli sviluppatori effettuano dei test per verificarne il corretto funzionamento.

Nel caso della blockchain, in questa fase avviene il controllo di errori e

viene consolidato il suo funzionamento per garantire la sicurezza. Una volta conclusa questa fase, la blockchain viene resa pubblica e diventa accessibile a chiunque.

Fase Beta: si intende lo stadio in cui si mette alla prova la solidità di un software tramite una fase di test da parte di un gruppo di utenti selezionati, i beta-tester. Una blockchain è accessibile agli utenti a partire dal momento in cui viene pubblicata, perciò non esiste una categoria di persone selezionate per fare i beta-tester. È possibile quindi considerare i beta-tester come quella categoria di utenti che per primi decidono di usufruire di una particolare

blockchain e di contribuire al suo sviluppo. Questa categoria può meglio essere definita come quella degli early adopter (utenti precoci), ovvero coloro che possiedono già conoscenze specifiche e contribuiscono perché credono nella validità della tecnologia.

Gli early adopter si identificano con orgoglio come visionari, dal momento che prima degli altri hanno riconosciuto il potenziale di un progetto o prodotto. A differenza dell'utenza che si avvicina con esitazione, essi non vengono spaventati da eventuali problemi che la piattaforma incontrerà, ma al contrario cercano di contribuire il più possibile al suo perfezionamento e sono spesso le colonne di supporto delle community.

Tuttavia, sebbene una piattaforma sia aperta al pubblico, ciò non significa che sia pronta. Di conseguenza, un utilizzo massivo in questa fase ne potrebbe provocare il collasso per via di un'infrastruttura non ancora solida.

La congestione di una blockchain

In riferimento alle criptovalute, si è già assistito negli ultimi mesi del 2017 ad avvenimenti analoghi a quelli descritti.

L'aumento di interesse nel Bitcoin in quel periodo ha causato una

spaventosa crescita della domanda, e quindi del numero delle transazioni. Tuttavia la blockchain di Bitcoin (e di molti altri progetti) non era ancora pronta per supportare volumi di transazioni così alti, e il risultato è stato una congestione della blockchain. Quello che ne è conseguito è stato un estremo rallentamento nella velocità delle transazioni, unito a un forte incremento del loro costo (passando da pochi centesimi fino a toccare 52 dollari per transazione!).

La blockchain del Bitcoin quindi deve ancora risolvere dei problemi prima di poter supportare l'intera utenza che intende servire, come se fosse ancora in fase Beta. Le soluzioni a questo grosso vincolo sono in fase di sviluppo e potrebbero essere il

tassello mancante che permetterebbe di incrementare enormemente l'efficienza della blockchain e al contempo di rimuovere ogni limite di scalabilità.

La speculazione nel mercato

L'altra conseguenza dell'esplosione di interesse nelle criptovalute è stato l'enorme aumento di valore di tutto il mercato, passato in poco più di un mese da 250 miliardi a quasi 840 miliardi di dollari. Questo fenomeno è stato principalmente causato da

fenomeni speculativi, che hanno portato per esempio il prezzo di un bitcoin da 6.000 a quasi 20.000 dollari (Figura 1.2).

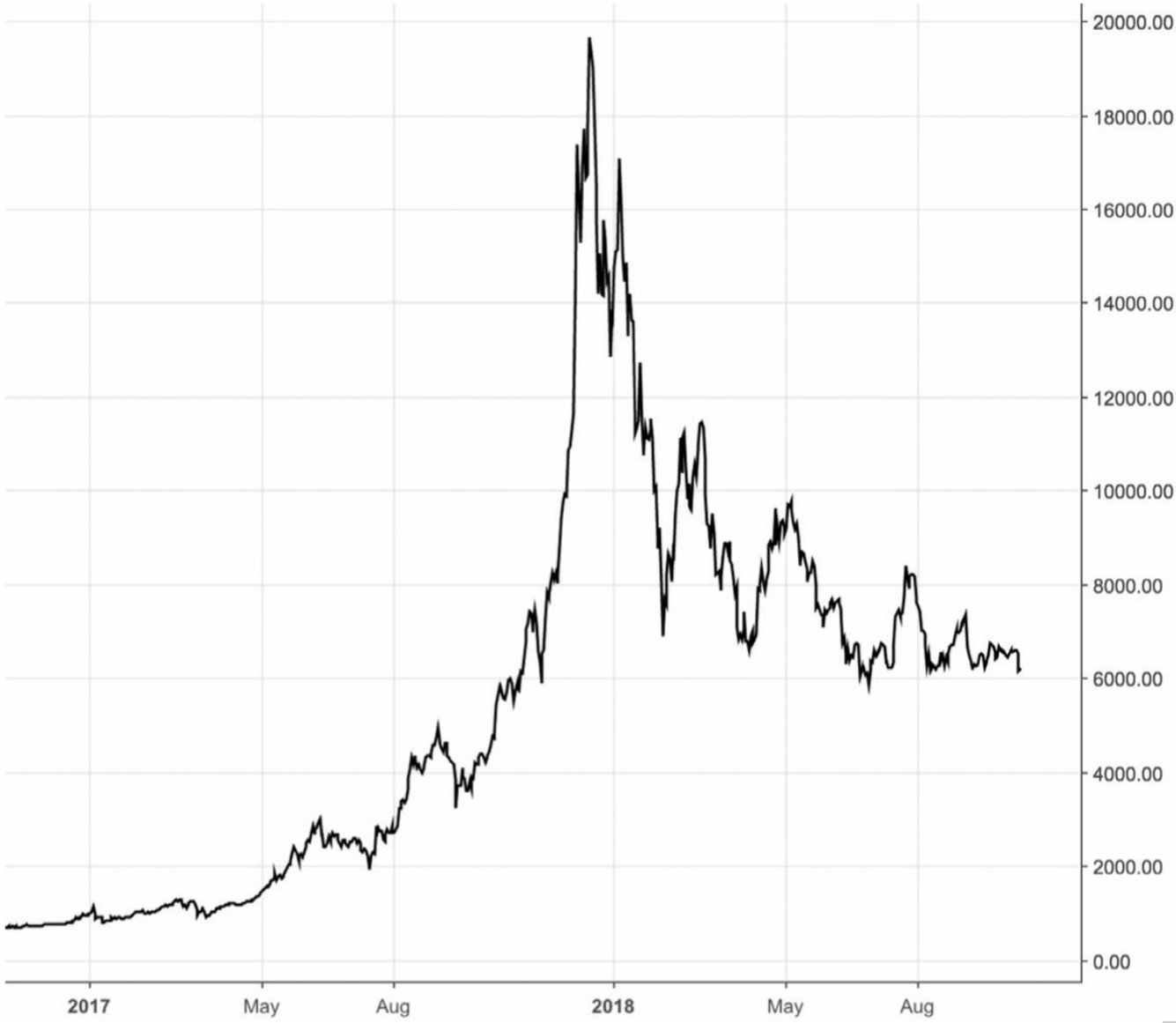


Figura 1.2 – Il grafico del prezzo del bitcoin (© TradingView).

Il crollo immediatamente successivo è stato principalmente dovuto alla speculazione degli

investitori che hanno venduto i propri bitcoin per trarre un forte guadagno dal rialzo improvviso.

Lancio della tecnologia: come ci insegna il successo dell'iPhone e quello di tanti altri prodotti, una tecnologia avrà tanto più successo quanto più il suo utilizzo è semplice e intuitivo.

Così come l'utente medio di servizi come Facebook o Amazon non si pone il problema dei vari protocolli utilizzati o della sua infrastruttura tecnologica, è facile immaginare un futuro dove l'utente medio che vorrà utilizzare le criptovalute o sfruttare una particolare

blockchain non dovrà necessariamente avere competenze di programmazione o conoscenze sulla tecnologia.

Tuttavia prima che questo accada, la blockchain e le criptovalute dovranno essere sottoposte a una rigorosa procedura di miglioramento tecnologico finché non saranno affidabili (lo scopo della fase Beta), così come risolvere problemi di natura politico-sociale assieme a istituzioni e governi per consentire una efficace regolamentazione.

Per quanto riguarda le criptovalute, dal 2009 a oggi è stata fatta molta strada, e un futuro dove sarà possibile utilizzare una o più criptovalute non è così difficile da immaginare.

Per quanto riguarda invece la tecnologia blockchain, non è da escludersi che potrà diventare una tecnologia totalmente integrata nell'infrastruttura delle applicazioni che finiremo per utilizzare quotidianamente, similmente a come oggi consideriamo il cloud.

Se considerata nel suo complesso, la tecnologia blockchain si trova ai primi stadi di una fase Beta – sebbene con qualche complicazione derivante dalla natura digitale e intrinsecamente complessa dell'argomento.

Agli early adopter si vanno infatti ad aggiungere altri gruppi fra cui gli hacker (che spingono la piattaforma a essere

sempre più sicura) e gli speculatori (che sfruttano la predisposizione del mercato delle criptovalute alla speculazione). Ai fini dello sviluppo della piattaforma, gli speculatori aiutano a perfezionare il funzionamento delle piattaforme stesse (cioè a sostenere alti volumi di transazioni), ma assieme agli hacker aumentano la percezione del pubblico che il mercato delle criptovalute sia incerto e pieno di insidie.

Per quanto riguarda la sicurezza, sappiate che le criptovalute non sarebbero neanche potute nascere se la blockchain non fosse stata un'infrastruttura praticamente inespugnabile. La sicurezza è infatti uno dei suoi maggiori punti di forza, e nei

capitoli seguenti analizzeremo in dettaglio come questo problema venga affrontato.

La barriera di ingresso al mercato delle criptovalute e le difficoltà incontrate dagli utilizzatori non sono quindi da vedersi negativamente, dal momento che rappresentano uno stato naturale nello sviluppo di una tecnologia.

L'informazione nella blockchain

La piramide della conoscenza

Un individuo interessato ad approfondire un aspetto specifico di questa tecnologia o un progetto basato su di essa ha in genere due possibilità: fidarsi ciecamente del parere di uno o più esperti oppure informarsi autonomamente. Per chi invece volesse sviluppare un progetto su blockchain, conoscere nel dettaglio la tecnologia è un requisito fondamentale.

Abbiamo cercato di raffigurare quali sono a nostro parere i diversi stadi di apprendimento che permettono di ottenere una reale comprensione di questi temi, considerando che la conoscenza dei concetti alla base della

piramide aumenta l'affidabilità e il livello di comprensione dei concetti dei livelli successivi (Figura 1.3).

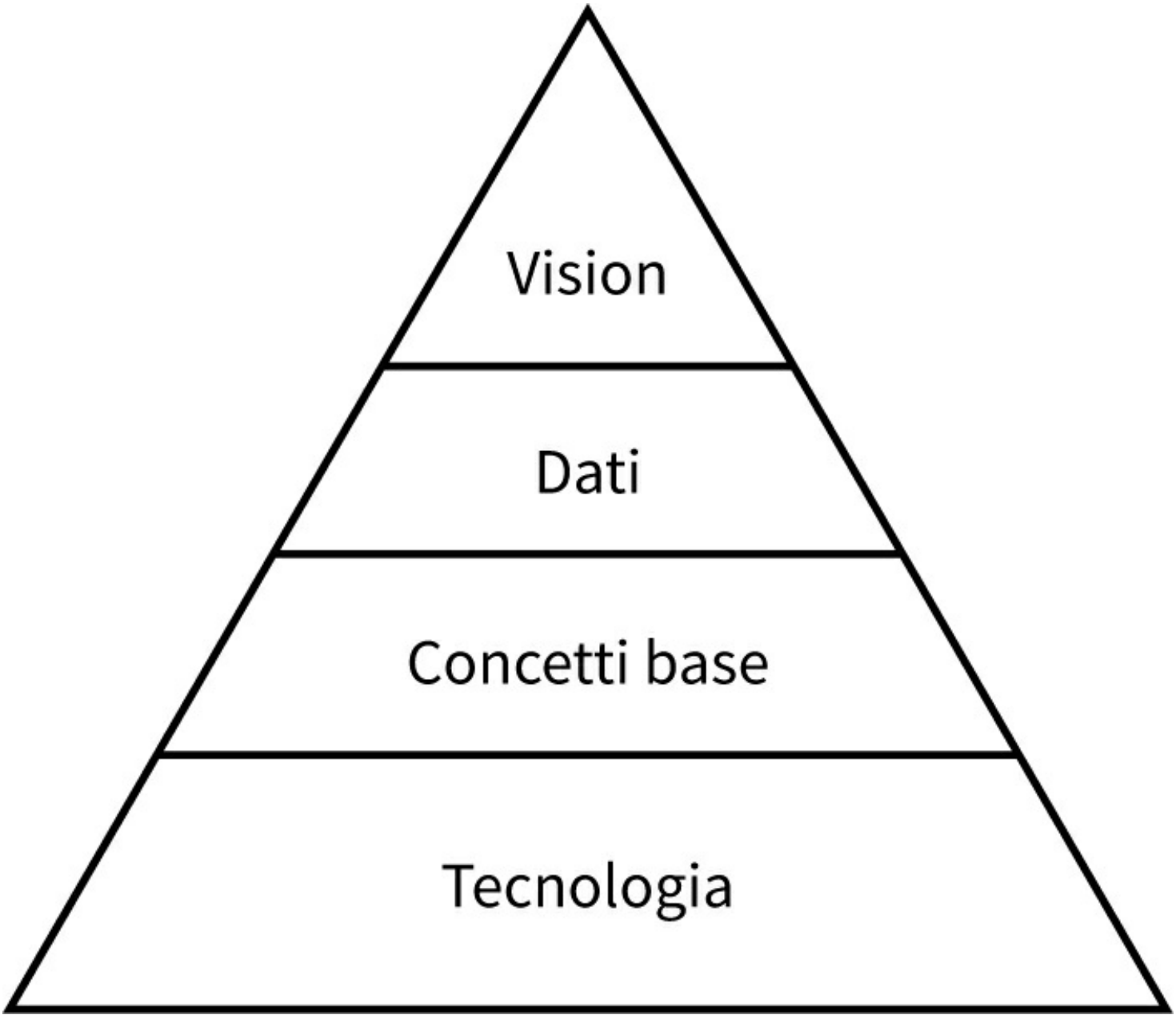


Figura 1.3 – La piramide della conoscenza nella blockchain.

Alla base della piramide vi è la **conoscenza della tecnologia blockchain** e delle sue principali

caratteristiche e applicazioni. Con "tecnologia" intendiamo i concetti ampiamente discussi in questo libro riguardo la sua struttura e le sue proprietà: i ruoli dei nodi e dei blocchi in una blockchain, gli algoritmi di consenso, il concetto di decentralizzazione, le caratteristiche degli smart contract ecc.

A un secondo livello, **la conoscenza dei concetti fondamentali di un token o di un progetto su blockchain**: il whitepaper, il problema che viene risolto, l'uso specifico della tecnologia nel progetto, l'affidabilità del team ecc.

A un terzo livello, **la capacità di analizzare criticamente i dati e le informazioni**: analisi del mercato,

rilevanza delle notizie, obiettivi raggiunti dal team di sviluppo ecc.

All'ultimo livello, la capacità di correlare i dati tramite una **visione d'insieme**. Chi si affida esclusivamente alle analisi o alle spiegazioni necessariamente semplificate dei media o, come ancor più spesso capita, al passaparola o a opinioni circolanti sui social media, viene limitato a una comprensione parziale dell'argomento, che spesso gli impedisce di afferrarne il reale potenziale.

Una volta giunti alla fine di questo libro, avrete tutti gli strumenti necessari non solo per valutare i singoli progetti, ma anche per riconoscere la validità dei

consigli degli esperti e le informazioni con cui potreste venire a contatto.

Il ruolo dell'esperto

In un settore come quello della blockchain, la figura dell'esperto è di fondamentale importanza, dal momento che in molti si affidano a lui per capire meglio alcuni argomenti o le conseguenze di un particolare evento.

Se fino a pochi anni fa un esperto di blockchain poteva essere uno sviluppatore di software con competenze specifiche, si rende ora necessario rivalutare la figura dell'esperto di pari passo con

l'evoluzione della tecnologia.

Le implicazioni socioeconomiche della blockchain e delle criptovalute hanno fatto sì che per avere una visione completa sul panorama delle criptovalute non sia sufficiente avere conoscenze solo in ambito informatico ma anche in quello finanziario, sociologico, legale ecc. L'esperto non è più quindi una figura con competenze specifiche, ma piuttosto un individuo costantemente aggiornato e con competenze trasversali che gli consentono di avere un'accurata visione d'insieme.

Riprendendo il concetto della piramide, un esperto, per potersi definire tale, dovrebbe possedere

conoscenze su tutti e quattro i livelli della piramide. La conoscenza di uno solo di questi livelli, specialmente di quelli superiori come l'analisi dei dati o la visione d'insieme, in mancanza di una comprensione della tecnologia rappresenta spesso un grosso campanello di allarme circa l'affidabilità della persona e della sua opinione.

Sebbene siano casi isolati, alle volte le opinioni di alcuni di questi esperti possono essere estremamente dannose non solo per chi si affida a loro ma per l'intera comunità.

Infine, come in molti altri contesti e situazioni, la strada che sembra più

corta non è sempre quella migliore. Nel caso della blockchain, dedicare tempo ad approfondire la tecnologia piuttosto che affidarsi alle opinioni degli altri, è sempre la scelta più conveniente.

Detto questo, è altrettanto importante riconoscere la presenza delle numerose figure di spicco estremamente competenti nel settore, che contribuiscono enormemente allo sviluppo della tecnologia e alla sensibilizzazione del pubblico sull'argomento, come per esempio Vitalik Buterin (il fondatore di Ethereum) e Andreas M. Antonopoulos (scrittore e punto di riferimento della community mondiale).

La disinformazione e le criptovalute

Attualmente, in Italia così come nel resto del mondo, c'è molta disinformazione sull'argomento sia nell'opinione pubblica che nella divulgazione da parte dai media. Questi, il più delle volte, si limitano a una trattazione delle criptovalute di natura prettamente speculativa, snaturando l'idea per cui sono nate.

Per esempio, provate a immaginare se le uniche notizie divulgate su Apple fossero quelle relative al suo valore in borsa, al punto che un lettore non sia in grado di associarla all'iPhone o ad altri prodotti perché non ne ha mai sentito

parlare. Una tale situazione può sembrare impensabile, eppure è esattamente quello che accade nel caso delle criptovalute, dove le notizie riguardano quasi esclusivamente l'andamento del mercato – la rivendicazione della presenza di una bolla speculativa nei periodi negativi, così come la spinta all'investimento nei periodi positivi.

Altre volte, invece, l'intera categoria delle criptovalute viene identificata con il Bitcoin, tralasciando le altre criptovalute di centrale rilevanza all'interno del panorama mondiale. Pensiamo per esempio a Ripple, che già viene utilizzato da istituti finanziari in tutto il mondo per consentire pagamenti

internazionali istantanei a costo zero, oppure a IOTA, che ha creato una piattaforma progettata per le transazioni macchina-macchina, o ancora a Golem, che sta costruendo un supercomputer decentralizzato.

I valori che solitamente ricoprono importanza nella finanza tradizionale, come il valore di un token o il market cap, sono degli indicatori finanziari che spesso non hanno alcun legame con il prodotto o il progetto. Non dovrebbero quindi essere utilizzati come parametri su cui basare supposizioni o opinioni di natura tecnica. Leggiamo dell'affluenza di investitori spinti dalla possibilità di avere immensi guadagni nel giro di

giorni o di settimane, delle analogie col dot-com boom, della presenza di innumerevoli truffe, delle opinioni di presunti esperti che garantiscono che in futuro le monete normali non esisteranno più perché rimpiazzate dalle criptovalute, così come quelle di altrettanti esperti che garantiscono che il mercato delle criptovalute non sia altro che una bolla speculativa destinata a svanire in un nulla di fatto.

Tuttavia, è molto raro che si parli delle ragioni per cui le varie criptovalute sono nate e dei problemi che tentano di risolvere.

Ciò che ne consegue è che l'opinione del pubblico viene indirizzata su aspetti che non sono legati a una

criptovaluta in sé ma alla reazione che il pubblico stesso o le istituzioni hanno già avuto finora nei suoi confronti.

NOTA Nel caso delle criptovalute si dovrebbe dare importanza in primo luogo allo scopo per cui è nato un determinato progetto, alle caratteristiche della sua blockchain e al modo in cui la tecnologia aiuta a risolvere un problema.

Riprendendo il concetto della piramide, i media e le opinioni reperibili online divulgano notizie che appartengono alla punta della piramide, ma se chi legge le informazioni non possiede la conoscenza

delle basi, è facile che giunga a conclusioni errate, che non riflettono la realtà.

Il consiglio che si vuole dare a questo proposito è quello di cercare sempre di consultare direttamente le fonti ufficiali e le informazioni dalle principali community[3].

L'elefante nella stanza

È probabile che vi sia capitato di sentire che le criptovalute siano sinonimo di truffa, o di come queste siano addirittura il mezzo preferito dai criminali per riciclare denaro in tutto il mondo.

Questo è uno degli esempi più

eclatanti di disinformazione che l'intera community ha dovuto affrontare, spesso influenzato anche da personaggi o entità con una discreta fama. La distorsione dei fatti e la proliferazione delle fake news sono una piaga ben conosciuta che affligge quasi ogni settore in tutto il mondo.

In risposta a questo proposito, le criptovalute non nascono per favorire la criminalità o il riciclaggio di denaro. Questi problemi sono sempre esistiti nel mondo e sono possibili tramite qualsiasi forma di scambio di valore. Le criptovalute, al contrario, possono essere una possibile soluzione a questi e a molti altri problemi. Tuttavia, quello che realmente conta è mantenere un

atteggiamento critico nei confronti delle informazioni con cui si viene in contatto, ed essere interessati ad acquisire le conoscenze per valutarle in maniera autonoma. Nuovamente, tutto parte dalla comprensione della tecnologia.

La regolamentazione nel mondo

Nel momento in cui scriviamo questo libro, il mondo della blockchain sta assistendo alla nascita di numerosi progetti nei settori più disparati, ma allo stesso tempo il mondo delle criptovalute sta attraversando una fase di regolamentazione in vari Paesi.

Mentre per quanto riguarda la tecnologia blockchain non c'è nessuna particolare restrizione al suo utilizzo, le regolamentazioni sulle criptovalute possono essere raggruppate in tre macro-aree, nelle quali ogni Paese ha una posizione più o meno definita:

- l'utilizzo delle criptovalute come mezzo di pagamento;
- le ICO, la distinzione di utility e security token, e in generale le modalità di raccolta fondi tramite l'emissione di un token;
- le modalità di operazione degli exchange.

A titolo esemplificativo, è possibile

identificare una categoria di Stati "prevalentemente a favore" delle criptovalute, e in alcuni casi con una regolamentazione già definita. Fra questi possiamo citare la Svizzera, Malta, l'Estonia e il Giappone, dove sono in corso gran parte dei progetti basati su blockchain.

Nel luglio 2018 Malta diventa il primo Paese ad approvare una legislazione integrale sulle DLT (Distributed Ledger Technologies) costituita da tre leggi per regolamentare ICO (VFA Act), criptovalute, blockchain e smart contract (MDIA Act) ed Exchange (ITAS Act) [1][4].

Un'altra categoria sono gli Stati al

momento “prevalentemente contro” l’utilizzo delle criptovalute. La Cina per esempio vieta espressamente le ICO e le transazioni fiat-crypto sugli exchange, mentre incentiva l’utilizzo della tecnologia blockchain.

Per quanto riguarda invece l’Italia, nel settembre 2018 è entrata a far parte della European Blockchain Partnership assieme ad altri 26 Stati membri dell’UE [2]. Sebbene nel momento in cui questo libro viene scritto ancora molti aspetti siano in via di definizione, uno degli obiettivi è quello di regolamentare le criptovalute e le modalità di investimento basate su di esse (ICO), assieme a una spinta per l’implementazione della tecnologia da

parte delle imprese.

La situazione è perciò estremamente variegata e in costante evoluzione. Questa mancanza di sicurezza è proprio uno degli ostacoli principali per un'assunzione su scala mondiale, ma si sta lentamente definendo una situazione complessivamente positiva che lascia intravedere un futuro in cui queste tecnologie possano essere sfruttate al massimo del loro potenziale[5].

Il potere dell'innovazione

Era il 1975 quando Steven Sasson, un

ingegnere della Eastman Kodak Company, realizzò quella che viene considerata la prima fotocamera digitale. L'azienda, al tempo leader nel settore chimico e delle pellicole, gli disse di mantenere questa invenzione privata, preoccupata dei potenziali impatti negativi sul suo business. Nel 2007 Nokia sfiorava l'incredibile quota di mercato del 50% nel settore dei telefoni cellulari [3]. Poco dopo, quando Apple e Google esordirono con i sistemi iOS e Android, Nokia non comprese il ruolo centrale del software negli smartphone, scegliendo di non concentrare i propri sforzi nell'evoluzione del suo OS Symbian. Nel frattempo, Blackberry rimase

convinta che usare metà dispositivo per la tastiera fosse una buona idea. Sappiamo tutti com'è andata a finire.

La storia, soprattutto nell'era digitale, è piena di società leader che hanno finito col perdere grandi opportunità, sono state ridimensionate pesantemente o sono fallite a causa della loro incapacità di comprendere appieno l'innovazione che una nuova tecnologia o una nuova idea avrebbero potuto portare. Le nuove idee hanno il potere di distruggere interi mercati nel giro di pochi anni, proprio come Napster ha distrutto la Tower Records semplicemente mostrando che era possibile condividere file musicali tra le

persone. Napster è stato chiuso, ma una volta che il mondo ha compreso l'innovazione alla base, nessuno ha più considerato un negozio di dischi come un investimento redditizio. Uber ha creato un nuovo modello di business e, anche se i legislatori di alcuni Stati stanno cercando di fermarlo, l'idea di diventare un tassista non è più così allettante.

> L'innovazione non può essere fermata, non è possibile "disinventare" Internet o la sharing economy.
>
> L'innovazione deve essere compresa e adottata.

L’ingresso di un nuovo giocatore

Sempre più spesso negli ultimi anni abbiamo sentito i media nominare il termine Bitcoin. Certe volte per le incredibili oscillazioni di valore che hanno portato al paragone con la bolla dei tulipani del 1637[6] [4] o la bolla dot-com [5], altre per il suo utilizzo in attività criminali (per esempio come metodo di pagamento nei ransomware [6]).

Nel frattempo, alcune persone hanno iniziato ad approfondire questo fenomeno, cercando di capire come fosse possibile che individui sparsi per il mondo riuscissero a trasferire denaro

senza passare per un'istituzione centrale. Quello che hanno trovato è stato un sistema aperto, pubblico e sicuro, dove era possibile innovare senza chiedere il permesso ad alcuna istituzione: la blockchain.

Questa tecnologia sta rapidamente diventando una priorità strategica per molte aziende, con la promessa di ridurre i costi e le inefficienze, trasformando radicalmente i modelli di business che conosciamo oggi.

Il double-spending

Uno degli aspetti che differenzia maggiormente il mondo "fisico" da

quello digitale è l'estrema facilità con cui è possibile copiare dati e informazioni.

Questa caratteristica è in netto contrasto con le proprietà che deve avere il denaro. Per questo motivo fino a oggi tutte le forme di denaro digitale hanno sempre dovuto far affidamento su un'autorità centrale, come per esempio una banca, che fungesse da detentore unico della verità impedendo che il denaro digitale potesse essere duplicato e quindi speso più volte (double-spending).

> Per la prima volta, grazie alla blockchain, si può risolvere il

problema della doppia spesa senza fare affidamento su un'autorità centrale.

L'aspetto rivoluzionario di questa tecnologia non si limita però a questo. La blockchain permette di affrontare in maniera completamente diversa uno degli aspetti cardine della nostra società: il problema della fiducia.

Il problema della fiducia

"Il problema alla base delle valute convenzionali è dovuto alla quantità di fiducia necessaria per far funzionare il

sistema.
Dobbiamo fidarci del fatto che le banche non svalutino
la moneta, ma purtroppo la storia è piena di momenti in cui
questa fiducia non è stata rispettata. Dobbiamo fidarci del fatto
che le banche conservino i nostri soldi, ma spesso sono scoppiate
bolle legate ìal credito bancario, e solo una frazione dei soldi
era effettivamente in possesso della banca. Dobbiamo riporre
in queste istituzioni la nostra fiducia in termini di privacy,
e fidarci del fatto che i ladri

d'identità non svuotino i nostri conti correnti."[7]

—**Satoshi Nakamoto**, creatore del Bitcoin

Immaginiamo che un uomo, un uomo qualunque, in un negozio di alimentari, scelga i prodotti di cui ha bisogno e vada alla cassa. Arrivato il momento di pagare, si accorge di aver dimenticato il portafoglio a casa. Così, candidamente, cerca di spiegare al proprietario che gli occorre giusto il tempo di arrivare a casa, recuperare il portafoglio e tornare indietro a pagare. Il commerciante però risponde che non può accettare.

Un paio d'ore più tardi, una signora si accorge di essere stata ugualmente

sbadata, e chiede cortesemente al commerciante se può tornare il giorno dopo a pagare.

Sono amici da una vita, di conseguenza il proprietario non ha alcun problema ad aspettare il giorno seguente.

Cos'è cambiato dal punto di vista del commerciante? La fiducia verso la sua amica.

Non si fida dello sconosciuto, d'altronde non ha nessuna garanzia che avrebbe effettivamente ricevuto il denaro che gli spetta. Questo esempio riassume quello che viene definito come "rischio di controparte", ovvero il rischio che una delle parti coinvolte in

una transazione non rispetti i vincoli dell'accordo.

Il concetto di fiducia non è solamente legato al denaro ma si applica a molti contesti della vita quotidiana.

Riponiamo fiducia nel fatto che un prodotto fairtrade abbia soddisfatto i requisiti necessari per usare quella certificazione. Ci aspettiamo che il denaro che doniamo in beneficenza arrivi prontamente alle persone in difficoltà. Poniamo cieca fiducia nelle banche quando paghiamo con il nostro bancomat e siamo sicuri che il nostro provider di email non ci estrometterà dal servizio.

La nostra società si regge su fondamenta di fiducia costruite da

diversi attori, dal commerciante locale alle grandi corporation. Se perdiamo fiducia anche in un solo anello della catena, nessuna transazione è più possibile.

Al giorno d'oggi, però, per ogni business, guadagnare la fiducia dei suoi utenti e mantenerla nel tempo è un'attività molto dispendiosa.

Cosa succederebbe se fossimo in grado di trasferire la fiducia a un sistema pensato per essere incorruttibile?

Un sistema incorruttibile

Questo è ciò che la blockchain è stata in grado di conquistare: il problema della fiducia è stato risolto cambiando totalmente le fondamenta del sistema, sviluppando una tecnologia in cui la fiducia è costruita intrinsecamente all'interno della tecnologia stessa.

Grazie alla blockchain, la nostra inclinazione a fidarci di un sistema non dipende più dalle intenzioni di alcun partecipante. Abbiamo quindi l'opportunità di creare delle applicazioni basate su un nuovo tipo di fiducia: una fiducia riposta direttamente nel sistema su cui sono costruite.

3. Per esempio Coindesk, Hackernoon, Techcrunch, Reddit, Bitcointalk.
4. I numeri tra parentesi quadre fanno riferimento alla bibliografia/sitografia in fondo al volume.
5. Per conoscere le regolamentazioni vigenti in merito alla legalità delle criptovalute come mezzo di pagamento potete consultare https://www.bitcoinregulation.world.
6. La prima bolla speculativa della storia: un picco di domanda dei tulipani aveva causato un drastico aumento del loro prezzo, poi inevitabilmente crollato.
7. http://p2pfoundation.ning.com/forum/topics/bit open-source.

2

La tecnologia blockchain

Il concetto di blockchain fu introdotto per la prima volta nel 2008 da Satoshi Nakamoto (pseudonimo di un personaggio ancora oggi sconosciuto) in un articolo intitolato “Bitcoin: A Peer-to-Peer Electronic Cash System” [7], e successivamente (2009) implementato come parte del Bitcoin[8].

Ci teniamo però a sottolineare che

Bitcoin e blockchain sono due cose separate. Il Bitcoin è soltanto una delle innumerevoli applicazioni della tecnologia blockchain. A oggi, il Bitcoin è senza dubbio il progetto più popolare, ma la tecnologia alla base di esso va ben oltre il concetto di una semplice valuta digitale. Per essere chiari, si può dire che la blockchain sta al Bitcoin come Internet sta a Google. Parafrasando Andreas Antonopoulos: come la natura è in grado di creare sistemi estremamente complessi unendo un gran numero di elementi semplici (si pensi agli esseri umani dal punto di vista chimico, o alla coordinazione tra gruppi di animali), così la blockchain si può descrivere come un network che

combina un numero molto grande di macchine, ognuna delle quali segue una serie di semplici regole matematiche.

Questa particolare struttura permette di sviluppare applicazioni impossibili da ottenere con altri sistemi[9].

Possiamo immaginare la blockchain come un protocollo che garantisce specifiche proprietà alle applicazioni sviluppate su di esso. Non si tratta di una normale transizione tecnologica, bensì di un totale cambio di paradigma nelle caratteristiche chiave dei business di oggi: la centralizzazione diventa decentralizzazione, i sistemi chiusi diventano aperti, passando dall'essere entità territoriali a organi globali,

garantiti da una fiducia non più riposta in singole entità ma nelle fondamenta stesse della tecnologia.

Come potete immaginare, la blockchain non è un concetto semplice, e le tecnologie alla base di essa riflettono questa complessità, ma per avere una reale comprensione delle potenzialità e dei punti critici a essa connessi, è fondamentale acquisire una conoscenza dei meccanismi che ne costituiscono il cuore pulsante. In questo capitolo vi accompagneremo attraverso le caratteristiche chiave, cercando di fare chiarezza sulle funzionalità, per proseguire il viaggio spiegandone le applicazioni di oggi ma soprattutto quelle di domani.

La definizione

È possibile trovare molte definizioni della blockchain. Alcune si concentrano sulla sua struttura, altre sulle tecnologie alla base di essa o sulle implicazioni sul business e la società. Tutti questi aspetti sono ugualmente importanti e contribuiscono a dare una panoramica esaustiva sull'argomento.

La definizione di blockchain

La blockchain è un libro mastro (d'ora in poi "ledger") digitale, decentralizzato e distribuito su un network, strutturato come una catena di registri (i "blocchi") responsabili dell'archiviazione dei dati (dalle transazioni di valore a intere applicazioni digitali).

È possibile aggiungere nuovi blocchi di informazioni, ma non è invece possibile la modifica o la rimozione di blocchi precedentemente aggiunti alla catena.

In questo ecosistema, la crittografia e i protocolli di consenso garantiscono sicurezza e immutabilità.

Il risultato è un sistema aperto, neutrale, affidabile e sicuro, dove la nostra capacità di utilizzare e di avere fiducia nel sistema non dipendono dalle intenzioni di nessun individuo o

istituzione.

La blockchain è molto più di un'infrastruttura di pagamento, di un sistema di monitoraggio della supply chain o di un gestore di identità digitale.

È un sistema con le potenzialità per portare un nuovo livello di fiducia nelle applicazioni, introducendo un cambio di paradigma nelle modalità con cui esse vengono realizzate e dandoci l'opportunità di innovare liberamente.

La definizione nel box è piuttosto esauriente, ma contiene molti concetti che possono risultare complessi o creare confusione.

Cosa sono i protocolli di consenso? Se cambiamo la decentralizzazione in centralizzazione abbiamo ancora una blockchain o qualcosa di diverso? Come possiamo garantire l'immutabilità delle informazioni? Come possiamo far rispettare le regole?

Analizziamo ora questi e molti altri concetti chiave della blockchain.

Ledger, database e blockchain

Iniziamo la nostra esplorazione della tecnologia blockchain partendo dal concetto di informazione.

Possiamo affermare che uno degli scopi principali di una blockchain sia quello di salvare informazioni. Come vedremo in seguito, le informazioni salvate possono essere di qualunque tipo, da una semplice transazione di un bene a interi programmi (smart contract). Per semplicità, partiamo dal caso più vicino all'esperienza quotidiana, ovvero le transazioni monetarie.

Al centro della blockchain c'è il concetto di registrazione delle transazioni all'interno del ledger. L'idea è molto simile a un libro mastro tradizionale (un registro della contabilità in cui sono riuniti i valori

che compongono un sistema contabile), con la possibilità di registrare transazioni di ogni categoria di bene, dalle valute alle proprietà immobiliari.

> Un ledger è uno strumento utilizzato per registrare transazioni.

I ledger sono in uso da ben prima della blockchain, essendo parte integrante dei processi commerciali fin dai tempi antichi.

Mentre il concetto di ledger non è cambiato nel tempo, la tecnologia a supporto di esso si è evoluta, passando da registri cartacei ad archivi digitali.

La blockchain, essendo completamente digitale, richiede ovviamente che tutto sia salvato nel ledger in forma digitale.

> La blockchain è un ledger digitale.

Per chi si intende di database, ledger e database potrebbero sembrare molto simili. Alla base di entrambe le tecnologie c'è infatti l'idea di salvare dei dati, ma mentre in un database è possibile inserire, cancellare e modificare i dati, in un ledger è possibile unicamente l'aggiunta di nuove informazioni. Questo è reso possibile da

una combinazione di vari fattori, tra i quali la decentralizzazione, la crittografia, la teoria dei giochi e altri concetti che analizzeremo in seguito.

A questo punto si potrebbe pensare di implementare un ledger utilizzando un database tradizionale e imponendo dei vincoli alle operazioni disponibili. La blockchain, però, garantisce molte altre proprietà che vanno oltre i semplici database e formano un vero e proprio ecosistema piuttosto che un semplice archivio di informazioni.

Un ledger può essere dunque visto come un database nel quale è possibile solamente aggiungere informazioni (Figura 2.1).

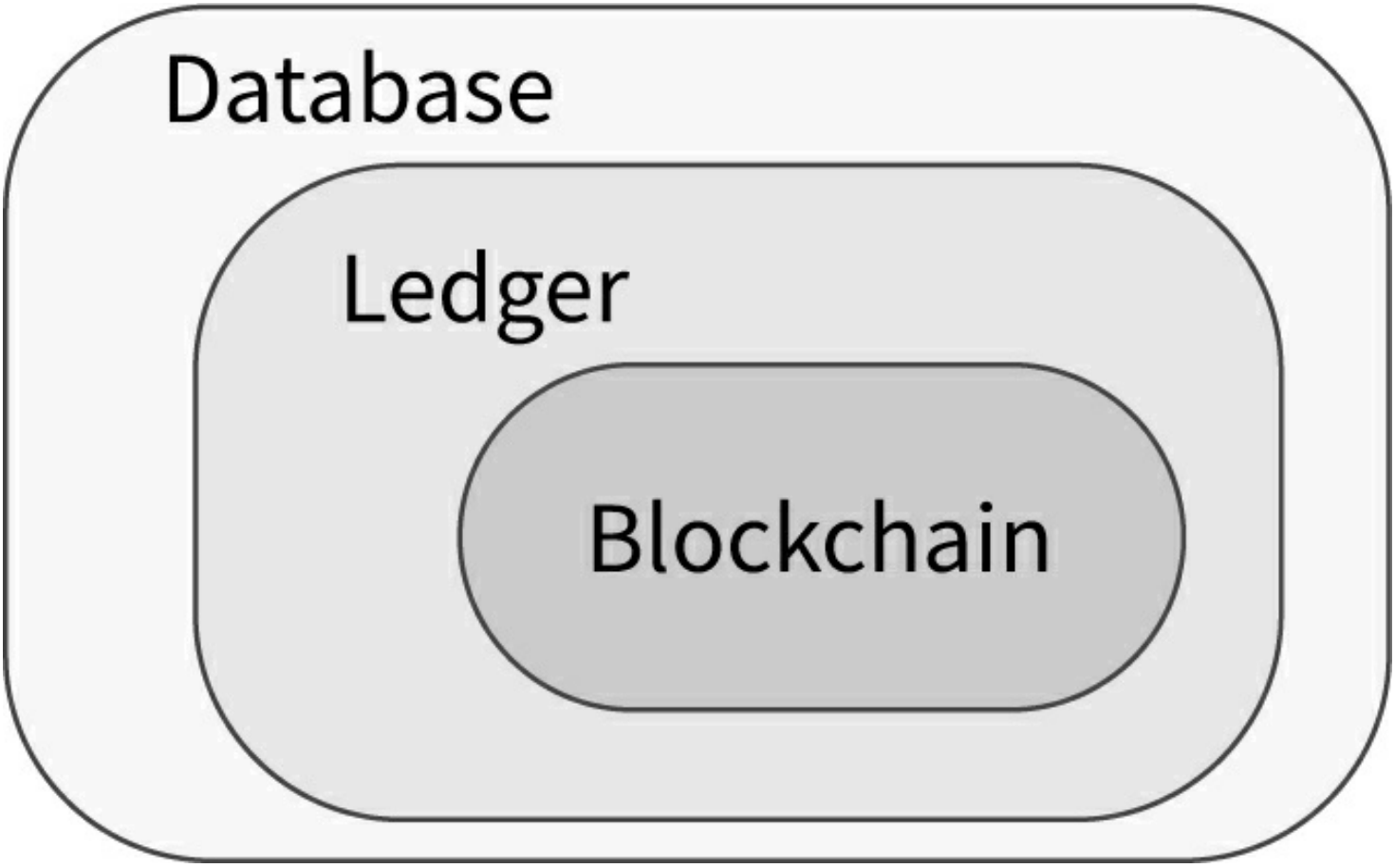


Figura 2.1 – La distinzione fra database, ledger e blockchain.

È giusto chiarire che la blockchain difficilmente rimpiazzerà i database tradizionali. Alcuni dei contesti che oggi includono l'utilizzo di un database si evolveranno verso sistemi blockchain, ma nessuno dei due sostituirà

completamente l'altro.

> Database e blockchain sono pensati per affrontare problematiche differenti.

Molte delle proprietà che caratterizzano la blockchain rendono questa tecnologia attraente per diversi scenari.

Per esempio, un database tradizionale richiede un sistema di accesso controllato. In altre parole, la gestione è direttamente demandata a individui noti e affidabili (che si tratti di una persona, un'organizzazione o una macchina). Una blockchain, invece, può essere utilizzata da parti sconosciute e

non “fidate”, senza la necessità di alcuna forma di controllo degli accessi.

Di conseguenza, la blockchain risulta molto utile in scenari in cui fiducia, sicurezza e immutabilità sono requisiti fondamentali.

Dal punto di vista strutturale, come accennato in precedenza, nel cuore di una blockchain c’è un ledger digitale. In una blockchain, il ledger digitale è strutturato come una catena di blocchi (Figura 2.2), ognuno dei quali è responsabile della memorizzazione di informazioni, come per esempio registri di transazioni oppure programmi (chiamati smart contract, come vedremo in seguito).

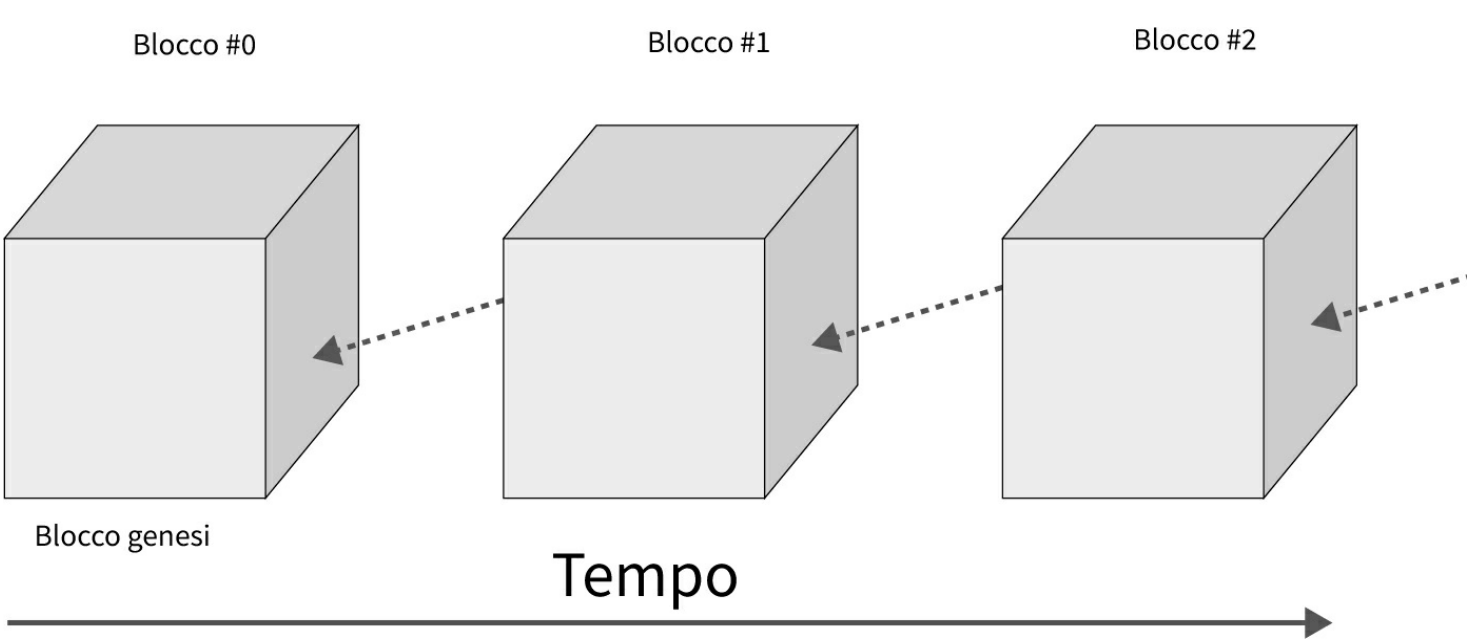


Figura 2.2 – La catena di blocchi in una blockchain.

Ci teniamo a specificare che nel corso del libro adotteremo la convenzione di mostrare tramite una freccia il collegamento tra i blocchi. La direzione della freccia, quindi, non evidenzia la successione temporale dei blocchi, ma la loro dipendenza l'uno dall'altro.

I blocchi, mattoni della blockchain

I blocchi sono strutture di dati aggiunte alla blockchain in modo sequenziale, un blocco alla volta. Ognuno di essi contiene una prova matematica, generata mediante l'utilizzo della crittografia, che ne assicura la sequenzialità dal blocco precedente, risultando in una "catena di blocchi" (Figura 2.3). Il primo blocco di ogni blockchain è chiamato "blocco genesi".

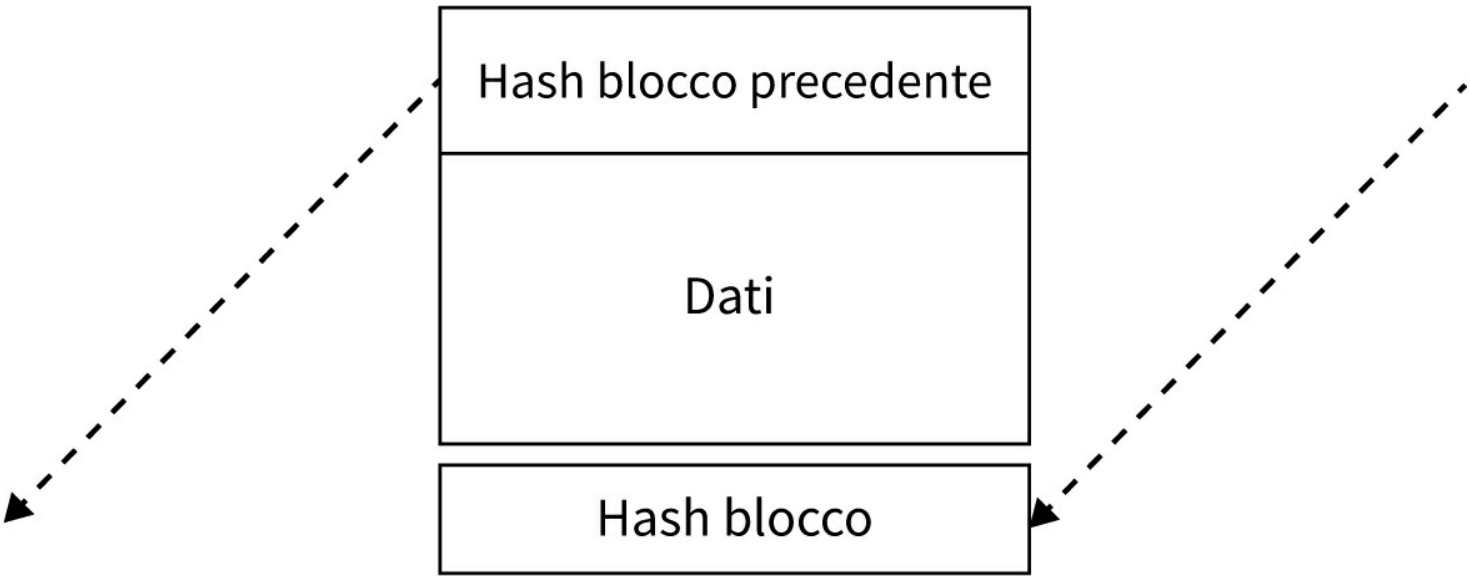


Figura 2.3 – La struttura di un blocco.

> L'hash del blocco non viene solitamente salvato nel blocco, ma viene calcolato ogni volta che sia necessario[10].

Il concetto di catena di blocchi è comune a quasi tutti i sistemi blockchain[11], ma il design di questi blocchi si differenzia a

seconda dello scopo per cui è stata progettata la blockchain.

Per esempio, i blocchi nella blockchain del Bitcoin si differenziano da quelli della blockchain di Ethereum.

A seconda di come il sistema è progettato, i blocchi possono avere dimensioni diverse e memorizzare vari tipi di informazioni.

La connessione tra blocchi viene generata mediante una funzione crittografica (nello specifico la **funzione crittografica di hash**), la quale crea un collegamento matematico indissolubile tra essi.

La funzione di hash

Tale funzione è utilizzata per mappare dati di dimensioni arbitrarie in dati di dimensioni fisse. In altre parole, l'input di una funzione di hash può essere praticamente qualsiasi cosa (un file mp3, un pdf, un foglio di calcolo, un'intera blockchain), ma l'output, chiamato "hash", avrà sempre un numero finito di bit. Esplorare i dettagli matematici delle funzioni di hash va oltre lo scopo di questo libro[12]. I concetti fondamentali da tenere a mente per proseguire nella lettura sono:

- Lo stesso input produce sempre lo stesso output (funzione

deterministica), ossia un hash, che ha la forma di una stringa di lettere e numeri[13].

- Anche la più lieve modifica nell'input produce un cambiamento drastico nell'output della funzione.
- È una funzione **unidirezionale**: è computazionalmente molto facile generare un hash a partire da qualsiasi input, ma è molto complesso calcolare l'input partendo dall'hash (ovvero calcolare la funzione inversa). Non esiste un modo per passare dall'hash all'input se non provando tutte le possibili

combinazioni (metodo brute-force).

Tabella 2.1 – Esempi di output della funzione di hash.

Input	Funzione hash	Output
hello	SHA-256	2CF24DBA5FB0A30E26E83B2AC
Hello	SHA-256	185F8DB32271FE25F561A6FC938

SHA-256 è una delle più comuni funzioni di hash.

Si può pensare a un hash come all'impronta digitale di un file digitale.

Poiché una piccola modifica all'input altera completamente l'hash, una volta calcolato l'hash di un file, qualora il file venisse modificato anche il relativo hash subirebbe delle modifiche.

Se venisse pubblicata la copia digitale di questo libro insieme al suo hash, chiunque potrebbe verificare di possedere la versione originale semplicemente calcolando l'hash del file scaricato. Se gli hash non fossero uguali, allora saprebbe che il file è stato modificato in qualche modo.

Confrontare gli hash è quindi molto più conveniente e veloce rispetto al confronto di interi file.

Hash e blockchain

I sistemi blockchain fanno un uso frequente della funzione di hash, in quanto essa fornisce un modo molto conveniente per esprimere l'intero stato della blockchain in una singola stringa di lunghezza definita. Per ogni nuovo blocco generato, l'hash del blocco precedente viene inserito nell'input per generare l'hash del nuovo blocco (Figura 2.4)[14].

In pratica, ogni blocco contiene al suo interno delle informazioni, dei dati (per esempio transazioni) e l'hash del blocco precedente (Figura 2.5).

Di conseguenza, se qualcuno tentasse di aggiungere, rimuovere o modificare

alcune informazioni in qualsiasi blocco, andrebbe a cambiare l'hash del blocco e di conseguenza tutti gli hash successivi, e ciò risulterebbe subito evidente (Figura 2.6).

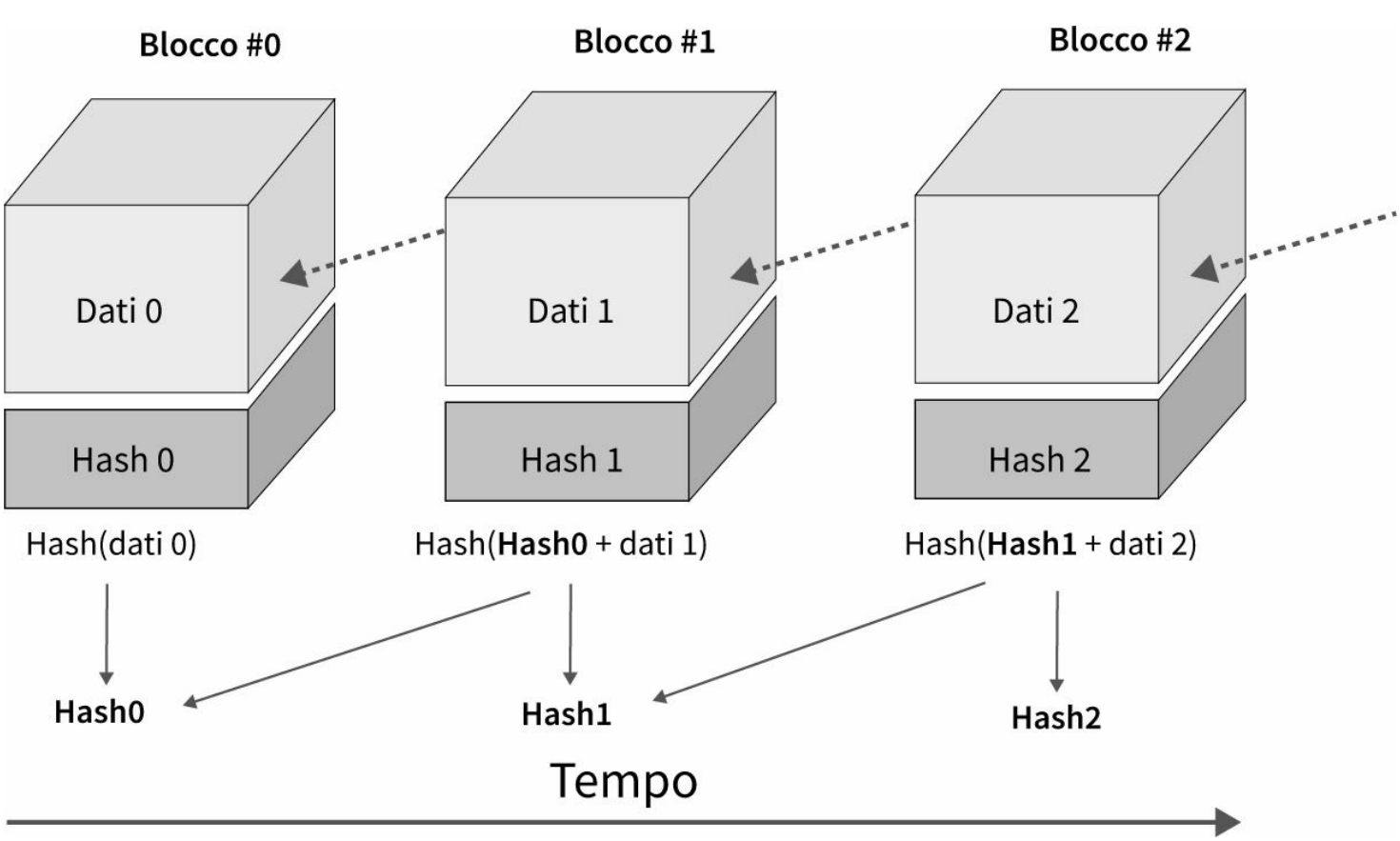


Figura 2.4 – La funzione Hash nel collegamento di nuovi blocchi.

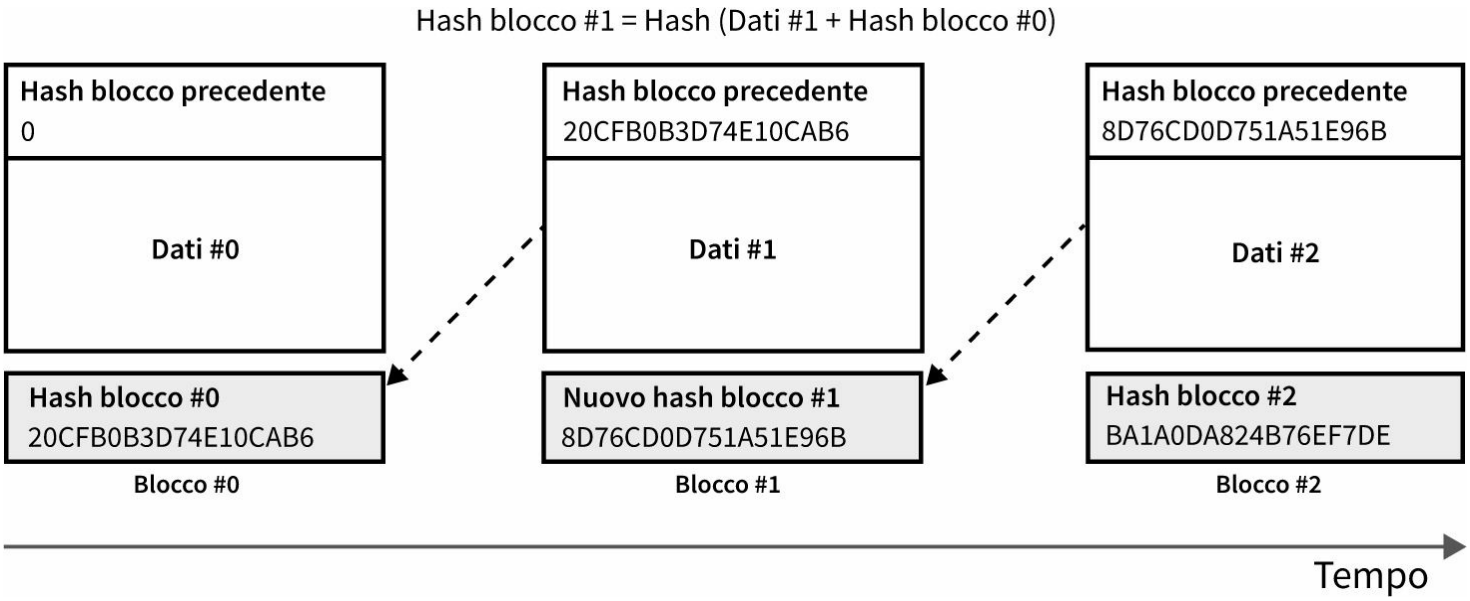


Figura 2.5 – Dettaglio dell'hash nella struttura dei blocchi.

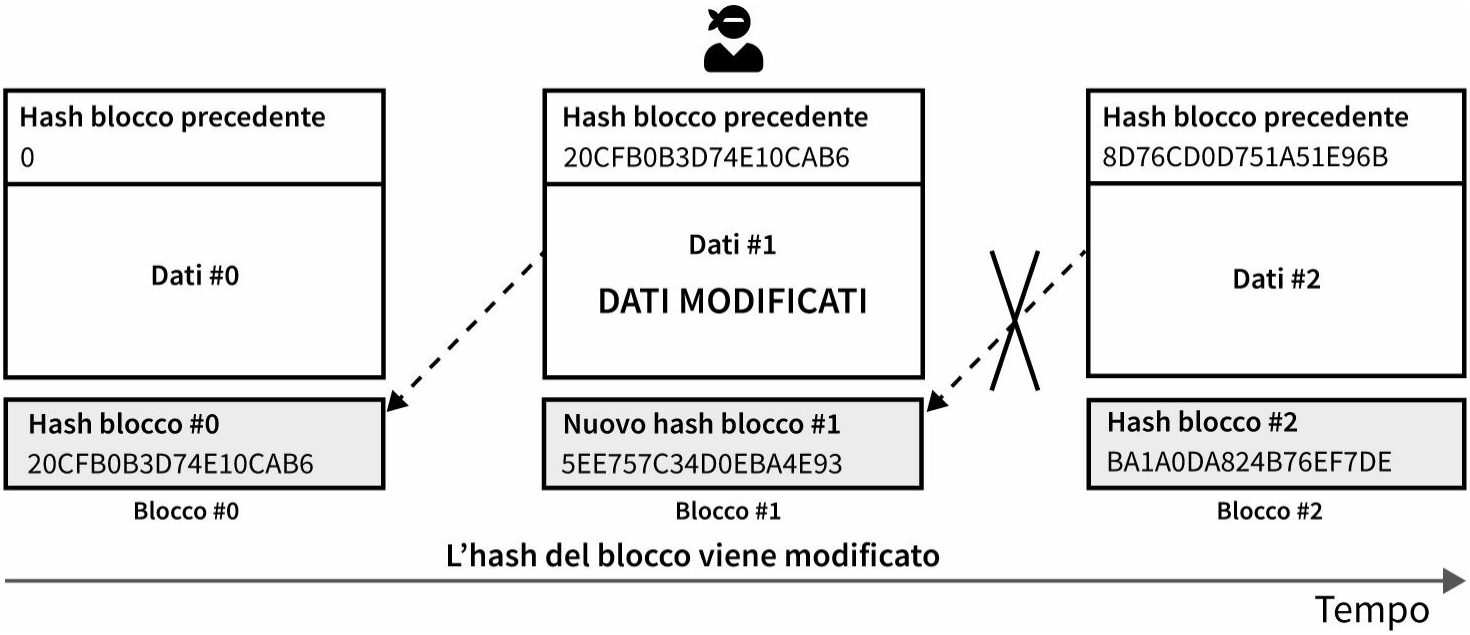


Figura 2.6 – La modifica dei dati invalida tutti gli hash successivi.

La blockchain di Bitcoin occupa attualmente oltre 180 gigabyte[15], ma è possibile rappresentare l'intera blockchain con un singolo hash.

Per valutare lo stato corrente di una blockchain non serve dunque analizzare ogni volta l'intero contenuto: è sufficiente guardare l'hash dell'ultimo

blocco. Questo risulta estremamente utile nel valutare diverse versioni della stessa blockchain (Figura 2.7).

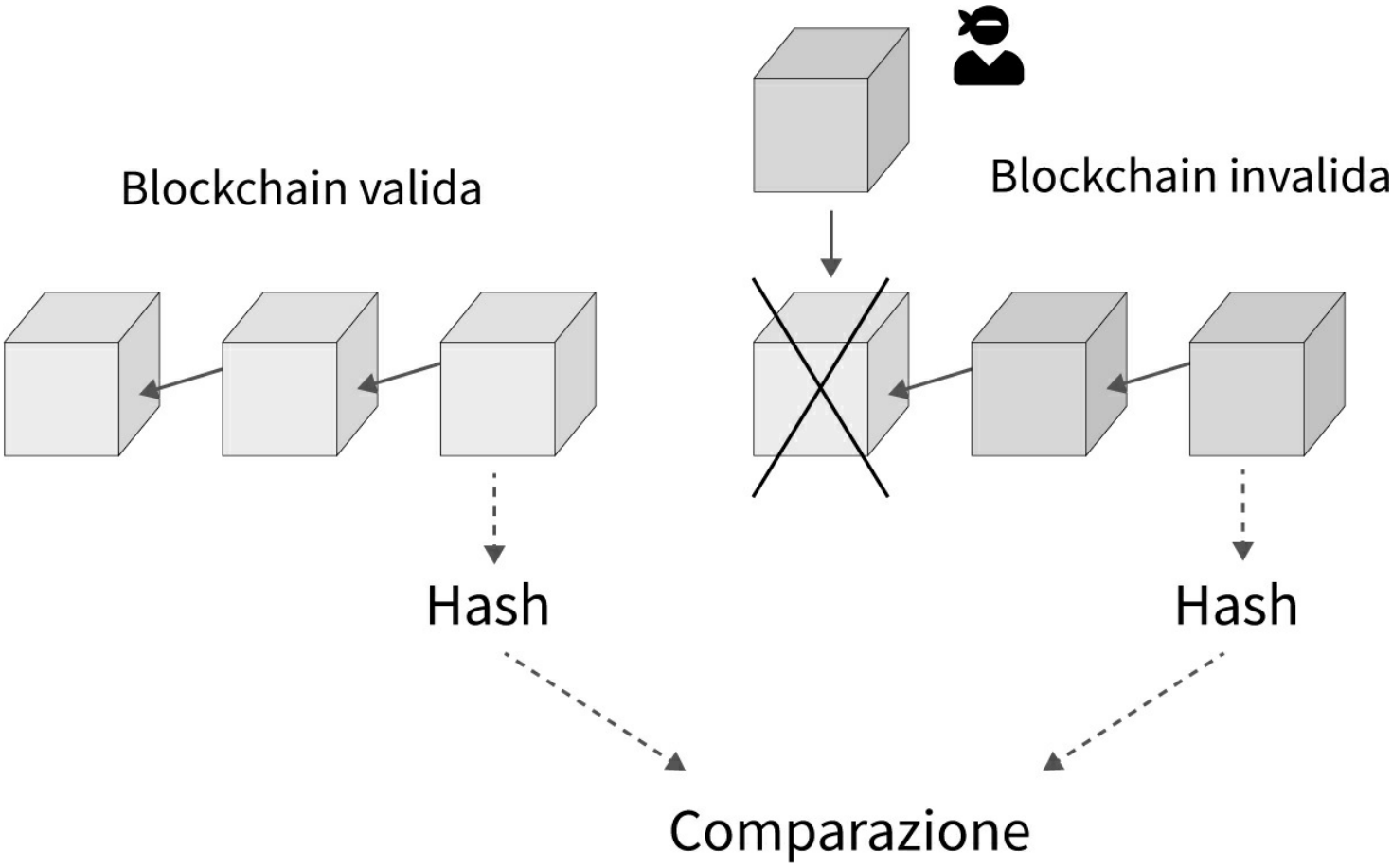


Figura 2.7 – La comparazione degli hash per riconoscere una blockchain non valida.

8. Il paper di Satoshi è una lettura a nostro parere estremamente affascinante, perché vi darà modo di capire in che modo Bitcoin e blockchain siano nati. La versione in italiano è

la seguente: https://bitcoin.org/files/bitcoin-paper/bitcoin_it.pdf.

9. Questo concetto viene espresso, seppur in maniera differente e più articolata, da Andreas M. Antonopoulos nella prefazione del libro *Mastering Bitcoin,* O'Reilly Media, 2014. Potete leggere la prefazione su https://github.com/bitcoinbook/bitcoinbook/blo

10. Riprenderemo più nel dettaglio la struttura dei blocchi nel Capitolo 8.

11. In seguito distingueremo tra le blockchain e le più generiche Distributed Ledger Technologies che, sebbene non utilizzino sempre una struttura lineare, vengono solitamente considerate delle tecnologie blockchain.

12. Per approfondire la sicurezza delle funzioni di hash: https://stackoverflow.com/questions/6776050/l long-to-brute-force-a-salted-sha-512-hash-salt-provided e

https://www.reddit.com/r/askscience/comments
13. Un esempio per i più curiosi: la parola "Hello" usando la funzione di hash SHA-256 produce questo risultato: 2CF24DBA5FB0A30E26E83B2AC5B9E29E1
14. Con Hash(X) indichiamo la funzione di hash applicata al valore X, mentre con HashX indichiamo il risultato della funzione hash(X).
15. https://www.blockchain.com/charts/blocks-size.

3

Il network della blockchain

Uno degli scopi principali della tecnologia blockchain è permettere a chiunque, in qualsiasi parte del mondo, di effettuare transazioni senza la necessità di affidarsi a un'istituzione centrale (nel caso di transazioni monetarie, una banca)[16].

Per fare ciò, la blockchain deve essere distribuita su un **network** (rete).

Possiamo definire un network come un gruppo di macchine interconnesse che si scambiano informazioni tramite canali di comunicazione, come per esempio Internet.

Una macchina connessa a un network è chiamata **nodo** (Figura 3.1).

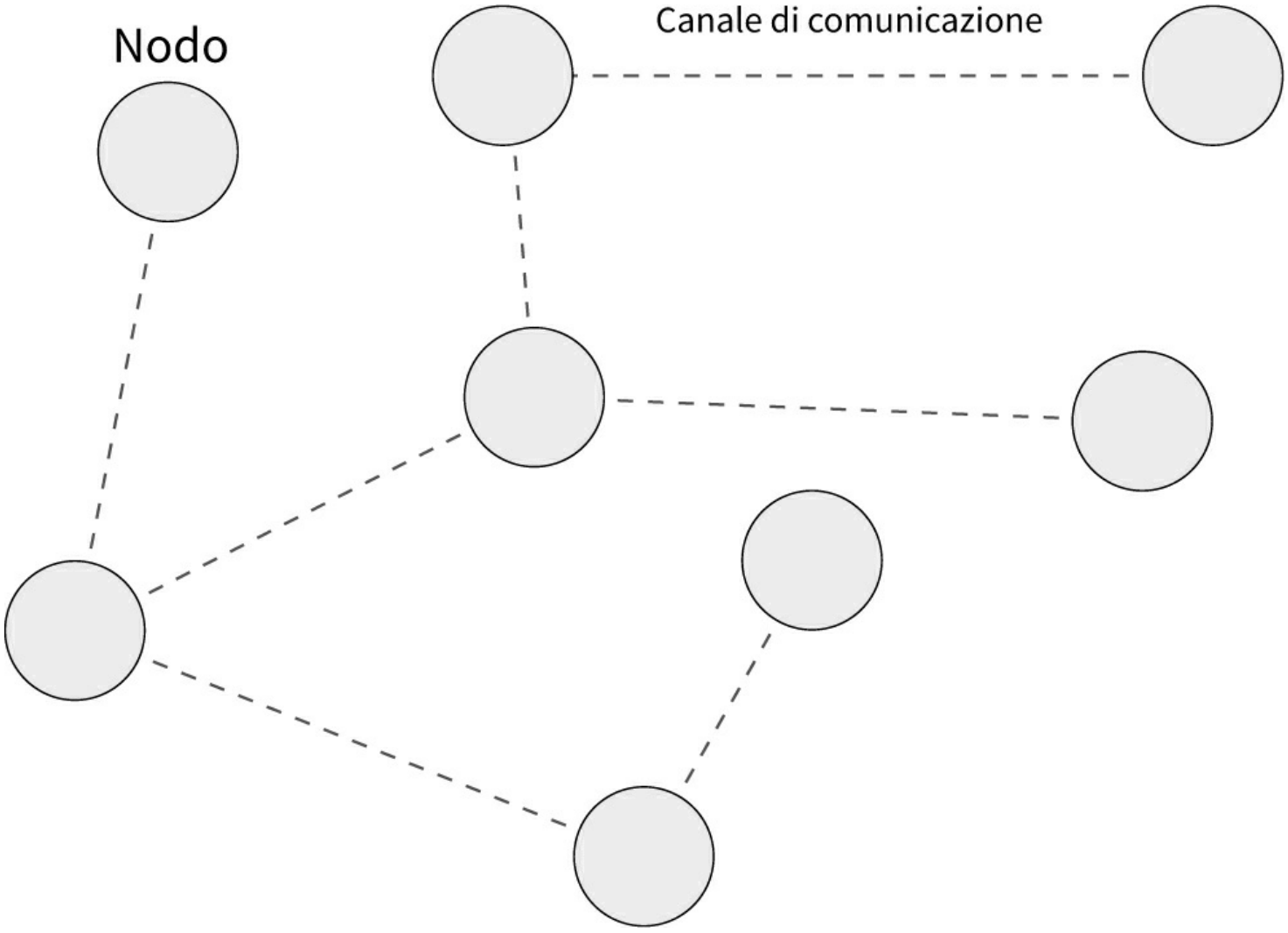


Figura 3.1 – La comunicazione tra i nodi in un network.

I nodi in una blockchain

Ogni macchina connessa alla rete della blockchain è un nodo. È possibile fare una distinzione tra:

- **Nodo completo (full-node):** scarica e archivia localmente una copia completa della blockchain e controlla che ogni transazione e blocco seguano le regole definite dal sistema. Qualora si presentasse un'anomalia, il blocco (o la transazione) verrebbe sempre rifiutato, anche se ritenuto valido da ogni altro nodo della rete.

  Un full-node è a tutti gli effetti indipendente. Non ha bisogno di avere fiducia in nessun altro

nodo e segue le regole indipendentemente da tutto, propagando i blocchi e le transazioni validi, ignorando quelli non validi.

Usare un full-node è il modo più sicuro per interagire con una blockchain, ma può essere piuttosto scomodo, poiché richiede il download dell'intera blockchain (nel caso della blockchain del Bitcoin parliamo di oltre 180 gigabyte a ottobre 2018).

- **Nodo light (light-node):** non memorizza l'intera blockchain ma riceve solo i dati di cui ha

bisogno da un nodo fidato (un full-node). Di conseguenza, l'utilizzo di questa tipologia di nodo implica la delega della fiducia a una terza parte (il full-node), in cambio della semplicità di utilizzo. L'utente medio tipicamente utilizza un light-node e non ha la capacità di verificare in modo indipendente la correttezza dei dati.

Un light-node può essere, per esempio, un wallet su un dispositivo mobile (Figura 3.2).

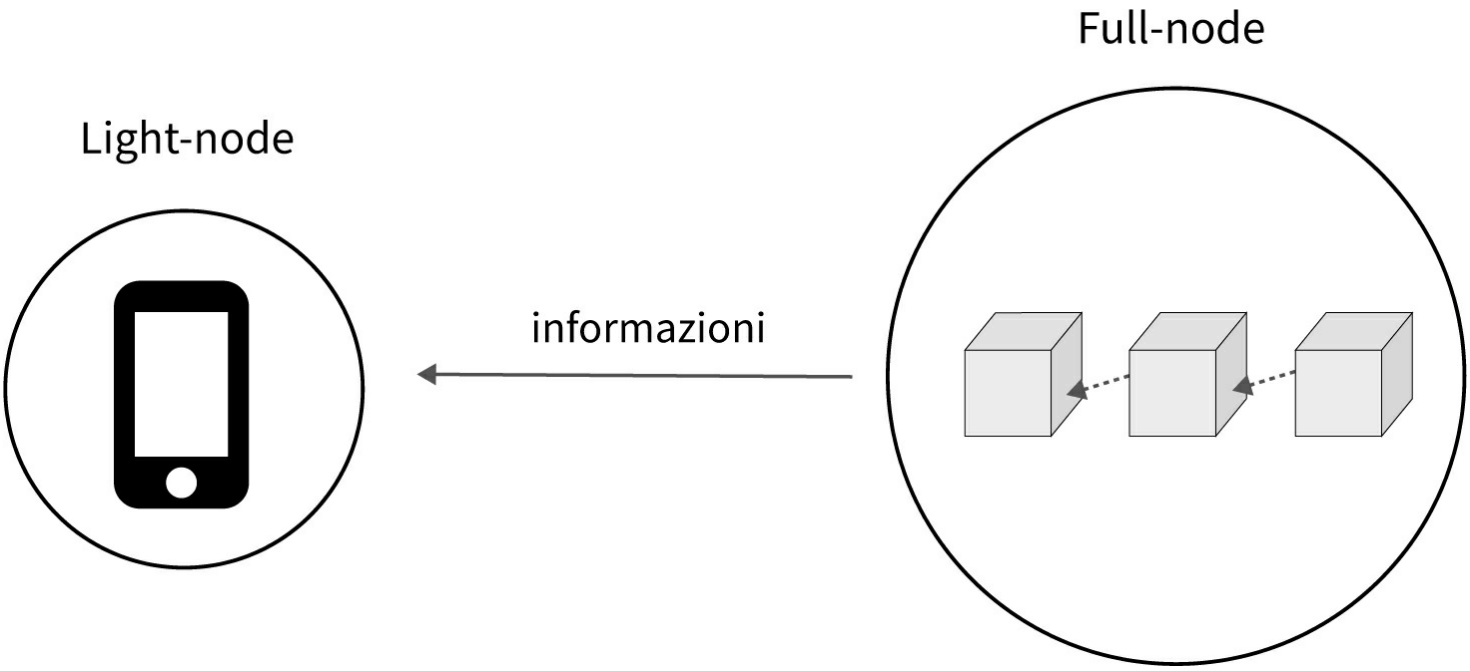


Figura 3.2 – Lo scambio di informazioni tra light-node e full-node.

Il vantaggio delle macchine

Oltre alla decentralizzazione dei dati, una delle ragioni che ha condotto alla nascita della tecnologia blockchain è stata la ricerca di un sistema che fosse

libero dai condizionamenti e dagli errori che caratterizzano gli esseri umani[17].

Un full-node segue categoricamente le regole imposte dal sistema, a prescindere dalle decisioni di tutti gli altri nodi.

Ne consegue che è un sistema intrinsecamente privo dei problemi che da sempre affliggono le istituzioni centralizzate, come la corruzione o la mancanza di imparzialità nelle scelte effettuate.

Architettura del network

Il network è una componente fondamentale in un sistema blockchain. Basandosi sulla struttura della rete e sul ruolo di ciascun nodo, è possibile identificare tre modelli di rete: centralizzate, decentralizzate e distribuite.

Reti centralizzate e decentralizzate

Il grado di centralizzazione è un concetto tramite il quale è possibile analizzare un sistema a diversi livelli. Noi raggrupperemo i sistemi secondo la loro centralizzazione dal punto di vista di architettura, autorità e logica[18].

Architettura

Una rete centralizzata a livello di architettura è un'infrastruttura con un punto centrale di errore (single point of failure) che, se compromesso, impedirebbe all'intero sistema di funzionare correttamente. Per fare un esempio, un'applicazione web che comunica con un singolo server è un sistema centralizzato dal punto di vista dell'architettura (Figura 3.3).

Anche un aereo con un singolo motore è un sistema con un'infrastruttura centralizzata: se quel motore si guasta, l'aereo precipita.

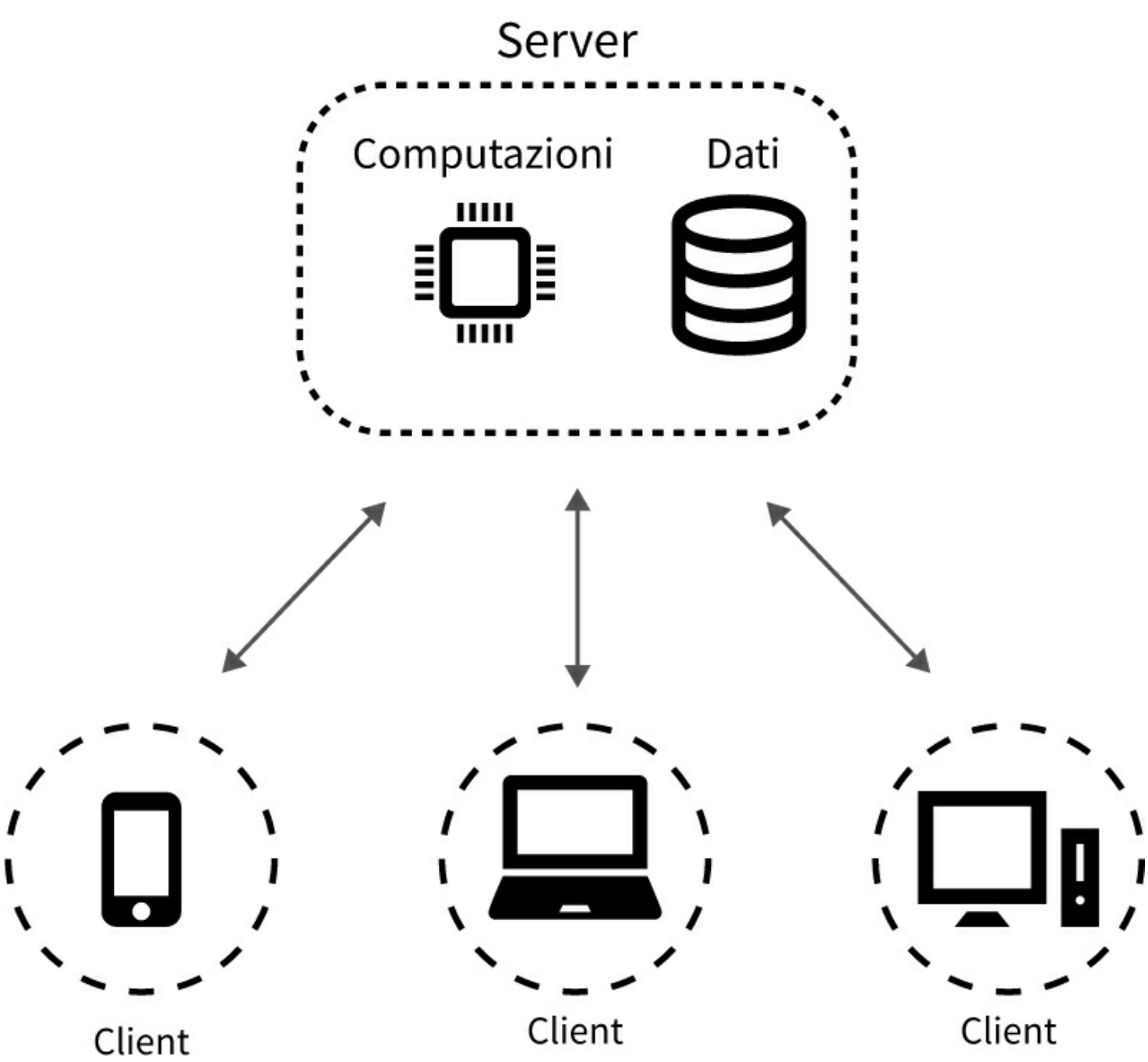


Figura 3.3 – La comunicazione tra client e server in un'architettura centralizzata (modello client-server).

In una **rete decentralizzata**, le risorse

sono distribuite e possibilmente replicate nei nodi della rete e, di conseguenza, un'applicazione viene eseguita da tutti i suoi partecipanti senza generare un singolo punto di possibile fallimento infrastrutturale (Figura 3.4). In altre parole, per fare in modo che un sistema decentralizzato smetta di funzionare è necessario "spegnere" tutti i nodi che lo compongono (per esempio, nella blockchain del Bitcoin, bisognerebbe spegnere più di 10.000 nodi).

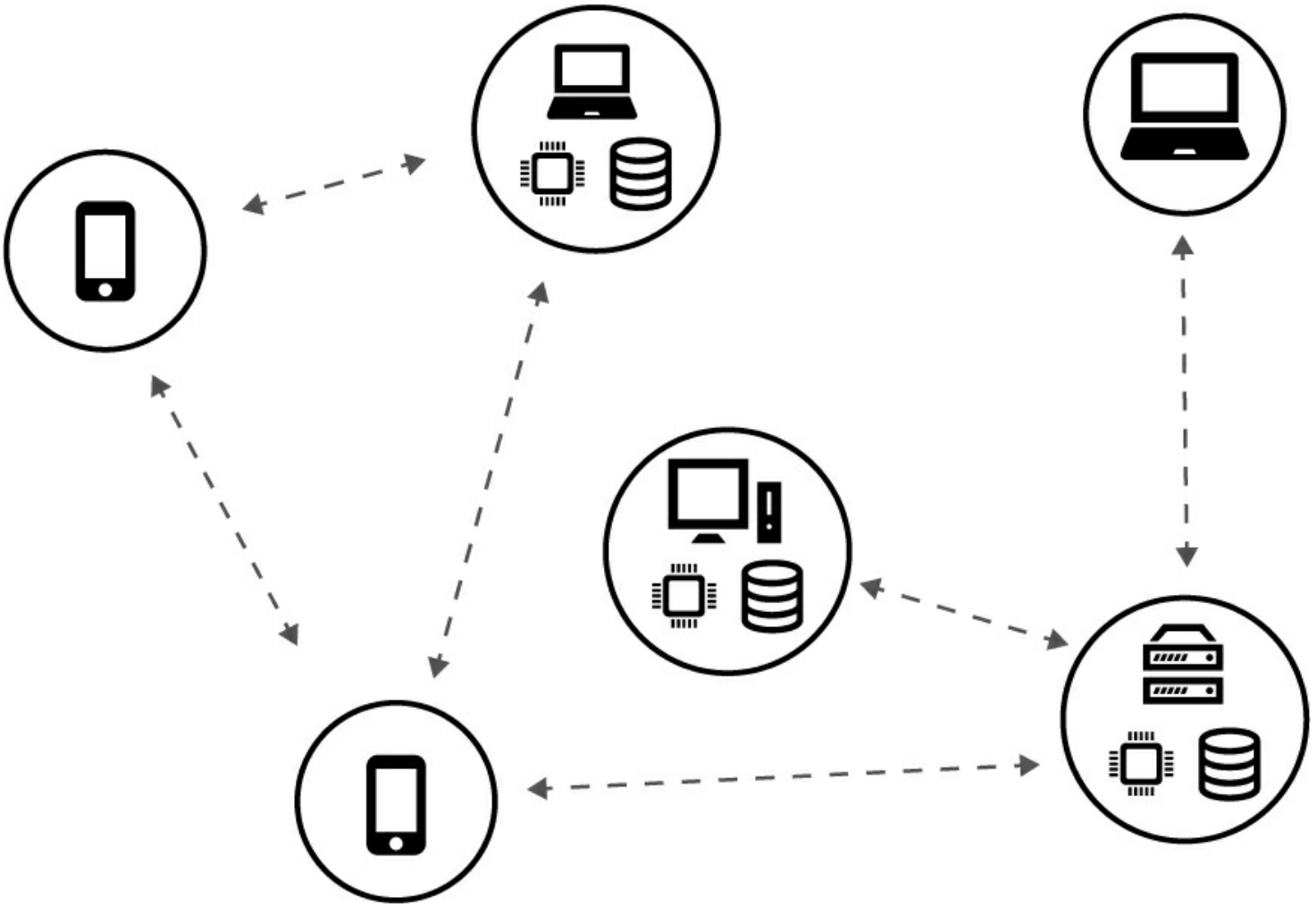


Figura 3.4 – La comunicazione tra i nodi in un'architettura decentralizzata (modello p2p).

Una blockchain è **architetturalmente decentralizzata**.
Non esiste un singolo punto di fallimento.

Autorità

Una rete sottoposta ad **autorità centralizzata** è caratterizzata da un ente centrale che ne controlla i dati, le operazioni e gli utenti. Per fare qualche esempio, Facebook, Amazon, Google o una qualsiasi banca sono tutti sistemi caratterizzati da un'autorità centrale.

Essa definisce tutte le regole del sistema e ha il potere di applicare tali regole ai suoi utenti, decidendo di conseguenza cosa è giusto e cosa sbagliato, richiedendo la fiducia incondizionata degli utenti.

In una rete con **autorità decentralizzata** non esiste un'autorità centrale e tutti i nodi sono considerati

uguali. Nessuno infatti detiene il controllo della rete e di conseguenza nessuno può impedire delle azioni o forzare la censura dei contenuti.

> Una blockchain è caratterizzata da **autorità decentralizzata**.
> Nessuna autorità centrale ne detiene il controllo.

Logica

Una rete **logicamente centralizzata** deve essere identificata in ogni istante da un singolo stato per funzionare correttamente. Di conseguenza è

necessario che tutti i partecipanti siano d'accordo su quale sia lo stato del sistema. Esiste quindi un unico stato logico sul quale tutti i partecipanti concordano. L'esempio classico è un database centrale globale in cui tutti i dati vengono salvati e mantenuti coerenti.

In una rete **logicamente decentralizzata** possono esserci diverse copie dei dati e qualsiasi nodo può modificare la propria copia senza alterare il normale funzionamento del sistema (Figura 3.5).

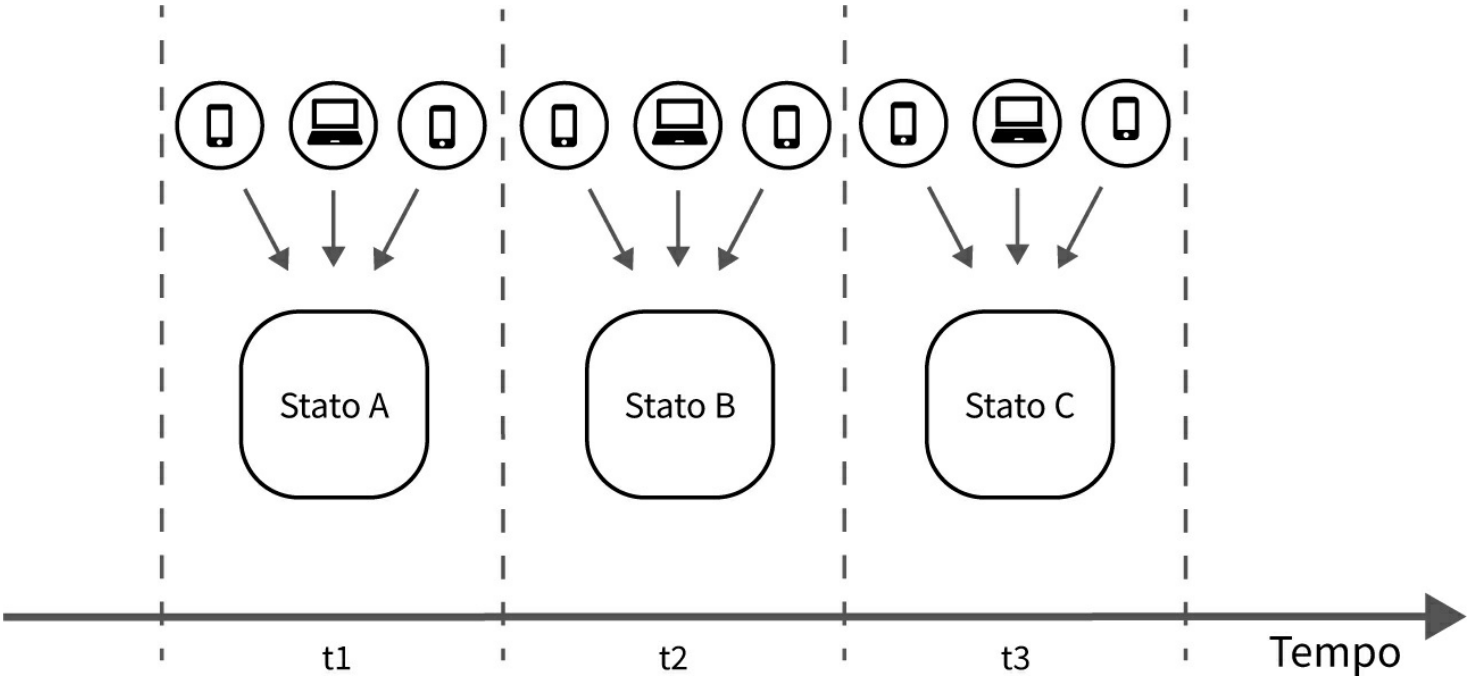


Figura 3.5 – L'evoluzione dello stato in una blockchain.

Per esempio, nel caso delle email: se io cancello una mail nella mia casella di posta, non la cancello anche nelle caselle delle altre persone a cui l'ho inviata.

Una blockchain è **logicamente centralizzata**.

È sempre caratterizzata da un singolo stato logico.

Reti distribuite

In una rete distribuita, i dati e le computazioni sono distribuiti su più nodi, ma l'autorità può rimanere centralizzata.

Un server sottoposto ad autorità centralizzata è tipicamente distribuito, e infatti società come Google, Facebook e Amazon adottano queste caratteristiche nei loro sistemi. Per minimizzare i rischi e le complessità di gestione, le reti distribuite non possiedono un solo, enorme, server o database, bensì vari data center sparsi in tutto il mondo

(Figura 3.6).

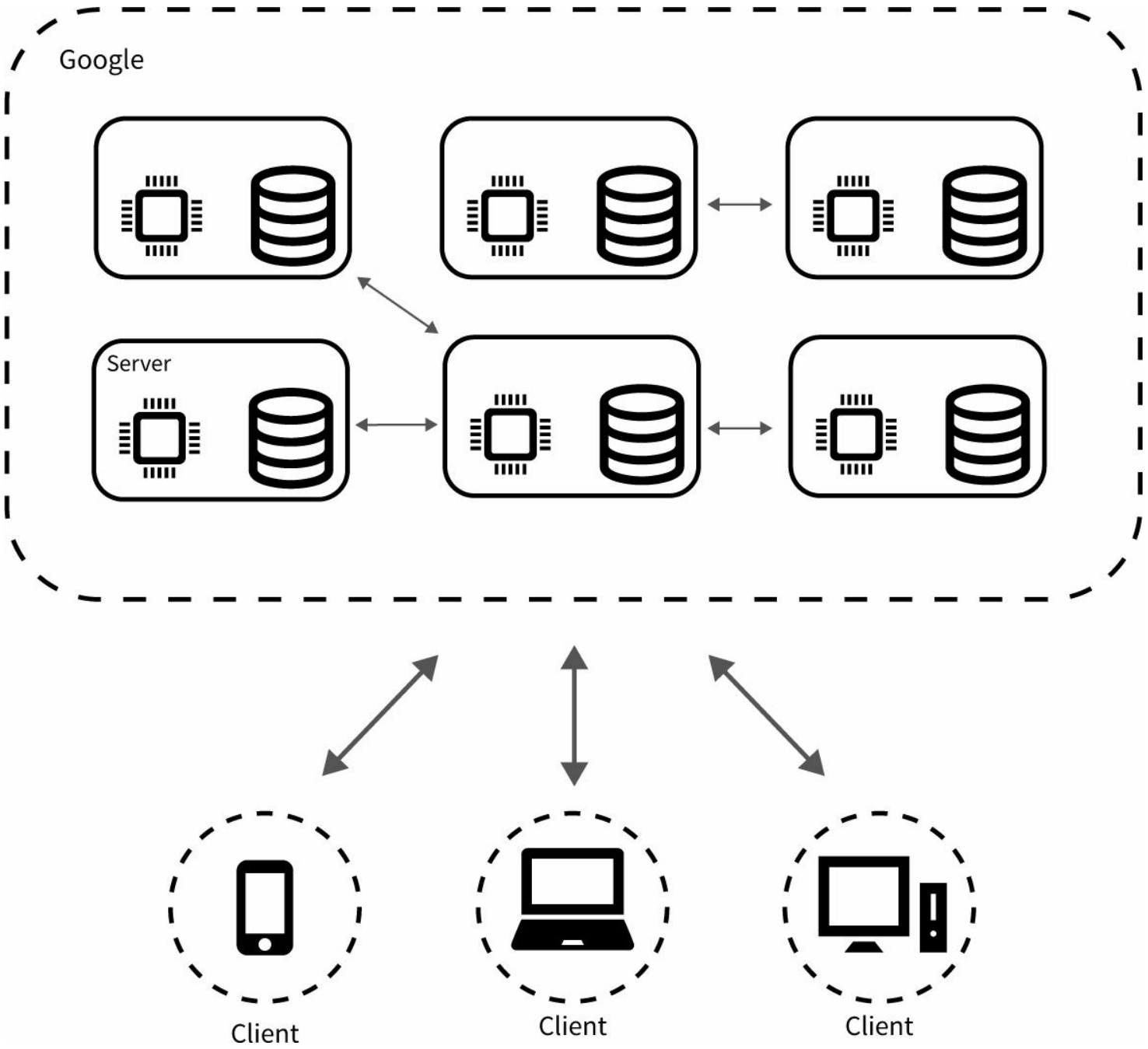


Figura 3.6 – La comunicazione tra client e server in una rete distribuita (con autorità centralizzata).

La rete di una blockchain è

anche distribuita.
Ogni full-node possiede una copia della blockchain.

Modelli di blockchain

La blockchain può essere utilizzata in ogni scenario in cui è richiesto uno stato globale logicamente centralizzato ma una struttura del sistema distribuita e decentralizzata.

Uno stato logicamente centralizzato è fondamentale per il funzionamento di ogni blockchain. Tuttavia in alcuni casi l'autorità in una blockchain può non essere decentralizzata, ma tendere alla centralizzazione. Nello specifico, a

seconda di come viene gestita l'autorità, esistono tre modelli di blockchain: **pubblica, ad autorizzazione** e **privata**.

Blockchain pubbliche (permissionless)

Il modello di blockchain pubblica è attualmente quello più noto e utilizzato.

Una blockchain pubblica è un sistema:

- ad architettura **decentralizzata**
- ad autorità **decentralizzata**
- a logica **centralizzata**

La decentralizzazione è un aspetto

chiave di questo modello, dal momento che qualsiasi tentativo di centralizzazione introdurrebbe una debolezza nel sistema esponendo un potenziale punto di fallimento o di controllo.

Non esiste una singola autorità. Tutti possono unirsi alla rete (aperta) e non c'è possibilità di essere esclusi (resistenza alla censura).

Una blockchain aperta non discrimina in base a origine, destinazione o contenuto (neutrale). Ogni nodo ha uguali diritti e responsabilità. Ognuno ha la possibilità di esplorare e verificare ogni transazione (pubblica e analizzabile).

Di solito, una blockchain aperta è

anche open source, rendendo pubblicamente disponibile e consultabile il codice che ne regola il funzionamento. Ciò consente a tutti di verificarne la correttezza o di suggerire dei miglioramenti.

Quando si parla di blockchain, solitamente ci si riferisce alle blockchain pubbliche.

Blockchain private (permissioned)

Sebbene le blockchain pubbliche abbiano delle proprietà uniche, queste stesse proprietà possono renderle non ideali in alcuni contesti, per esempio in ambito industriale.

Le blockchain private sacrificano

una completa decentralizzazione in cambio di un controllo sui permessi di accesso e solitamente delle migliori performance.

> Le blockchain private possiedono un livello di verifica degli accessi controllato da una o più autorità.

Il livello di verifica degli accessi ha il compito di decidere chi può leggere/scrivere i dati sulla blockchain e chi può partecipare al processo di verifica delle transazioni. Il sistema viene considerato affidabile solo se gli

attori scelti per il processo di verifica sono affidabili.

Tipicamente si distingue tra blockchain **completamente private** e **consortium**, dove nelle prime il controllo e l'autorità viene concentrata in una singola entità, mentre nelle seconde viene distribuita tra i partecipanti del network. Dal momento che le blockchain completamente private rimuovono totalmente la decentralizzazione e con essa gran parte dei vantaggi peculiari della tecnologia, quelle che riscuotono il maggiore interesse sono le blockchain consortium, dal momento che si presentano come una soluzione ibrida tra blockchain pubbliche e completamente private.

Per governi, istituzioni o aziende, entrambi i modelli possono risultare più convenienti specialmente quando è necessario un certo grado di controllo sui dati o sui partecipanti nel sistema, quando si vuole instaurare un regime di collaborazione autonomo tra diverse aziende, o per mantenere confidenziali dati sensibili. Analizzeremo nel dettaglio questo argomento nel Capitolo 12.

---

16. Questa è l'ideologia che sta dietro la più famosa blockchain, quella del Bitcoin.
17. Nel primo blocco della blockchain del

Bitcoin, quello creato da Satoshi Nakamoto nel 2009, era infatti stato salvato un messaggio in chiaro riferimento alle azioni che avevano causato la crisi finanziaria del 2008.

18. Questa è anche la suddivisione utilizzata dal fondatore di Ethereum, Vitalik Buterin. Vedi https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274.

4

Indirizzi, wallet e transazioni

Crittografia a chiave pubblica (crittografia asimmetrica)

Per crittografia si intende lo studio delle tecniche di comunicazione sicura in un ambiente ostile (come per esempio

Internet). La blockchain è un sistema nel quale la crittografia (nello specifico la crittografia a chiave pubblica) occupa un posto di particolare rilievo.

La crittografia a chiave pubblica è un sistema crittografico ampiamente utilizzato su Internet, e ricopre un ruolo fondamentale in molti dei processi che coinvolgono la blockchain. Come vedremo in seguito, gli **indirizzi** sulla blockchain vengono generati utilizzando questo sistema crittografico e le transazioni vengono autenticate utilizzando delle **firme digitali** – cioè una delle applicazioni più famose della crittografia a chiave pubblica.

Le chiavi crittografiche

L'idea di base è quella di utilizzare una coppia di chiavi in relazione matematica tra loro (Figura 4.1):

- una **chiave privata** generata casualmente, che deve restare segreta;
- una **chiave pubblica** derivata matematicamente dalla chiave privata, che può essere condivisa con chiunque[19].

Le chiavi non sono altro che dei numeri estremamente grandi, solitamente rappresentati in esadecimale (0-9 per rappresentare numeri dallo zero al nove e a-f per rappresentare numeri dal dieci al

quindici).

Nel Bitcoin, per esempio, la chiave privata corrisponde a un numero che occupa 256 bit (in altre parole, una sequenza di 256 uno e zero). Si può generare una chiave privata lanciando una moneta 256 volte, aggiungendo un 1 quando esce testa e uno 0 quando esce croce.

Il numero più grande che può essere salvato in 256 bit è 2^256 (115792089237316195423570985008687

Per rendere l'idea, 2^256 ≃ 10^78, mentre il numero di atomi nell'universo osservabile è di circa 10^80[20]. Generare due chiavi private uguali, seppur matematicamente possibile, è *estremamente* improbabile.

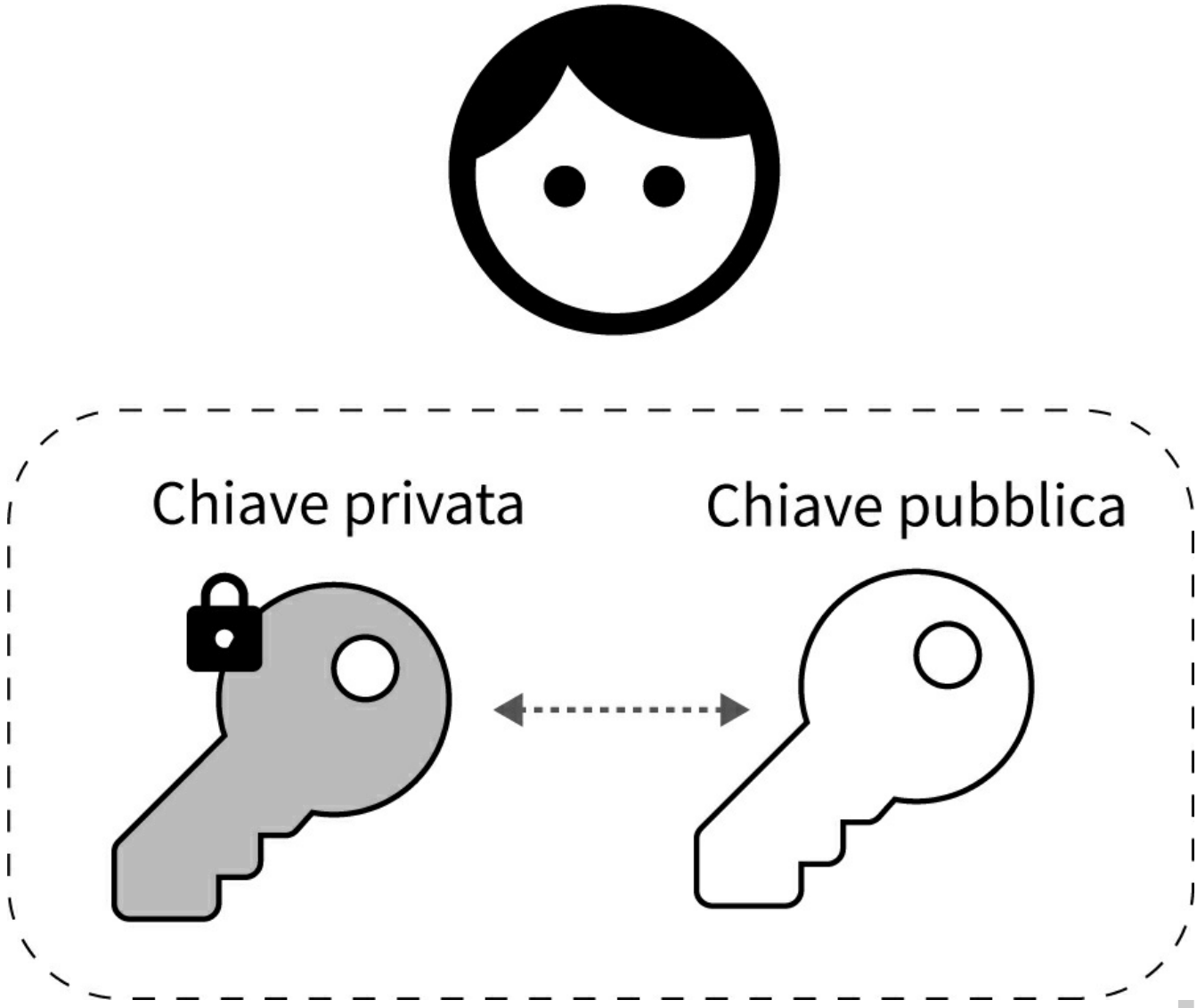


Figura 4.1 – La coppia di chiavi privata e pubblica.

Generare una chiave pubblica partendo da una chiave privata è computazionalmente molto facile, ma

invertire questa operazione (trovare la chiave privata partendo dalla chiave pubblica) è praticamente impossibile. Con i supercomputer più potenti attualmente in circolazione servirebbero milioni di anni.

La crittografia a chiave pubblica può essere utilizzata per garantire alcune proprietà come **criptazione, autenticazione, integrità** *e* **non-ripudio**, in un ambiente non sicuro come Internet.

Criptazione

Per criptazione si intende un

processo tramite il quale un messaggio, o in generale delle informazioni, sono codificate in modo che solo le persone autorizzate possano avere accesso alle informazioni originali.

L'utilizzo più esemplificativo della crittografia è quello di nascondere un messaggio in modo che non possa essere letto da persone non autorizzate[21]. Una volta che un messaggio viene criptato utilizzando un algoritmo a chiave pubblica, questo messaggio può essere trasferito attraverso un canale non sicuro come per esempio Internet, ma

garantendo lo stesso la confidenzialità del messaggio.

Per fare ciò, si cripta il messaggio utilizzando la **chiave pubblica** della persona che deve ricevere questo messaggio. Se per esempio Marco vuole mandare un messaggio ad Alice in modo che solo lei possa essere in grado leggerlo, basterà che Marco cripti questo messaggio con la chiave pubblica di Alice (Figura 4.2).

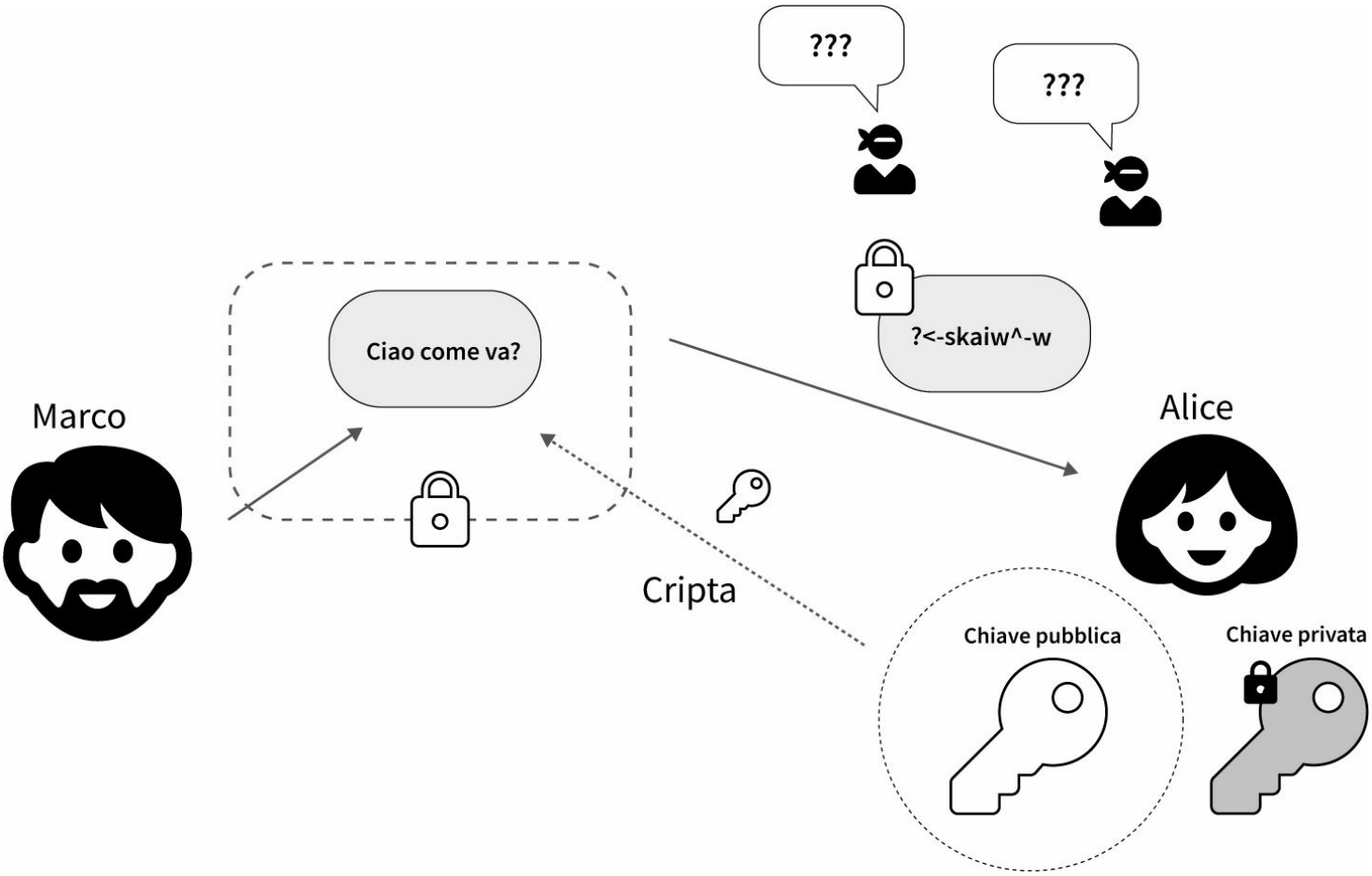


Figura 4.2 – La criptazione di un messaggio con la chiave pubblica del destinatario.

Così facendo solo il possessore della chiave privata collegata a quella chiave pubblica (si spera sia Alice) potrà essere in grado di decriptare il messaggio (Figura 4.3).

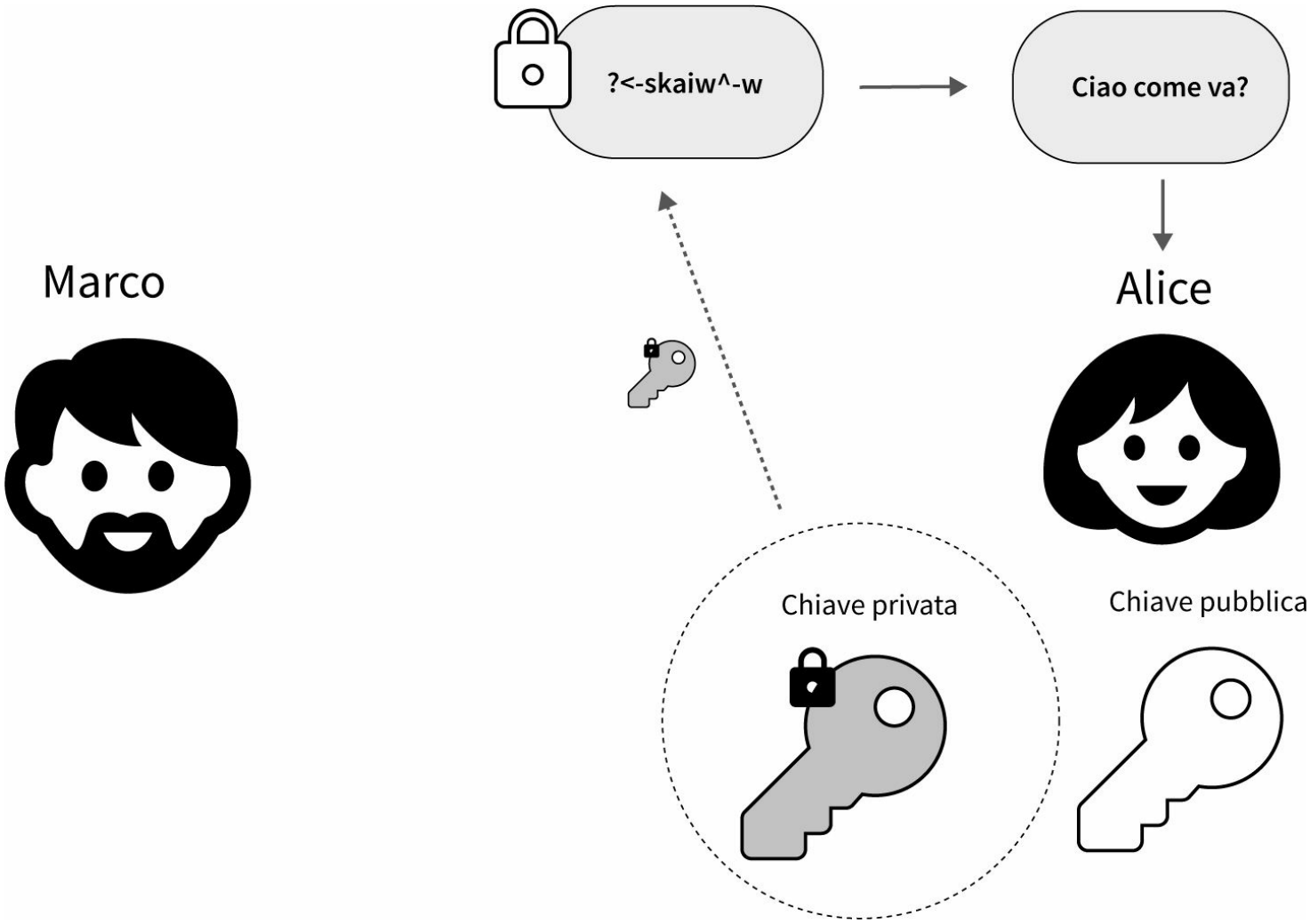


Figura 4.3 – La decriptazione di un messaggio con la chiave privata del destinatario.

Sorge però un problema: un messaggio criptato nasconde il contenuto a tutti coloro che non sono in possesso della chiave privata, però rimane possibile **modificare** questo messaggio anche

senza effettivamente capire cosa ci sia scritto. Per ovviare a questo problema, si usa unire alla criptazione altre tecniche, come per esempio l'hashing.

Hashing e criptazione

Qualcuno potrebbe trovare delle similitudini tra hashing e criptazione. In realtà hanno scopi molto diversi, anche se spesso sono usati insieme.

La criptazione codifica i dati con lo scopo principale di garantirne la confidenzialità. Se un dato viene criptato utilizzando la crittografia a chiave pubblica, esso può essere decriptato solo con la chiave privata associata.

Una funzione di hash al contrario non

è pensata per criptare un messaggio e non può essere invertita (funzione unidirezionale).

Firma digitale

Le firme digitali, come le firme tradizionali, sono un modo per dimostrare l'identità di qualcuno senza la sua presenza fisica, con la differenza che viene usata la matematica al posto di una firma manuale. Le firme digitali vengono create con una combinazione di hashing e crittografia a chiave pubblica (Figura 4.4).

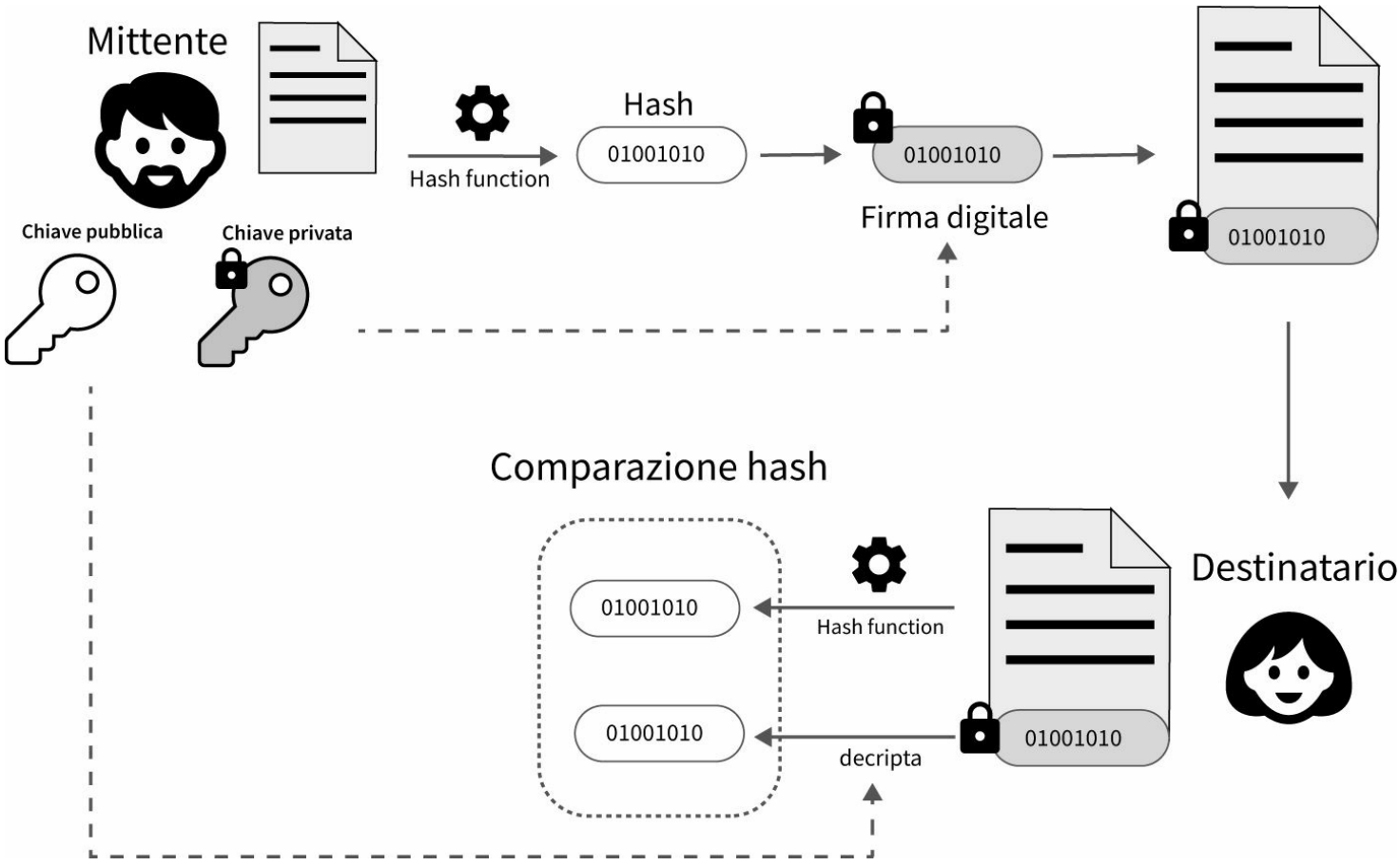


Figura 4.4 – Il processo di firma digitale.

Con una firma digitale è possibile ottenere:

- **Autenticazione:** una chiave privata è collegata a un utente specifico. Una firma valida dimostra inequivocabilmente che

il messaggio è stato inviato da quell'utente. L'autenticazione non richiede di conoscere la vera identità dell'utente, ma richiede di fornire un'informazione connessa alla sua identità (la chiave privata).

- **Integrità:** se un messaggio è firmato digitalmente, qualsiasi modifica al messaggio successiva alla firma invalida la firma stessa (questa è una proprietà derivante dall'hashing).
- **Non ripudio:** se qualcuno firma un messaggio, non può, in un secondo momento, negare di

averlo firmato.

Tutte queste proprietà sono valide fintanto che la chiave privata resta, appunto, privata.

Indirizzi

Su una blockchain non ci sono profili utente, ma piuttosto indirizzi.

Gli indirizzi non contengono criptovalute, ma sono solo degli identificatori che rappresentano la destinazione di una transazione.

> Gli indirizzi sono degli identificatori usati per

trasferire asset digitali.

Lo scopo di un indirizzo è quello di abilitare le transazioni verso (e da) un'entità unica. È possibile avere numerosi indirizzi che possono essere condivisi liberamente senza alcun problema di sicurezza, proprio come è sicuro condividere una chiave pubblica.

Generazione di un indirizzo

Da un punto di vista tecnico, un indirizzo è il risultato di un'operazione matematica che coinvolge la crittografia a chiave pubblica e l'hashing.

1. Per prima cosa viene generata

una chiave privata. È fondamentale che la chiave privata sia generata da un numero casuale, altrimenti potrebbe crearsi una vulnerabilità critica.

2. Dalla chiave privata viene derivata la corrispondente chiave pubblica, tramite un processo matematico. Come abbiamo già detto, questo calcolo può essere eseguito molto facilmente (da un computer).

3. La chiave pubblica viene passata attraverso una serie di algoritmi crittografici (diversi

tipi di funzioni hash) per ottenere un indirizzo sulla blockchain. Il risultato finale assomiglia a questo: *3GaR1AXseWNnLhishxnRGr3GZMfh* (indirizzo Bitcoin) o questo *0x8e4884a8F4 8e524377CCA3517b24700234ECfb2* (indirizzo Ethereum).

Da una chiave privata viene generata una chiava pubblica e dalla chiave pubblica viene generato un indirizzo sulla blockchain (Figura 4.5).

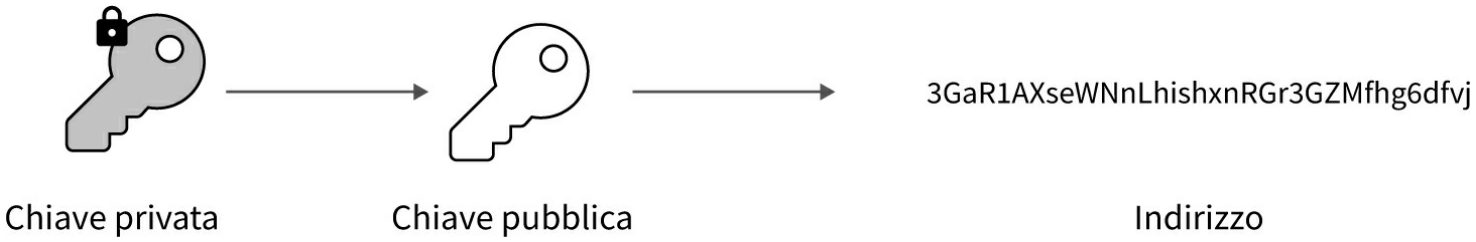


Figura 4.5 – La generazione di un indirizzo a partire dalla chiave privata.

Collisioni

Abbiamo detto in precedenza che un indirizzo viene generato a partire da una chiave privata random. Ma anche se è incredibilmente improbabile, cosa accadrebbe se due persone generassero la stessa chiave privata? La risposta è che entrambe le persone avrebbero accesso allo stesso indirizzo, e quindi alle stesse criptovalute. La legislazione in questo

caso è molto vaga e non si sa effettivamente come potrebbe essere gestita una situazione del genere[22].

Dove sono le mie criptovalute?

Abbiamo detto che gli indirizzi non contengono criptovalute. Dove sono quindi salvate queste criptovalute? In realtà da nessuna parte. È importante ricordare sempre che una blockchain è solo una lista di transazioni, non esiste il concetto di moneta come oggetto fisico che deve essere conservato da qualche parte. Le monete sono solo

voci contabili e il saldo finale di un indirizzo è un calcolo effettuato esaminando tutte le transazioni che coinvolgono quell'indirizzo.

Se questo concetto può sembrare strano, bisogna ricordare che nel nostro sistema monetario circa il 92% di tutto il denaro in circolazione esiste esclusivamente come voce contabile in sistemi informatici.

Indirizzo multisignature (firma multipla)

Il multisignature (multisig) è una tecnica utilizzata per aumentare la sicurezza delle transazioni, dove viene richiesta

più di una firma (quindi più di una chiave privata) per autorizzare una transazione. Un indirizzo multisignature è un indirizzo associato a più di una chiave privata. Gli indirizzi di questo tipo vengono solitamente definiti "m-of-n": sono richieste almeno *m* chiavi private su *n* totali per effettuare una transazione. Le chiavi private possono essere tutte in possesso della stessa persona (ma tenute ovviamente in posti diversi) oppure appartenere a persone diverse.

Prendiamo, per esempio, il caso di una persona che decide di creare un indirizzo multisignature con 3 chiavi, dove sono necessarie almeno 2 chiavi per autorizzare una transazione (2-of-3

multisig address). In questa situazione la persona può decidere di tenere una chiave sul suo telefono, un'altra chiave in una cassaforte in banca e la terza chiave in un server sicuro dove vengono eseguiti dei controlli antifrode simili a quelli delle carte di credito (Figura 4.6).

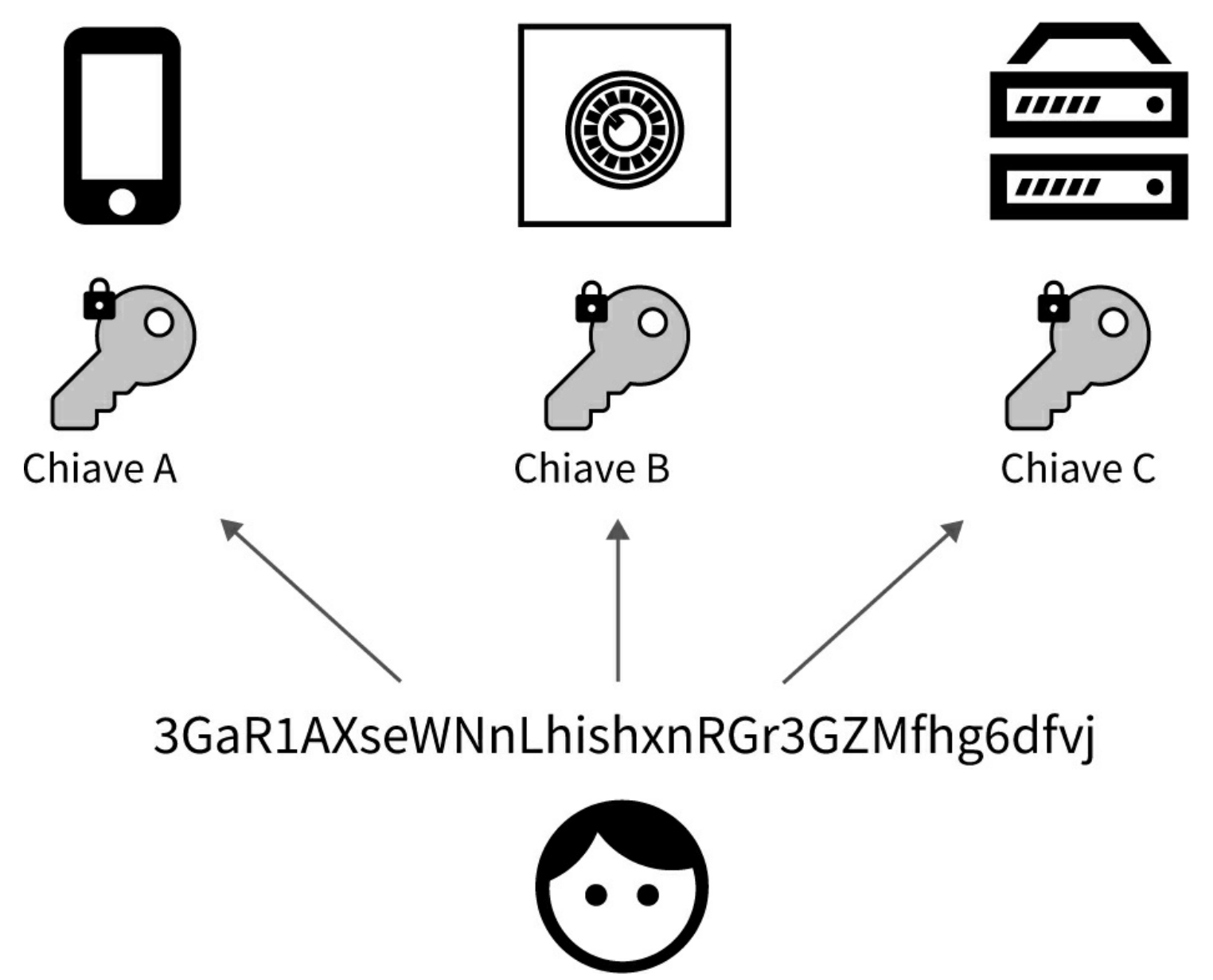


Figura 4.6 – Gli indirizzi multisignature, associati a più chiavi private.

Quando l'utente vorrà eseguire una transazione, per esempio pagare un caffè al bar, avrà bisogno di almeno due

chiavi private, in particolare la chiave sul suo smartphone e la chiave sul server, che verrà richiesta in automatico dall'applicazione mobile (Figura 4.7).

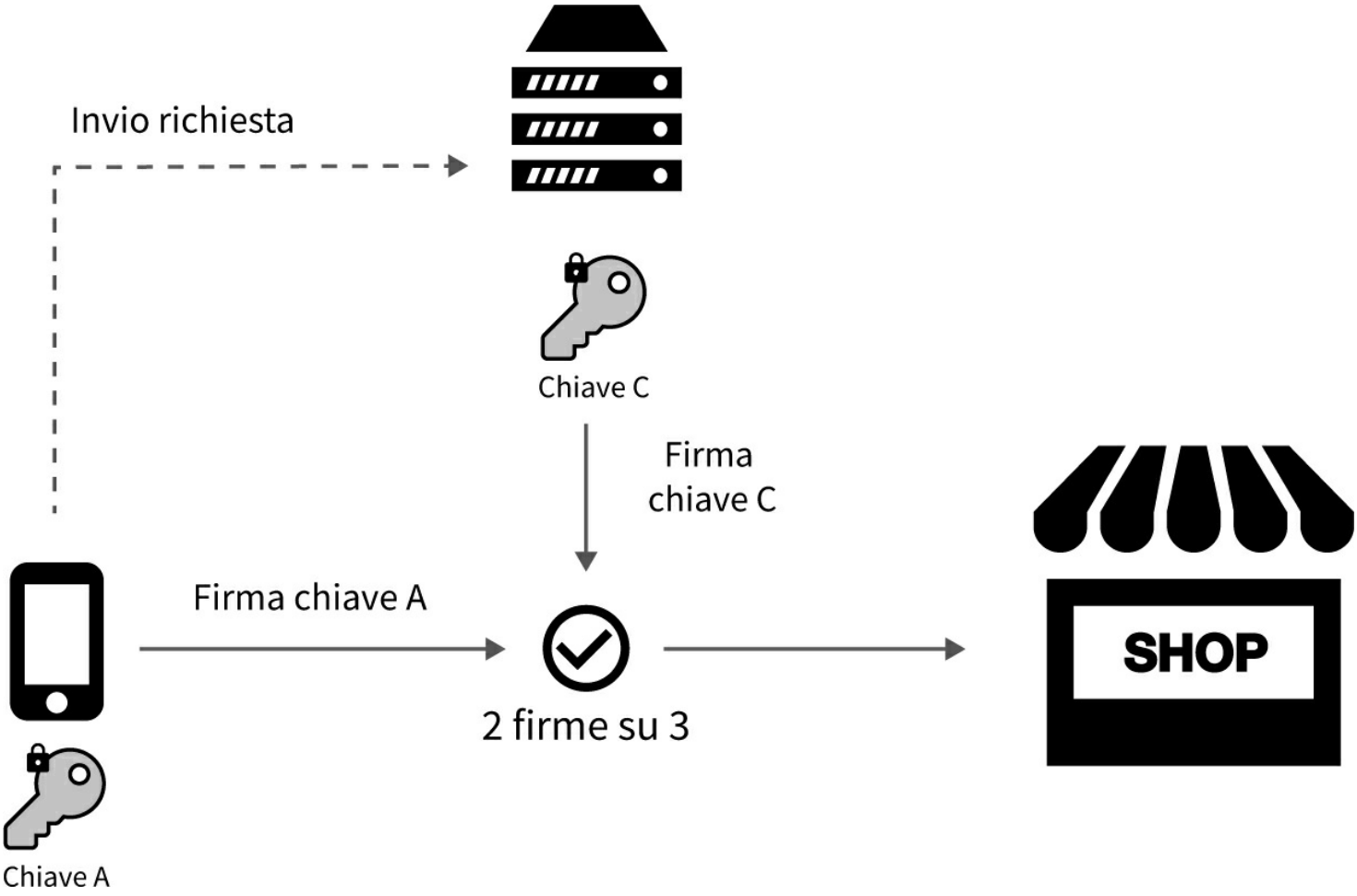


Figura 4.7 – La creazione di una transazione in un indirizzo multisignature.

Se l'utente perde una delle chiavi private, per esempio, se smarrisce il telefono, può utilizzare la chiave privata contenuta nella cassaforte per riprendere l'accesso al suo indirizzo.

Lo stesso concetto vale anche nel caso che si diano le chiavi a persone diverse. Così facendo si crea un indirizzo dove la proprietà è condivisa ed è necessario avere il consenso di più persone per effettuare transazioni. Questo scenario è molto comune nelle aziende per evitare che qualcuno possa creare transazioni errate o peggio rubare i fondi.

Per esempio un indirizzo multisig può essere assegnato a 10 persone ma richiedere almeno 7 persone per effettuare transazioni. Nessuno può scappare con i soldi e anche il rischio fisico di essere rapiti o minacciati viene mitigato, in quanto una singola persona

non può effettuare transazioni.

Wallet

Gli indirizzi vengono generalmente gestiti utilizzando strumenti specifici denominati wallet. A differenza dei portafogli tradizionali, però, non contengono denaro.

> Un wallet memorizza le chiavi pubbliche e private di un indirizzo, e può essere visto come “il tuo account”. I dati corrispondenti agli indirizzi sono sempre memorizzati sulla

blockchain.

Non è possibile quindi perdere le criptovalute, ma solo perdere le chiavi private che danno accesso a quelle criptovalute.

Solitamente i wallet forniscono anche un'interfaccia per tracciare il saldo finale di tutti gli indirizzi posseduti da un utente, e automatizzare alcune funzioni come la firma delle transazioni o il suggerimento delle commissioni per una transazione[23]. Esistono tre tipi principali di portafogli: **software, hardware** o **cartacei**. Inoltre, a seconda dell'ambiente in cui operano questi

wallet, è possibile fare un'altra distinzione tra **cold storage** e **hot storage**.

Hot storage e cold storage

Un wallet hot storage è un wallet collegato in qualche modo a Internet, ovvero le chiavi private sono state create o sono attualmente memorizzate su una macchina connessa a Internet. Al contrario, un wallet cold storage fa riferimento a un wallet le cui chiavi private non sono mai entrate in contatto con Internet.

Una soluzione cold storage è estremamente più sicura, in quanto è

molto più difficile rubare qualcosa che non sia connesso a Internet.

Paper wallet

Un paper wallet è la forma più semplice possibile di cold storage. In pratica è la coppia chiave privata-indirizzo stampate su un pezzo di carta. La sicurezza di un paper wallet è direttamente collegata alla sicurezza del posto in cui il foglio di carta viene conservato (Figura 4.8).

Figura 4.8 – Esempio di paper wallet (© bitaddress.org).

Software wallet

Un software wallet è un'applicazione che può essere installata su un computer o su uno smartphone. La chiave privata è codificata con una password e memorizzata sulla macchina stessa. I software wallet sono spesso scelti per la loro semplicità di utilizzo (Figura 4.9). Tuttavia, se la macchina su cui sono installati venisse compromessa, le chiavi private potrebbero essere rubate.

Figura 4.9 – Esempio di software wallet (Exodus Wallet - © Exodus Movement, Inc.).

Hardware wallet

Un hardware wallet memorizza le chiavi private in un dispositivo fisico (hardware). Ha grandi vantaggi in termini di sicurezza rispetto ai software

wallet, in quanto le chiavi private sono memorizzate in un'area protetta del dispositivo dalla quale non possono essere estratte. Le transazioni vengono firmate all'interno del dispositivo stesso e quindi, anche se il wallet venisse collegato a una macchina compromessa, le chiavi private resterebbero al sicuro (Figura 4.10).

Gli hardware wallet rappresentano attualmente il miglior compromesso in termini di sicurezza e semplicità di utilizzo.

Figura 4.10 – Esempio di hardware wallet

(Ledger Nano S. © Ledger SAS).

Exchange “wallet”?

Una precisazione per quanto riguarda gli exchange centralizzati come Coinbase o Binance: parlare di exchange wallet non è propriamente corretto, in quanto un utente che deposita i fondi sull’exchange non ha accesso alle proprie chiavi private, ma sta di fatto delegando la gestione del suo wallet all’exchange stesso. Un exchange è quindi in possesso di numerosi wallet che contengono le criptovalute degli utenti, i quali poi vengono gestiti internamente dall’exchange. Questo argomento verrà

largamente approfondito nel paragrafo sugli exchange del Capitolo 11.

Backup e HD wallet

Solitamente la prima volta che viene utilizzato un wallet (hardware o software) viene comunicata una lista di parole da salvare. Questa lista, chiamata "passphrase", consente di ripristinare il wallet, riacquisendone l'accesso.

Come è possibile ripristinare un portafoglio utilizzando una passphrase? Questo significa che le chiavi private sono quindi archiviate altrove? No, questa non sarebbe una pratica sicura.

In questi tipi di wallet, chiamati

wallet HD (Hierarchical Deterministic) la passphrase è il punto d'origine da cui vengono generate le chiavi private. Le parole che compongono la passphrase rappresentano la **casualità** (randomness). Questi wallet implementano un sistema per derivare le chiavi da un singolo punto di partenza noto come "seed" (specificato in BIP 32 e BIP 39[24], Bitcoin Improvement Proposal).

Il seed consente all'utente di eseguire il ripristino di un wallet senza bisogno di altre informazioni. Se un computer, un hard disk o un wallet hardware venissero distrutti, sarebbe facilmente possibile ripristinare le

chiavi private su un altro dispositivo semplicemente re-inserendo questo seed su un altro dispositivo.

Un esempio di passphrase potrebbe essere: “wild never seat speak jazz lumber length oppose ignore house fence invest”.

È importante ricordare che la passphrase è equivalente alle chiavi private e che deve essere conservata con la stessa attenzione.

Transazioni

Ora che abbiamo un’idea più chiara dei componenti principali di una blockchain,

siamo pronti a eseguire (finalmente) la nostra prima transazione.

> Una transazione (valida) è l'unità elementare di informazione che viene scritta sulla blockchain.

Una transazione valida implica un cambio di stato nella blockchain. Come abbiamo spiegato precedentemente, una blockchain è logicamente centralizzata, ovvero deve esserci un singolo stato che sia ritenuto valido dal network. Una transazione genera un nuovo stato. Le transazioni possono essere monetarie, come l'invio di bitcoin, o coinvolgere

altri asset digitali (stock, certificati di proprietà ecc.).

Il consenso in breve

Poiché non esiste un'autorità centrale, risulta necessario trovare un modo per raggiungere un accordo sullo stato corretto della blockchain, e cioè decidere quali transazioni sono avvenute e in quale ordine.

Il consenso rappresenta l'unica verità possibile sul corretto stato della blockchain.

Di conseguenza, una transazione è valida soltanto se approvata dal consenso del network.

Esploreremo in seguito più in

dettaglio in che modo viene raggiunto il consenso.

Transazioni deterministiche

Una transazione può essere valida e quindi modificare lo stato della blockchain, oppure essere invalida e lasciare la blockchain nel suo stato corrente (Figura 4.11). Per questo motivo si dice che una transazione è un'**operazione atomica**, ovvero non può generare uno stato intermedio.

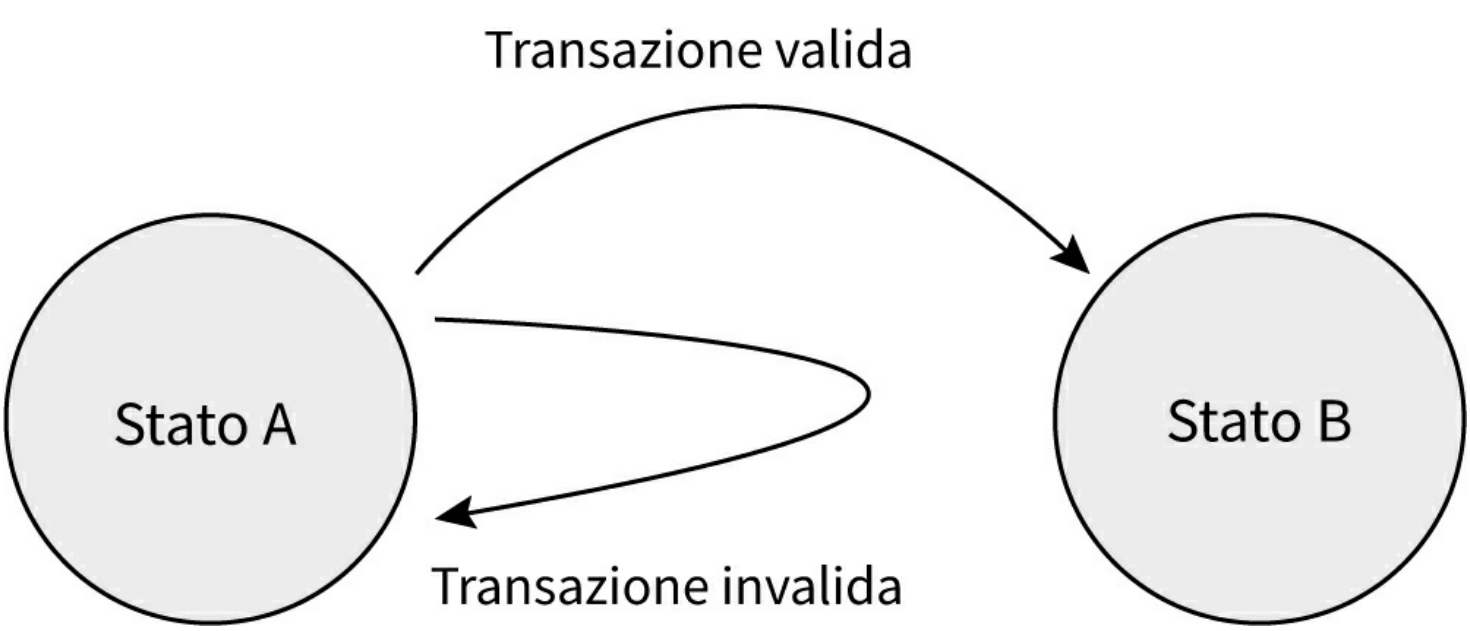


Figura 4.11 – Una transazione valida modifica lo stato della blockchain.

Così come non è possibile che una transazione valida venga rifiutata, non è possibile modificare una transazione una volta accettata.

Una transazione è immutabile.

Normalmente siamo abituati alla

possibilità di poter annullare una transazione (per esempio nelle transazioni bancarie o con PayPal). È una funzionalità a volte conveniente, ma che presuppone un sistema tutt'altro che immutabile.

In una blockchain, se si crea una transazione valida, non è possibile per nessuno eliminarla, annullarla o modificarla. La transazione verrà eseguita e modificherà lo stato della blockchain.

È possibile tuttavia aggiungere una o più condizioni a una transazione, per esempio decidere di confermare un pagamento solo dopo aver soddisfatto dei vincoli specifici (come succede nel caso degli smart contract, che andremo a

vedere in seguito). Se le condizioni sono soddisfatte, tutte le parti coinvolte nella transazione sapranno per certo cosa succederà. Non è possibile cambiare il risultato.

Creare una transazione

Il requisito di base per la creazione di una transazione su una blockchain (e in qualsiasi altro scenario) è possedere l'oggetto della transazione. Per esempio, se si desidera trasferire alcuni bitcoin, è necessario dimostrare di possedere quei bitcoin in primo luogo. In un sistema totalmente digitale, questo è possibile grazie alle **firme digitali.**

Un bitcoin, per esempio, non è mai associato a una persona, ma sempre a un indirizzo. Possedere le chiavi private di quell'indirizzo significa possedere i bitcoin collegati a esso.

Il mittente firma digitalmente ogni transazione con la chiave privata dell'indirizzo utilizzato (Figura 4.12).

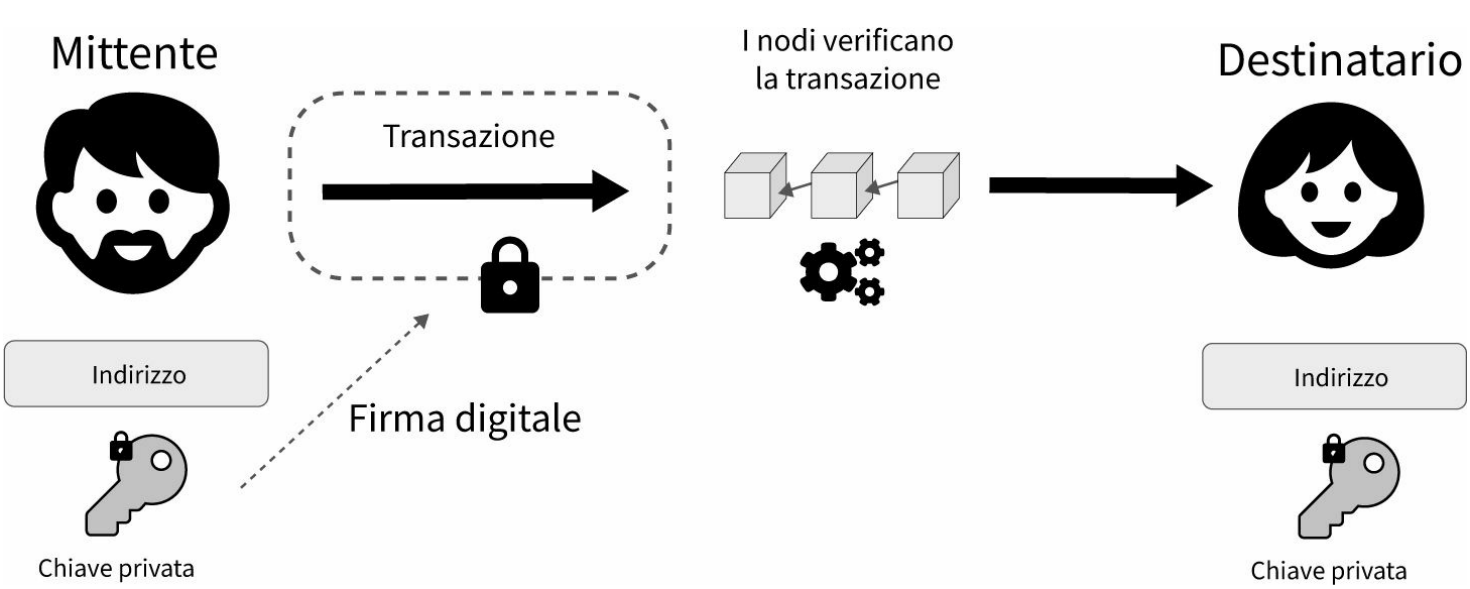


Figura 4.12 – La creazione e verifica di una transazione sulla blockchain.

La firma digitale garantisce che:

- L'indirizzo che ha creato la transazione appartiene all'utente. Quindi un utente che vuole inviare 1 bitcoin ha bisogno di possedere le chiavi private di un indirizzo con almeno 1 bitcoin associato. La transazione è firmata con la chiave privata

dell'utente (**autenticazione**).

- La transazione non è stata modificata dopo la firma (**integrità**).
- L'utente proprietario della chiave privata (utilizzata nella transazione) non può negare di aver creato la transazione (**non ripudio**).

Ricordiamo inoltre che in una transazione di criptovalute non c'è nessun trasferimento fisico di denaro, in quanto si tratta di voci contabili di un ledger digitale. Una transazione non fa altro che registrare nel ledger l'importo trasferito dal mittente al destinatario.

Le transazioni offline

Sebbene per comunicare con la blockchain sia necessario essere connessi al network, la creazione e la firma digitale di una transazione può avvenire tranquillamente su un computer che non si trova online. La creazione offline di una transazione è una pratica che serve principalmente ad aumentare la sicurezza. Paradossalmente è possibile creare una transazione a mano, scriverla su un foglio di carta e spedirla per posta a un altro nodo del network (non lo consigliamo, ma è teoricamente possibile).

Una volta che la transazione è stata creata e firmata, può essere propagata ai nodi limitrofi, i quali hanno il compito di verificarne la validità e decidere se propagarla ulteriormente o meno (Figura 4.13).

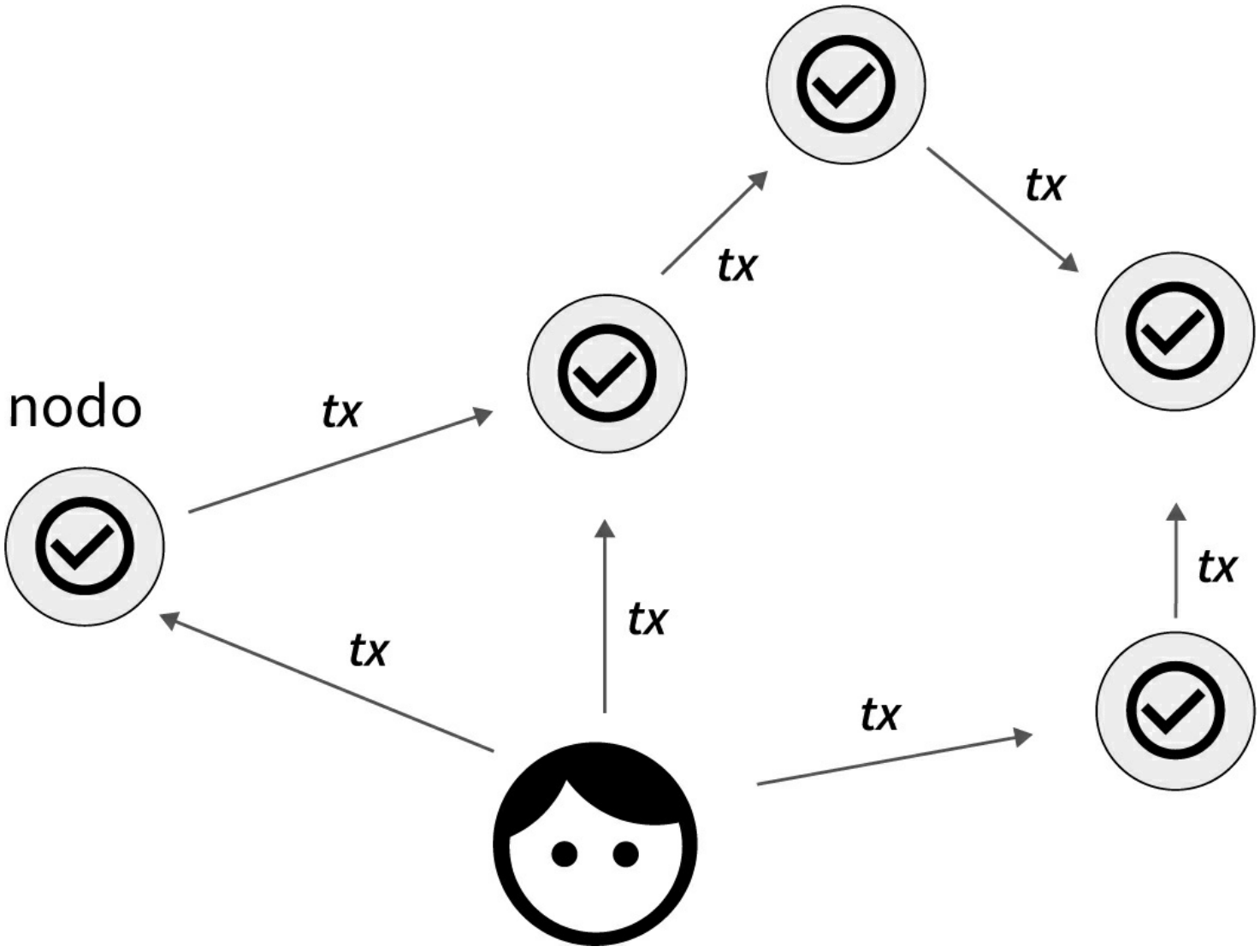


Figura 4.13 – La propagazione di una transazione ai nodi del network.

La transazione valida viene quindi propagata ai nodi del network, ma non è ancora registrata in modo immutabile sul ledger distribuito (la blockchain).

Conferme

Prima di approfondire in che modo i nodi decidono se una transazione sia valida o meno, spieghiamo brevemente in cosa consistono le conferme in una transazione.

Le transazioni sono raggruppate in blocchi. I blocchi sono aggiunti alla blockchain in modo sequenziale.

Ogni transazione deve passare attraverso un processo di verifica prima di essere inclusa in un blocco (e quindi nella blockchain). Prima di essere aggiunta in un blocco, una transazione è **senza conferme**. Una volta che una transazione viene inclusa in un blocco ha **1 conferma**. Quando viene creato il

blocco successivo, la stessa transazione ha 2 conferme, e così via[25].

Il numero di conferme di una transazione corrisponde al numero di blocchi successivi a quello in cui la transazione viene inclusa (Figura 4.14).

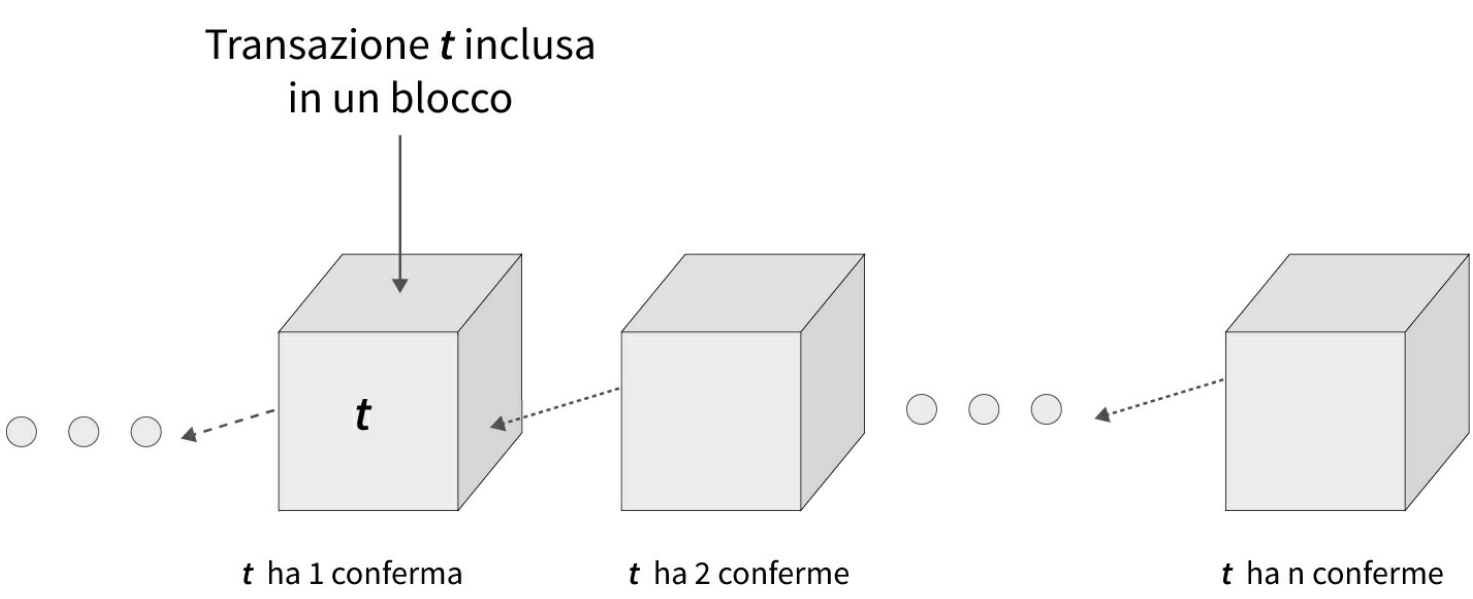


Figura 4.14 – Il numero di conferme di una transazione all'aumentare dei blocchi.

Per varie ragioni che vedremo meglio in seguito, solitamente una transazione con una singola conferma non viene ancora considerata immutabile.

Nel Bitcoin, per esempio, una transazione è considerata immutabile dopo sei conferme (circa 1 ora). In Ethereum si consiglia di attendere 12 conferme (3 minuti). È possibile anche

aspettare solo 1 conferma (o addirittura nessuna) per una transazione di piccola entità, ma per quantità rilevanti è meglio attendere più conferme.

Una volta ottenute abbastanza conferme, una transazione non può essere annullata/modificata da nessuno.

Commissioni di transazione

Solitamente una transazione include una commissione. Le commissioni di transazione corrispondono al costo necessario per effettuare una determinata transazione, e vengono usate per ricompensare i miner (vedremo chi sono più avanti).

Si tratta quindi di commissioni che il mittente potrebbe dover includere nella sua transazione affinché vada a buon fine.

Ogni blockchain ha il suo sistema per determinare le commissioni di transazione. La commissione di transazione viene decisa dal mittente, può essere in alcuni casi pari a zero e non è correlata all'importo trasferito. La commissione di solito influenza il tempo necessario affinché una transazione venga confermata.

Specie in momenti di particolare congestione, una transazione con commissione pari a zero può richiedere la generazione di diversi blocchi prima

di venire inclusa e conseguentemente verificata.

Molti wallet consigliano automaticamente la commissione per una transazione, ma è anche possibile trovare in vari siti Internet la commissione attuale media di una blockchain[26].

---

19. Per chi volesse approfondire: nel Bitcoin, per generare le chiavi si utilizza un algoritmo basato sulle curve ellittiche chiamato ECDSA.

20. https://www.wolframalpha.com/input/?i=number+of+atoms+in+the+universe.

21. Similmente a come avviene con servizi di messaggistica come Whatsapp, che utilizzano

la crittografia end-to-end per garantire la confidenzialità dei messaggi.

22. Per chi volesse approfondire la questione c'è un progetto chiamato Large Bitcoin Collider che sta cercando di trovare almeno una collisione.

23. Le commissioni di transazione variano a seconda della blockchain. In alcuni casi possono essere anche nulle. Saranno approfondite nelle pagine successive.

24. https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki https://github.com/bitcoin/bips/blob/master/bip-0039/english.txt.

25. Nella blockchain del Bitcoin viene creato un blocco ogni circa 10 minuti; in quella di Ethereum ogni 10-19 secondi.

26. Per esempio quella del bitcoin: https://bitinfocharts.com/comparison/bitcoin-transactionfees.html#6m.

5

Consenso e mining

Computer e software sono lontani dall'essere sistemi perfetti: possono bloccarsi, essere hackerati, comportarsi negativamente di proposito o persino comportarsi in modo pseudo-casuale. Quando colleghiamo diversi computer insieme in un network, l'incertezza del sistema finale cresce esponenzialmente. In una blockchain potrebbero esserci milioni di nodi che funzionano in modo indipendente e non è possibile

prevedere come si comporterà ciascuno di questi nodi.

> In una blockchain permissionless non è possibile fidarsi di nessuna entità coinvolta.

Se non è possibile fidarsi di alcuna entità, come è possibile che il network riesca a raggiungere un accordo su un singolo stato? Come fa un nodo a decidere di accettare o meno un blocco? Chi è incaricato di decidere cos'è giusto e cos'è sbagliato? Chi impone le regole? Chi decide se una transazione è valida[27]?

Consenso

> Nonostante l'incertezza, i nodi di una blockchain devono giungere a un accordo su un singolo stato.

Una blockchain è basata su regole (matematiche), ma non ha governanti. Il network ha il compito di raggiungere una decisione su cosa è avvenuto all'interno della blockchain, attraverso un processo chiamato **consenso**.

> Il consenso è un accordo generale tra i membri di un

dato gruppo (in questo caso i nodi della blockchain), ognuno dei quali ha una parte del potere decisionale.

In una blockchain il consenso è un accordo su ciò che è accaduto, e detiene l'unica possibile verità sullo stato attuale della blockchain.

Il consenso non va però inteso come un processo discreto dove in un istante non c'è consenso e l'istante dopo il consenso viene raggiunto, ma piuttosto come un processo continuo che coinvolge diversi partecipanti, ognuno con i propri ruoli e le proprie

responsabilità. Come vedremo in seguito, i due attori principali in questo processo sono i full-node e i **miner**.

Possiamo dire che il consenso di una blockchain sia il garante della fiducia che riponiamo in questo sistema (Figura 5.1).

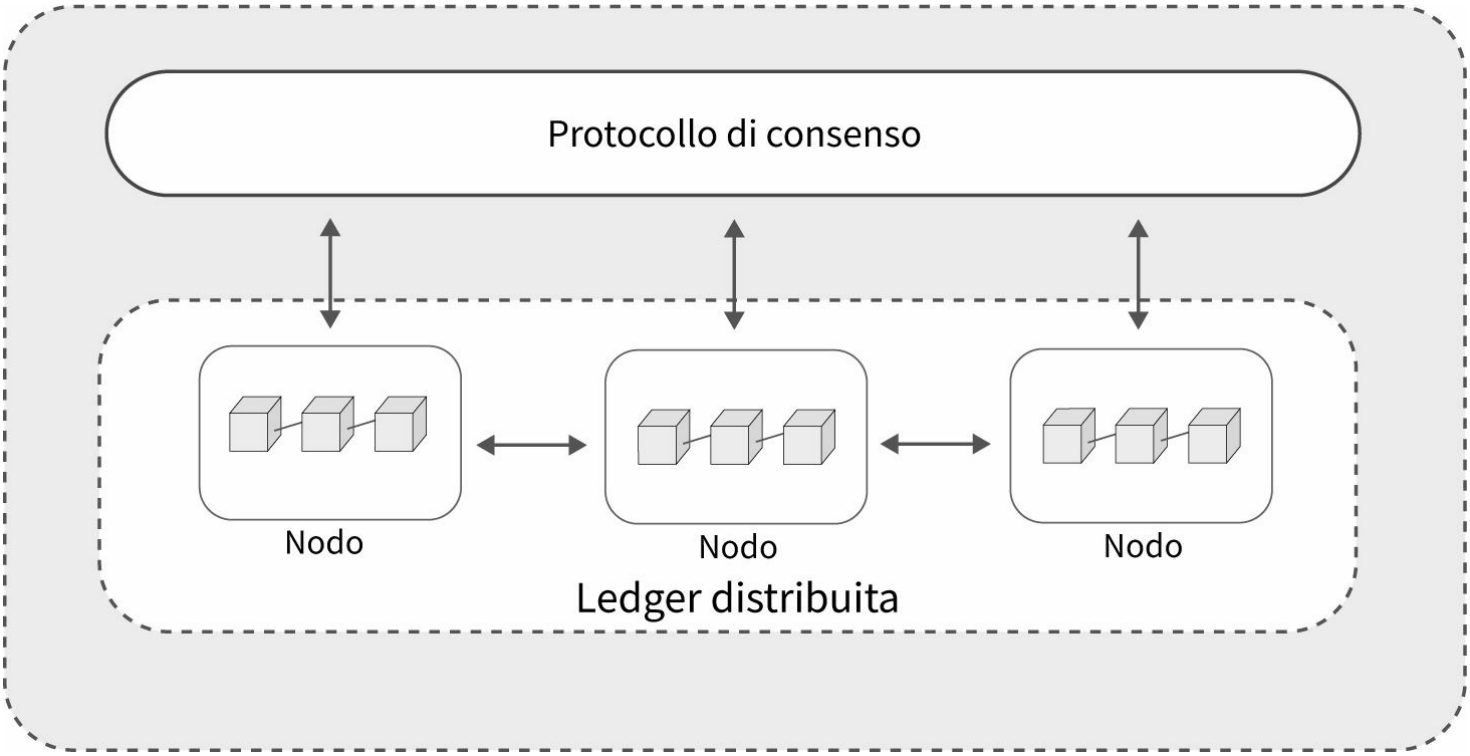


Figura 5.1 – Il protocollo di consenso in una blockchain.

Una blockchain utilizza matematica, economia e teoria dei giochi per incentivare tutti gli attori a raggiungere un accordo su un singolo stato. Tuttavia il raggiungimento del consenso in un sistema distribuito e decentralizzato rimane un problema molto complesso.

Questa situazione è spiegata chiaramente dal **problema dei generali bizantini.**

Il problema dei generali bizantini

Da Wikipedia: “Il problema dei generali bizantini è un problema ben noto nel calcolo distribuito. È un problema di accordo in cui un gruppo di generali, ciascuno al comando di una parte dell’esercito bizantino, circonda una città. Questi generali desiderano formulare un piano per attaccare la città. I generali devono decidere se attaccare o ritirarsi. Alcuni generali preferiscono attaccare, altri preferiscono ritirarsi. La

cosa importante è che tutti i generali alla fine concordino su una decisione comune, al fine di evitare una situazione in cui solo una parte dei generali attacca e l'altra si ritira. Il problema è complicato dalla presenza di generali traditori che possono non solo esprimere un voto per una strategia subottimale, ma possono farlo in modo selettivo. Per esempio, se nove generali votano, quattro dei quali sostengono l'attacco mentre altri quattro sono a favore della ritirata, il nono generale può comunicare ai generali favorevoli alla ritirata di ritirarsi e comunicare un voto di attacco ai restanti generali. Chi ha ricevuto il voto di ritiro dal nono generale si ritirerà, mentre il resto attaccherà. Il

problema è ulteriormente complicato dal fatto che i generali sono fisicamente separati e che devono inviare i loro voti tramite messaggeri che potrebbero non arrivare o falsificare i voti."

Questa situazione si adatta perfettamente allo scenario in cui opera una blockchain. I generali possono essere paragonati ai nodi, i traditori possono essere paragonati a nodi maligni, i messaggeri possono essere il canale di comunicazione tra i nodi.

La blockchain deve raggiungere un consenso distribuito anche in uno scenario come quello sopra descritto (deve essere "Byzantine fault tolerant").

Sono stati progettati diversi

algoritmi per risolvere questo problema. I due algoritmi più utilizzati nell'ambito delle blockchain sono il Proof of Work (PoW) e il Proof of Stake (PoS), ciascuno con le proprie varianti.

I nodi che partecipano attivamente al processo di consenso (aggiungono nuovi blocchi, garantiscono la validità delle transazioni) sono chiamati **miner** e svolgono un processo chiamato **mining**.

Mining

Il mining è un concetto generale e non è correlato ad alcuna blockchain in particolare (anche se molte persone

associano il mining solo al Bitcoin, il progetto che di fatto lo ha usato per primo).

Può essere visto come un processo che consente al network della blockchain di validare le transazioni, raggrupparle in blocchi e aggiungerle alla catena di blocchi. Queste operazioni permettono di raggiungere il consenso distribuito e di rendere il network sicuro.

> Il mining è il processo attraverso il quale le transazioni vengono validate, aggregate in blocchi e aggiunte alla blockchain.

I nodi che prendono parte al processo di mining sono chiamati miner.

Più in generale, il mining può essere visto come il meccanismo decentralizzato tramite il quale viene raggiunto il consenso distribuito e garantita la sicurezza del network.

Precedentemente abbiamo parlato di consenso come di un processo continuo nel quale miner e full node lavorano per aggiungere nuovi blocchi alla blockchain e verificare la validità di questi blocchi (e delle transazioni al suo

interno). Più nel dettaglio un miner è responsabile di:

- assieme ai nodi, verificare che le *transazioni* siano valide[28] e in caso positivo propagarle al resto della rete;
- assieme ai nodi, verificare che i nuovi *blocchi* siano validi e in caso positivo propagarli al resto della rete;
- scegliere le transazioni, ordinarle e aggregarle in un blocco.

Un full-node è responsabile di:

- verificare che le *transazioni*

siano valide e in caso positivo propagarle al resto della rete;

- verificare che i nuovi *blocchi* siano validi e in caso positivo propagarli al resto della rete.

Un full-node quindi contribuisce alla sicurezza della blockchain controllando la validità di ogni transazione e di ogni blocco, in modo da garantire che i miner non "imbroglino" (Figura 5.3).

È per questo motivo che precedentemente, quando avevamo introdotto la distinzione tra full-node e light-node, avevamo detto che un full-node è il modo più sicuro di utilizzare la blockchain. Un full-node non accetterà mai una transazione o un blocco che non

rispetta le regole.

Se un miner crea un blocco non valido, gli altri nodi lo rifiuteranno (Figura 5.4). Quando il blocco di un miner viene aggiunto alla blockchain, questo viene ricompensato per il lavoro svolto in base alle regole definite nella blockchain. Solitamente la ricompensa consiste nelle commissioni di transazione del blocco ed eventualmente, come nel caso del Bitcoin, delle criptovalute generate all'aggiunta di un nuovo blocco[29].

Manca però ancora un tassello importante per completare il discorso sul mining, ovvero gli algoritmi utilizzati nel processo di creazione di un blocco.

La transaction pool

Ogni blocco può contenere un numero limitato di transazioni, che varia a seconda delle regole definite nella blockchain presa in considerazione. Di solito un miner sceglie le transazioni con le commissioni più alte al fine di massimizzare il suo potenziale profitto (questo è il motivo per cui le transazioni con commissioni più alte richiedono solitamente meno tempo per essere confermate).

Le transazioni (abbreviate TX) una volta validate sono inserite in una **transaction pool** (letteralmente, vasca di transazioni), in attesa di essere aggiunte a un blocco (Figura 5.2).

Un miner sceglie le transazioni e le raggruppa in un blocco, chiamato **blocco candidato**. Una volta creato un nuovo blocco, viene trasmesso alla rete di nodi che ne controllano la validità.

Tutti verificano il lavoro di tutti.

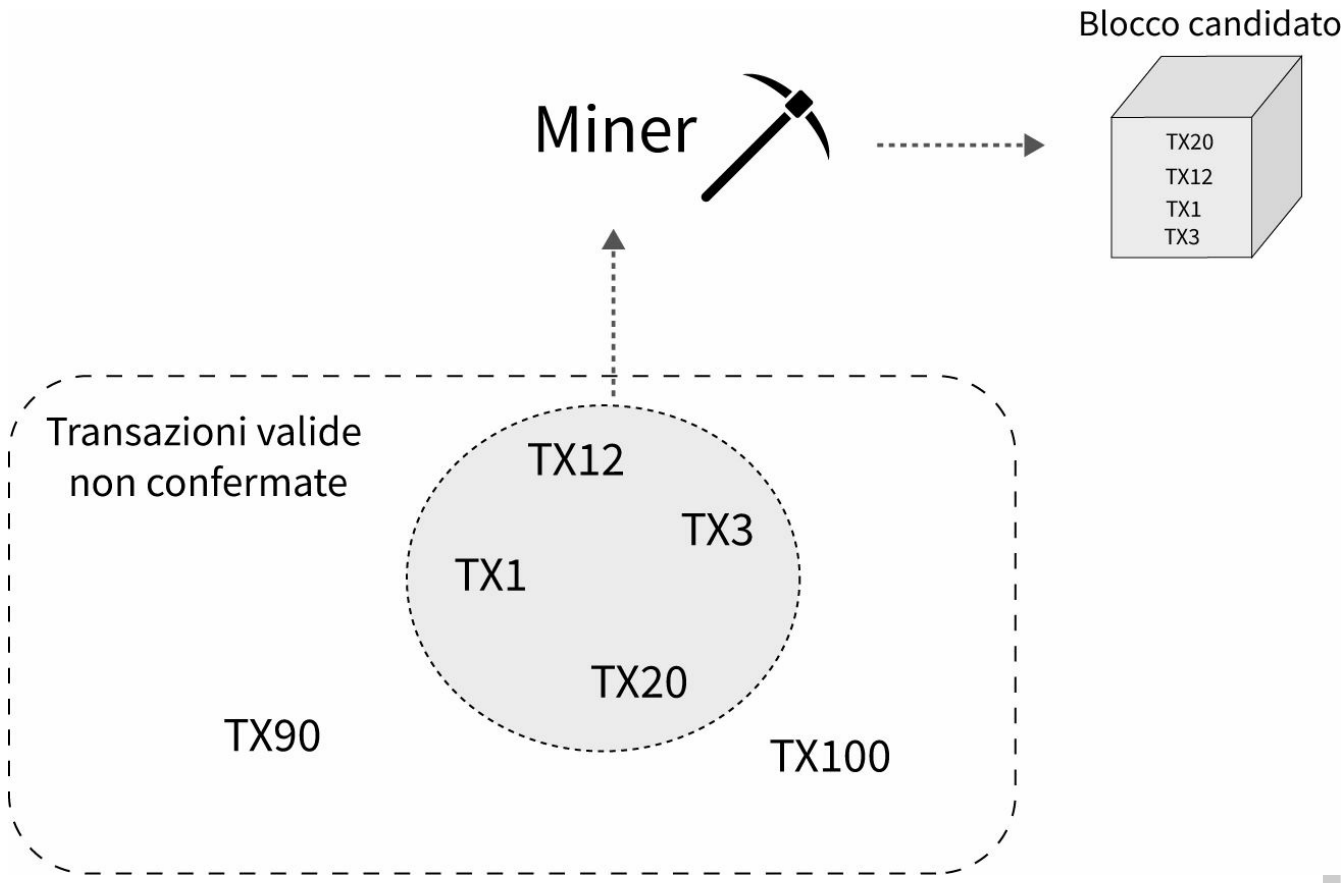


Figura 5.2 – Le transazioni scelte da un miner.

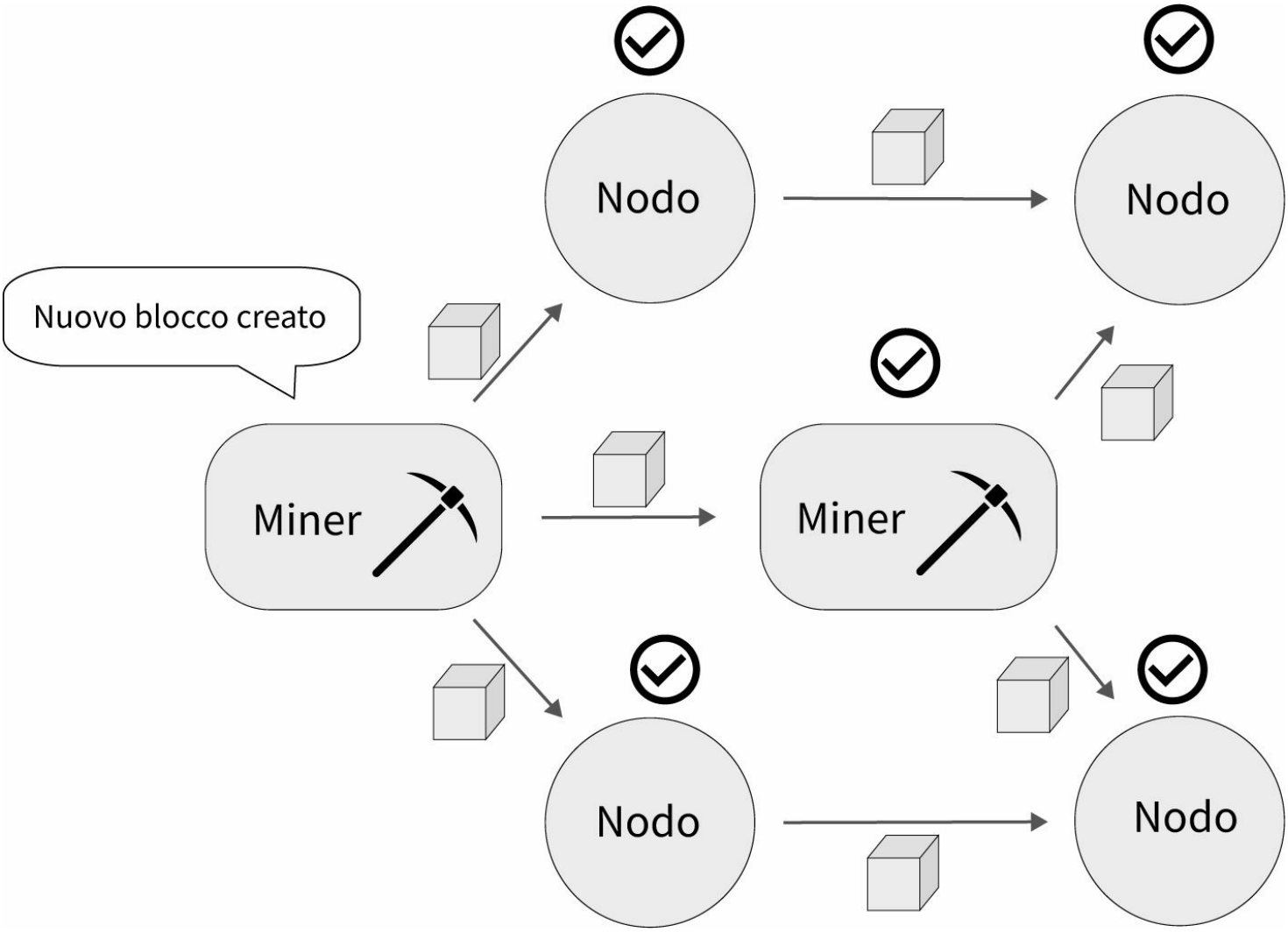


Figura 5.3 – Il processo di validazione di un blocco da parte del network.

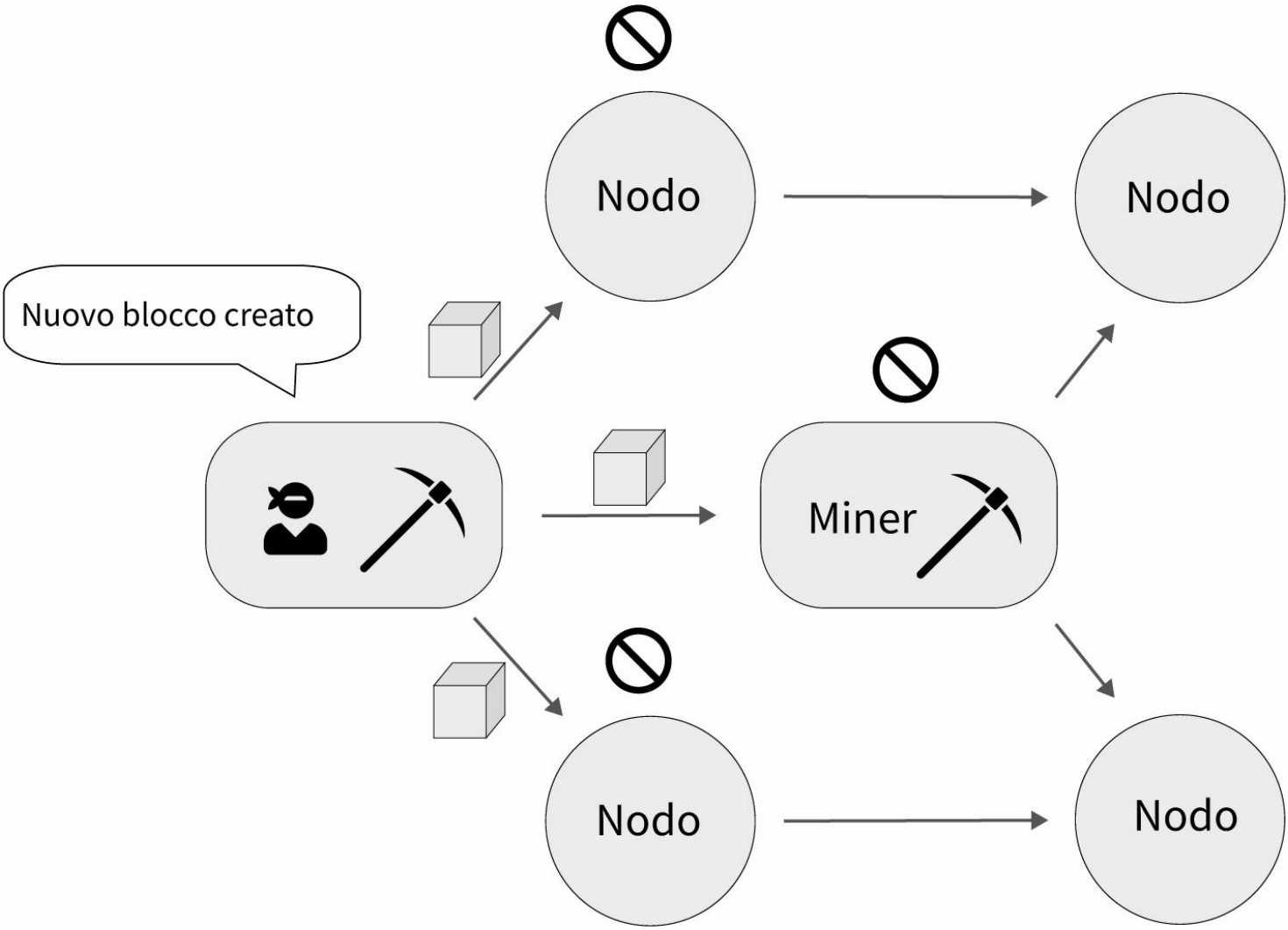


Figura 5.4 – L'interruzione della propagazione di un blocco non valido.

Proof of Work (PoW)

Il Proof of Work (letteralmente "prova del lavoro") è un protocollo utilizzato

nel processo per raggiungere il consenso distribuito. Concretamente, il Proof of Work si basa sulla ricerca di un numero computazionalmente difficile da trovare, ma una volta trovato diventa facile per tutti gli altri nodi verificarne la correttezza. In un sistema che utilizza il PoW, un blocco è valido solo se contiene una soluzione valida al PoW[30].

L'hash nel PoW

Il valore da trovare nel PoW sembra avere tutte le caratteristiche di un hash, e infatti il PoW si basa sugli algoritmi di hash. Facciamo un breve recap delle

caratteristiche di una funzione di hash prima di addentrarci nel meccanismo del PoW.

Una funzione di hash prende come input un valore di lunghezza arbitraria e lo trasforma in un output di lunghezza definita.

È inoltre una funzione non invertibile, ovvero dato un hash, l'unico modo per conoscere l'input che ha generato quell'hash è provare tutti i possibili input (brute-force).

Proof of Work è un protocollo utilizzato per raggiungere il consenso distribuito nel quale il potere di voto si basa sulla potenza computazionale.

PoW mining

Nel PoW-mining, i nodi del network competono per risolvere un problema matematico complesso (un hash inverso con alcuni vincoli). Risolvere questo problema è un processo casuale con probabilità molto bassa e l'unico modo per trovare una PoW valida è provare tutte le possibili combinazioni finché non si trova quella giusta.

Il primo miner che risolve il problema ha il diritto di creare il blocco successivo e guadagnare la ricompensa. Una volta creato un nuovo blocco, viene trasmesso alla rete, in attesa che gli altri nodi ne verifichino la validità. È molto facile per i restanti nodi verificare se la

soluzione sia corretta. Se il blocco è valido viene inoltrato ai nodi vicini, altrimenti viene ignorato.

Il mining, in un sistema basato su PoW, può essere riassunto nei seguenti punti:

1. Le transazioni vengono create e trasmesse a tutta la rete di nodi.

2. Ogni miner sceglie le transazioni che vuole (solitamente quelle con le commissioni maggiori) e le raccoglie in un blocco chiamato blocco candidato, in quanto non è ancora valido, non avendo una soluzione valida al PoW.

3. Ogni miner inizia a eseguire i calcoli per trovare la risoluzione del problema matematico e generare una valida PoW per il blocco da lui assemblato. A ogni soluzione non valida il miner cambia il valore di un numero, chiamato **nonce**, che viene aggiunto all'input del PoW per cambiare il valore finale della soluzione.

4. Quando un miner genera una PoW valida per il nuovo blocco, trasmette il blocco alla rete.

5. Tutti i nodi nella rete verificano se il nuovo blocco è valido o

meno.

6. Se il blocco è ritenuto valido, il miner si aggiudica il blocco (e le commissioni delle transazioni in esso contenute). Il nuovo blocco viene inoltrato alla rete di nodi e aggiunto alla blockchain.

Hashrate

Nel PoW, quando parliamo di potenza di calcolo, ci riferiamo all'**hashrate**, poiché solitamente il problema da risolvere è un hash inverso con alcuni vincoli.

L’hashrate è il numero di hash calcolati al secondo (H/s).

L’hashrate totale, o hashrate della rete, è la somma di tutti gli hashrate dei miner. La probabilità di un miner di trovare per primo una PoW valida è la seguente:

Probabilità di essere il primo miner a risolvere la PoW = hashrate del miner / hashrate del network.

L’hashrate dipende dallo specifico algoritmo di hash usato dalla blockchain e dalla potenza della macchina utilizzata dal miner. Considerando il Bitcoin, per

esempio, una persona ha un hashrate di circa 0,00003 H/s[31], il che significa che calcolare un singolo hash a mano richiederebbe circa 9-10 ore. Un miner ASIC (Application Specific Integrated Circuit, una macchina progettata esclusivamente per il mining) può calcolare più di 14TH/s (Tera Hash, un trilione di hash al secondo). Nel 2018, l'hashrate del network della blockchain del Bitcoin è pari a più di 50 milioni di TH/s[32].

Nonce

Nonce è un valore che serve per variare l'input della funzione di hash utilizzata nel calcolo della PoW. Questo valore

viene modificato fino a quando l'hash risultante non soddisfi uno specifico valore chiamato **difficoltà**.

Tabella 5.1 – I calcoli per arrivare alla soluzione al PoW.

Input (tx = transazione)	**Nonce**	**Output**	**Valido?**
tx1 + tx2 + tx3 + … + txn	1	hash-1	No
tx1 + tx2 + tx3 + … + txn	2	hash-2	No
…	…	…	No
tx1 + tx2 + tx3 + … + txn	1253	hash-1253	Sì

Difficoltà

Una PoW per essere considerata valida deve soddisfare un vincolo chiamato *difficoltà*.

> La difficoltà è un valore che esprime quanto sia difficile trovare una PoW valida.

In pratica, si può settare il target della difficoltà imponendo che l'hash da trovare inizi (per esempio) con 5 zeri. Cioè significa che i primi 5 valori dell'hash dovranno essere tutti 0 per soddisfare il target di difficoltà. In generale, più aumentiamo il numero di zeri più aumenta la difficoltà.

Uno dei controlli che fanno i nodi

quando ricevono un nuovo blocco è controllare che la difficoltà della PoW di quel blocco rispetti i vincoli sulla difficoltà. Nel caso del Bitcoin, un blocco generato a ottobre 2018 aveva il seguente hash: 00000000000000000028daaa4c3f398a Come potete vedere, inizia con 19 zeri.

La difficoltà viene aggiornata periodicamente (retargeting) in relazione all'hashrate del network per mantenere il tempo necessario per la generazione di un blocco il più costante possibile. Per esempio, nel Bitcoin la difficoltà viene regolata ogni 2.016 blocchi (pari a circa 14 giorni) basandosi sul tempo medio che è stato necessario per trovare i 2.016 blocchi precedenti.

Ricompensa

Per incentivare i miner a generare nuovi blocchi e mantenere il network sicuro, sono previste delle ricompense. I miner che creano un nuovo blocco sono ricompensati con tutte le commissioni delle transazioni incluse nel blocco, più eventualmente le nuove monete (criptovalute) create insieme al blocco (block-reward).

In questo momento, per esempio, nel Bitcoin, per ogni nuovo blocco, vengono creati 12,5 bitcoin, i quali vengono assegnati al miner che crea il nuovo blocco. Di solito il numero di nuove monete create con ogni blocco

diminuisce nel tempo, poiché la maggior parte delle criptovalute ha un limite nel numero massimo di monete esistenti (nel Bitcoin questo limite corrisponde a 21 milioni di bitcoin).

NOTA Il protocollo PoW è equo nei confronti dei miner: un miner che possiede il 5% della potenza di calcolo totale del network in media "vince" la PoW e ottiene il diritto di creare un nuovo blocco (e guadagnare la ricompensa) il 5% delle volte.

PoW: pro e contro

Il vantaggio principale del Proof of

Work è la forte garanzia di immutabilità. È davvero difficile, se non impossibile, modificare una transazione dopo che questa ha ricevuto un numero sufficiente di conferme. Ricordiamo che le conferme corrispondono al numero di blocchi aggiunti alla blockchain partendo dal blocco nel quale la transazione è inserita.

Perciò modificare una transazione, o le informazioni in essa contenute, diventa progressivamente più difficile mano a mano che nuovi blocchi vengono generati (Figura 5.5).

Se un utente maligno tentasse di manomettere una transazione nel blocco 103, l'attacco potrebbe avere successo in un solo modo, cioè ricalcolando la

Proof of Work per tutti i blocchi seguenti (103-110) prima che gli altri miner riescano a minare il blocco 110 (Figura 5.6).

L'utente maligno per fare ciò deve quindi essere in possesso di un'incredibile potenza di calcolo, e il tutto solo per manomettere una transazione avvenuta 8 blocchi prima (circa 1 ora e 20 minuti prima nel caso del Bitcoin).

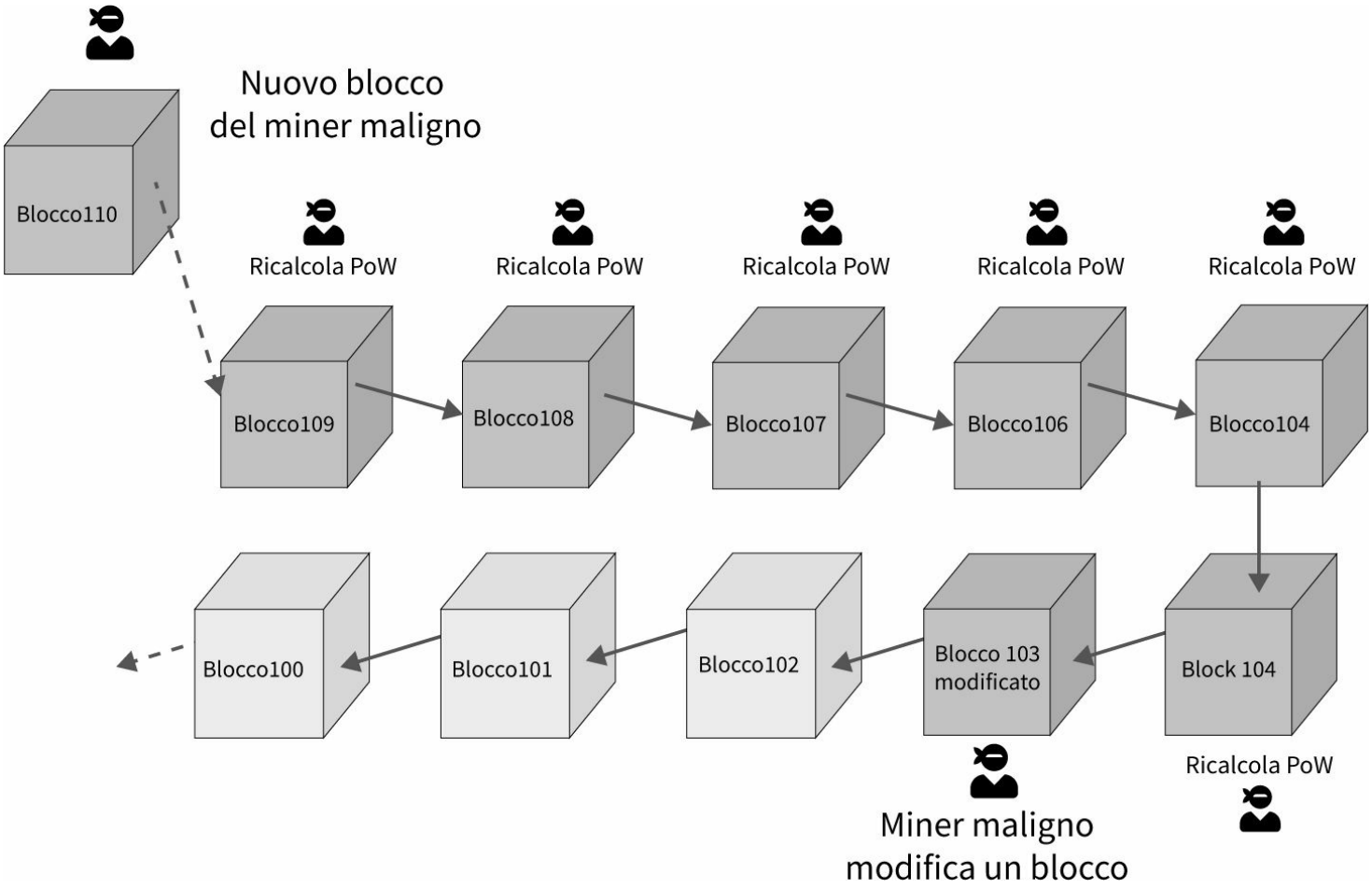


Figura 5.5 – La potenza di calcolo necessaria per modificare un blocco precedente.

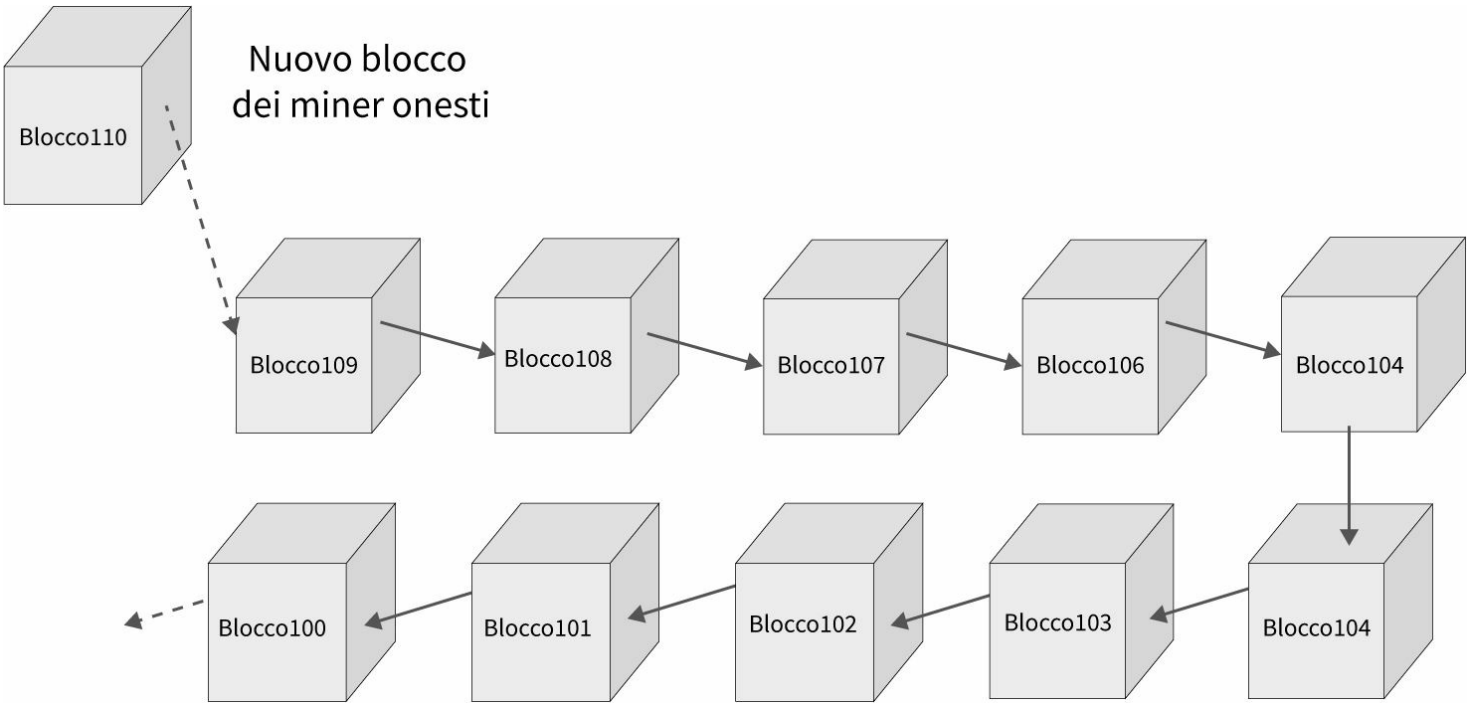


Figura 5.6 – Il processo di mining su una catena corretta durante un attacco.

Grazie alla funzione hash, la modifica di un blocco implica il ricalcolo dell'intera PoW per tutti i blocchi che seguono il blocco manomesso.

Più si torna indietro nel tempo, meno è

probabile che un attacco abbia successo. Questo è il motivo per cui si consiglia di attendere più di una conferma (6 conferme nel Bitcoin) per poter assumere con sufficiente sicurezza l'immutabilità di una transazione.

Una parte della comunità, tuttavia, non pensa che il PoW sia il metodo migliore da utilizzare nel processo per raggiungere il consenso e ha sollevato diverse problematiche riguardanti il PoW. Le principali sono:

- **Massiccio consumo di energia**. Bitcoin, il più grande progetto che utilizza il PoW, consuma attualmente circa lo 0,3% dell'elettricità mondiale (oltre 1

milione di dollari al giorno tra elettricità e hardware per il mining[33]) e molti ritengono che questa situazione non sia sostenibile nel lungo periodo. Tuttavia l'enorme consumo di energia è la ragione per cui un processo di consenso basato sul Proof of Work sia difficile da attaccare. È l'enorme quantità di potenza di calcolo necessaria per validare la blockchain che ne garantisce l'immutabilità. La potenza di calcolo e l'elettricità utilizzata sono la prova effettiva del lavoro eseguito.

- **Difficile da scalare.** Il PoW è

uno dei colli di bottiglia nella possibilità di scalare il sistema. Molti sostengono che la lentezza delle transazioni e le commissioni elevate stiano bloccando l'adozione su grande scala della blockchain.

È però possibile rendere scalabile questo tipo di blockchain senza modificare l'algoritmo di consenso, adottando soluzioni off-chain (nel caso del Bitcoin o simili, si parla di Lightning Network) o modificando la dimensione del blocco (per esempio Bitcoin Cash, che approfondiremo in

seguito).

- **È vulnerabile a un attacco del 51%**. Se un miner raggiungesse il 51% della potenza di calcolo totale del network, sarebbe (teoricamente) in grado di creare blocchi più velocemente di tutti i restanti miner insieme. Potrebbe quindi succedere che il miner in questione sia in grado di invertire o modificare alcune delle proprie transazioni (double spending) o di bloccare la conferma di nuove transazioni (censura di transazioni[34]).

  Tuttavia, se un miner riuscisse con successo a eseguire un

attacco del 51%, non sarebbe comunque in grado di modificare le vecchie transazioni, poiché dovrebbe ricalcolare la PoW di tutti i blocchi successivi mentre gli altri miner onesti continuano a minare sulla blockchain corretta. Un attacco di questo tipo richiederebbe l'utilizzo di una quantità incredibile di risorse per l'attacker. Se qualcuno effettivamente riuscisse a mettere insieme più del 51% della potenza di calcolo, sarebbe molto più redditizio per lui seguire le regole della blockchain (un concetto che esploreremo quando parleremo

di cripto-economia).

C'è da sottolineare però che questo discorso vale per blockchain con un hashrate totale elevato come può essere il Bitcoin. Un attacco del 51% su blockchain minori è realizzabile, ed è già stato effettuato diverse volte [8].

- **Discriminazione geografica, economie di scala e centralizzazione**. Al momento, la maggior parte dei miner (soprattutto nel caso del Bitcoin) sono concentrati in luoghi dove il costo dell'elettricità e le temperature sono bassi (per

risparmiare su elettricità e impianti di raffreddamento). Inoltre, le economie di scala vengono utilizzate per negoziare prezzi più convenienti sia per l'elettricità che per le macchine necessarie per il mining. Tutto ciò spesso si traduce in una centralizzazione del processo di mining, portando i miner a concentrarsi in poche aree geografiche oppure a unirsi condividendo la potenza di calcolo.

Proof of Stake (PoS)

Il Proof of Stake è un altro protocollo utilizzato nel processo per raggiungere il consenso distribuito. Lo scopo del Proof of Stake è lo stesso del PoW, ma il processo per raggiungere l'obiettivo finale è diverso. A differenza del Proof of Work, nel quale vengono premiati i miner che risolvono problemi matematici, nel Proof of Stake vengono alternati dei validatori (validator, possono essere considerati l'equivalente dei miner nel PoW) scelti in anticipo basandosi sulla quantità di criptovalute in loro possesso per la relativa blockchain, definita anche come **stake**.

Proof of Stake è un protocollo

utilizzato per raggiungere il consenso distribuito nel quale a ogni token corrisponde un voto.

PoS mining (staking)

Nel PoS-mining, al posto della potenza di calcolo posseduta, vengono utilizzati i token posseduti. Gli utenti in possesso di token possono "puntare" (**staking**) i propri token (tecnicamente, puntare significa bloccare temporaneamente i token fino a quando il processo di staking si conclude) per avere in cambio il diritto di confermare le transazioni di un blocco (diventare un validatore) e

ricevere una ricompensa.

Il creatore di un nuovo blocco viene quindi scelto in anticipo utilizzando una combinazione di diversi parametri, a seconda del tipo di algoritmo utilizzato. Alcuni parametri possono essere il numero di token (stake), o il tempo in cui il validatore è stato in possesso di quei token.

Come il PoW, anche il protocollo PoS è equo nei confronti dei validatori: un validatore che possiede il 5% dell'ammontare totale dei token, in media ottiene il diritto a creare un nuovo

blocco (e guadagnare la ricompensa) il 5% delle volte.

Per fare un esempio, consideriamo 3 validatori: Alice con 50 ETH, Marco con 30 ETH e Luca con 20 ETH (utilizziamo gli ETH perché, come vedremo successivamente, Ethereum sta pianificando il passaggio al protocollo PoS). Lo stake totale del network è quindi 100 ETH. Utilizzando un protocollo PoS che considera solo la quantità di criptovalute possedute, Alice verrà scelta in media il 50% delle volte, Marco il 30% e Luca il 20% (Figura 5.7).

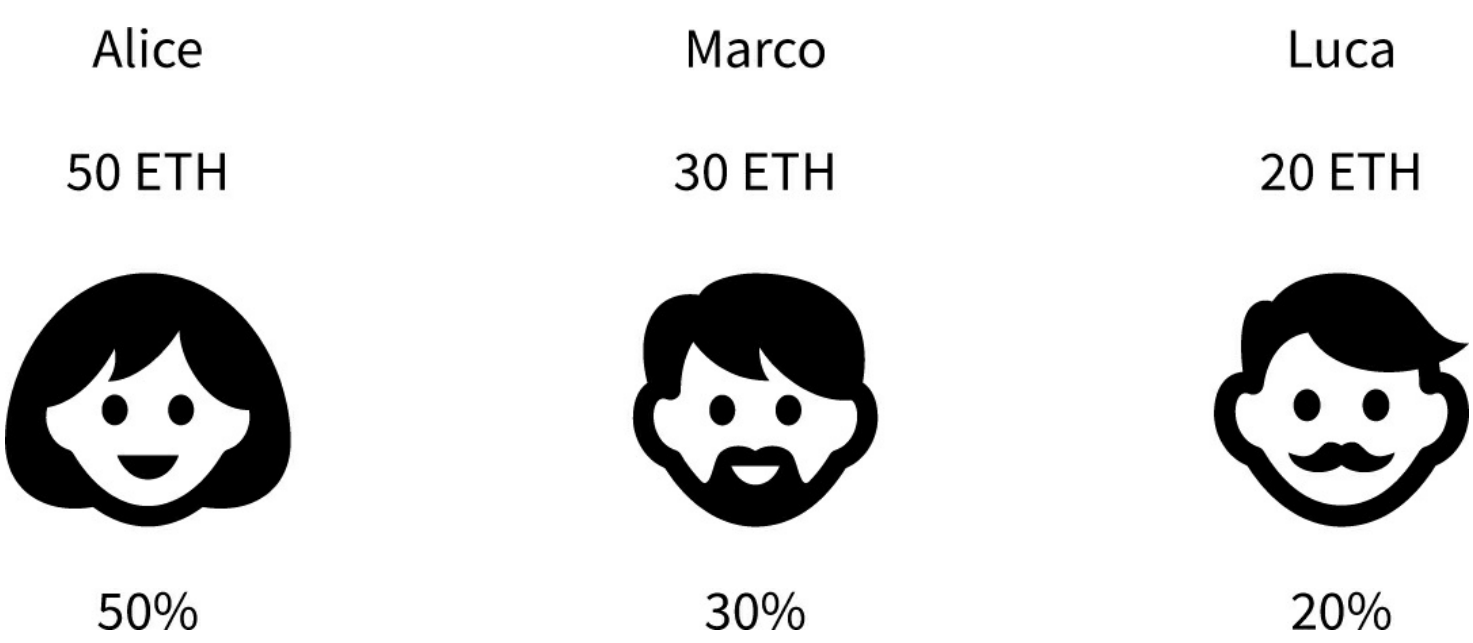


Figura 5.7 – La scelta dei validatori nel PoS.

Si può quindi affermare che:

> potere di voto = stake del validatore / stake totale del network.

Rispetto al PoW, il Proof of Stake è più efficiente, in quanto non è necessario eseguire calcoli complessi per ogni

nuovo blocco.

I sostenitori del PoS affermano che rispetto al PoW, PoS ha i seguenti vantaggi:

- **Gli attacchi sono più costosi**. Anche il PoS è teoricamente vulnerabile a un attacco del 51%. Un attaccante, in questo caso, non avrà bisogno del 51% dell'hashrate totale ma del 51% dei token totali.

  Tuttavia, se un attaccante cercasse di acquistare il 51% dei token, il mercato reagirebbe con un rapido aumento del prezzo del token. Inoltre le persone con molti token sono

meno incentivate ad attaccare la blockchain, dal momento che un attacco avrebbe la controproducente conseguenza di distruggere la fiducia in quella blockchain, e di conseguenza il valore di quel token.

- **Più economico.** Non essendoci costi di elettricità e di hardware per il mining, tutte le persone possono permettersi di partecipare al network, riducendo l'attuale centralizzazione dei sistemi basati sul PoW.
- **Punizioni.** È possibile creare dei disincentivi economici per gli

attori malevoli, per esempio distruggendo il loro stake.

- **Lealtà**. I miner sono incoraggiati a rimanere sulla stessa blockchain. Se volessero partecipare al PoS su un'altra blockchain, dovrebbero obbligatoriamente cambiare i token in loro possesso. Nel PoW, invece, se la moneta che si sta minando non è più redditizia, si può semplicemente cambiare blockchain.

PoW vs PoS

PoW e PoS sono due differenti metodi

per raggiungere lo stesso scopo: il consenso distribuito. Per ricapitolare le differenze, vedi Tabella 5.2.

Tabella 5.2 – Le differenze tra Proof of Work e Proof of Stake.

	PoW	**PoS**
Cosa serve	Potenza di calcolo	Stake (criptovalute + altri parametri)
Chi crea un nuovo blocco	Miner, scelto in maniera casuale in base alla sua potenza di calcolo	Validatore, scelto in anticipo in base allo stake
Equo	Sì	Sì
Tempo per generare un blocco	Variabile, dipende dal tempo necessario a risolvere il PoW	Fissato
	Variabile, dipende	

Tempo per generare	dal tempo necessario a risolvere il PoW	Fissato
Potenza di calcolo richiesta	Molto elevata	Minima
Ricompensa al miner	Commissioni di transazione + eventualmente criptovalute generate assieme al nuovo blocco	Commissioni di transazione + eventualmente criptovalute generate assieme al nuovo blocco

Fork

Spesso nell'ambito delle blockchain si sente parlare di **fork** ma non è sempre chiaro cosa sia una fork e cosa effettivamente comporti. Sebbene il

termine venga spesso utilizzato per indicare la divisione di una blockchain (**chain-split**), in realtà esso racchiude un insieme di diversi possibili scenari.

Una fork è una situazione in cui accade una delle seguenti cose:

- Nodi diversi hanno opinioni **temporaneamente** diverse sulla cronologia delle transazioni, ma rimangono invariate le regole della blockchain (**fork regolare**). In questo caso c'è una temporanea divisione della blockchain (il consenso sulla cronologia delle transazioni è perso temporaneamente).
- Le regole della blockchain sono

cambiate in maniera **retrocompatibile** e tutti i nodi condividono la stessa cronologia delle transazioni (**soft fork**). Non c'è una divisione della blockchain.

- Le regole della blockchain sono cambiate in maniera **non retrocompatibile** ma tutti i nodi si aggiornano alle nuove regole e condividono la stessa cronologia delle transazioni (**hard fork**). Non c'è una divisione della blockchain.
- Le regole della blockchain sono cambiate in maniera **non retrocompatibile** e nodi diversi

hanno opinioni diverse sulle regole della blockchain, non condividendo la stessa cronologia delle transazioni (**hard fork con chain split**). C'è una divisione della blockchain (il consenso sulla cronologia delle transazioni è perso definitivamente).

Una **fork regolare** non cambia le regole del consenso. Soft fork e hard fork implicano al contrario una modifica di queste regole (Figura 5.8).

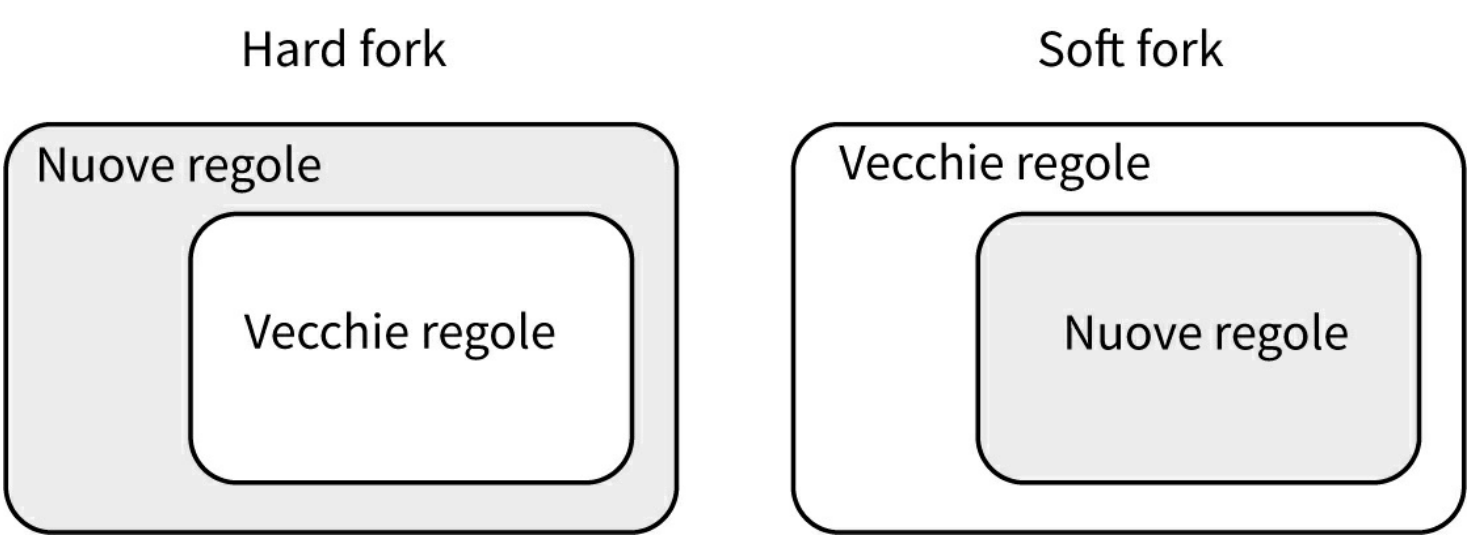


Figura 5.8 – Differenza tra hard fork e soft fork.

Se le nuove regole sono meno rigide (non retrocompatibili) si ottiene una hard fork. Se le regole diventano più rigide (compatibili con le versioni precedenti) si ottiene una soft fork (Figura 5.9).

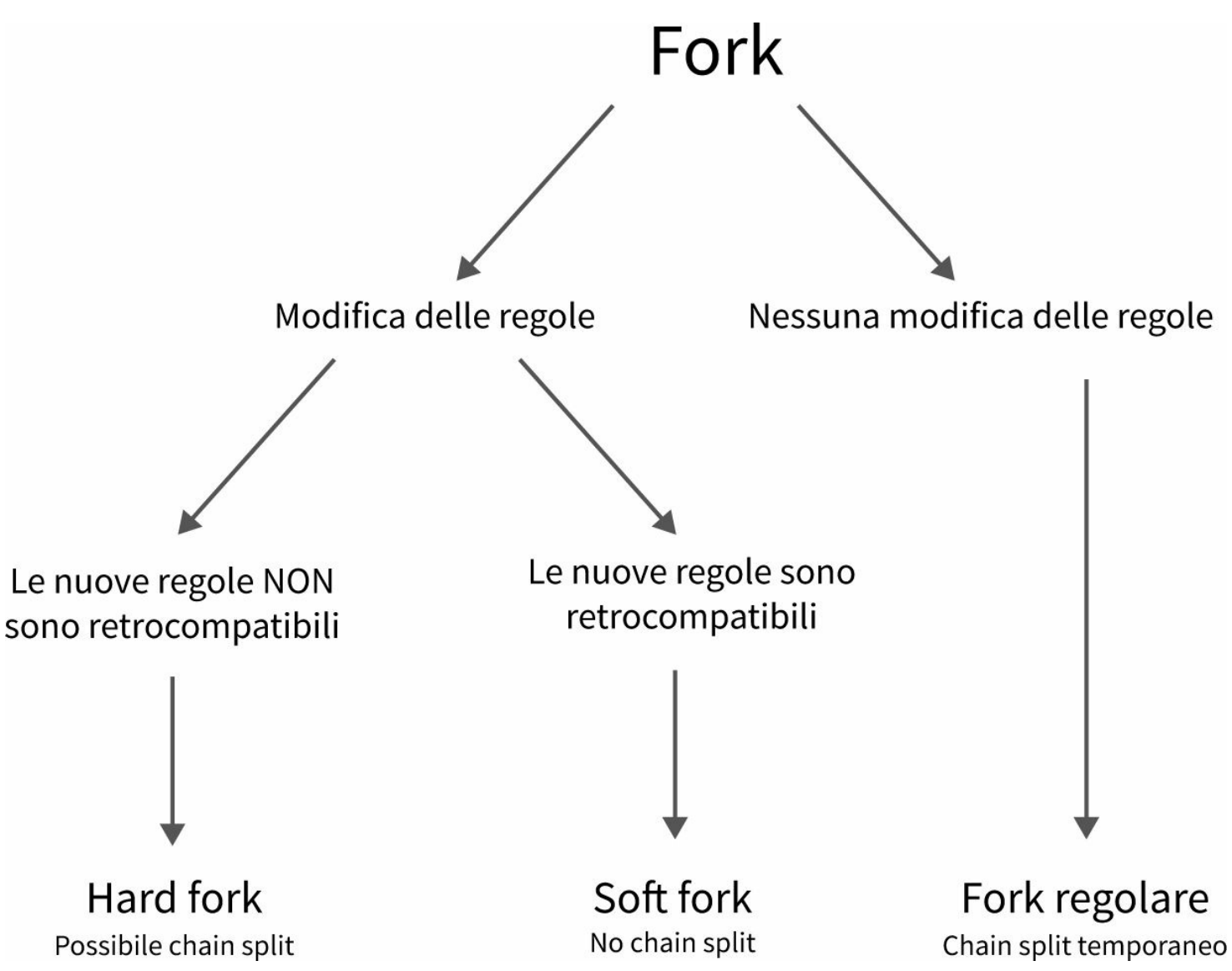


Figura 5.9 – Le diverse tipologie di fork.

Per citare Andreas Antonopoulos: "Se gestisci un ristorante vegetariano e lo trasformi in un ristorante vegano, allora è una soft fork. Se al contrario inizi a cucinare anche la carne, è una hard fork"

[9].

Fork regolare

Una fork regolare è una divergenza temporanea nello stato di una blockchain che si verifica quando due o più miner creano un blocco (quasi) nello stesso momento.

Il tempo di propagazione e le latenze di network fanno sì che non tutti i nodi ricevano lo stesso nuovo blocco. Di conseguenza la blockchain si divide temporaneamente in due diverse catene, in quanto nodi diversi hanno una diversa cronologia delle transazioni.

In pratica, durante una fork regolare,

la blockchain diverge temporaneamente in due catene separate e ogni catena è considerata valida da alcuni nodi.

Se due miner, il miner A che si trova negli Stati Uniti e il miner B che si trova in Cina, creano un nuovo blocco in una finestra temporale abbastanza breve da non consentire la propagazione del nuovo blocco a tutti i nodi della rete, si verifica una fork regolare. Tutti i miner vicini ad A penseranno che A abbia trovato il nuovo blocco e aggiungeranno questo blocco alla loro blockchain, mentre i miner vicini a B penseranno lo stesso di B (Figura 5.10).

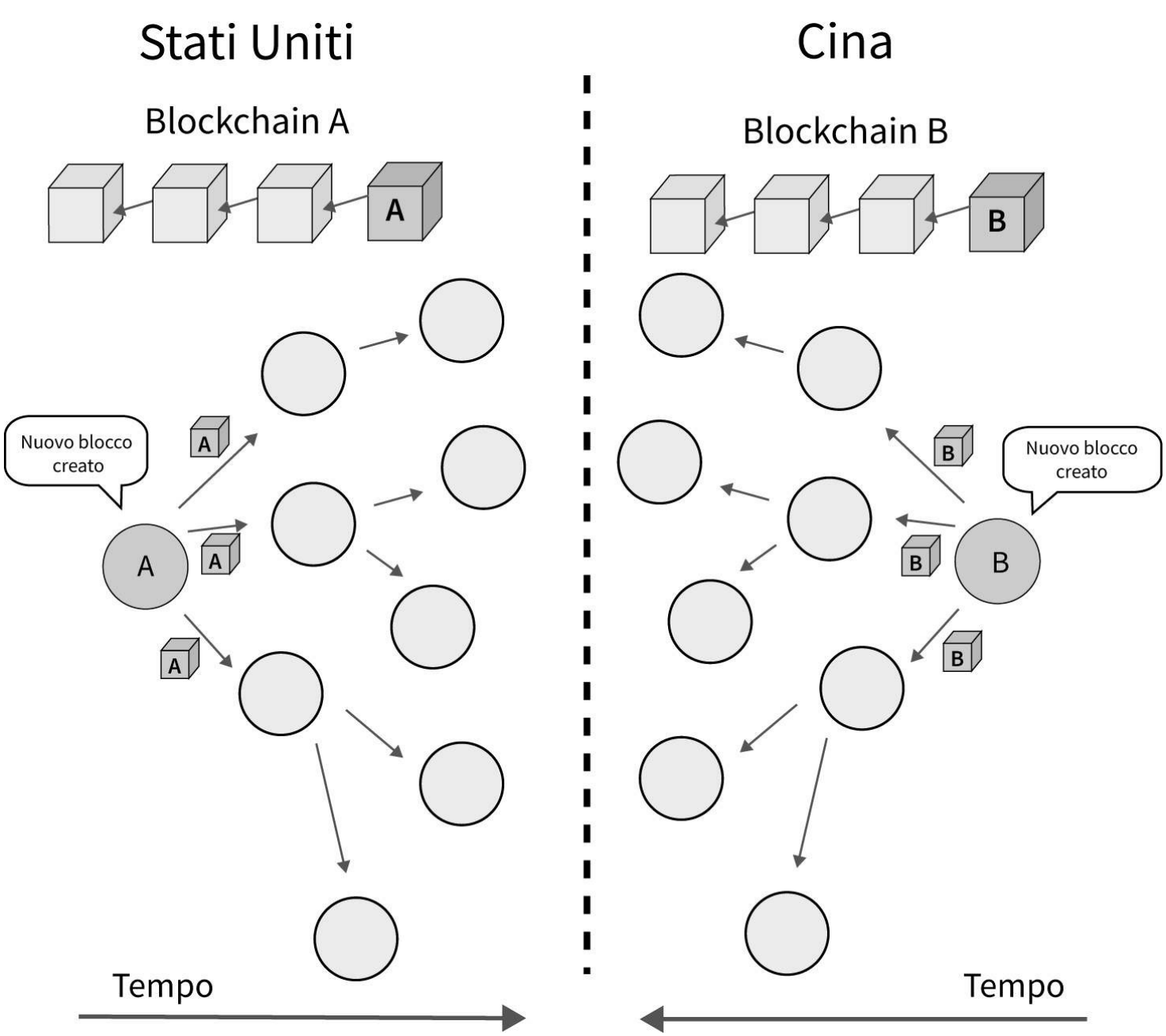


Figura 5.10 – La creazione di una fork regolare.

Poiché non esiste un'autorità centrale per risolvere l'ambiguità, la catena rimane divisa finché non viene trovato il

blocco successivo e quindi una delle due catene diventa più lunga. In caso di conflitto, infatti, i nodi seguono sempre la catena più lunga.

Nel momento in cui una delle blockchain crea il blocco successivo prima dell'altra, tutti i nodi si uniscono alla catena più lunga (Figura 5.11).

Per fare un esempio, in T4 la blockchain viene divisa a causa di una fork regolare. In T5, i miner che riconoscono come valida la blockchain **A**, trovano un nuovo blocco e la blockchain **A** diventa così la catena più lunga. I nodi che hanno riconosciuto come valido il blocco **B** si rendono conto che stanno minando sulla

blockchain sbagliata (quella più corta) e si uniscono alla blockchain **A** (questo è un altro motivo per cui è solitamente meglio attendere più di una conferma per una transazione). Le transazioni che erano state inserite nel blocco **B** vengono messe di nuovo nella transaction pool in attesa di essere riconfermate sulla blockchain **A**.

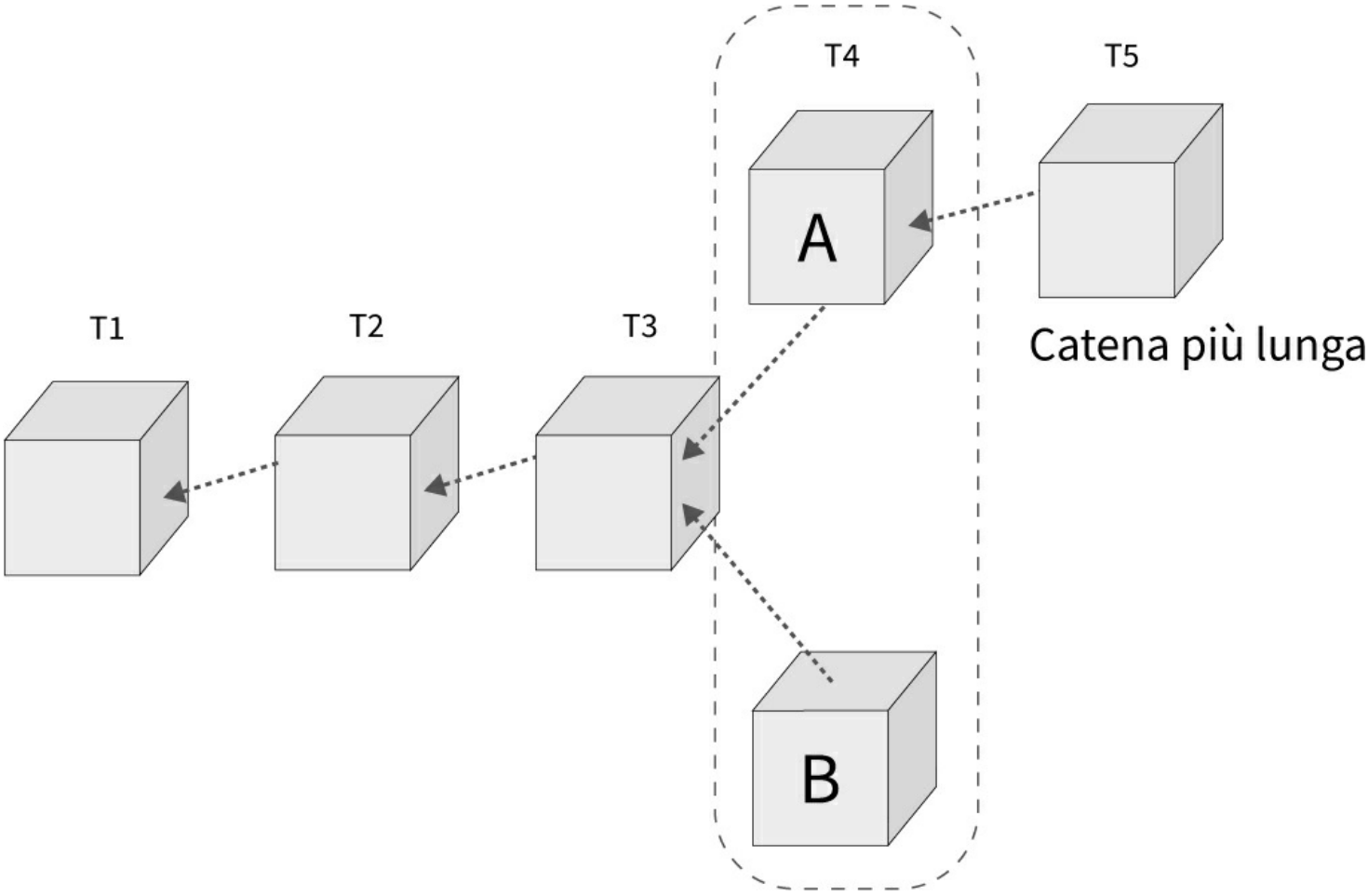


Figura 5.11 – La risoluzione di una fork regolare.

Soft fork

Una soft fork è un cambiamento nelle regole del consenso di una blockchain dove le vecchie regole rimangono però

valide. Non è obbligatorio per tutti i nodi conformarsi alle nuove regole per poter interagire con la blockchain. I blocchi creati con le nuove regole sono riconosciuti come validi sia dai nodi che seguono le nuove regole sia da quelli che seguono le vecchie regole.

> Una soft fork è una modifica delle regole compatibile con le regole precedenti. I nodi che seguono le vecchie regole accettano i blocchi creati dai nodi che seguono quelle nuove e viceversa.
>
> Le nuove regole sono un sottoinsieme delle vecchie

regole.

Una soft fork, per esempio, potrebbe ridurre la dimensione di un blocco da 2 MB a 1 MB. Le soft fork sono in genere un'ottimizzazione del protocollo esistente.

Hard fork

Un hard fork è una modifica delle regole di consenso non retrocompatibile, rendendo validi blocchi precedentemente non validi.

Dopo un hard fork, sulla rete inizieranno a comparire blocchi che in precedenza erano considerati invalidi e i nodi che non si aggiornano non saranno in grado di riconoscere i nuovi blocchi come validi.

Se tutti i nodi si aggiornano alle nuove regole di consenso, non vi è alcuna divisione della blockchain; in caso contrario, se alcuni nodi decidessero di non aggiornarsi, ciò causerà una divergenza nello stato della blockchain, cioè una divisione in due blockchain separate (**chain split**) (Figura 5.12).

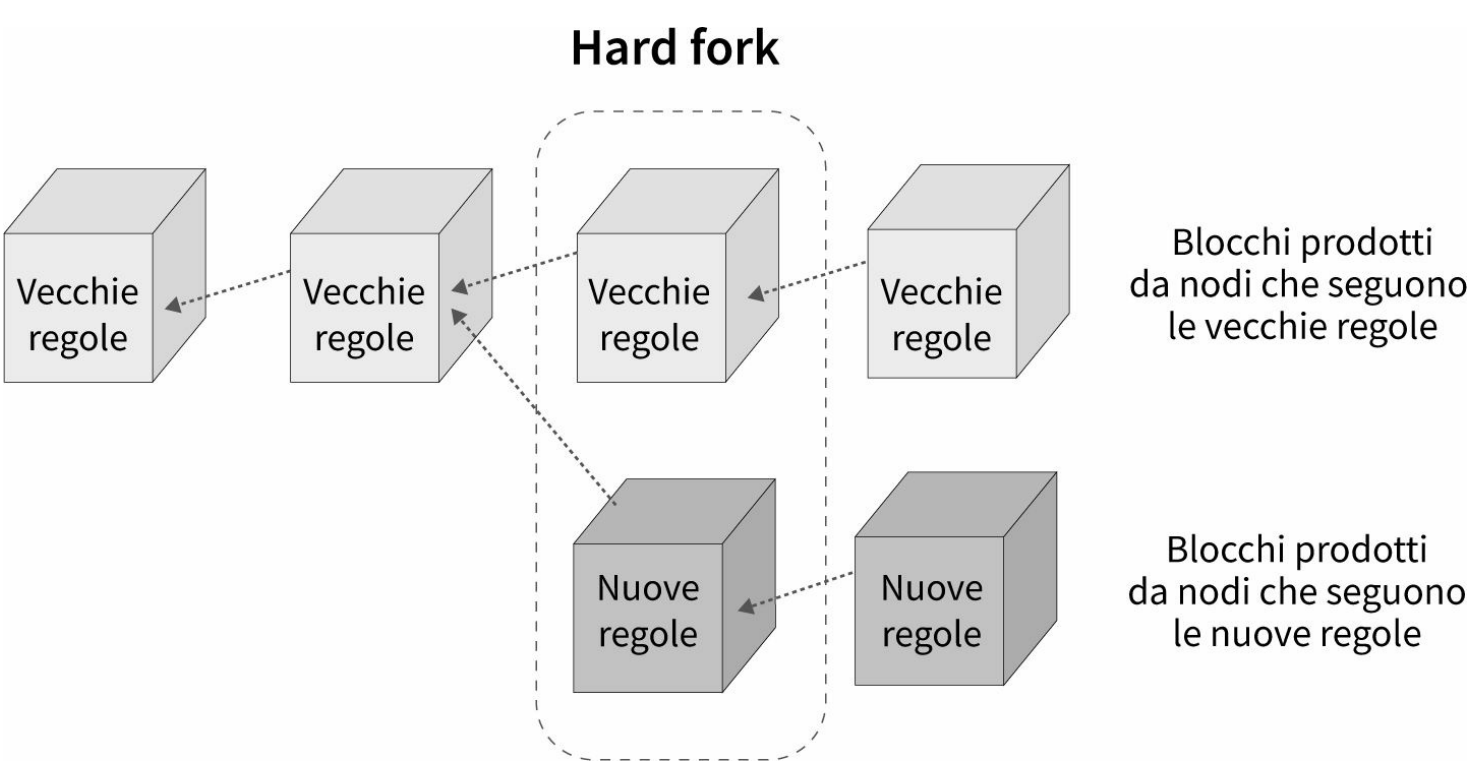


Figura 5.12 – La divisione di una blockchain a causa di una hard fork.

Una divisione della blockchain si verifica quando c'è una rottura irrisolvibile all'interno della comunità e un gruppo di utenti decide di cambiare alcuni aspetti della blockchain. Il gruppo che non è d'accordo con il protocollo corrente effettua una fork e ogni nodo che crede nel nuovo protocollo aggiorna

i propri sistemi, lasciando la blockchain precedente e unendosi a quella nuova.

Possono esserci varie ragioni che portano a un hard fork:

- correggere i rischi per la sicurezza che richiedono un cambiamento importante nelle regole di consenso;
- aggiungere nuove funzionalità;
- opinioni diverse nella comunità (per esempio tra miner, sviluppatori o utenti);
- cambiare la cronologia delle transazioni (per esempio rimuovere transazioni in seguito a un attacco).

Ethereum Hard Fork

Nel luglio 2016 uno smart contract (The DAO) in esecuzione sulla blockchain di Ethereum è stato hackerato e sono stati rubati circa 3,6 milioni di Ether (60 milioni di dollari, in quel periodo). Una parte della comunità ha deciso di eseguire una hard fork e annullare l'attacco, mentre l'altra non ha voluto invalidare il principio di immutabilità della blockchain.

Il risultato è stato una hard fork che ha creato due blockchain: Ethereum (la blockchain che ha eseguito la fork) ed Ethereum Classic (la blockchain originale).

Bitcoin Cash hard fork

Un altro esempio di disaccordo nella comunità che ha portato a una hard fork con chain split è stata la creazione di Bitcoin Cash, derivante da una fork del Bitcoin. Il disaccordo riguardava le misure da adottare per affrontare il problema della scalabilità. Da una parte veniva sostenuta l'adozione della SegWit (vedi il paragrafo "SegWit" nel Capitolo 8), dall'altra si volevano misure più drastiche, in particolare l'aumento della dimensione del blocco (portandolo in un primo momento a 8 megabyte).

Il risultato è stato quindi la creazione del Bitcoin Cash. Tra i

sostenitori della fork ci sono Bitmain, il più grande produttore al mondo di hardware per il mining, e Roger Ver, attuale proprietario del dominio bitcoin.com[35].

Duplicazione dei token

Una delle conseguenze di una divisione in una blockchain è la condivisione della cronologia delle transazioni prima della hard fork (tutte le transazioni prima della fork sono condivise).

> Dopo una divisione in una blockchain, un utente si troverà in possesso della

stessa quantità di token su entrambe le blockchain.

Se un utente possedeva 1 ETH prima della fork, dopo la fork si sarebbe ritrovato con 1 Ethereum Classic (ETC) e 1 Ethereum (ETH). Lo stesso con Bitcoin (BTC) e Bitcoin Cash (BCH) (Figura 5.13).

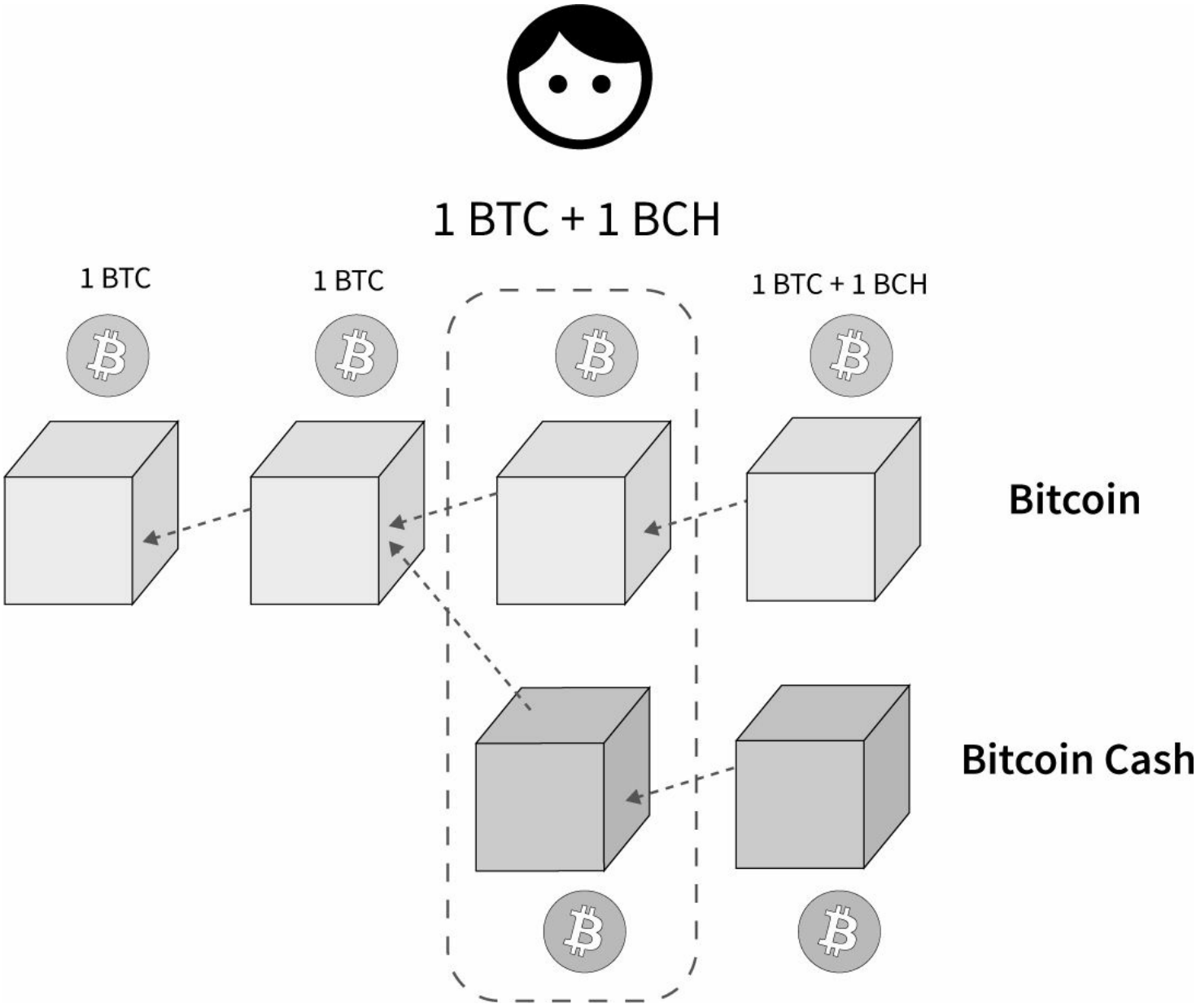


Figura 5.13 – La duplicazione dei token in una chain split.

Riassumiamo le differenze nella Tabella 5.3.

Tabella 5.3 – Le differenze fra i diversi tipi di fork.

Fork regolare	Soft fork	Hard fork
La blockchain si divide temporaneamente	La blockchain non si divide	La blockchain potrebbe dividersi
Nessuna modifica alle regole	Le nuove regole sono retrocompatibili	Le nuove regole non sono retrocompatibili.

Attivare una fork

In una blockchain non ci sono autorità centrali. Al contrario, ci sono diversi gruppi di persone che non sempre condividono la stessa visione. Miner, sviluppatori, utenti, exchange e commercianti potrebbero avere opinioni

diverse su come un progetto debba evolversi.

Ogni gruppo ha le sue idee, ma nessun gruppo può effettuare modifiche senza il consenso degli altri gruppi. Gli sviluppatori non possono proporre un aggiornamento o una fork senza il consenso dei miner o quello degli utenti, e lo stesso vale per tutti gli altri gruppi coinvolti. Un equilibrio deve essere trovato per mantenere la fiducia nel sistema. Il rischio di una situazione in cui i diversi attori non riescono a raggiungere un consenso è quello di una possibile perdita di fiducia nella blockchain. E questo sarebbe negativo per tutte le parti coinvolte.

27. Solitamente è un'autorità centralizzata che prende queste decisioni, come per esempio una banca, ma in un sistema decentralizzato come la blockchain questo scenario non è possibile.
28. Il miner verifica che l'importo da trasferire sia effettivamente disponibile, che la transazione sia stata firmata con la chiave privata corretta, che la struttura della transazione rispetti le regole, che la transazione non sia duplicata ecc.
29. Nel caso del Bitcoin, la ricompensa per ogni nuovo blocco generato all'inizio era di 50 bitcoin, e si dimezza ogni 210.000 blocchi (circa 4 anni). La ricompensa attuale è 12,5 bitcoin. Vedi https://www.bitcoinblockhalf.com.
30. Il PoW indica sia l'algoritmo Proof of Work che la soluzione al problema da risolvere. Questa soluzione viene anch'essa chiamata Proof of Work. Perciò ci riferiremo

al PoW (maschile) quando parliamo dell'algoritmo, e alla PoW (femminile) quando parliamo della soluzione al problema.

31. Grazie all'utente di Reddit *C121* per i calcoli.

32. https://www.blockchain.com/it/charts/hash-rate.

33. https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQs#what-is-proof-of-stake.

34. Per approfondire ulteriormente, consigliamo il seguente articolo: https://medium.com/coin-monks/what-is-a-51-attack-or-double-spend-attack-aa108db63474.

35. Per questo motivo il sito web bitcoin.com in realtà promuove il Bitcoin Cash.

6

Aspetti della decentralizzazione

Immutabilità

Come illustrato precedentemente, la blockchain permette di salvare informazioni in modo permanente e immutabile. A prima vista potrebbe sembrare che l'immutabilità sia garantita dal legame di hashing tra i blocchi.

Infatti, se un utente malintenzionato

modificasse una transazione in un blocco del passato, provocherebbe la modifica dell'hash del blocco e quindi a catena di tutti quelli successivi, portando la blockchain in uno stato finale differente, il quale verrebbe rifiutato dal consenso della rete. Senza le funzioni di hash, i nodi non sarebbero in grado di sapere se l'integrità della blockchain sia stata preservata nel tempo.

> Tuttavia, l'hashing non garantisce l'immutabilità. Garantisce solo che se qualcosa venisse modificato sarebbe immediatamente evidente per tutti i nodi.

L’hashing rende ogni manomissione della blockchain evidente, ma non rende la blockchain a prova di manomissione.

Un sistema dove ogni manomissione è evidente non è sufficiente a garantire l’immutabilità. È necessario avere un sistema che sia a prova di manomissione, e non solamente uno in cui la stessa venga resa evidente. Chiunque potrebbe modificare la propria copia della blockchain, ma il vero problema sorge quando si tenta di convincere il network che la blockchain manomessa sia quella corretta.

NOTA Manomettere una blockchain è facile, far accettare la blockchain manomessa al resto del network è difficile. L'immutabilità non risiede nella struttura di una blockchain ma nel protocollo di consenso.

Una blockchain è quindi immutabile solo se il protocollo di consenso è in grado di garantirne l'immutabilità.

Rischio

Il rischio non è qualcosa che si può misurare in maniera assoluta. Ogni

sistema ha un livello di rischio associato che dipende da diversi fattori. In generale possiamo dire che:

$$\text{Rischio} = \text{Vulnerabilità} \times \text{Minacce} \times \text{Asset}$$

Questa non vuole essere una formula matematica precisa, ma piuttosto un modo per esprimere il rischio in funzione di alcuni altri parametri. In particolare:

- **Vulnerabilità**: si intende tutto ciò che può essere sfruttato per eseguire un attacco. Ogni sistema ha delle vulnerabilità, alcune possono essere rimosse mentre

altre sono intrinseche al sistema (potrebbero essere mitigate ma non rimosse).

Non tutte le vulnerabilità sono sfruttabili. Per esempio, gli algoritmi crittografici sono vulnerabili agli attacchi brute-force (procedere a tentativi fino a che non si indovina), ma spesso questa vulnerabilità non è sfruttabile poiché nessuno ha abbastanza potenza computazionale e tempo per eseguire un attacco di questo tipo su tali algoritmi.

- **Asset**: tutto ciò che ha un valore è un asset. Dati, denaro,

macchine, computer, fiducia, reputazione ecc. È la stima della perdita causata da un attacco riuscito. Se il valore dell'asset è zero, il rischio è zero.

In una blockchain l'asset non è solo dato dal valore delle criptovalute ma anche dalla fiducia che gli utenti ripongono nella blockchain. Se per esempio qualcuno riuscisse a eseguire un attacco (anche di piccola entità) con successo al Bitcoin, la prima conseguenza sarebbe una distruzione della fiducia degli utenti, che porterebbe molte persone a vendere i propri

bitcoin.

- **Minaccia**. Tutti i potenziali fattori che potrebbero portare a sfruttare una vulnerabilità. Questo valore non può essere controllato poiché è esterno al sistema.

  Fattori che influenzano il livello di minaccia possono essere per esempio: quanto è abile un attacker, quanti attaccanti ci sono, quanto sono motivati ecc.

Aziende come Google, Facebook e Amazon cercano di ridurre il rischio agendo sul controllo degli accessi,

limitando il numero di attori autorizzati che possono eseguire determinate azioni o avere accesso a particolari dati. Al contrario, le blockchain (almeno le blockchain pubbliche) non possono basarsi sul controllo degli accessi per mitigare i rischi. Tutto è aperto e pubblico. Ci sono miliardi di dollari in indirizzi pubblici in un sistema costantemente sotto attacco.

È la natura distribuita e decentralizzata della blockchain che, unita ai protocolli di crittografia, mantiene il sistema sicuro.

Non esiste un punto

centrale di attacco.

Fiducia

> “Ci vogliono vent’anni per costruirsi una reputazione e cinque minuti per distruggerla.”

Una blockchain è un sistema aperto e neutrale. La fiducia in questo sistema non dipende da nessuna istituzione o dalle intenzioni di nessun particolare attore coinvolto. In una blockchain non è necessario fidarsi di nessuno, ma allo

stesso tempo si può essere sicuri che le transazioni verranno elaborate correttamente senza alcuna manomissione o censura.

Con la blockchain cambia completamente il concetto di fiducia, ma non viene eliminata. La fiducia è ancora necessaria, ma invece di essere concentrata in un unico posto, come potrebbe essere nel caso di una banca, è distribuita tra molti attori diversi.

La fiducia viene trasferita da istituzioni e persone a un

network.

La fiducia viene garantita tramite una combinazione di crittografia, protocolli di consenso e un sistema economico che incoraggia gli attori a cooperare con le regole definite dalla blockchain. È tuttavia impossibile che un sistema sia sicuro al 100% e sarà sempre necessario un certo grado di fiducia. Per fare un esempio, bisogna:

- **Fidarsi della crittografia**. La crittografia è perfetta sulla carta, ma quando si passa all'implementazione nel mondo reale possono sorgere alcuni problemi. Per esempio, il

generatore di numeri casuali usato per creare una chiave privata non è veramente casuale, oppure si trova vulnerabilità matematica in un algoritmo considerato sicuro. Al momento, nessuno ha abbastanza potenza di calcolo per poter attaccare una qualsiasi delle funzioni crittografiche usate solitamente nelle blockchain, ma il rischio che vengano scoperte delle vulnerabilità nelle implementazioni di quegli algoritmi non è nullo.

- **Fidarsi del consenso distribuito**. Il consenso distribuito è ciò che

garantisce che le regole definite in una blockchain vengano effettivamente rispettate e impedisce a chiunque di eseguire attacchi potenzialmente dannosi. Una maggior centralizzazione potrebbe risultare in una minaccia al consenso distribuito.

- **Fidarsi dei miner**. Se un gruppo di miner decidesse di colludere, non è da escludere che potrebbero eseguire con successo un attacco del 51%. Nel Bitcoin, per esempio, più della metà dell'hashrate è concentrata in 5 mining pool e oltre il 70% dell'hashrate è

concentrato in Cina[36]. Uno scenario di questo tipo è lontano dall'idea di decentralizzazione. Alcune blockchain minori sono state vittime di attacchi del 51% e, anche se i danni sono stati mitigati, hanno subito un duro colpo dal punto di vista della reputazione. Nel PoS uno scenario simile potrebbe accadere se un gruppo di exchange con più del 51% dei token di una particolare blockchain nei loro portafogli decidesse di colludere.

- **Fidarsi dei wallet**. Se il wallet utilizzato ha un bug (per esempio

non genera correttamente le chiavi private o ha una backdoor), questo potrebbe comportare il furto delle criptovalute in esso contenuti.

- **Fidarsi degli sviluppatori**. Anche se il codice molto spesso è open source, solo una percentuale minima di utenti ha le competenze e il tempo per comprendere e analizzare questo codice. Bisogna fidarsi che gli sviluppatori scrivano un buon software.

  La programmazione è difficile. Programmare un sistema in grado di gestire miliardi di dollari in

maniera decentralizzata e sicura è ancora più difficile.

- **Fidarsi degli smart contract**. Uno smart contract, come vedremo in seguito, è un'applicazione che viene eseguita all'interno di una blockchain. Come qualsiasi applicazione potrebbe contenere delle vulnerabilità. Alcuni smart contract sono stati hackerati dopo aver raccolto milioni di dollari (per esempio The DAO, hackerato dopo aver raccolto 150 milioni di dollari [10]) oppure hanno bloccato i fondi degli utenti (Parity multisig smart

contract, che a causa di un bug ha bloccato al suo interno circa 280 milioni di dollari di Ethereum [11]).

- **Fidarsi di se stessi**. Se qualcuno scopre le tue chiavi private, i tuoi fondi possono essere facilmente rubati e non c'è alcun modo di recuperarli.

Cripto-economia

Una blockchain opera in un ambiente estremamente avverso (si ricordi il problema dei generali bizantini). Questo ecosistema è composto da attori onesti

che rispettano le regole imposte dalla blockchain, così come da altri che intendono rubare denaro oppure distruggere l'intero sistema.

Per sopravvivere in un ambiente così ostile, le blockchain adottano un approccio particolare, ovvero una combinazione di crittografia, network peer-to-peer (p2p), protocolli di consenso ed economia, che possiamo chiamare un approccio cripto-economico (dall'unione delle parole crittografia ed economia).

Se la crittografia studia le tecniche per la comunicazione sicura in un ambiente avverso, la cripto-economia può essere vista come lo studio dell'interazione economica in un

ambiente avverso.

> La cripto-economia studia la progettazione di un sistema che opera in un ambiente avverso in cui imbrogliare (o tentare di imbrogliare) è meno conveniente rispetto a comportarsi onestamente, ovvero dove i benefici di un comportamento disonesto sono inferiori ai costi. Ciò si ottiene combinando crittografia e incentivi economici.

Nella cripto-economia l'output

desiderato è solitamente noto e l'attenzione è rivolta alla progettazione del processo migliore per raggiungere questo risultato, utilizzando incentivi economici e crittografia. Se supponiamo che la maggior parte degli utenti sia economicamente razionale, è possibile influenzare il loro comportamento attraverso incentivi e punizioni economiche.

Gli incentivi economici costringono un utente razionale a comportarsi in un determinato modo e ciò, insieme alla crittografia, rende possibile creare fiducia in un sistema come la blockchain.

NOTA La fiducia è creata grazie a un sistema economico che incentiva gli attori a cooperare con le regole definite dal protocollo.

Possibili incentivi per gli attori che contribuiscono onestamente alla creazione di fiducia potrebbero essere:

- ricompense monetarie (per esempio criptovalute);
- privilegi decisionali (per esempio decidere quali transazioni possono essere incluse in un blocco).

D'altra parte la punizione possibile per l'attore malintenzionato potrebbe essere:

- perdita economica, sotto forma di elettricità (PoW) o token (PoS);
- perdita dei privilegi, come per esempio la possibilità di verificare le transazioni.

Scalabilità

Una delle maggiori promesse della tecnologia blockchain è la possibilità di effettuare transazioni istantanee con costi estremamente bassi. Attualmente questa tecnologia è ancora nella fase iniziale di sviluppo e non è esente da sfide. Come ogni nuova tecnologia, ci

sono molti problemi che devono essere risolti prima che un'adozione su larga scala sia possibile. Uno dei problemi più evidenti è la difficoltà che le blockchain stanno affrontando nello scalare.

> **NOTA** La scalabilità è la capacità di un sistema di gestire una quantità crescente di lavoro. In una blockchain, di solito, si riferisce alla capacità di elaborare un numero crescente di transazioni senza che le prestazioni ne risentano.

Le conseguenze pratiche dei problemi di scalabilità sono:

- **Basso throughput**: le due principali blockchain possono elaborare solo un numero limitato di transazioni al secondo (**tps**). Bitcoin gestisce circa 7 tps, Ethereum 10-30 tps, mentre Visa può raggiungere teoricamente le 50.000 tps (ma solitamente non va oltre le 1.700 tps). Le transazioni che superano questo limite vengono accodate ed elaborate successivamente (Figura 6.1).
- **Transazioni lente**: il tempo richiesto per creare un nuovo blocco (specialmente nel PoW) è elevato (10 minuti in media nel

Bitcoin). Se aggiungiamo che una conferma di solito non è sufficiente, il tempo necessario per considerare una transazione immutabile è tutt'altro che immediato.

- **Commissioni elevate**: quando una blockchain non riesce a scalare, le commissioni di transazione di solito aumentano. I miner, infatti, preferiscono processare in primo luogo transazioni con commissioni elevate rispetto a transazioni con commissioni basse.

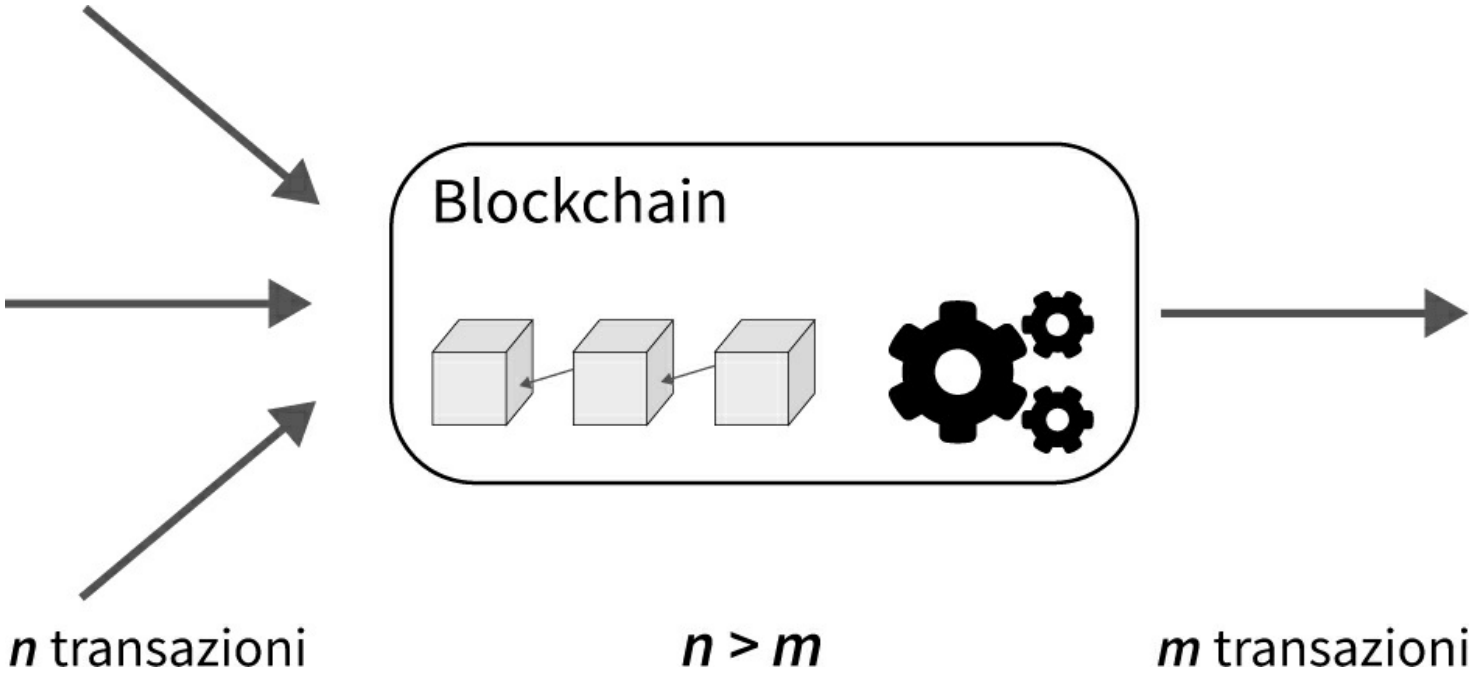


Figura 6.1 – Il problema del basso throughput nella blockchain.

Il trilemma della scalabilità

Il trilemma della scalabilità[37] afferma che un sistema basato su blockchain può avere al massimo due delle seguenti proprietà (Figura 6.2):

- decentralizzazione;
- scalabilità;
- sicurezza.

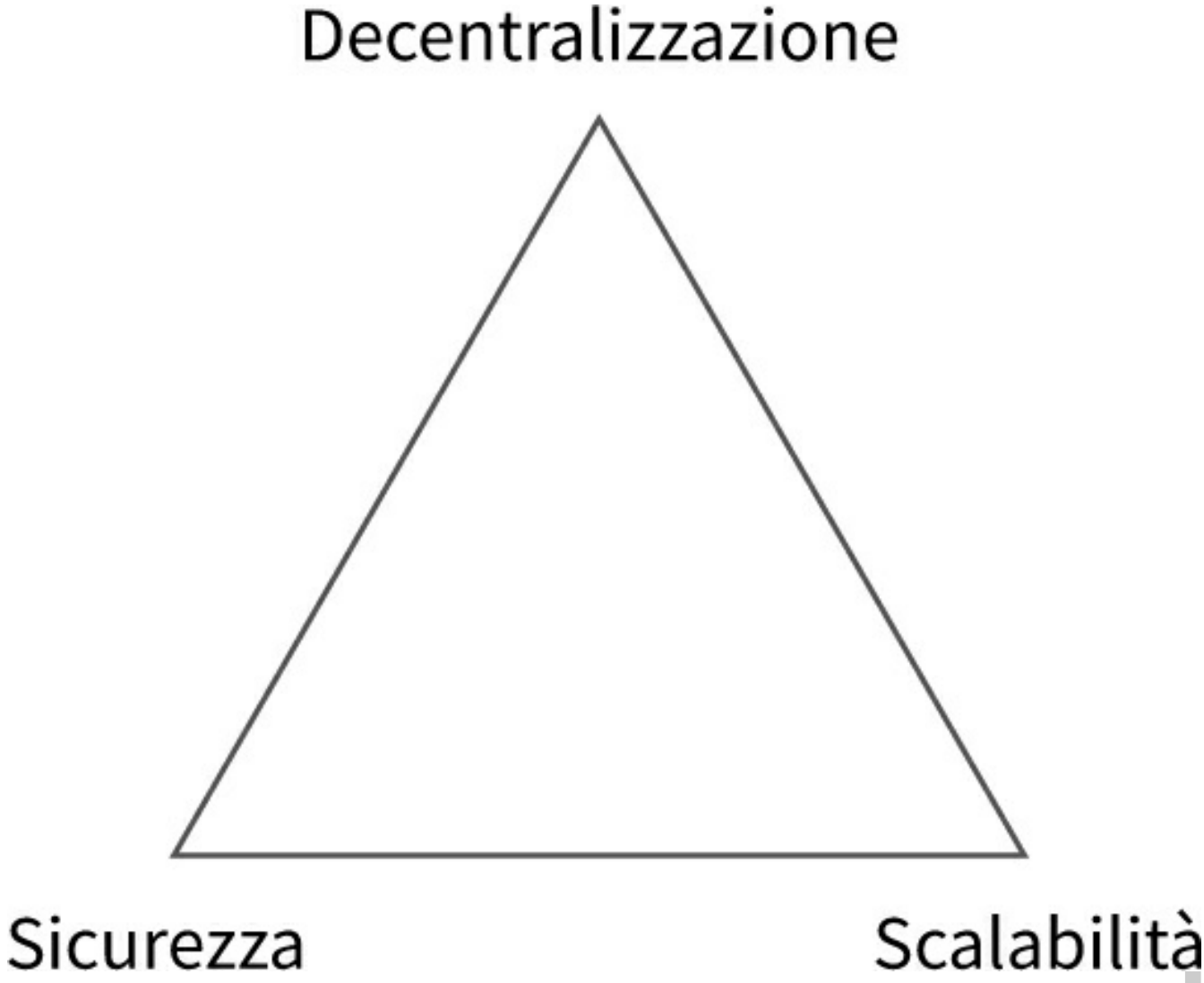


Figura 6.2 – Il trilemma della scalabilità.

Quali soluzioni esistono per risolvere, anche solo parzialmente il problema della scalabilità?

Sono state studiate molte soluzioni per aumentare il numero di tps che potrebbero essere elaborate da una blockchain. Le principali sono:

- aumentare la dimensione dei blocchi (SegWit, Bitcoin Cash ecc.);
- cambiare il protocollo di consenso (PoS);
- spostare le transazioni off-chain in canali di pagamento pubblici (per esempio Lightning Network);
- modificare la struttura della blockchain (per esempio IOTA con il tangle).

Spostare le transazioni in canali di pagamento pubblici off-chain è ritenuta da molti una delle soluzioni più interessanti.

Transazioni off-chain

L'idea di utilizzare canali di pagamento **off-chain** (fuori dalla blockchain) deriva dal fatto che la maggior parte delle transazioni di tutti i giorni potrebbe essere gestita esternamente alla blockchain.

Una transazione off-chain, al contrario di una transazione **on-chain** (transazione normale), non viene direttamente salvata nella blockchain ma

viene eseguita su un layer costruito sulla blockchain (second layer) utilizzando canali di pagamento appositamente progettati (Figura 6.3).

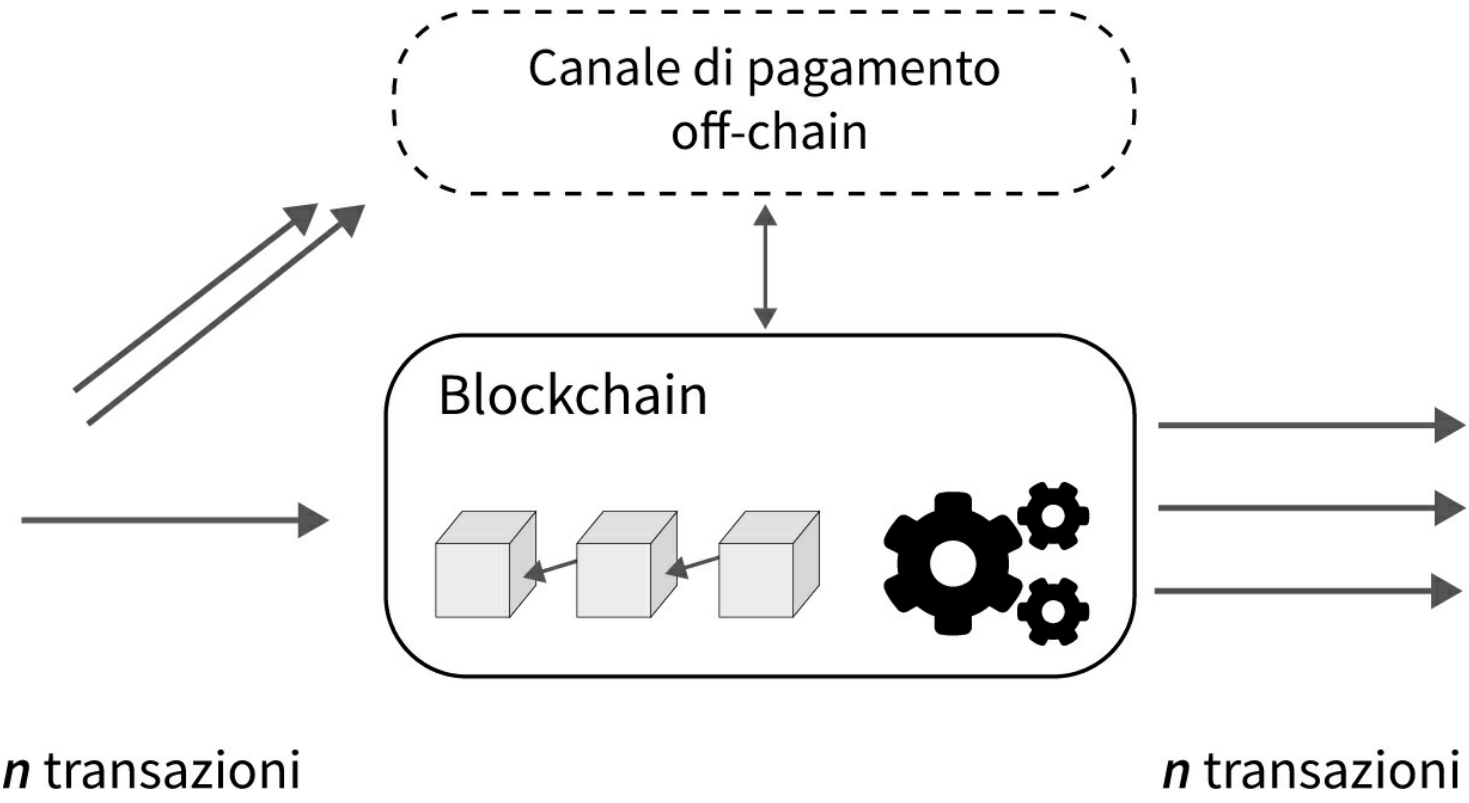


Figura 6.3 – Un canale off-chain come soluzione al limite di scalabilità.

I canali di pagamento off-chain consentono agli utenti di trasferire denaro tra loro senza la necessità di scrivere immediatamente ogni transazione sulla blockchain ma allo stesso tempo mantenendo tutte le proprietà garantite dalla blockchain

(immutabilità, sicurezza). In questo modo è possibile ridurre al minimo la quantità di transazioni che avvengono sulla blockchain. Il più promettente protocollo second layer in questo momento è il Lightning Network: ne parleremo nel Capitolo 8.

Distributed Ledger Technologies

Per superare alcuni dei problemi della blockchain, in particolare la difficoltà di scalare e gli alti costi di transazione, diversi progetti hanno cercato di ridisegnare la struttura sottostante della

blockchain mantenendo però intatti i concetti principali.

Chiamiamo Distributed Ledger Technologies (DLT) tutte le applicazioni che sfruttano il concetto di una ledger distribuita, ma non strutturano necessariamente questa ledger come una catena di blocchi (Figura 6.4).

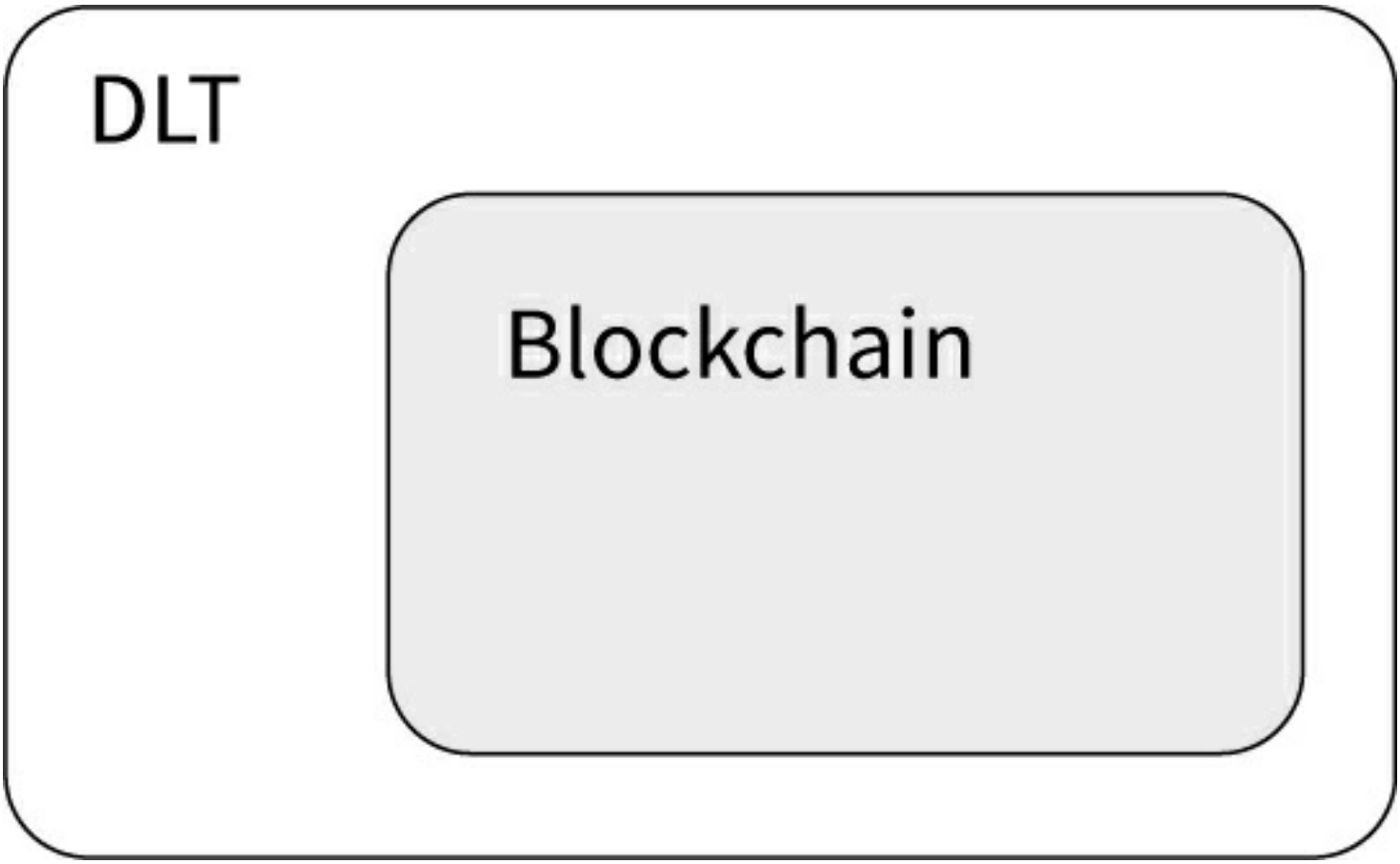


Figura 6.4 – La blockchain fa parte delle Distributed Ledger Technologies.

> Una blockchain è un particolare tipo di DLT in cui il ledger distribuito è strutturato come una catena di blocchi.

Un esempio di DLT che non utilizza una struttura lineare per la ledger distribuita è IOTA, un progetto che ha creato una nuova struttura dati, chiamata tangle, pensata specificamente per l'utilizzo in ambito IoT.

Tangle (IOTA)

Tangle è una struttura dati creata da IOTA come base per la criptovaluta.

> Un tangle è un tipo speciale di architettura di ledger distribuita basato su un grafo aciclico diretto (DAG, Directed Acyclic Graph).

Un DAG è un grafo in cui ogni nodo è connesso ad altri nodi tramite collegamenti diretti e non sono presenti cicli (Figura 6.5).

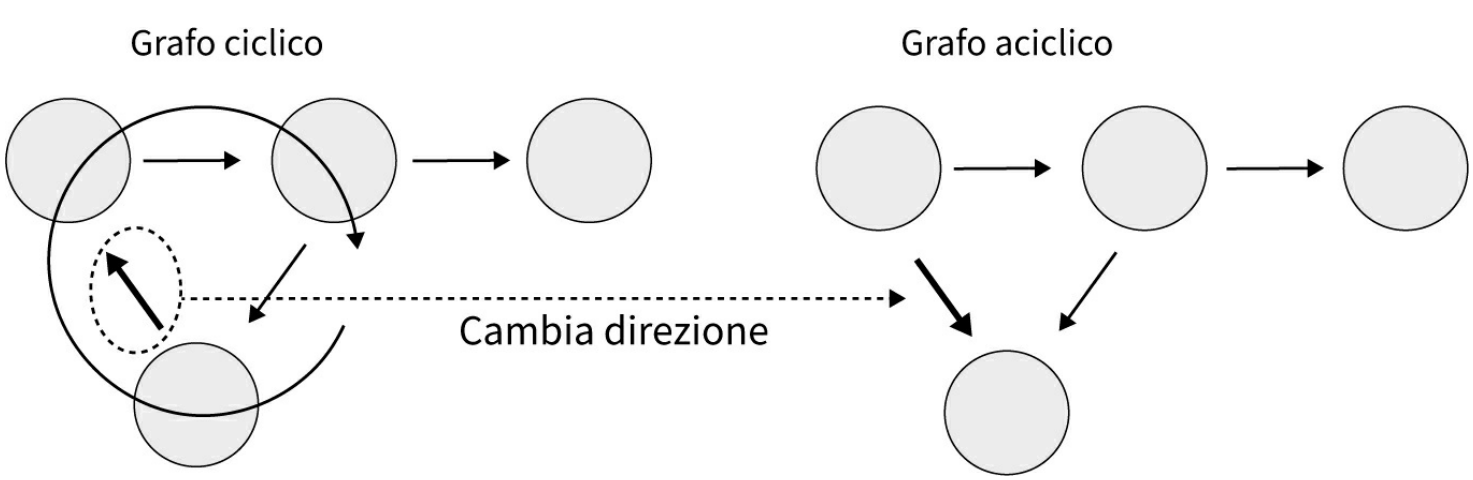


Figura 6.5 – Il grafo aciclico di IOTA.

L'idea alla base di IOTA è quella di rendere possibili micro-transazioni m2m (machine-to-machine). Non trovando nelle blockchain già esistenti una soluzione che potesse adattarsi a questo caso d'uso, IOTA ha deciso di sviluppare una sua DLT basata sul tangle.

In un tangle non vi è alcun concetto di blocco, di catene o di mining inteso come processo a sé stante. Ogni utente,

per poter eseguire una transazione, deve prima validare altre due transazioni scelte in modo casuale, diventando di fatto anche un miner.

È quindi una struttura nella quale ogni utente prende parte al processo di validazione, eliminando di fatto ogni limite di scalabilità: più transazioni vengono create, più transazioni vengono validate (Figura 6.6).

Il risultato è un sistema autosostenibile e infinitamente scalabile (non esiste un limite teorico di tps[38]).

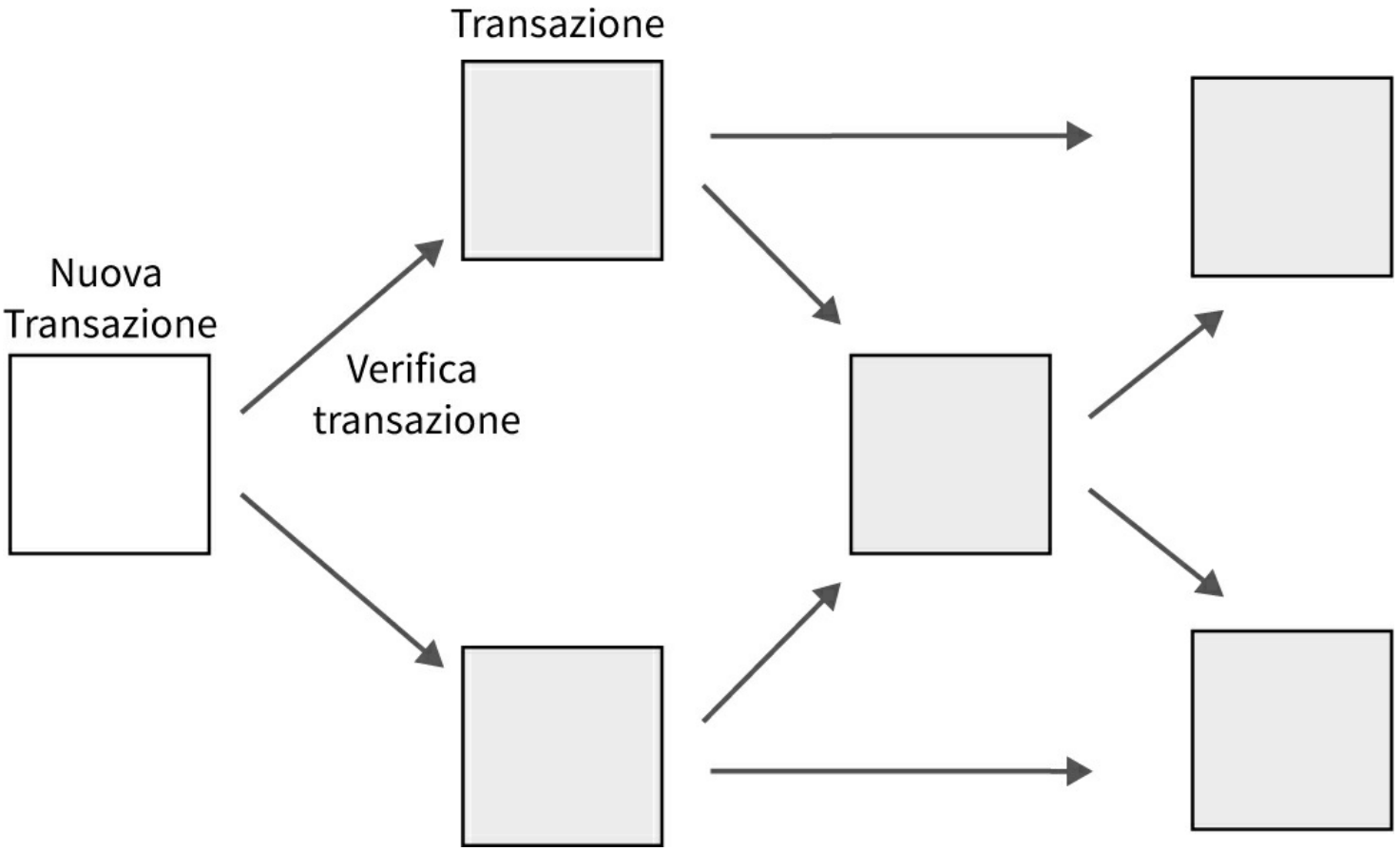


Figura 6.6 – La validazione delle transazioni nel tangle.

---

36. https://www.blockchain.com/pools.
37. https://github.com/ethereum/wiki/wiki/Sharding-FAQs#this-sounds-like-theres-some-kind-of-

scalability-trilemma-at-play-what-is-this-trilemma-and-can-we-break-through-it.

38. IOTA nasce infatti per il mercato IOT, ed è quindi strutturato per servire triliardi di utenti (macchine).

7

Criptovalute

Blockchain e criptovalute

Le possibilità create dall'utilizzo di ledger distribuiti come la blockchain hanno portato alla prima e ovvia applicazione: lo scambio di valore. Per la prima volta è possibile scambiare valore senza la necessità di una terza parte che funga da garante, come per

esempio una banca. Tramite questo tipo di tecnologia viene infatti reso possibile eseguire direttamente delle transazioni finanziarie senza incorrere nel rischio di controparte.

> Il rischio di controparte è il rischio che l'altra parte coinvolta nella transazione non tenga fede alle condizioni definite nella transazione.

Le criptovalute intese come mezzo di scambio sono state la prima applicazione a sfruttare le potenzialità della tecnologia blockchain creando un nuovo paradigma nel mondo dei

pagamenti. È il primo esempio di **Internet del valore**.

Internet del valore

Internet si basa sul protocollo TCP/IP, dove TCP sta per Transmission Control Protocol e IP per Internet Protocol. TCP/IP definisce come devono essere trasmessi i dati tra due dispositivi interconnessi su Internet.

Grazie a questo protocollo siamo riusciti a scambiare dati in tutto il mondo per oltre trent'anni.

Quando i dati viaggiano su Internet vengono sempre trasferiti come copia. Se carichiamo un'immagine su

Instagram, stiamo creando una copia digitale indistinguibile da quella originale, cioè stiamo duplicando la foto. Una foto può es sere duplicata tutte le volte che vogliamo senza che questo comporti alcun problema (Figura 7.1).

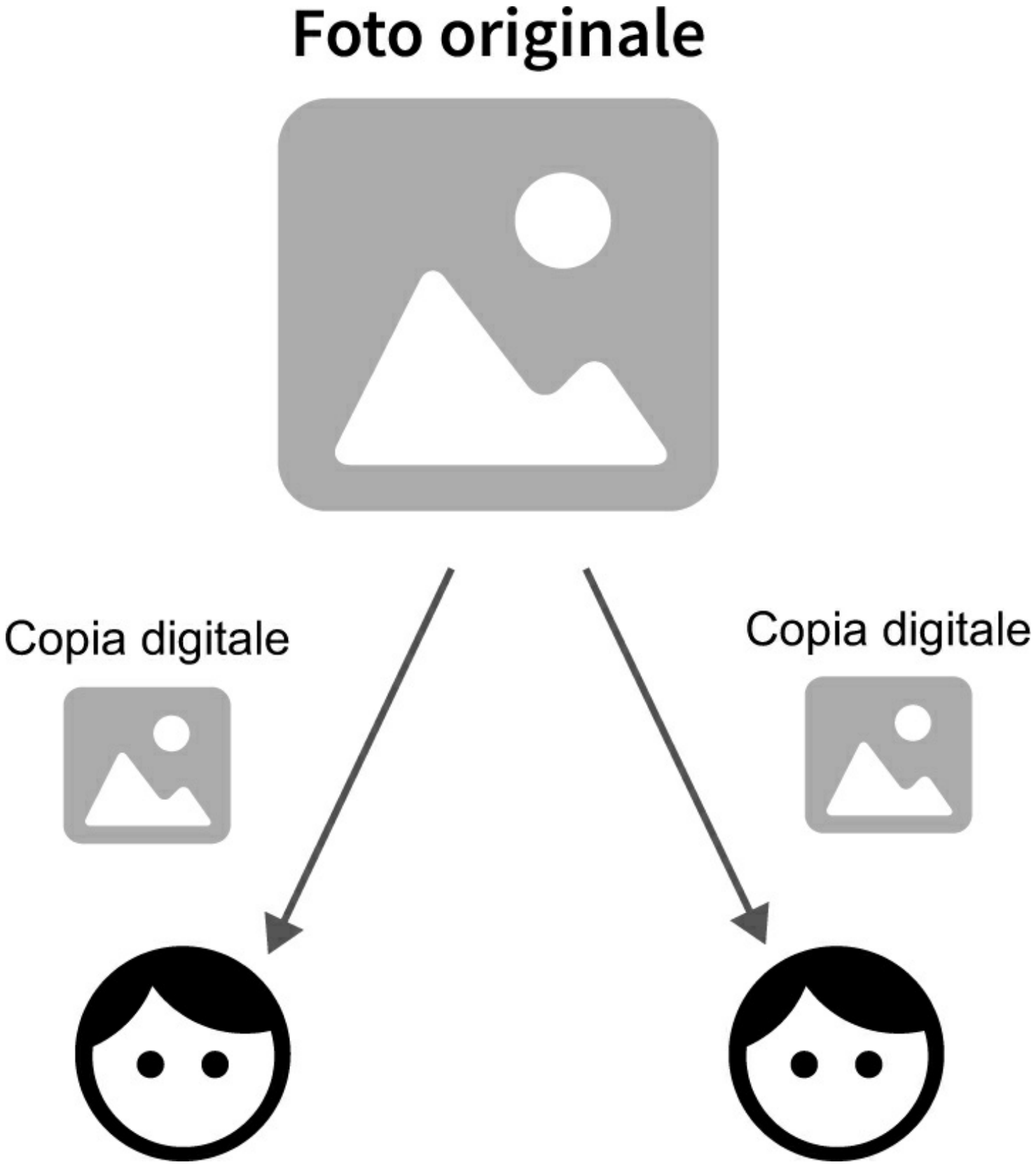


Figura 7.1 – La copia di un file digitale.

Ma cosa succede se vogliamo trasferire valore?

Un modello in cui le entità digitali possono facilmente essere duplicate non si adatta a uno scenario in cui vengono trasferiti beni reali come il denaro. Qualsiasi oggetto con un valore non dovrebbe essere duplicato quando viene trasferito, poiché il suo valore risiede nella sua unicità. Non è ipotizzabile uno scenario in cui si possa trasferire denaro come copia, dal momento che sarebbe possibile spenderlo più volte.

NOTA Il problema della doppia spesa

(double spending) è una situazione in cui esiste più di una copia digitale di qualcosa che dovrebbe essere unico.

L'esempio più chiaro è quello di spendere gli stessi soldi in più di una transazione. Ma è un problema che può essere esteso a qualsiasi altro scenario in cui le entità dovrebbero essere uniche, come per esempio un voto digitale.

In un sistema tradizionale, la doppia spesa viene evitata grazie a un'autorità centrale come una banca, che ha il ruolo di detentore assoluto della verità. Se un utente desidera effettuare un pagamento online, invia le informazioni a un

gateway, come PayPal, che a sua volta gestisce le interazioni con la banca. La banca infine evita le doppie spese aggiornando correttamente l'account dell'utente.

> **NOTA** Le DLT e le blockchain sono le prime tecnologie in grado di risolvere il problema della doppia spesa in maniera decentralizzata, affidandosi totalmente a loro stesse, senza coinvolgere una terza parte.

In una blockchain non è possibile spendere due volte lo stesso denaro: il consenso del network non lo

autorizzerebbe. Una transazione verrebbe approvata per prima e l'altra rifiutata. L'impossibilità di spendere due volte una risorsa digitale crea il concetto di **scarsità digitale.**

La blockchain ci dà quindi la possibilità di rimuovere le terze parti nelle transazioni finanziarie, consentendo agli utenti di trasferire valore direttamente tra loro.

> La tecnologia blockchain è un protocollo di scambio di valori proprio come il TCP/IP è un protocollo di scambio di informazioni. Internet è per i dati quello che la blockchain è

per i valori.

Il denaro come linguaggio

Il denaro può essere visto come un mezzo tramite il quale si converte il concetto astratto di valore di un bene o un servizio in qualcosa di concreto, e ci permette di comunicarlo ad altre persone. Il denaro può quindi essere paragonato a una forma di linguaggio.

Da un punto di vista tecnico possiamo dire che:

> Il denaro è tutto ciò che può essere accettato come pagamento di beni, servizi o

debiti in un contesto specifico.

Le principali funzioni del denaro sono:

- **Mezzo di scambio**. Il denaro viene utilizzato per intermediare lo scambio di beni e servizi.
- **Misura del valore**. Il denaro è usato per confrontare i valori di diversi beni e servizi. Per esempio, è possibile confrontare beni e servizi utilizzando i dollari come misura.
- **Riserva di valore**. Il denaro è un deposito di valore che mantiene il potere d'acquisto futuro. Per agire come riserva di valore, il

denaro deve essere in grado di mantenere il suo valore nel tempo.

A seconda di come un determinato tipo di denaro adempie a tali funzioni, potremmo dire quanto è valida quella specifica forma di denaro. L'euro potrebbe essere considerato un buon mezzo di scambio se ci si trova nell'Unione Europea, ma non altrettanto efficace in un paese distante come il Brasile. L'oro potrebbe essere una valida riserva di valore, ma non è un efficace mezzo di scambio in quanto difficile da trasportare.

Evoluzione del denaro

Il denaro si è evoluto insieme alla società adattandosi per affrontare interazioni finanziarie sempre più complesse. Dal baratto all'utilizzo di metalli preziosi, alla carta, al denaro fiat, il denaro ha continuato a evolversi. Le criptovalute sono solo un altro passo in questo processo evolutivo.

Baratto

Scambiare cibo e animali per altri beni o servizi (per esempio, il lavoro) sono esempi di baratto.

Tecnicamente il baratto non dovrebbe essere considerato denaro, dal momento che beni o servizi sono scambiati direttamente senza utilizzare alcun livello di astrazione.

Questo sistema è stato utilizzato sin nei primi mercati ed è ancora usato oggi in contesti con un'offerta monetaria molto bassa o dove non c'è fiducia nelle istituzioni (per esempio situazioni di iperinflazione).

I prodotti utilizzati nel baratto tuttavia non sono molto adatti alle transazioni finanziarie in quanto:

- non sono un buon deposito di

valore (cibi e animali sono deperibili);

- non sono un buon mezzo di scambio, dal momento che bisogna trovare qualcuno interessato ai prodotti, altrimenti una transazione non può aver luogo;
- non sono una buona misura di valore, poiché spesso sono presenti differenze nella qualità dei prodotti;
- non sono pratici da portare in giro;
- non sono facili da dividere.

Per tutti questi motivi, le persone sono passate dal baratto ad altri tipi di sistemi di pagamento, creando dei livelli di astrazione rispetto a beni e servizi materiali.

Denaro commodity

Il denaro commodity può essere considerato la prima forma di denaro convenzionale. Ha valore perché è costituito da una merce con un valore intrinseco. Il valore risiede nelle proprietà fisiche della merce ed è riconosciuto come prezioso da entrambe le parti nella transazione.

L'esempio tipico di commodity sono

le materie prime come l'oro o altri materiali preziosi. Il denaro commodity potrebbe essere un buon deposito di valore, ma manca di altre funzionalità:

- è difficile da portare in giro;
- è difficile capire se la merce sia stata manomessa in qualche modo (per esempio l'oro potrebbe essere stato mescolato con altri materiali più economici);
- è difficile da dividere;
- la disponibilità totale di un determinato materiale è solitamente sconosciuta.

Denaro commodity-backed (paper money)

Per superare il problema del trasporto delle commodity, si è iniziato a lasciare le materie prime (le commodity) come l'oro nelle banche e a portare con sé un documento ufficiale emesso dalla banca (IOU, I Owe You) che garantisca il possesso di quella commodity. È molto più facile da portare in giro, può essere suddiviso in IOU più piccoli ed è un buon deposito di valore, dal momento che è collegato direttamente alla merce. L'IOU *rappresenta* una commodity. Il denaro commodity-backed è un documento che rappresenta una merce immagazzinata da qualche altra parte

(Figura 7.2).

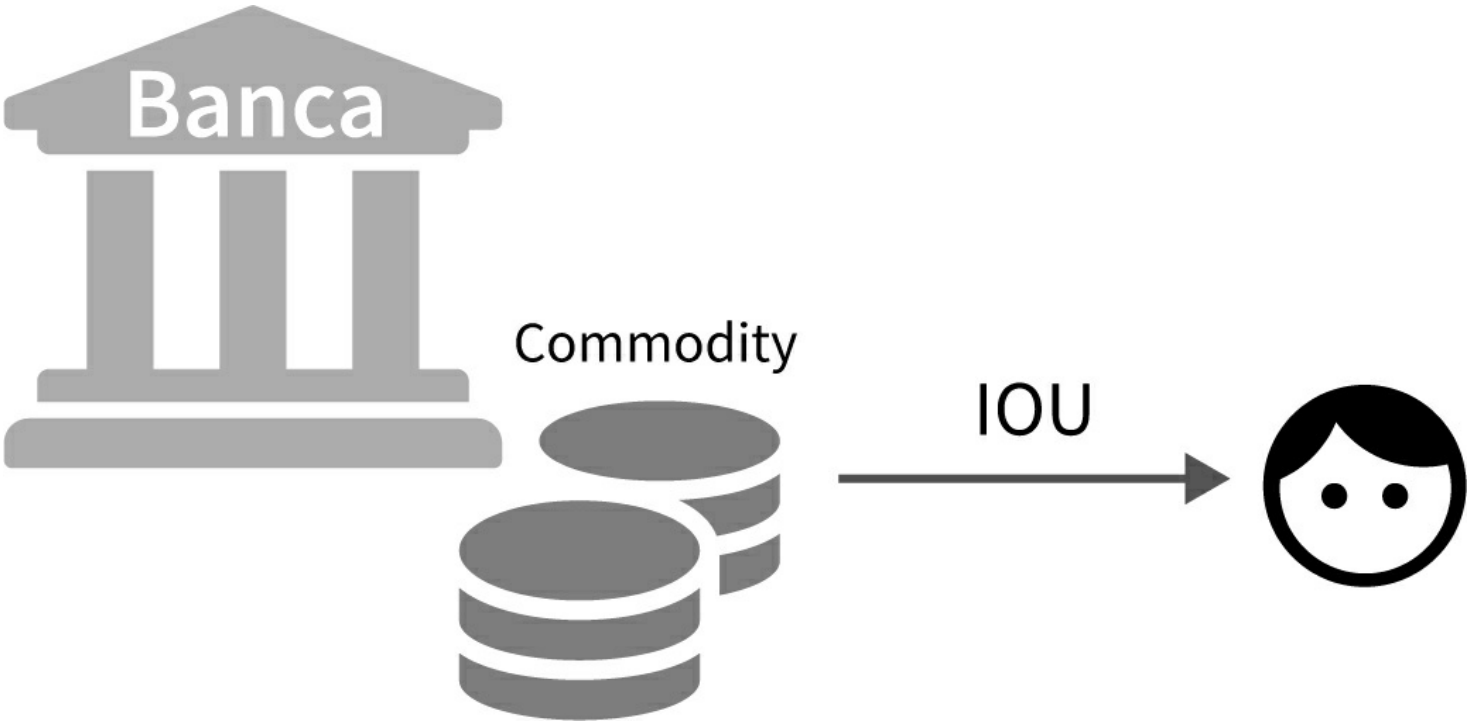


Figura 7.2 – Il denaro commodity-backed.

Denaro fiat

Il denaro fiat (cioè le banconote e monete usate al giorno d'oggi) è un'alternativa al denaro commodity e commodity-backed. In questo caso, invece di fidarsi di una commodity, ci si fida di un'istituzione centrale (un

governo o una banca centrale) che emette questa moneta.

Il denaro fiat non ha valore intrinseco, e non è collegato a nessun bene di valore, ma riceve il suo valore da un'istituzione che lo dichiara moneta in corso legale, vale a dire che deve essere accettato come pagamento entro i limiti legali stabiliti dall'istituzione che lo ha emesso.

In Italia, per esempio, un negozio deve accettare euro ma può non accettare dollari, in quanto l'euro è moneta in

corso legale in Italia.

Il denaro fiat è il primo esempio di sistema monetario centralizzato. Il denaro circolante è controllato da un'istituzione centrale che ha potere decisionale sulla quantità circolante. Ciò consente ai governi di gestire meglio l'inflazione e altre proprietà del sistema monetario.

Denaro digitale

Il denaro digitale (da non confondere con le criptovalute) è una forma digitale del denaro fiat. Esiste solo sotto forma di numeri sui sistemi informatici, ma può

eventualmente essere convertito in denaro fisico. Il denaro digitale rappresenta gran parte del denaro posseduto da parte delle banche e costituisce la maggior parte delle transazioni in tutto il mondo (circa il 92% di tutto il denaro esiste solo in forma digitale)[39].

Panoramica sulle criptovalute

Le criptovalute possono essere viste come un sottoinsieme delle valute digitali. Ogni criptovaluta è una valuta digitale, ma non tutte le valute digitali

sono criptovalute (Figura 7.3).

Con il termine “criptovaluta” ci riferiamo a tutti gli asset digitali basati sulla tecnologia blockchain (o sulle DLT, il concetto alla base rimane lo stesso).

Le criptovalute attualmente, al contrario del denaro fiat, non hanno corso legale e non sono supportate o gestite da alcuna istituzione.

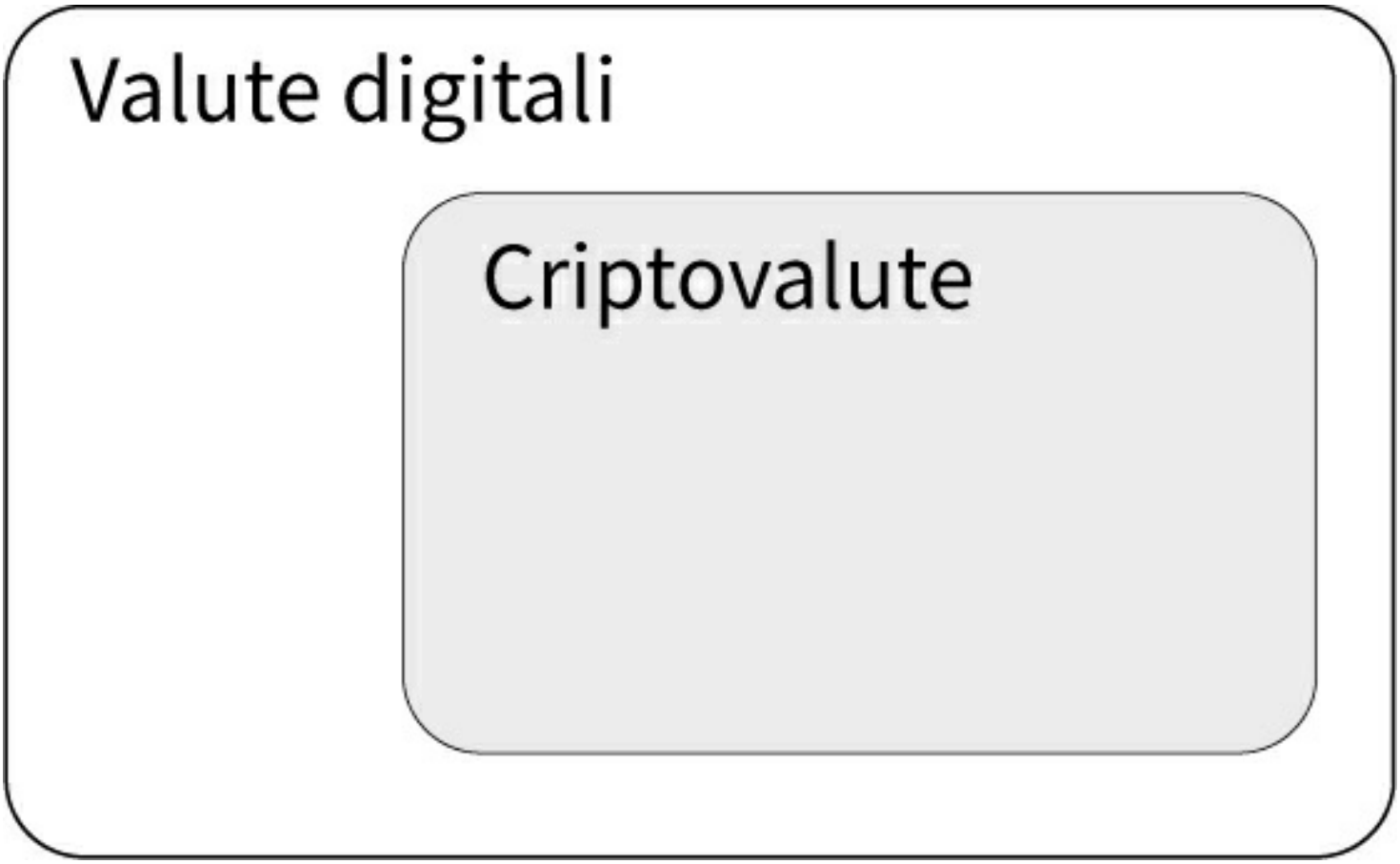


Figura 7.3 – La distinzione tra valute digitali e criptovalute.

Con le criptovalute per la prima volta esiste un modo per chiunque di creare denaro senza un'autorità centrale. Le criptovalute hanno proprietà simili al denaro commodity ma possono essere scambiate come le valute digitali.

Criptomonete e token

Il termine “criptovaluta” è abbastanza generico e talvolta viene scambiato con altri termini come **criptomonete**, **token**, o semplicemente **coin**. Tutti questi termini fanno riferimento a degli asset digitali che esistono all’interno di una blockchain. Lo scopo principale di una criptomoneta (coin) è quello di agire come mezzo di scambio (pagamento). Il termine “token” viene invece solitamente utilizzato per identificare una criptovaluta che rappresenta una particolare risorsa (per esempio, l’accesso a dei servizi). Tuttavia molte criptovalute rientrano in entrambe le definizioni e non è facile fare una

divisione netta tra i due termini. Si può in generale utilizzarli entrambi e lasciare che sia il contesto a definire sotto quale categoria rientra una particolare criptovaluta.

Caratteristiche delle criptovalute

Una criptovaluta eredita tutte le proprietà della blockchain sopra la quale è sviluppata. A seconda di come è progettata la blockchain, è possibile costruire criptovalute focalizzate su velocità, privacy, decentralizzazione o qualsiasi altra caratteristica.

La maggior parte delle criptovalute

tuttavia condivide un insieme di caratteristiche comuni:

- **Digitali/virtuali**. Tutte le criptovalute esistono solo in forma digitale come unità di conto in un ledger distribuito. Non esiste un equivalente fisico di una criptovaluta.
- **Trustless**. Non è necessario fidarsi di una persona, di una materia prima o di un'istituzione centrale per fare transazioni. La fiducia viene trasferita da un'autorità centrale a un sistema di consenso distribuito.
- **Globali**. Le criptovalute non

sono soggette a confini fisici o politici. È possibile per chiunque effettuare una transazione.

- **Sicure**. La proprietà (ownership) delle criptovalute può essere dimostrata esclusivamente crittograficamente. Non importa se si tratti di un essere umano o di una macchina, le criptovalute appartengono a coloro che possiedono le chiavi private. Una transazione può essere creata solo se si è in possesso delle chiavi crittografiche necessarie.
- **Immutabili**. Una volta che una

transazione viene confermata e aggiunta alla blockchain, nessuno può modificarla o eliminarla.

- **Basate sul consenso**. In una criptovaluta, le regole sono programmate nel meccanismo di consenso che governa il network decentralizzato. Il consenso è il processo incaricato di decidere se una transazione sia valida o meno e di definire la politica monetaria di una criptovaluta.
- **Aperte**. In una criptovaluta non vi è (di solito) nessun livello di controllo e nessuna autorità centrale incaricata di decidere cosa sia possibile fare. Tutti

sono liberi di innovare.

- **Neutrali**. Una criptovaluta non discrimina in base al mittente, al destinatario o all'oggetto della transazione. È un sistema privo di censura. È possibile trasferire l'equivalente di 1 dollaro o 100 milioni di dollari a chiunque, non fa nessuna differenza. Per esempio, la più grande transazione sul network del Bitcoin è stata di 150 milioni di dollari (500.000 BTC) effettuata nell'aprile 2015 senza pagare alcuna commissione[40] (Figura 7.4).

Figura 7.4 – La più grande transazione sul network del Bitcoin.

Politiche monetarie

La politica monetaria può essere vista come il processo che regola le dimensioni e il tasso di crescita monetaria, così come il suo modello di distribuzione. Nelle criptovalute la politica monetaria è decisa dal consenso del network.

Una criptovaluta ha solitamente un tasso di crescita definito

matematicamente. È possibile sapere con precisione quante monete esistono in ogni momento e in alcuni casi quante monete saranno presenti tra dieci anni.

Per ogni criptovaluta si possono definire i seguenti parametri:

- **Quantità totale (Total supply)**: quantità totale di monete che è già stata generata.
- **Quantità spendibile (Circulating supply)**: la quantità di monete in circolazione potenzialmente trasferibili, generalmente inferiore o uguale alla quantità totale. I principali scenari nei quali la quantità spendibile è inferiore alla

quantità totale sono:

- qualcuno ha perso le chiavi private di un indirizzo bloccando per sempre quelle monete;
- il creatore di una criptovaluta ha bloccato parte delle monete (che potrebbero essere rilasciate successivamente).

Le monete che non sono spendibili non dovrebbero influenzare la capitalizzazione di mercato di una criptovaluta (la capitalizzazione di mercato rappresenta il valore totale di tutte le monete in circolazione,

calcolata moltiplicando la quantità spendibile per il prezzo della singola moneta).

- **Quantità massima (max supply)**: la quantità di monete che potrà mai esistere per una particolare criptovaluta (è un parametro opzionale e non tutte le criptovalute hanno una quantità massima). Per esempio, la quantità massima nel Bitcoin è di 21 milioni di BTC, la quantità massima nel Litecoin è di 84 milioni di LTC. Questo numero è definito dal consenso del network e non può essere modificato da nessuno.

A seconda del fatto che una criptovaluta abbia o meno una quantità massima si può distinguere tra:

- **Quantità limitata:** il numero massimo di monete che esisteranno è fisso e noto in anticipo.
- **Quantità illimitata:** non esiste un limite al numero di monete che possono essere create (per esempio una criptovaluta che aumenta la quantità totale dell'1% ogni anno).

Modello di distribuzione

Le criptovalute possono essere distribuite in vari modi. Ognuno può infatti creare una propria criptovaluta e deciderne la politica monetaria e il modello di distribuzione. Attualmente i due modelli di distribuzione più diffusi sono: **mining** e **vendita diretta**. In base a questa distinzione si possono identificare due categorie: criptovalute **minabili** e criptovalute **non-minabili**.

Nelle criptovalute **minabili** vengono create nuove monete (fino al raggiungimento della eventuale quantità massima) ogni volta che un miner aggiunge con successo un nuovo blocco alla blockchain. La distribuzione di monete attraverso il mining garantisce un

modello di distribuzione decentralizzato, fornendo incentivi economici ai miner affinché continuino a creare blocchi. Il Bitcoin fa parte di questa categoria.

Le criptovalute **non-minabili** sono tutte le monete che vengono generate nel momento in cui una blockchain viene creata, le quali vengono poi vendute direttamente alle persone (per esempio Ripple con XRP).

---

39. http://money.visualcapitalist.com/all-of-the-worlds-money-and-markets-in-one-visualization/?link=mktw.
40. https://www.blockchain.com/btc/address/1M8s2

8

Bitcoin

> “Una versione puramente peer-to-peer
> di denaro elettronico consentirebbe di inviare
> i pagamenti online direttamente da una entità all’altra
> senza passare attraverso un istituto finanziario.”
>
> **—Satoshi Nakamoto**

Bitcoin è la prima criptovaluta a essere

stata creata. Il blocco genesi è stato minato il 3 gennaio 2009 e riportava il messaggio "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks[41]" ("Il cancelliere sull'orlo del secondo salvataggio delle banche", un riferimento alla crisi finanziaria di quel periodo). Il Bitcoin formalmente è stato creato nel 2008 con la pubblicazione di un documento, un cosiddetto whitepaper, firmato da Satoshi Nakamoto in cui viene presentata l'idea di una versione puramente peer-to-peer di denaro elettronico, che avrebbe consentito di effettuare trasferimenti diretti di valore da un'entità all'altra senza alcun istituto

finanziario coinvolto [7].

Satoshi Nakamoto è il nome usato dalla persona (o dalle persone) che ha creato il Bitcoin. La vera identità di Satoshi rimane sconosciuta.

Il Bitcoin per la prima volta ha dimostrato come fosse possibile risolvere il problema della doppia spesa nel digitale utilizzando una rete globale, senza confini, aperta, decentralizzata e soprattutto senza un'autorità centrale.

La convenzione nel Bitcoin

“Bitcoin” con la B maiuscola si riferisce all’intero ecosistema Bitcoin, che include:

- il network peer-to-peer decentralizzato;
- il ledger distribuito (la blockchain);
- il processo di mining, usato come modello di creazione e distribuzione di nuova valuta e sistema di reward per i miner;
- i protocolli di verifica decentralizzata della validità di transazioni e blocchi.

Invece “bitcoin” con la b minuscola fa riferimento alla criptovaluta identificata dal simbolo BTCTuttavia, non è sempre facile fare una divisione

netta tra i due termini.

Si può in generale utilizzarli entrambi e lasciare che sia il contesto a definire il significato.

Overview tecnica e politica monetaria

Il bitcoin è una criptovaluta minabile con un protocollo di consenso basato sul Proof of Work. Ogni volta che un nuovo blocco viene creato, il sistema genera anche una quantità definita di bitcoin che viene usata come ricompensa per il miner che crea il blocco.

I miner generano un nuovo blocco mediamente ogni 10 minuti, e ricevono una ricompensa in forma di bitcoin e commissioni di transazione.

Inizialmente il premio per la generazione di un blocco era di 50 BTC. Ogni 210.000 blocchi (210.000 × 10 min ≃ 4 anni) la ricompensa del blocco viene dimezzata (attualmente è 12,5 BTC, nel 2020 scenderà a 6,25 BTC) (Figura 3.5). La quantità massima di bitcoin (BTC) che potrà mai essere in circolazione è fissata a 21 milioni. L'inflazione nel Bitcoin è definita matematicamente. È quindi possibile conoscere la quantità di moneta circolante in ogni istante presente,

passato e futuro. Fino a oggi sono stati creati circa 17 milioni di bitcoin, su un totale di 21 milioni [12]. Ciò significa che il bitcoin raggiungerà asintoticamente la quantità massima intorno al 2140, quando la ricompensa del blocco sarà 1 satoshi (10^-8 BTC, unità bitcoin minima) (Figura 8.2).

Per questa particolare politica monetaria, il Bitcoin è quindi da molti definito un sistema deflazionario (riferito alla quantità circolante di una moneta, non al suo valore). Una volta che il bitcoin avrà raggiunto la quantità massima, l'inflazione diventerà zero e i miner guadagneranno solo dalle commissioni sulle transazioni. È tuttavia molto difficile prevedere cosa accadrà

avvicinandosi a questo evento, poiché attualmente la ricompensa dei blocchi è una parte fondamentale del meccanismo su cui è costruito il sistema cripto-economico del Bitcoin.

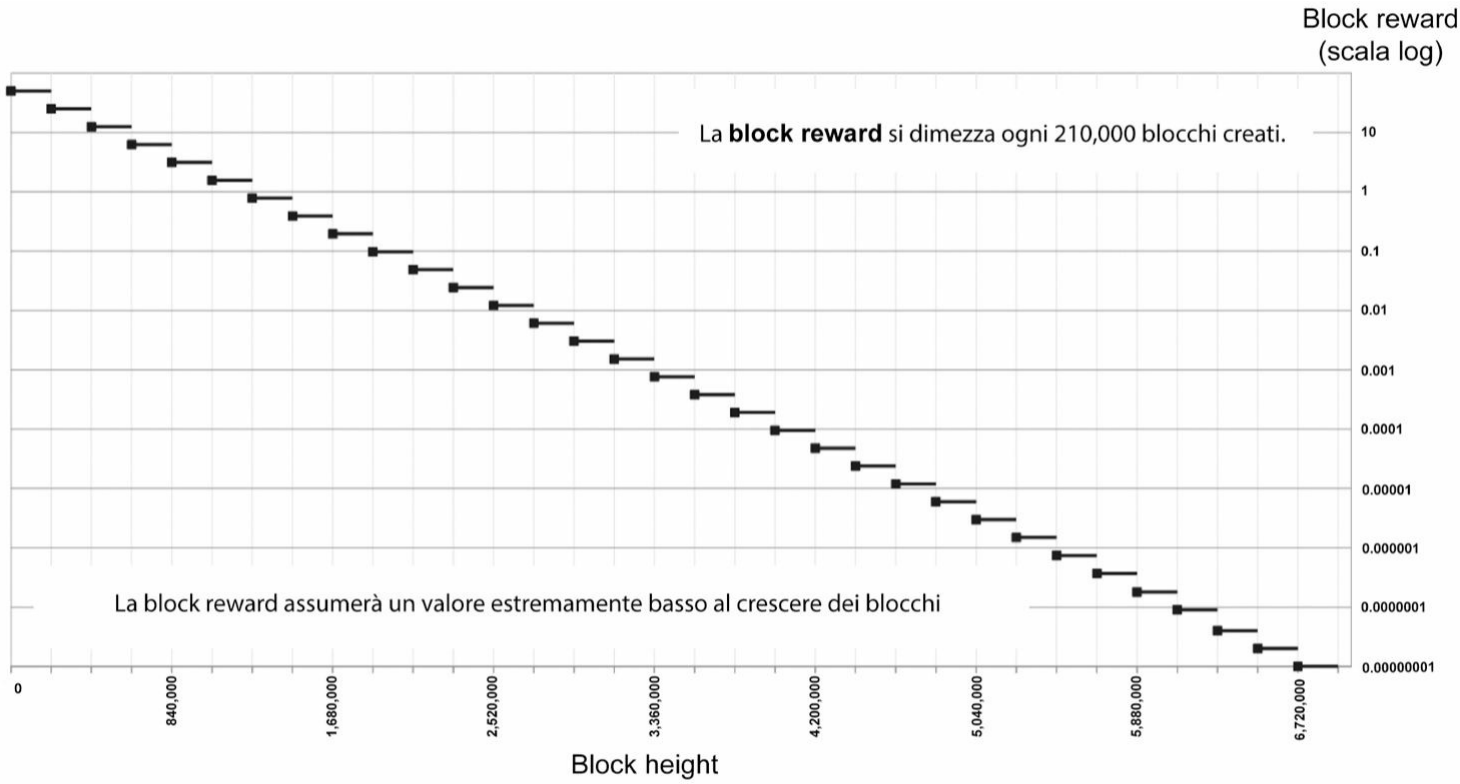


Figura 8.1 – Dimezzamento dei bitcoin generati con ogni nuovo blocco al passare del tempo, in scala logaritmica (bitcoin.it/wiki).

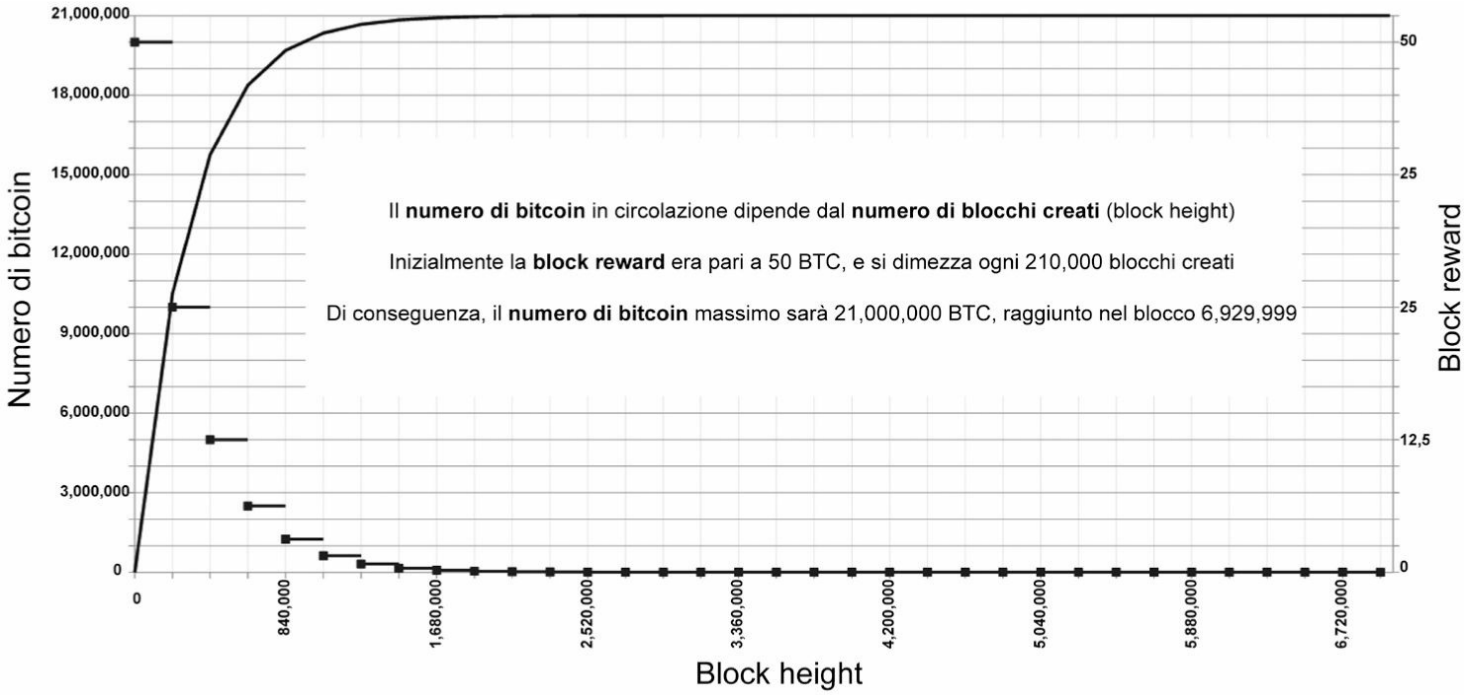


Figura 8.2 – Numero di bitcoin in circolazione al passare del tempo (bitcoin.it/wiki).

Blockchain e Bitcoin

In questo paragrafo riprendiamo alcuni dei concetti presentati nei primi capitoli e vedremo una loro applicazione concreta nella blockchain del Bitcoin.

Come già detto in precedenza, una

blockchain è una struttura dati composta da diversi blocchi. Ogni blocco è identificato da un hash e contiene un riferimento all'hash del blocco precedente. La funzione di hash usata dal Bitcoin è SHA-256. Un blocco è composto principalmente da due elementi: un **block header** (intestazione del blocco) e le **transazioni** in esso incluse.

Il block header contiene (Figura 8.3):

- un riferimento al blocco precedente (hash link);
- un timestamp che segna l'istante di creazione del blocco;

- il nonce usato nella Proof of Work del blocco (vedi Capitolo 5);
- la difficoltà della Proof of Work del blocco (vedi Capitolo 5);
- il Merkle root, un singolo hash che riassume tutte le transazioni, creato utilizzando un Merkle tree (che esploreremo nel prossimo paragrafo).

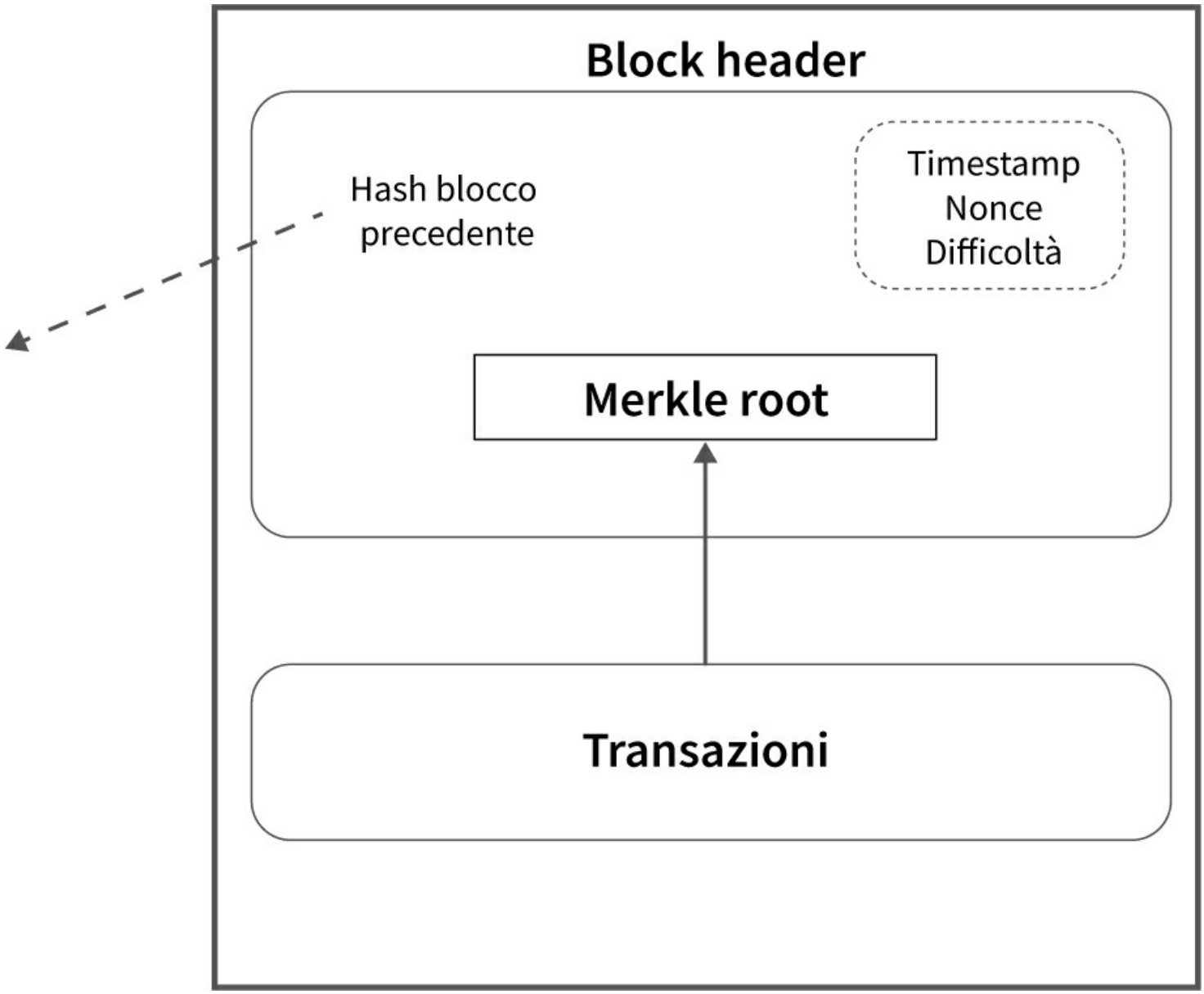


Figura 8.3 – La struttura di un blocco nella blockchain del Bitcoin.

Nel Bitcoin, l'hash univoco di ogni blocco si ottiene applicando due volte la funzione SHA-256 all'header del

blocco. Tutti gli elementi contenuti nell'header sono già stati introdotti, con l'eccezione del Merkle tree, un componente fondamentale per il funzionamento del Bitcoin e di molte altre blockchain.

Merkle tree

Un Merkle tree (da Ralph Merkle, che l'ha brevettato nel 1979) è una **struttura dati ad albero** usata per verificare in maniera efficiente e sicura grandi quantità di dati. I Merkle tree sono utilizzati in diverse applicazioni, in particolare nei sistemi peer-to-peer[42], o in scenari dove è richiesta una duplicazione dei dati su più nodi del

network. Il loro utilizzo nella blockchain del Bitcoin è stato introdotto da Satoshi Nakamoto nel suo whitepaper.

Albero (tree)

Un albero è una struttura dati utilizzata per esprimere informazioni in relazione gerarchica tra loro (Figura 8.4).

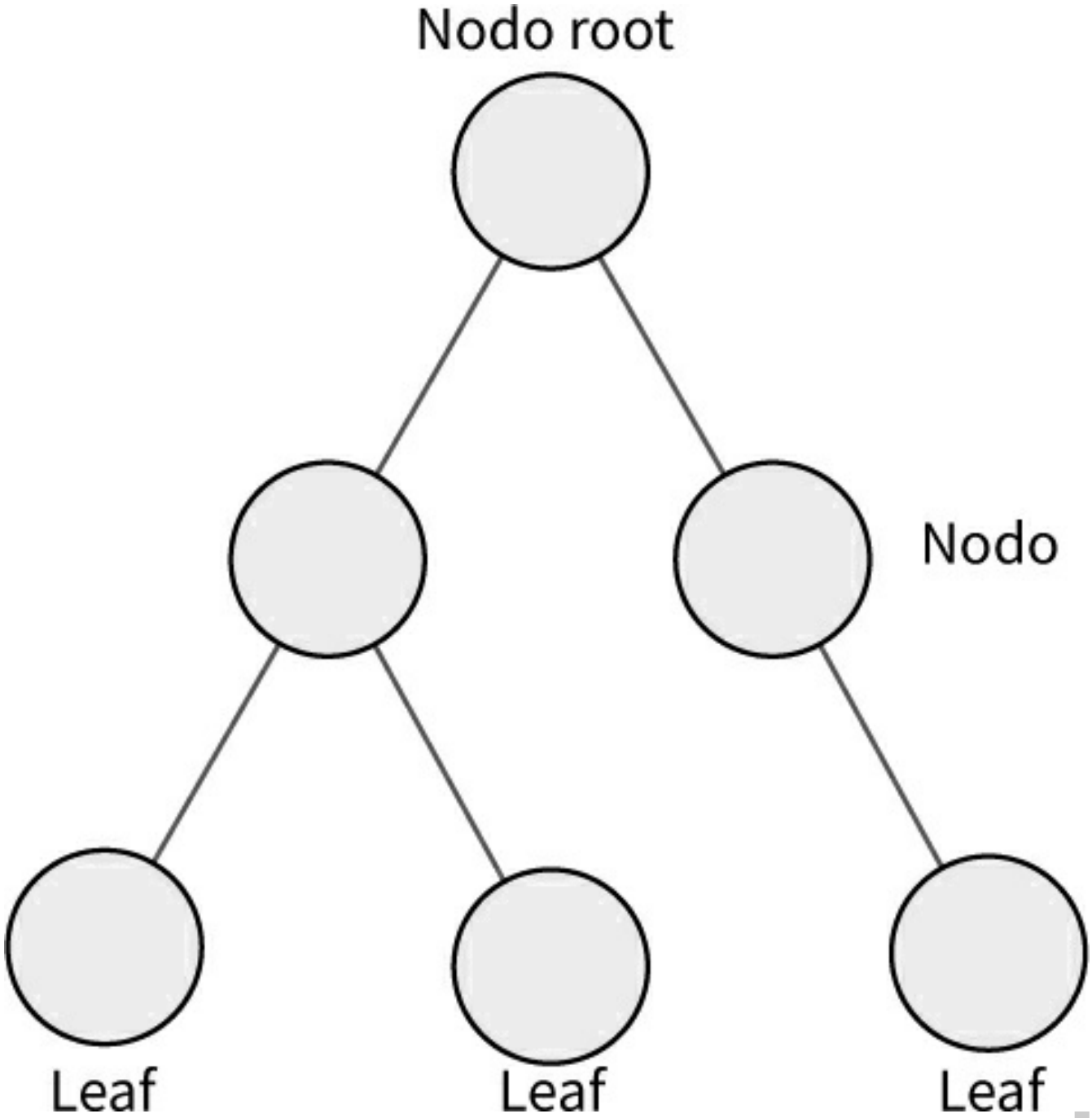


Figura 8.4 – La struttura di un albero.

Un albero è composto da diversi nodi distribuiti su più livelli. Ogni nodo contiene delle informazioni e può

avere uno o più **child node** (nodi figli). Il nodo in cima alla struttura è chiamato **root node** (nodo radice), mentre i nodi all'estremità inferiore (senza child node) sono chiamati **leaf** (foglie).

I Merkle tree sono degli alberi dove ogni nodo contiene un hash. Il valore di questo hash viene calcolato a partire dall'hash dei suoi child node. Le foglie infine contengono gli hash dei dati (Figura 8.5).

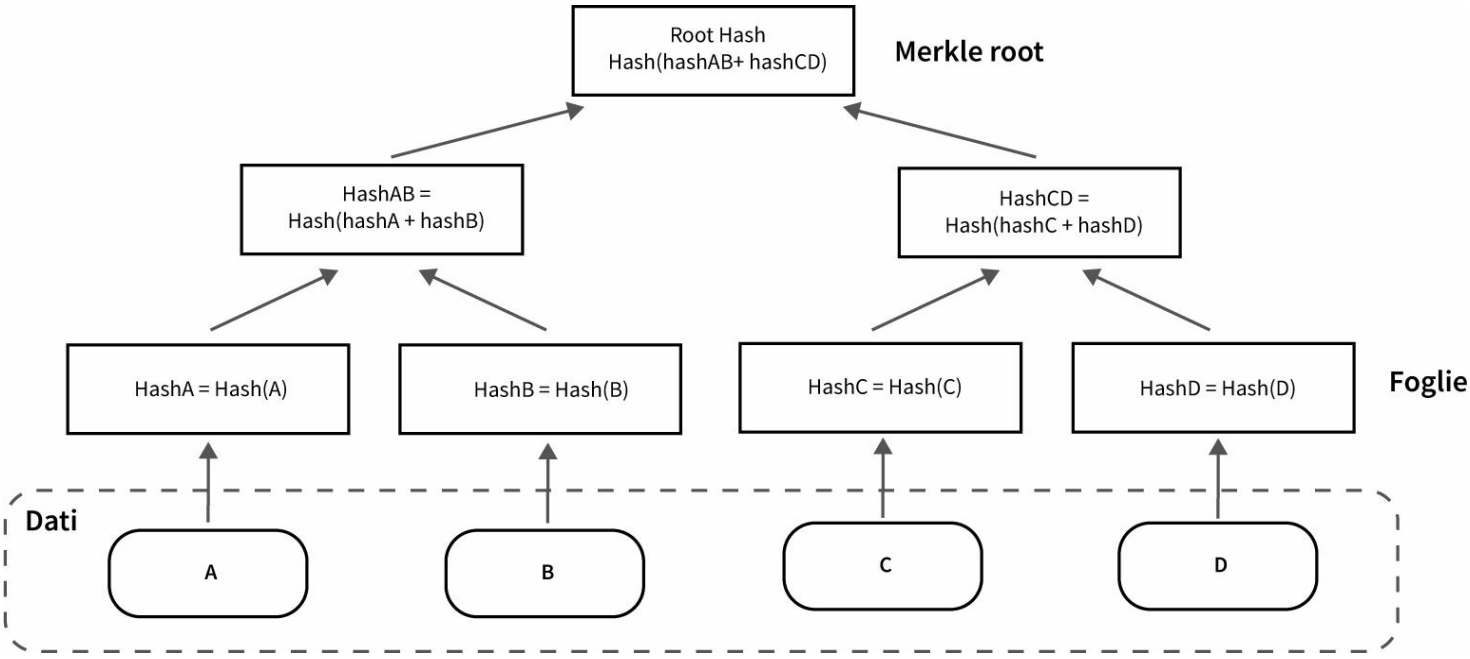


Figura 8.5 – Un esempio di Merkle tree.

Nel Bitcoin ogni foglia rappresenta l'hash di una transazione. Lo scopo del Merkle tree è quello di riassumere tutte le transazioni contenute in un blocco in un singolo hash (Merkle root) che può essere visto come l'impronta digitale delle transazioni.

Una volta che il Merkle tree è stato costruito, diventa possibile verificare

che una transazione sia effettivamente contenuta in un blocco in maniera efficiente[43], un processo anche noto come **Merkle proof** (o Merkle path).

Oggi un blocco nel Bitcoin contiene circa 1.000-2.000 transazioni. Per calcolare la Merkle proof di una transazione basta calcolare il percorso che connette la transazione alla cima dell'albero.

Per le proprietà degli hash, la modifica di una transazione comporta la modifica della Merkle root, rendendola subito evidente (Figura 8.6).

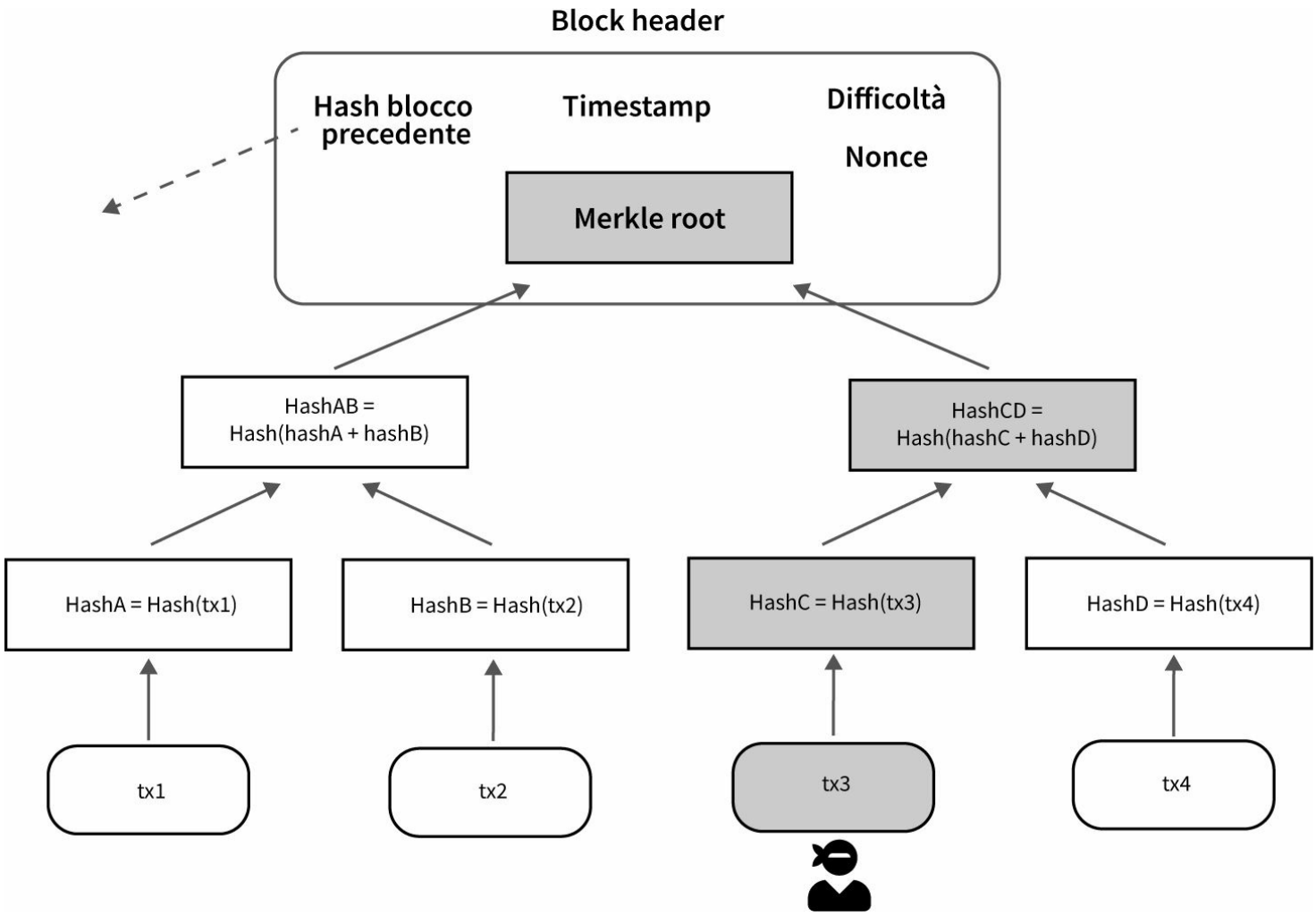


Figura 8.6 – La modifica di una transazione in un Merkle tree.

Scarsità

Il bitcoin come molte altre criptovalute, è una risorsa digitale artificialmente scarsa. Per questa ragione qualcuno

afferma che il bitcoin potrebbe essere considerato come una versione digitale dell'oro, ovvero una versione migliorata dell'oro reale.

Ogni Bitcoin può essere diviso in 100 milioni di unità più piccole chiamate **satoshi** (da Satoshi Nakamoto), quindi, analogamente all'euro, composto da 100 centesimi, il biticoin è composto da 100 milioni di satoshi.

Mining

Nel Bitcoin il mining utilizza il Proof of Work che si basa sulla risoluzione di un problema complesso per il quale è

necessaria molta potenza computazionale. A causa della bassa probabilità di trovare un blocco, i miner hanno realizzato che era più conveniente raggrupparsi e suddividere il problema del mining in più parti, assegnando ciascuna parte a un miner differente.

Al momento la maggior parte del mining di Bitcoin è raggruppata in grandi mining pool (una cooperativa di miner che mette insieme la propria potenza di calcolo e divide i profitti), e le prime cinque mining pool controllano oltre il 50% dell'hashrate totale. Minare bitcoin per una persona comune è pressoché impossibile a causa della competizione delle mining pool e dell'elevato costo per una

configurazione di mining competitiva (macchine + elettricità).

Indirizzi e privacy

Bitcoin utilizza una blockchain pubblica (le transazioni sono accessibili e analizzabili da chiunque). È possibile quindi visionare tutte le transazioni in cui è stato coinvolto un indirizzo specifico. Tuttavia, l'indirizzo pubblico non fornisce alcuna informazione diretta sul proprietario di quell'indirizzo. Questo è considerato un modello pseudo-anonimo, il che significa che i fondi non sono legati a delle entità del mondo reale ma piuttosto a degli

indirizzi che sono pubblici ma allo stesso tempo anonimi[44].

Alcuni esempi famosi sono:

- **1A1zP1eP5QGefi2DMPTfTL5SLmv** uno degli indirizzi appartenenti (si ipotizza) a Satoshi Nakamoto in quanto contiene i primi 50 bitcoin minati (Figura 8.7).
- **1HB5XMLmzFVj8ALj6mfBsbifRoD** l'indirizzo del wallet per le donazioni a Wikileaks, contenente attualmente oltre 4.000 bitcoin. Wikileaks ha infatti iniziato ad accettare donazioni in bitcoin dopo che nel 2010 i maggiori istituti finanziari (tra cui Visa, Master-Card e

PayPal) hanno congelato l'accesso ai conti a esso collegati.

- **16ftSEQ4ctQFDtVZiUBusQUjRrGh** l'indirizzo del cold wallet bitcoin di Binance, che contiene attualmente 160.000 BTC.

Figura 8.7 – L'indirizzo contenente i primi 50 BTC creati.

Scalabilità

Il Bitcoin ha sollevato molte

preoccupazioni riguardo alla sua capacità di scalare. Il problema è diventato evidente alla fine del 2017, quando le transazioni potevano richiedere diverse ore prima di essere confermate e le spese di transazione avevano superato i 50 dollari.

Per ovviare a questo problema, il Bitcoin ha eseguito una soft fork dove è stata introdotta la SegWit e sta attualmente testando l'implementazione del Lightning Network. I problemi di scalabilità sono stati inoltre alla base della hard fork che ha portato alla nascita del Bitcoin Cash.

SegWit

SegWit (Segregated Witness) è un esempio particolare di soft fork proposto dal core team del Bitcoin (nel Bitcoin Improvement Proposal 141, BIP 141[45]). In questo momento il protocollo del Bitcoin impone che un blocco sia di dimensione inferiore a 1 MB. Qualsiasi blocco maggiore di 1 MB viene rifiutato dai nodi. SegWit ha ampliato le dimensioni del blocco rimanendo però una soft fork (aumentare le dimensioni di un blocco non è un cambiamento retrocompatibile, quindi a rigor di logica dovrebbe essere una hard fork).

Senza entrare nei dettagli tecnici, SegWit ha modificato la struttura del blocco aggiungendo un nuovo elemento

chiamato **witness** (testimone), che contiene al suo interno le informazioni necessarie per controllare la validità delle transazioni (come la firma digitale).

Grazie a questa divisione viene liberato spazio nel resto del blocco. Infatti, mentre a un byte normale viene assegnato un peso di 4, i byte della witness hanno peso 1.

Concretamente, significa che lo spazio effettivo di un blocco passa da 1 MB a quasi 4 MB, senza però aumentarne la dimensione nominale, rimanendo così una soft fork.

Sebbene l'aumento della dimensione del blocco sia una conseguenza

importante, la vera rivoluzione della SegWit è stata l'introduzione della possibilità di creare **transazioni malleabili**[46], fondamentali per eseguire transazioni **off-chain** come richiesto per esempio dal Lightning Network.

Lightning network

Il Lightning Network è un sistema che consente di inviare e ricevere istantaneamente pagamenti, riducendo allo stesso tempo i costi delle transazioni.

Il Lightning Network è un protocollo di pagamento di secondo livello (proposto per la prima volta nel 2015)

costruito sulla base di una blockchain, e costituito da una rete di canali di pagamento bidirezionali tra gli utenti.

Il risultato finale è quello di gestire una serie di transazioni sul secondo livello off-chain e registrare solo il saldo finale sulla blockchain in un secondo momento, attraverso una singola transazione nel momento in cui il canale viene chiuso. Ne consegue che una blockchain che sfrutta il protocollo Lightning Network è in grado di effettuare transazioni istantaneamente e allo stesso tempo di ridurre drasticamente il carico di lavoro a cui la blockchain è sottoposta (Figura 8.8).

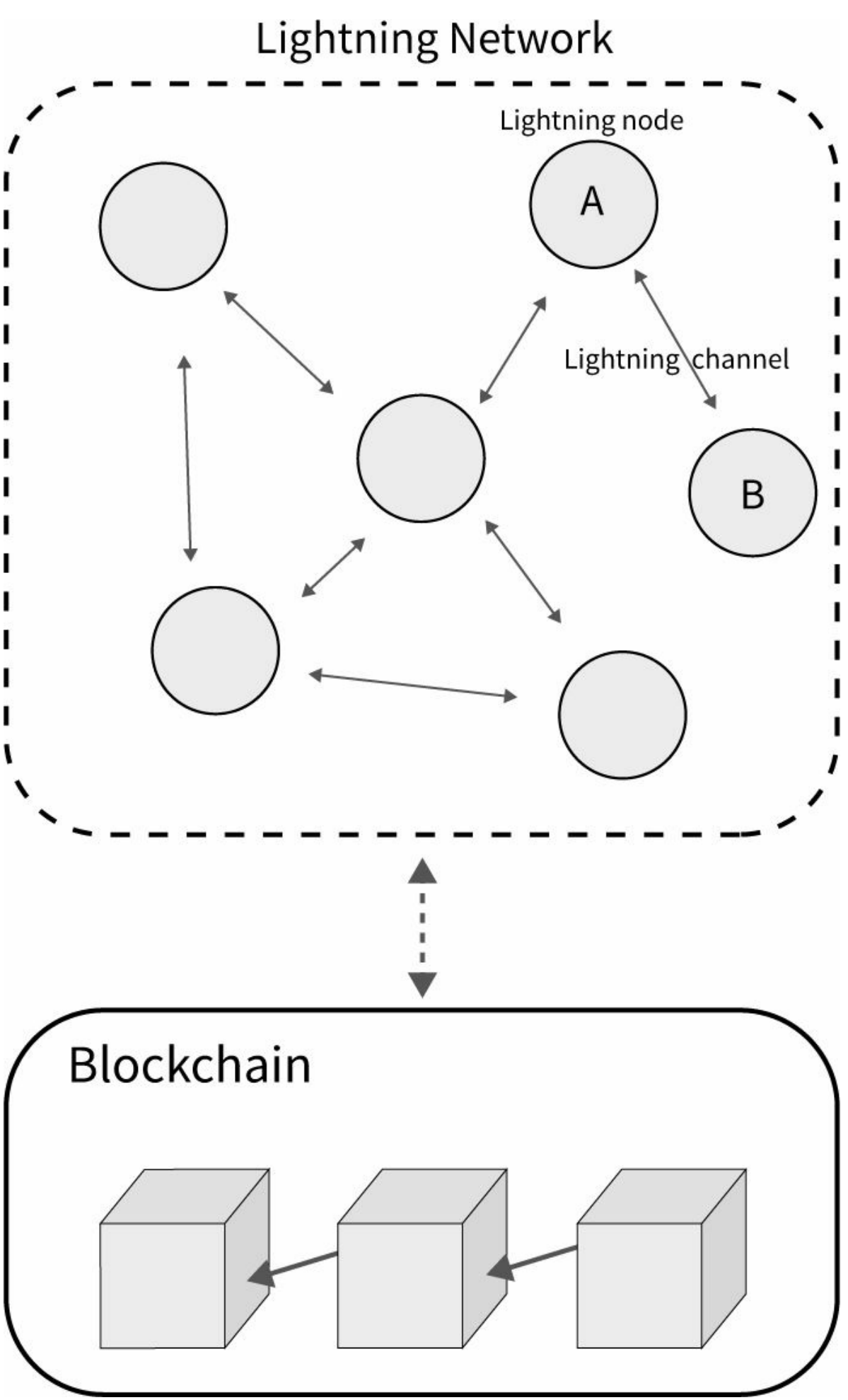

Lightning Network
Lightning node
A
Lightning channel
B
Blockchain

Figura 8.8 – Il Lightning Network.

Ogni canale è composto da un indirizzo multisignature creato da due utenti. Ogni utente aggiunge nell'indirizzo l'importo che intende utilizzare. Una volta creato questo canale, diventa per loro possibile effettuare tutte le transazioni che vogliono senza dover salvare ogni transazione sulla blockchain.

Il processo può essere riassunto in questi tre passaggi:

1. Due utenti (Alice e Marco) creano un indirizzo multisignature con la quantità di denaro che intendono utilizzare (per esempio, 1 BTC ciascuno).

Questo indirizzo diventa un contratto tra i due utenti e ha lo scopo di registrare l'ammontare posseduto da ciascuna parte dopo ogni transazione.

2. Il contratto viene salvato sulla blockchain e il canale di pagamento viene aperto (Figura 8.9).

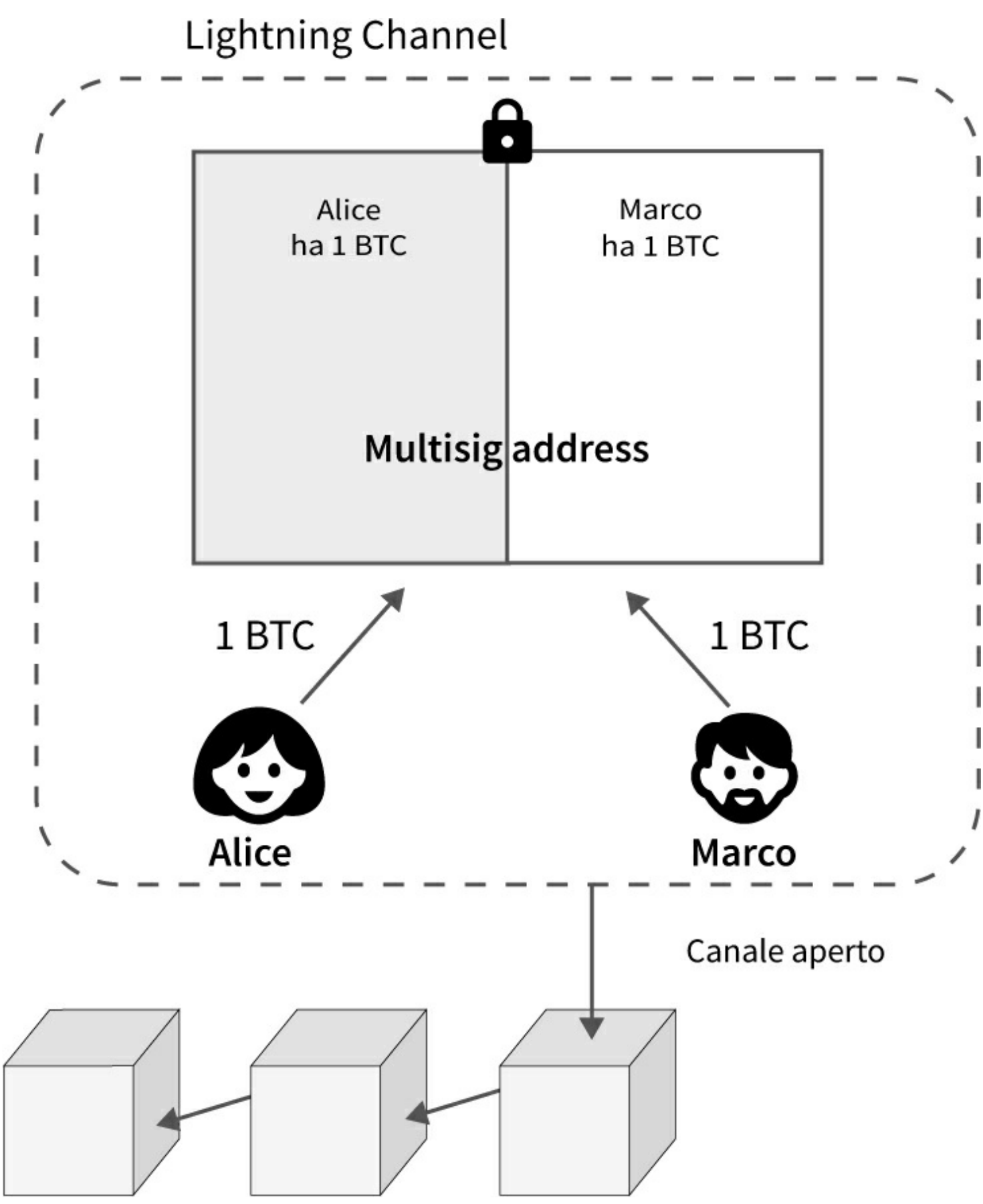


Figura 8.9 – L'apertura di un Lightning

Channel.

3. Da questo momento Alice e Marco possono effettuare transazioni tra loro istantaneamente, senza dover registrare le transazioni sulla blockchain. Tutto viene gestito all'interno del contratto, usando delle promesse concettualmente simili ai contratti IOU (I Owe You), nei quali vengono annotati gli scambi di valore fra le parti da essere saldate in un secondo momento. Non è necessario fidarsi dell'altra parte, dal momento che il Lightning Network protegge

automaticamente dal rischio di controparte (il rischio che una delle parti non rispetti i vincoli del contratto). Questi contratti utilizzati dal Lightning Network sono a tutti gli effetti degli smart contract dove la blockchain diventa il giudice che garantisce il pieno rispetto del contratto (esploreremo gli smart contract nel prossimo capitolo) (Figura 8.10).

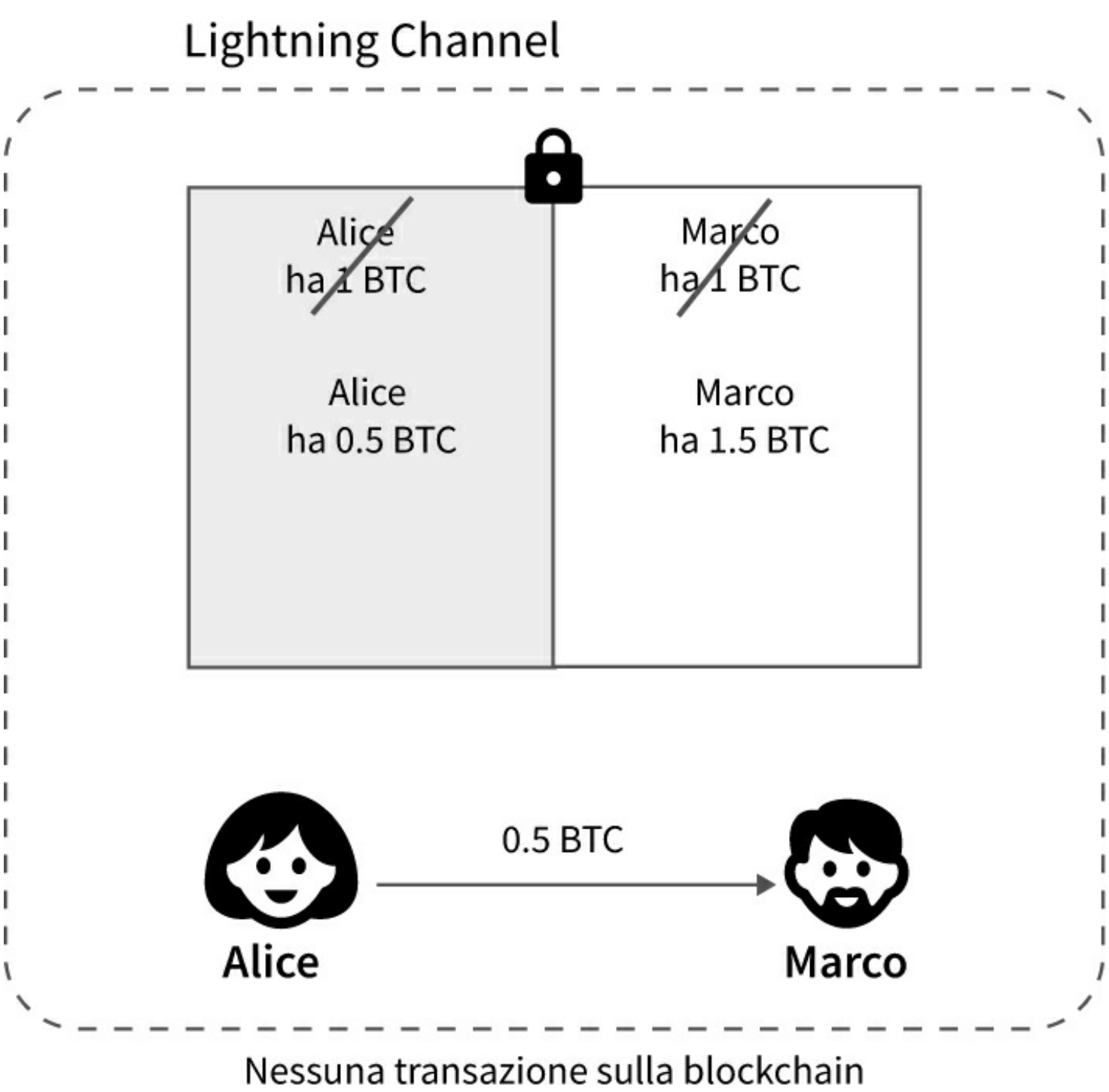


Figura 8.10 – L'aggiornamento del saldo su un Lightning Channel.

4. Quando uno degli utenti decide

di chiudere il canale, la blockchain risolve il contratto dando a ciascuna parte l'importo che gli spetta (Figura 8.11).

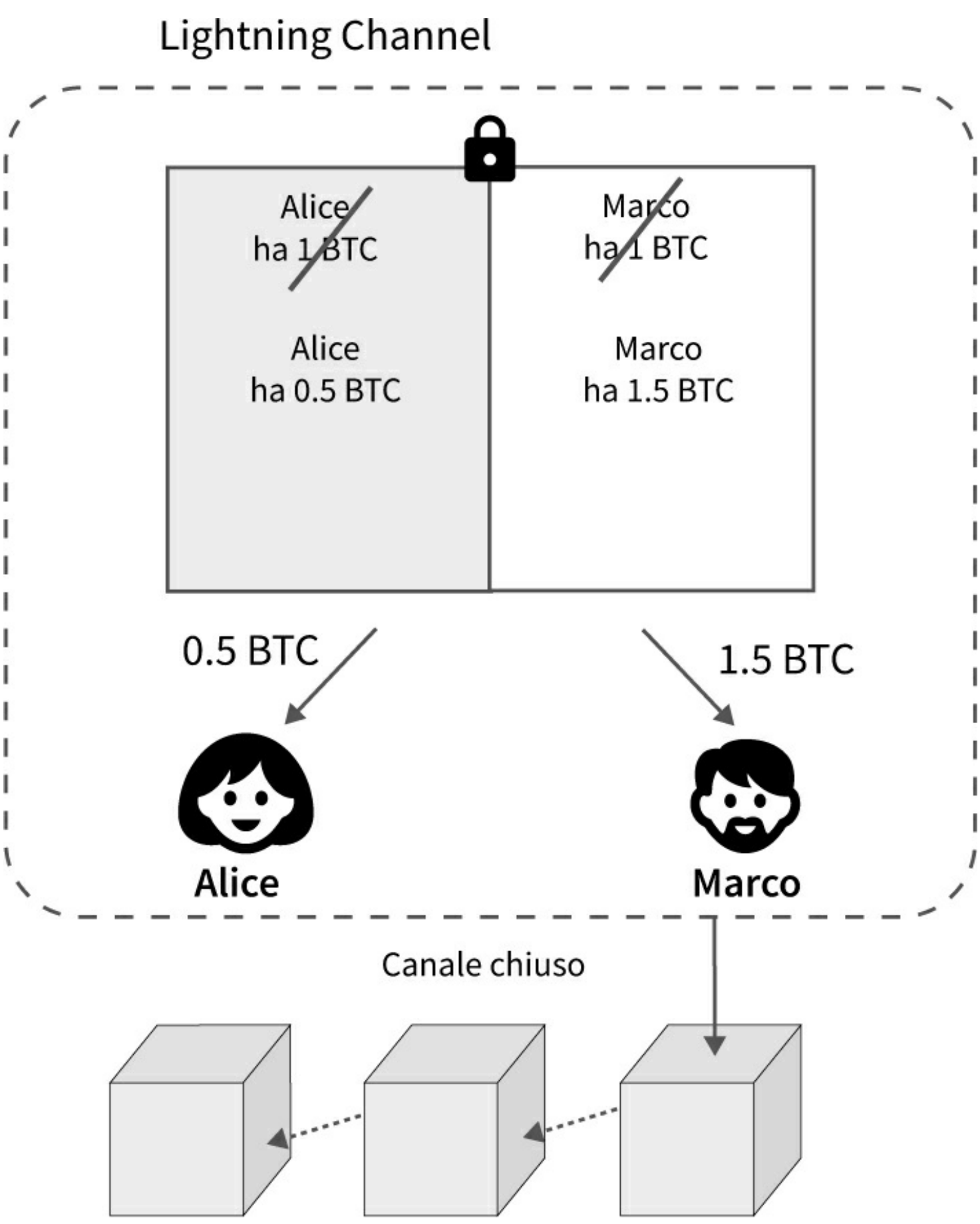


Figura 8.11 – La chiusura di un Lightning

Channel.

Rete di pagamenti

Aprire un canale ogni volta che un utente vuole effettuare una transazione non è una soluzione conveniente, dal momento che per aprire un canale è necessario effettuare comunque una transazione sulla blockchain. Ed è proprio questo il punto di forza del Lightning Network.

> Utilizzando il Lightning Network non è necessario aprire un canale diretto tra due parti se esiste già una percorso (indiretto) tra di

loro.

Se per esempio Alice desidera inviare denaro a Marco, non è necessario aprire un nuovo canale diretto tra loro, poiché molto probabilmente esiste già un percorso indiretto che li collega. Sfruttando le funzionalità di reindirizzamento della rete, diventa possibile instradare i pagamenti proprio come le informazioni sono instradate su Internet.

Se esiste più di un percorso, Alice può persino scegliere il percorso che preferisce, per esempio quello con la tariffa più bassa o quello più veloce (Figura 8.12).

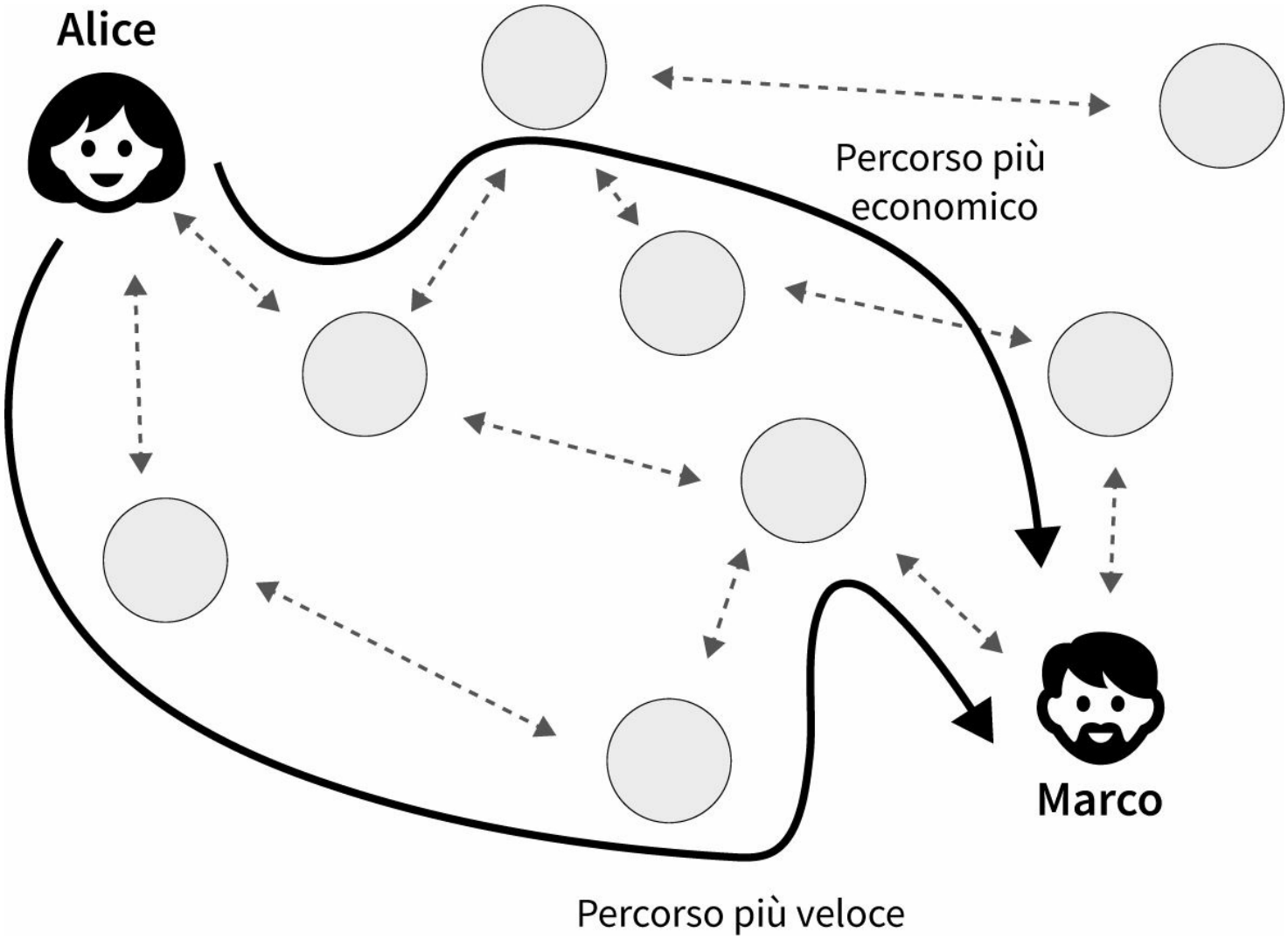


Figura 8.12 – La possibilità di scegliere il percorso nel Lightning Network.

Il Lightning Network è a tutti gli effetti un protocollo di instradamento di pagamenti.

Micro-pagamenti e pagamenti streaming

Un sistema in cui è possibile effettuare pagamenti istantanei, con (quasi) zero commissioni come il Lightning Network apre a un'ampia gamma di nuove possibili applicazioni. Potrà essere per esempio possibile per un'automobile pagare autonomamente l'assicurazione a ogni chilometro percorso, per un utente pagare per ogni kilobyte di un film visto in streaming, o per un dipendente essere pagato per ogni minuto di lavoro invece che a cadenza mensile.

Proprio come lo streaming dei dati è diventato una realtà grazie a Internet, lo streaming di denaro potrebbe diventare

una realtà grazie alla blockchain.

Il Bitcoin in sintesi

Nella Tabella 8.1 sono descritte le principali caratteristiche del Bitcoin.

Tabella 8.1 – Le caratteristiche principali del Bitcoin.

Creato da	Satoshi Nakamoto
Anno creazione	2008
Network live	2009
Protocollo di consenso	Proof of Work
Quantità massima	21 milioni
Quantità attuale (2018)	≃ 17 milioni
Modello blockchain	Pubblica
Tempo di blocco	10 minuti
Dimensioni di blocco	1 MB (4 MB con SegWit)

1 BTC	10^8 satoshi

Per un approfondimento sull'ecosistema Bitcoin, consigliamo i libri *Mastering Bitcoin* e *Internet of Money* di Andreas Antonopoulos [9, 13].

41. Per approfondire questo tema: https://www.thetimes03jan2009.com.
42. I Merkle tree sono una componente importante in protocolli come BitTorrent.
43. In tempo logaritmico $\log_2$(numero transazioni) invece che lineare.
44. È possibile esplorare tutti gli indirizzi

visitando blockchain.com.

45. https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki.

46. https://en.bitcoin.it/wiki/Transaction_malleabili

9

Smart contract

Che cos'è uno smart contract

Il termine smart contract è stato proposto per la prima volta da Nick Szabo nel 1994 e definito come "un protocollo di transazione digitale che esegue i termini di un contratto" [14]. L'obiettivo di uno smart contract è quello di soddisfare le condizioni contrattuali in maniera

automatica minimizzando la possibilità di azioni malevole e il bisogno di fiducia negli intermediari (rischio di controparte). Gli intermediari, infatti, soprattutto nella forma di autorità centralizzate, hanno la tendenza a essere inefficienti, lenti e costosi.

Un contratto è un accordo tra due o più parti applicabile come vincolo legale. I contratti sono essenziali per creare fiducia tra le parti coinvolte in una transazione e possono essere considerati gli elementi costitutivi di ogni business. Un contratto può

essere semplice, come un biglietto dell'autobus, o più complesso, come un contratto di lavoro.

Le criptovalute come mezzo di scambio e in generale i protocolli di scambio di denaro digitale sono degli esempi basilari di smart contract. Esempi più complessi possono essere l'applicazione di smart contract al concetto di proprietà di beni fisici o astratti (smart property) o al concetto di identità (smart identity), che esploreremo in seguito.

L'idea di smart contract si sposa perfettamente con le proprietà della

blockchain, fornendo un ecosistema dove la fiducia è intrinseca al sistema stesso.

Solitamente, quando si parla di smart contract, si fa riferimento all'implementazione di questi concetti utilizzando la tecnologia blockchain.

Nel contesto delle blockchain, uno smart contract è un termine che si riferisce a un programma generico in grado di avere tutte le caratteristiche di un contratto del mondo reale, ma che viene salvato ed eseguito all'interno di una blockchain. L'accordo non è vincolato dalla legge, ma dal contratto stesso attraverso il consenso del network.

Gli smart contract sono scritti in un

linguaggio di programmazione, quindi sono privi di ambiguità, e contengono tutta la logica necessaria al loro interno. Non è necessario inoltre che un'autorità esterna valuti le condizioni e prenda decisioni, poiché questo ruolo è sostituito dal consenso del network.

Gli smart contract definiscono le regole e automaticamente impongono alle parti coinvolte di rispettarle, in modo decentralizzato, senza la necessità di affidarsi ad autorità centrali. Nel momento in cui le condizioni del contratto vengono soddisfatte, lo smart contract esegue autonomamente delle azioni specifiche, per esempio trasferire denaro o la proprietà di un bene.

Uno smart contract può essere visto come un'applicazione IFTTT (If This Then That) che reagisce a determinati eventi, solitamente sotto forma di transazioni (Figura 9.1).

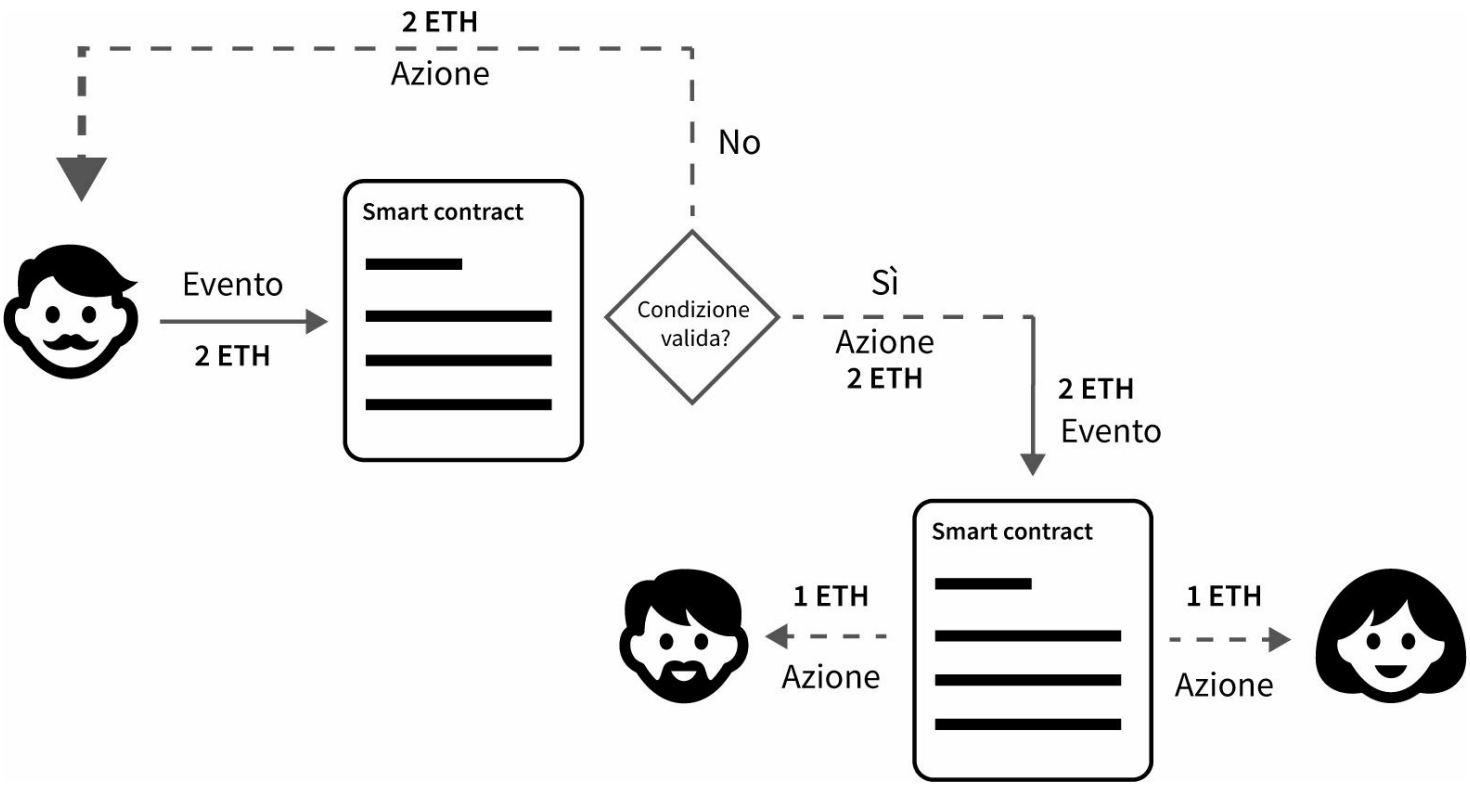


Figura 9.1 – Il processo IFTTT (If This Then That) negli smart contract.

Esempi di smart contract

Uno smart contract mira ad automatizzare gli scenari che richiedono

una qualche forma di azione contrattuale tra parti non fidate.

Di seguito vi presentiamo alcuni esempi che potrebbero spiegare meglio dei possibili casi d'uso.

Crowdfunding

Supponiamo di voler creare un clone di Kickstarter (la famosa applicazione di crowdfunding, www.kickstarter.com) usando degli smart contract.

Un utente pubblica un progetto, stabilisce l'obiettivo (la quantità di denaro di cui ha bisogno) e un tempo limite per raggiungerlo. Lo smart contract, in questo caso, potrebbe essere

utilizzato per eliminare gli intermediari e rendere trasparente il processo di raccolta fondi.

Tutti gli investitori potranno partecipare al progetto mandando le criptovalute allo smart contract, le quali verranno trattenute fino al completamento della campagna. Similmente, il creatore della campagna non potrà ritirarle fino a che non sarà conclusa (Figura 9.2).

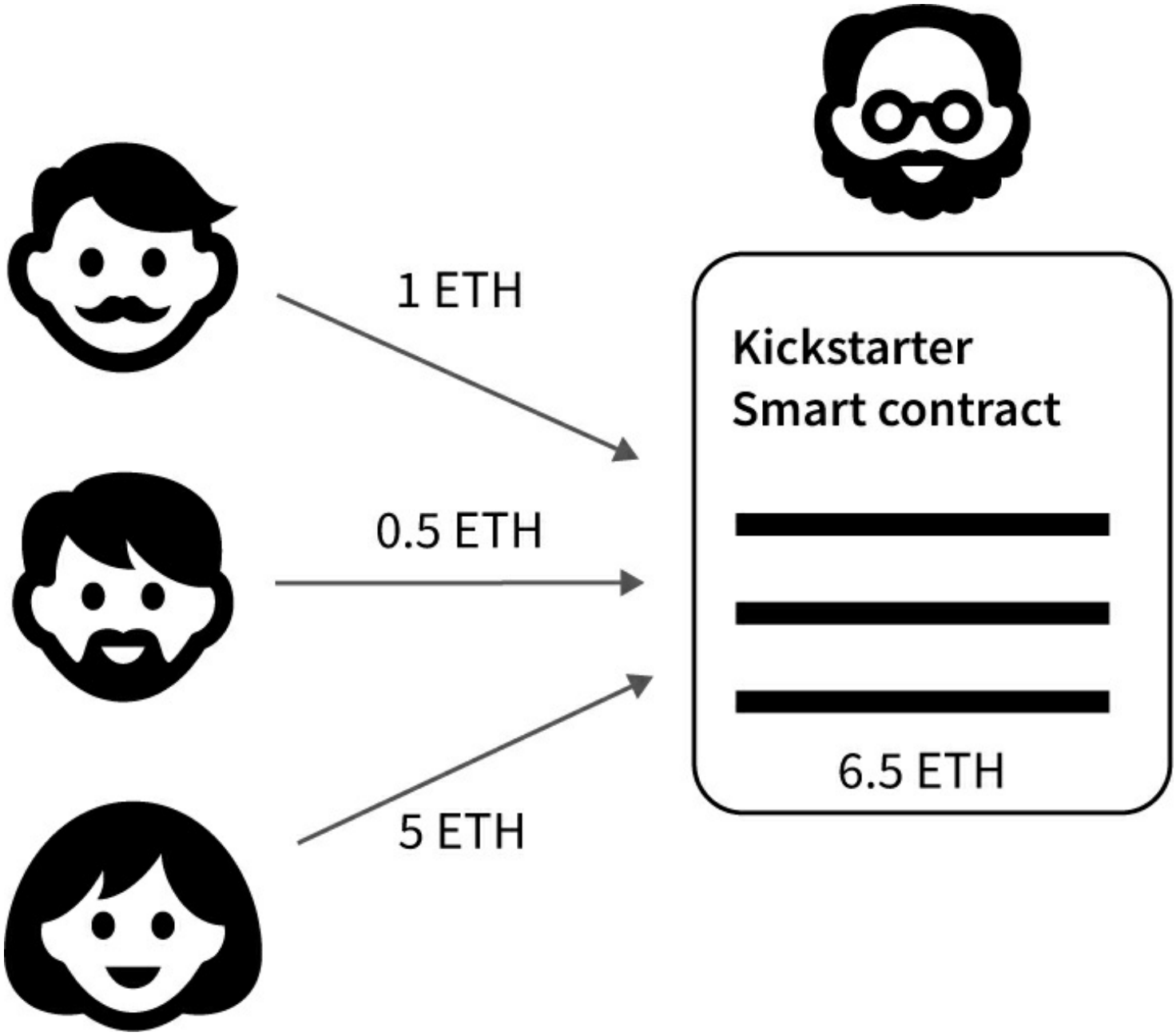


Figura 9.2 – L'invio di criptovalute a uno smart contract.

Se alla chiusura della campagna i requisiti del progetto sono soddisfatti

(l'obiettivo iniziale è raggiunto entro il tempo stabilito), il contratto sblocca automaticamente i fondi e li trasferisce al creatore del progetto. In caso contrario, i soldi raccolti vengono restituiti ai donatori (Figura 9.3).

Con uno smart contract non è necessario che una terza parte garantisca che i soldi vengano effettivamente inviati o restituiti, dal momento che la logica del processo è inclusa nel contratto stesso.

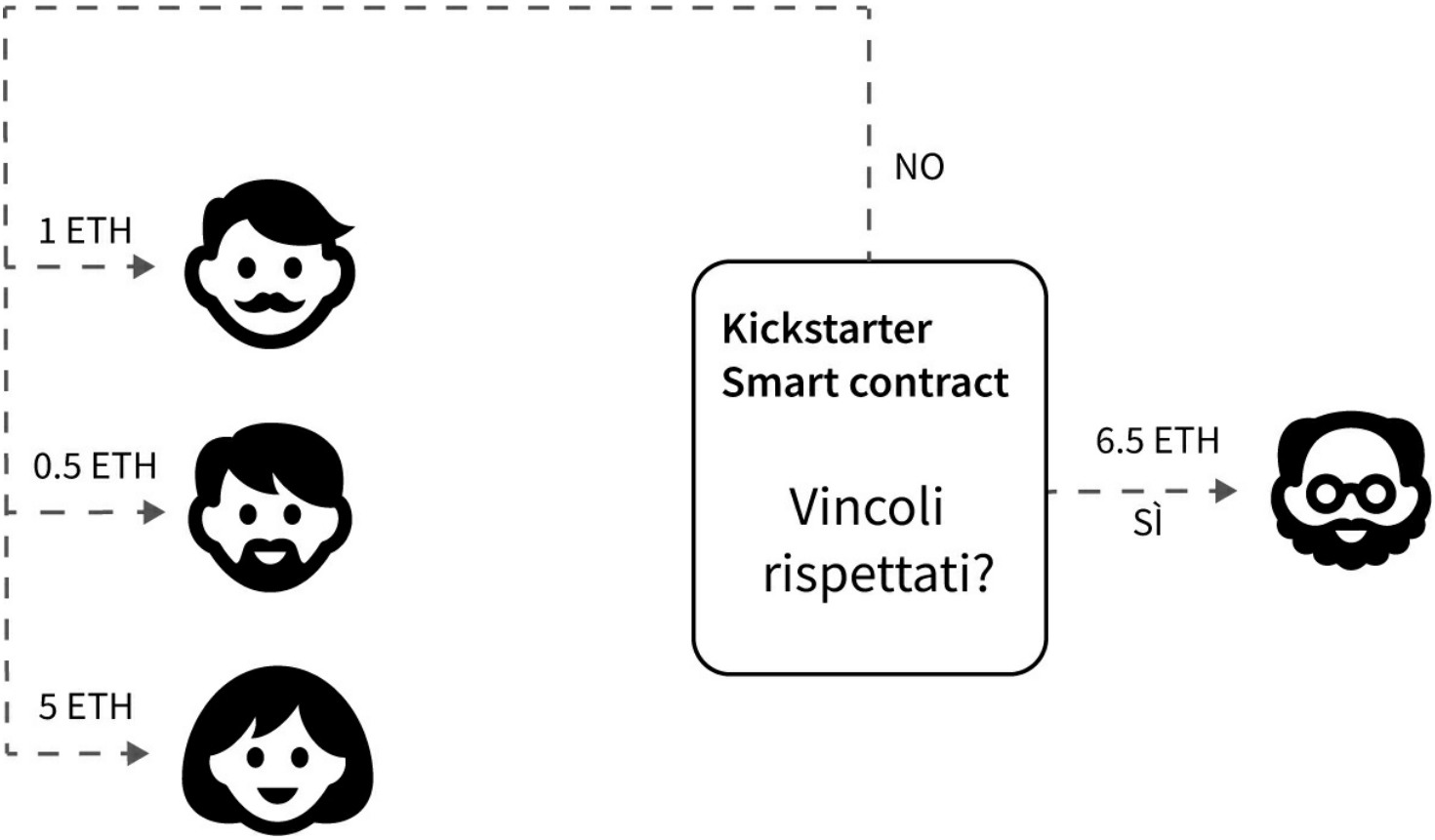


Figura 9.3 – Lo smart contract regola la consegna/restituzione dei fondi.

Consegna a domicilio

Un altro esempio potrebbe essere la consegna di cibo a domicilio. Si può creare uno smart contract che garantisca uno sconto sul prezzo del cibo in base al

tempo che è stato necessario per la consegna. Per esempio, se la consegna richiede:

- meno di 30 minuti: prezzo pieno;
- tra 30 e 45 minuti: sconto del 20%;
- più di 45 minuti: sconto del 30%.

Queste tre condizioni verrebbero salvate all'interno dello smart contract insieme a un timestamp (marca temporale) che identifica il momento in cui è stato effettuato l'ordine. Quando un cliente effettua l'ordine, l'intero importo viene bloccato all'interno dello smart contract e, una volta completata la consegna,

viene stabilito il prezzo effettivo da pagare in base al tempo impiegato per la consegna secondo le regole del contratto. Il tutto in maniera trasparente e automatica.

Token

In questo paragrafo approfondiremo il discorso introdotto nel Capitolo 7 riguardo le differenze tra moneta (coin) e token.

Una criptovaluta intesa come moneta (coin) può essere vista come un oggetto digitale il cui unico scopo è quello di trasferire valore. Quando si parla di

BTC (bitcoin), LTC (litecoin) o XMR (monero), solitamente si usa il termine moneta (coin) per sottolineare la loro funzione di mezzo di scambio di valore.

Se aggiungiamo le potenzialità di uno smart contract a una criptomoneta possiamo creare delle criptovalute con funzionalità che vanno oltre il semplice trasferimento di valore. In questo caso solitamente si parla di token.

> Nell'ambito della blockchain, gli smart contract sono strettamente collegati al concetto di token. I token rappresentano una risorsa che esiste all'interno di una

blockchain.

Questa risorsa può essere qualsiasi cosa, da un semplice mezzo di scambio di denaro alle quote di una società, ai diritti di utilizzo di un servizio, ai diritti di voto ecc.

A seconda delle modalità di utilizzo, i token si possono dividere in due categorie:

- **Utility token.** Sono dei token che forniscono esclusivamente un **diritto di accesso a un servizio.** Un utility token non è pensato per essere un investimento. Il suo valore è

collegato direttamente a domanda e offerta.

Riprendendo l'esempio precedente del clone di Kickstarter, in situazioni analoghe si usa creare un apposito utility token per finanziare il progetto, il quale conferisce l'accesso alle funzionalità della piattaforma che si intende sviluppare (parliamo in questo caso di ICO).

- **Security token.** Una security è un asset finanziario negoziabile. Non ci sono attualmente dei parametri chiari che definiscono

le caratteristiche di un security token, sebbene la Sec (U.S Securities and Exchange Commission) stia lavorando su una regolamentazione [15].

Attualmente ci sono delle linee guida che servono a stimare quanto è probabile che un determinato token rientri nella categoria delle security. Tra queste troviamo la distribuzione dei dividendi ai possessori dei token, oppure il collegamento a un asset (equity) societario, come per esempio delle quote societarie.

A seconda della categoria in cui rientra, un token è soggetto a diverse regolamentazioni, anche se a oggi la

situazione è tutt'altro che chiara e mancano ancora delle linee guida condivise. Questa suddivisione in tipologie di token è estremamente importante nel contesto delle ICO.

ICO

Una ICO (Initial Coin Offering) è una tipologia di raccolta fondi usata per finanziare progetti in ambito blockchain. Sebbene il nome ICO rimandi al concetto di IPO (Initial Public Offering, il processo di quotazione in borsa di una società), una ICO si avvicina molto di più al concetto di crowdsale,

l'equivalente in ambito cryptocurrency del crowdfunding.

Le ICO sono diventate estremamente popolari nel 2017, in seguito all'esplosione di interesse nelle criptovalute, portando alcuni progetti come Filecoin e Tezos a raccogliere le cifre record di rispettivamente 257 e 232 milioni di dollari [16]. Poco dopo, nel corso del 2018, EOS [17] ha raccolto 4 miliardi di dollari.

Se nel 2017 ci sono state 552 ICO che hanno raccolto un totale di 7 miliardi di dollari, solo nella prima metà del 2018 ne sono state lanciate 537, con un valore totale raccolto che supera i 13,7 miliardi di dollari. Il volume delle ICO è quindi

essenzialmente raddoppiato [18].

In numerosi casi le ICO sono state estremamente profittevoli per gli investitori, ma la maggioranza di esse fallisce pochi mesi dopo la fine della raccolta fondi [19]. Inoltre, viene stimato che nel 2017 il 20% delle ICO fosse basato su progetti "scam", ovvero per raccogliere soldi per progetti che non sarebbero mai stati fatti [20].

È quindi di fondamentale importanza approfondire sempre le ICO nel dettaglio e accertarsi della loro affidabilità, prima di investirci sopra del denaro. A tal proposito la Sec, l'organo incaricato della loro regolamentazione negli Usa, ha persino

creato un modello di ICO “scam” per rendere evidenti i principali campanelli d’allarme a cui prestare attenzione [21].

Struttura di una ICO

> Una ICO consiste nella vendita di un token in cambio di altre criptovalute (come ETH) o di denaro fiat, con lo scopo di finanziare un progetto in ambito blockchain.

Una delle caratteristiche di una ICO è quella di affidarsi a uno smart contract per gestire l’intero processo di vendita

dei token. È quindi necessario utilizzare piattaforme che supportino l'esecuzione di smart contract, come Ethereum, NEO o EOS. Ethereum domina il mercato delle ICO dal momento che più dell'80% dei progetti utilizzano questa piattaforma (il dato è dell'ottobre 2018[47]).

Il meccanismo di una ICO è molto semplice e l'idea è simile a quella esposta precedentemente con l'esempio di Kickstarter:

1. Una società vuole creare un nuovo progetto su blockchain e per raccogliere i fondi decide di avviare una campagna ICO.

2. La società crea quindi uno smart

contract con un proprio token (solitamente un token ERC 20), stabilisce la quantità massima di token vendibili (**hard cap**), la quantità minima di token per iniziare il progetto (**soft cap**), il prezzo di vendita del token, la durata della ICO, le forme di pagamento accettate (ETH, BTC, fiat) e le modalità di vendita.

3. A volte la ICO viene preceduta da una vendita privata (private sale) in modo da raccogliere fondi per finanziare le spese della ICO, come per esempio quelle per le campagne

pubblicitarie.

4. Una volta lanciata la ICO, gli investitori trasferiscono gli ETH (o qualsiasi altra valuta accettata) all'indirizzo dello smart contract che gestisce la crowdsale. Lo smart contract restituisce in maniera automatica i token agli investitori (Figura 9.4).

5. Una ICO finisce allo scadere del tempo prefissato oppure una volta raggiunto l'hard cap. Se alla fine della crowdsale non è stato raggiunto il soft cap, può essere che il progetto non parta (in questo caso i fondi raccolti

dovrebbero essere restituiti agli investitori) oppure subisca ritardi. Se il soft cap è stato superato ma rimangono dei token invenduti, sta alla società decidere come gestire i token in eccesso (per esempio tramite la distruzione dei token invenduti – token burn).

6. Una volta conclusa positivamente la ICO, la società utilizza i soldi raccolti per sviluppare il progetto.

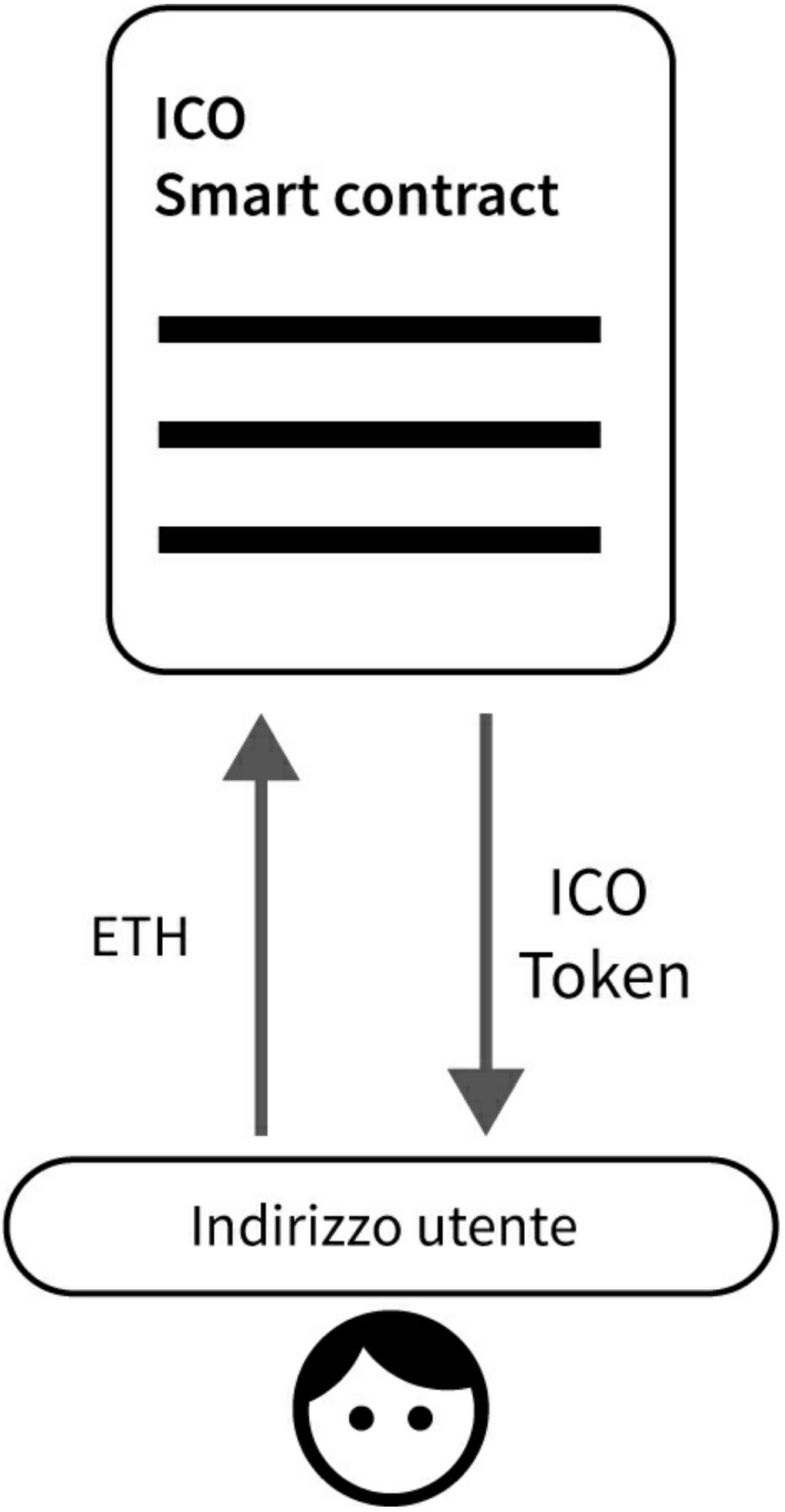

ICO
Smart contract
ETH
ICO
Token
Indirizzo utente

Figura 9.4 – Lo smart contract regola lo scambio di token in una ICO.

Il token in questione andrà a ricoprire un ruolo nel progetto che si sta cercando di finanziare. A seconda della sua funzione, si può distinguere tra utility token e security token, e la società che ha creato l'ICO dovrà quindi seguire le regolamentazioni della rispettiva categoria.

Perché avviare una ICO

I concetti alla base della ICO rispecchiano quelli di una blockchain, essendo una soluzione aperta, globale e

senza intermediari.

I motivi che possono spingere una società ad avviare una ICO sono molteplici. Ci possono essere motivi ideologici, come l'idea di creare un progetto globale e aperto, sostenibile da chiunque, o motivi più pratici, come la rimozione degli intermediari. Inoltre, a differenza delle modalità di investimento tradizionali come i VC (Venture Capital), che richiedono da parte della società il trasferimento di quote in cambio dei fondi ricevuti, nelle ICO tipicamente non c'è alcuna cessione/emissione di quote e di conseguenza nessuna diluizione della società.

Le regolamentazioni

Fino al 2017 le ICO, come del resto l'intero mondo delle criptovalute, erano per lo più un fenomeno di nicchia sconosciuto ai più e senza alcuna regolamentazione. È solo in seguito all'esplosione di interesse nelle criptovalute che il settore ha attirato l'attenzione degli organi istituzionali in tutto il mondo. Questo ha portato alla stesura delle prime regolamentazioni, seppur ancora molto vaghe e frammentarie, spesso nella forma di linee guida più che di vere e proprie normative. Le ICO hanno una regolamentazione specifica all'interno delle legislazioni nei diversi Paesi. Per

esempio, in alcuni Paesi è legale l'uso di criptovalute mentre è illegale avviare una campagna ICO.

Alcuni casi di rilievo sono quelli legati a Usa, Cina e Malta.

Negli Stati Uniti l'organo incaricato di gestire e regolamentare le ICO è la Sec. La Sec, sebbene abbia affermato di avere l'autorità di imporre l'attuale normativa sulle security alle ICO, non si è ancora espressa in maniera ufficiale. Molti progetti, quindi, impediscono agli investitori statunitensi di partecipare alle proprie ICO proprio a causa di questa incertezza.

La Cina nel settembre 2017 ha ufficialmente proibito tutte le ICO sul proprio territorio, benché abbia

precisato che questa è solamente una soluzione temporanea in attesa di regolamentazioni più chiare [22].

Per quanto riguarda l'Europa, alcuni Paesi come Svizzera, Estonia e Malta si sono dimostrati particolarmente aperti a questa nuova forma di funding. In particolare Malta ha creato un insieme di leggi che regolano tutto il mondo delle DLT e delle criptovalute [1]. Per questo motivo Malta sta attirando numerosi progetti in ambito blockchain, tra i quali anche Binance, il più grande exchange mondiale per volume di criptovalute [23].

Ethereum

Esistono diverse blockchain che supportano gli smart contract (anche Bitcoin supporta dei basilari smart contract, come quelli utilizzati nel Lightning Network), ma al momento (2018) questo settore è dominato da Ethereum.

Ethereum ha fatto la sua prima apparizione in un articolo pubblicato nel 2013 dal diciannovenne Vitalik Buterin[48]. L'idea alla base di Ethereum era costruire una blockchain che potesse essere utilizzata per eseguire programmi generici.

Ethereum può essere visto come un computer globale, nel quale i programmi (chiamati smart contract) sono eseguiti in modo decentralizzato, continuo e senza censure.

Overview tecnica e politica monetaria

Ethereum è una blockchain non specializzata, ovvero una blockchain che non ha uno scopo specifico ma può essere programmata, tramite l'utilizzo di smart contract, per adattarsi a diversi scenari (blockchain generalizzata).

La blockchain è pubblica, senza

autorizzazioni e utilizza un algoritmo di consenso basato sul Proof of Work, con un tempo di blocco di circa 10–20 secondi. Tuttavia Ethereum sta pianificando la migrazione, nel prossimo futuro, a un protocollo Proof of Stake chiamato Casper [24].

Ethereum utilizza una propria valuta, denominata Ether (ETH). Al momento non esiste una quantità massima di ETH e il tasso di inflazione viene controllato limitando il numero di ETH generati ogni anno. Ci sono diverse proposte per l'imposizione di una quantità massima in futuro.

Il token ETH può essere suddiviso in **wei** (1 ETH = 10^18 wei), unità di misura di riferimento quando si parla di

gas.

Gas

Il token ETH è utilizzato per pagare il gas, un'unità di misura usata per determinare la quantità di calcolo necessaria per eseguire un'operazione sulla blockchain. Il gas necessario per effettuare un'operazione viene spesso paragonato al carburante usato da un'automobile per compiere un tragitto.

Ogni operazione sulla blockchain ha un costo definito. Per esempio, calcolare un hash o sommare due numeri richiede un certo numero di gas[49].

Il gas è un concetto esclusivamente

collegato alle transazioni (non esiste un token gas in Ethereum).

Ogni transazione effettuata su Ethereum ha due parametri: il **prezzo del gas** e il **limite di gas.** In Ethereum non esiste il concetto di dimensione massima di un blocco come nel Bitcoin, ma piuttosto si fa riferimento al limite di gas di un blocco (da non confondere con il limite di gas di una transazione), che definisce la massima quantità di calcoli per ogni blocco.

Il funzionamento del gas in Ethereum

Il **prezzo del gas** è il numero di wei da pagare per unità di gas.

Il gas viene pagato dal mittente di

una transazione (utilizzando i propri Ether), che lo acquista al prezzo specificato nella transazione. Le transazioni possono stabilire il prezzo del gas che preferiscono, tuttavia i miner sono liberi di scegliere le transazioni che vogliono (di solito cercando di massimizzare il profitto). Di conseguenza una transazione con un prezzo del gas elevato è più probabile che venga inclusa per prima dai miner.

Se per esempio una transazione usa 10 gas e si decide di pagare 100 wei per ogni gas, il costo totale della transazione sarà di 1.000 (10 * 100) wei. Se si imposta un prezzo del gas di 1.000 wei per gas, allora il costo totale della transazione sarà di 10.000 (10 * 1.000)

wei. Nel secondo caso il miner viene pagato di più per lo stesso calcolo ed è quindi probabile che dia priorità a quella transazione.

Il **limite di gas** è la quantità massima di gas che può essere consumata in una transazione. Se, per esempio, una transazione richiede 15 gas per essere eseguita ma impostiamo un limite di 10 gas, l'esecuzione si interromperà quando verrà raggiunto il limite. In questo caso tutto il gas della transazione andrà perso.

Se al contrario fissiamo un limite di gas superiore a quello effettivamente utilizzato dalla transazione, il gas in eccesso viene restituito al mittente.

Attualmente per eseguire una transazione monetaria normale su Ethereum il limite di gas consigliato è di 21.000 gas (Figura 9.5).

Da questi due valori si può calcolare il costo di una transazione con la formula:

$$\text{Costo transazione} = \text{Limite di gas} \times \text{Prezzo del gas}$$

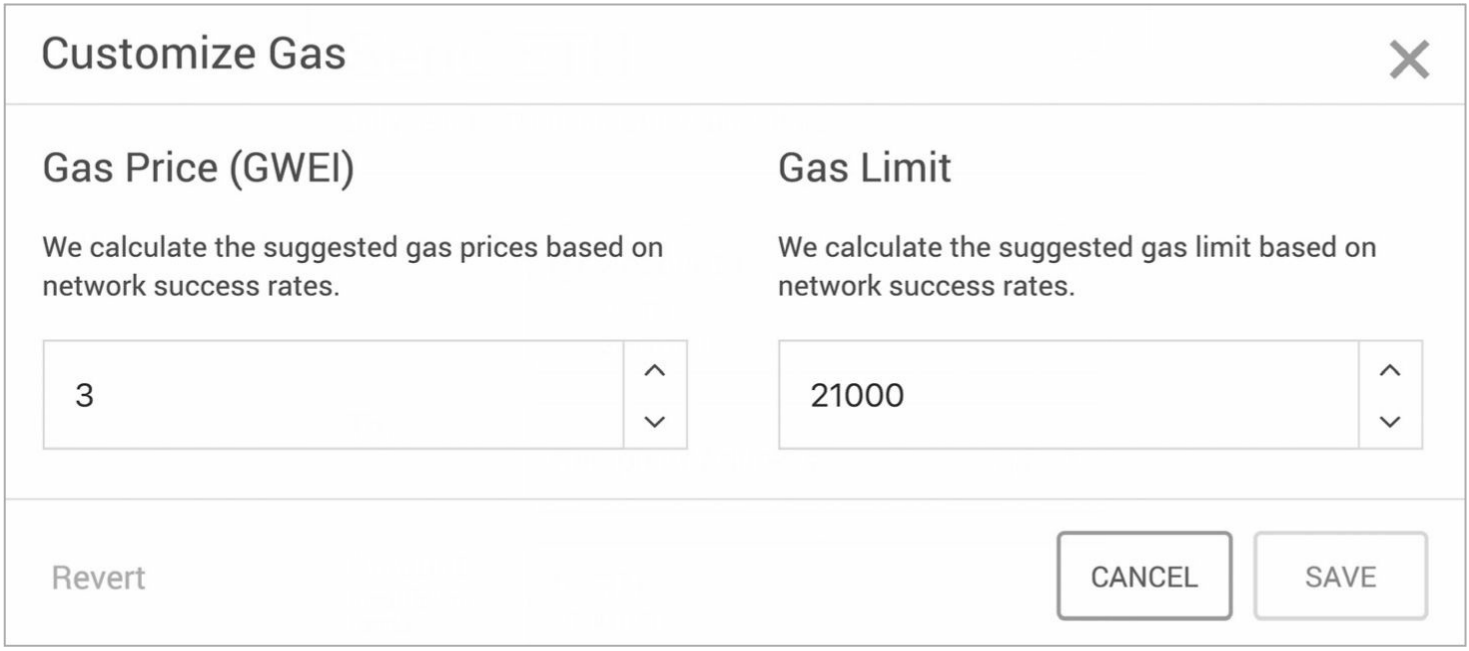


Figura 9.5 – Il settaggio di prezzo del gas limite di gas su Metamask.

Oltre a remunerare i miner, il costo delle transazioni nella blockchain di Ethereum è necessario per bloccare eventuali attacchi o errori di programmazione nei contratti che potrebbero sovraccaricare la blockchain. Uno smart contract può infatti eseguire computazioni

arbitrariamente complesse. Se, per esempio, una computazione entra in un ciclo infinito, il limite di gas andrà a interrompere l'esecuzione una volta esaurito il gas.

Account e indirizzi

In Ethereum esistono due tipi di account: account non associati a smart contract (account normali) e account associati a smart contract. Un account normale può ricevere e inviare transazioni, ma non è associato a nessuno smart contract e di solito è controllato da una persona.

Un account associato a uno smart contract, invece, contiene al suo interno

un programma che si attiva quando l'indirizzo a esso associato riceve una transazione, comportandosi come definito nello smart contract.

> Uno smart contract è un agente autonomo che vive sulla blockchain a un indirizzo specifico.

Alcuni esempi di indirizzi di Ethereum sono:

- 0xfbb1b73c4f0bda4f67dca266ce6ef42 Bittrex hot wallet, quasi 200M di dollari (ottobre 2018).
- 0x06012c8cf97bead5deae237070f958

l'indirizzo che contiene lo smart contract di Cryptokitties, un popolare gioco dove si possono scambiare gatti digitali.

EVM

L'Ethereum Virtual Machine (EVM) è l'ambiente all'interno del quale viene eseguito uno smart contract. Una Virtual Machine (macchina virtuale, VM) è un software che contiene al suo interno un sistema operativo completamente incapsulato. Per esempio è possibile utilizzare una macchina virtuale per utilizzare Windows all'interno di MacOS (il sistema operativo Apple). Le

macchine virtuali sono estremamente comode per separare due ambienti e far sì che siano completamente indipendenti.

L'EVM garantisce che ogni contratto venga eseguito nello stesso modo su ogni (full) node, in un ambiente isolato e sicuro. Lo stato dell'EVM viene salvato sulla blockchain.

ERC token

ERC è l'acronimo di Ethereum Request for Comment.

Gli ERC sono degli standard che identificano alcune funzionalità all'interno di uno smart contract. A

seconda delle funzionalità che si vuole attribuire a uno smart contract, si può scegliere uno standard specifico. Esistono diversi tipi di standard ERC. I più popolari attualmente sono lo standard ERC 20, comunemente usato nei token delle ICO, e lo standard ERC 721, utilizzato per creare dei token "non fungibili".

I token creati seguendo un determinato standard prendono la loro denominazione (Token ERC 20, Token ERC 721). Utilizzando inoltre uno degli standard esistenti, un programmatore che interagisce con il contratto saprà già che funzioni chiamare.

Perché sviluppare un'applicazione su Ethereum

Creare dei token su una blockchain come Ethereum ha numerosi vantaggi. Per esempio non è più necessario creare una propria blockchain, in quanto tutto viene gestito da Ethereum. Ogni token, inoltre, può essere conservato su un qualsiasi wallet compatibile con Ethereum, eliminando il problema di dover creare un wallet specifico.

In altre parole Ethereum fornisce un punto di partenza dal quale diventa molto più semplice costruire applicazioni su blockchain, totalmente

personalizzabile grazie alla possibilità di utilizzo degli smart contract.

Standard ERC 20

Molte delle criptovalute basate su Ethereum, soprattutto nell'ambito delle ICO, si basano sullo standard ERC 20.

L'ERC 20 è lo standard utilizzato per sviluppare i token sulla blockchain di Ethereum.

Un token ERC 20 è uno smart contract che implementa lo standard ERC 20, cioè che contiene al suo interno **almeno** le funzioni definite nello standard, tra le quali:

- **Total supply:** una funzione che definisca la quantità totale di token esistenti.
- **Balance of:** una funzione che definisca i token posseduti da uno specifico indirizzo.
- **Transfer:** una funzione per trasferire i token da un indirizzo a un altro.

Ci sarebbero in realtà altre funzioni, ma vanno oltre le finalità di questo testo.

ERC 721 token

Un altro standard diventato molto popolare è l'ERC 721, che descrive le

funzionalità dei token “non fungibili”, cioè unici.

Il concetto di fungibilità è legato al concetto di interscambio.

Una banconota da 5 euro è intercambiabile con qualsiasi altra banconota da 5 euro e il valore rimarrà sempre 5 euro.

Al contrario, se consideriamo altri beni come delle figurine, non abbiamo più il concetto di interscambio in quanto entrano in gioco altri fattori, come la rarità della figurina.

Le banconote possono quindi essere considerate dei beni fungibili, mentre le figurine rappresentano dei beni non fungibili.

Se volessimo per esempio

digitalizzare una collezione di figurine e trasferirla sulla blockchain di Ethereum, potremmo utilizzare lo standard ERC 721. Lo standard ERC 721 introduce il concetto di unicità nei beni digitali.

Questo standard ci garantisce che ogni token sarà associato a una singola specifica figurina. Per questo motivo i token ERC 721 vengono anche definiti “collezionabili”.

Lo standard ERC 721 è stato reso popolare dal gioco Cryptokitties, nel quale gli utenti potevano comprare e vendere dei gatti digitali.

Scalabilità

Il gioco Cryptokitties oltre ad aver reso popolare lo standard ERC 721 e i token collezionabili, ha mostrato i problemi di scalabilità della blockchain di Ethereum.

Attualmente ogni full-node del network di Ethereum salva tutto lo stato della blockchain e processa ogni singola transazione. Così facendo si ha la garanzia della massima sicurezza possibile, ma al costo della creazione di un enorme collo di bottiglia sulla capacità di scalabilità della blockchain (trilemma della scalabilità[50]). Gli sviluppatori di Ethereum stanno lavorando per risolvere i problemi di scalabilità. In particolare è previsto il

passaggio al PoS (con il protocollo Casper) nel 2019 e l'adozione di una tecnica chiamata **sharding** nel 2020 [24].

Casper è un protocollo PoS creato da Ethereum. È in grado di punire gli utenti malevoli che durante processo di validazione cercano di imbrogliare distruggendo il loro stake.

Sharding

Lo sharding è una soluzione molto complessa. Dovrebbe però portare enormi benefici alla capacità di scalare di una blockchain. Non è un concetto nuovo relativo solamente all'ambito blockchain, ma è stato già adottato con

successo in altri ambiti (per esempio nei database di Google). Alla base dello sharding c'è l'idea di dividere lo stato globale della blockchain in diverse parti indipendenti (ognuna con la propria cronologia delle transazioni) chiamate **shard.**

Ogni nodo sarebbe quindi in grado di processare solo le transazioni di alcuni shard, aumentando notevolmente l'**efficienza** totale del sistema[51].

Oracoli

Gli smart contract sono eseguiti in un ambiente controllato e isolato (Ethereum Virtual Machine) e non possono

interagire con il mondo al di fuori della blockchain.

Uno smart contract deve sempre avere un comportamento deterministico, cioè tutti i miner devono arrivare allo stesso risultato indipendentemente dalla macchina sul quale viene eseguito lo smart contract. Un'interazione con una fonte esterna di dati potrebbe potenzialmente portare a un comportamento non deterministico. Non vi è alcuna garanzia che domani una certa fonte di dati restituirà gli stessi dati restituiti oggi, o che due nodi diversi ricevano gli stessi dati. Ogni calcolo su una blockchain deve essere verificabile utilizzando solo i dati nella blockchain stessa.

Come fare quindi nel caso di uno smart contract che abbia bisogno di alcuni dati dal mondo esterno per effettuare un calcolo? Pensiamo a informazioni meteo, risultati sportivi, quotazioni azionarie, tassi di cambio ecc. Uno smart contract non è in grado di ottenere direttamente queste informazioni, ma ha invece bisogno di utilizzare un servizio che fornisca alla blockchain i dati di cui ha bisogno, che prende il nome di **oracolo**.

> Un oracolo è un servizio progettato specificamente per connettere una blockchain con il mondo esterno fornendo allo

smart contract tutte le informazioni necessarie per eseguire una computazione.

Gli oracoli sono ancora in stato embrionale, ci vorrà del tempo prima che siano effettivamente utilizzabili su larga scala. Per chi volesse approfondire consigliamo di fare riferimento ad Augur (www.augur.net), che ha creato un oracolo decentralizzato e un protocollo di previsioni su diversi eventi basato su blockchain.

47.

https://icowatchlist.com/statistics/blockchain.
48. Per approfondire: https://cointelegraph.com/ethereum-for-beginners/who-is-vitalik-buterin.
49. Una lettura molto interessante è quella del yellow paper di Ethereum: a pagina 25 c'è l'elenco di ogni operazione e il suo corrispettivo costo in gas. https://ethereum.github.io/yellowpaper/paper.pd
50. Parliamo di un limite di 7–15 tps, transazioni al secondo.
51. Una soluzione di questo tipo è estremamente complessa da implementare, in quanto si creano dei problemi di consistenza critici. Sono stati scritti libri interi su come affrontare questo tipo di problemi nei sistemi distribuiti. Per approfondire, consigliamo di leggere le implicazioni del teorema CAP e fare riferimento alle implementazioni dello sharding proposte da Ethereum o da Zilliqa.

10

Altcoin

Altcoin[52] è un termine generico che fa riferimento a tutte le criptovalute create dopo il Bitcoin. Molte di queste altcoin prendono ispirazione dal Bitcoin. Altre, invece, sono totalmente differenti, per esempio nella struttura della blockchain o nei protocolli di consenso: algoritmi di mining, distribuzione dell'autorità, politica monetaria ecc.

La possibilità per chiunque di creare la propria criptovaluta ha permesso la

nascita di oltre 2.000 altcoin presenti sui cripto-exchange, con decine di nuovi progetti che nascono ogni giorno.

In questo capitolo andremo a esplorare alcune tra le criptovalute più conosciute, suddivise in base al settore di applicazione, facendo riferimento al panorama recente.

Pagamenti

Ripple (XRP)

Ripple è un protocollo peer-to-peer creato da Ripple Labs[53] nel 2012 per il trasferimento globale di fondi in maniera

sicura, istantanea e a basso costo. Concepito per essere utilizzato da banche e istituzioni finanziarie, viene definito da Ripple stesso come “una tecnologia infrastrutturale per le transazioni interbancarie”. La valuta nativa utilizzata nel protocollo è il token XRP.

Tra le principali partnership di Ripple citiamo Accenture, American Express, Deloitte, Santander, UBS e Unicredit.

Il problema che risolve

Ripple punta a risolvere alcuni dei maggiori problemi che si trovano ad affrontare banche e istituti finanziari nel

trasferire globalmente denaro, in particolare per i pagamenti transfrontalieri. Questo scenario richiede infatti che le banche mantengano conti in giurisdizioni estere in valuta locale (**processo Nostro-Vostro**). Il processo Nostro-Vostro per le transazioni internazionali con valute fiat è lungo e costoso, richiedendo diversi giorni prima di sapere se sia andato a buon fine (oppure no). Questo solitamente crea numerosi problemi ed elevati costi per chi ha la necessità di trasferire denaro tra nazioni differenti, uno scenario in netto contrasto con un mondo nel quale le informazioni viaggiano istantaneamente in tutto il mondo grazie a Internet.

Ripple ha perciò creato un network di servizi, chiamato RippleNet, per interconnettere banche e istituti finanziari e ridurre drasticamente tempi e costi necessari per questo tipo di operazioni, diventando di fatto una soluzione alternativa al correntemente utilizzato circuito Swift[54].

I principali servizi offerti da RippleNet sono:

- **xCurrent**, un servizio che consente alle banche di scambiare messaggi istantaneamente e facilitare le riconciliazioni bancarie nei pagamenti internazionali. Il servizio xCurrent non prevede

l’utilizzo di XRP.

- **xRapid**, che aggiunge la possibilità di regolare istantaneamente i conti tra due banche tramite l’utilizzo di XRP come moneta di scambio. La riconciliazione avviene istantaneamente da parte di entrambe le banche e viene regolata dal servizio xRapid, perciò gli scambi non influiscono in alcun modo sul prezzo di mercato della valuta XRP.
- **xVia**, un servizio che consente agli utenti (società e istituzioni) di sfruttare la tecnologia

blockchain per monitorare gli spostamenti di denaro e accedere alle stesse informazioni a cui solitamente ha accesso una banca, così come inviare pagamenti su scala globale assieme ad altre informazioni (per esempio fatture).

A oggi l'unico servizio offerto ai partecipanti del circuito RippleNet è xCurrent, mentre xRapid e xVia sono in fase di sperimentazione e verranno implementati nei prossimi anni. È importante notare che XRP è pensato per essere principalmente utilizzato dalle banche stesse nella riconciliazione dei loro conti, e non da parte degli utenti che

effettuano il trasferimento di denaro. Un utente non vedrebbe mai movimenti di XRP, ma noterebbe solo una notevole riduzione del tempo necessario per il trasferimento (da circa 4 giorni a pochi minuti) assieme a una riduzione dei costi di commissione che diventerebbero pressoché nulli.

XRP può essere utilizzato come criptovaluta all'interno di RippleNet, diventando una "valuta ponte" (Figura 10.1) nelle situazioni in cui non è possibile uno scambio diretto tra due valute differenti.

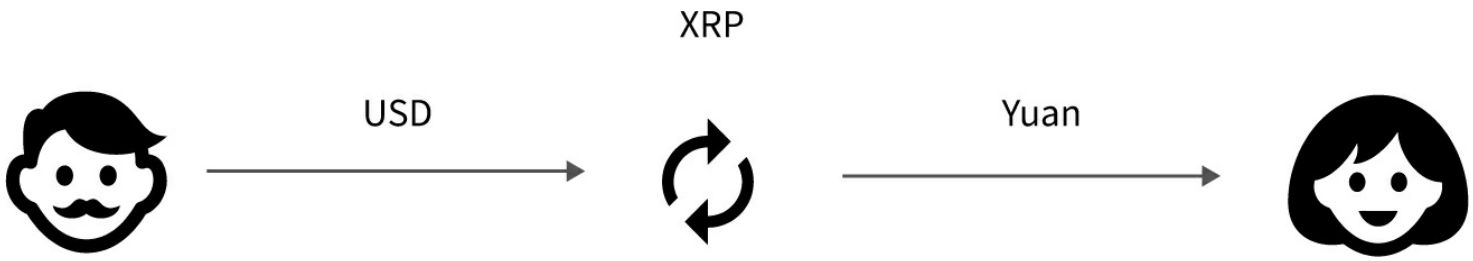


Figura 10.1 – L'uso di XRP come valuta ponte.

Politica monetaria

XRP rientra tra le criptovalute non-minabili e tutti i token sono stati generati nel momento della creazione della ledger (pre-mined). XRP ha una quantità massima di 100 miliardi di unità e una quantità circolante di circa 40. Il prezzo unitario più alto è stato raggiunto a gennaio 2018, con circa $3 per XRP e un market cap di oltre $140 miliardi. Ripple Labs è attualmente in possesso di oltre 50 miliardi di XRP in un deposito di garanzia. Ogni mese vengono rilasciati 1 miliardo di XRP, che Ripple

utilizza per estendere l'adozione dei propri servizi.

Tecnologia

Ripple utilizza una ledger distribuita pubblica, dove vengono salvate tutte le informazioni relative agli spostamenti di valore. Il consenso distribuito è raggiunto utilizzando un algoritmo di consenso distribuito chiamato RPCA (Ripple Protocol Consensus Algorithm). RPCA utilizza dei gruppi di nodi ritenuti affidabili dal network (UNL, Unique Node List). Almeno l'80% dei nodi dell'UNL deve considerare una transazione valida affinché venga inserita nella ledger. Questo algoritmo è

molto efficiente e permette di generare un nuovo stato della ledger ogni 3–5 secondi, potendo raggiungere circa 1.500 tps.

La ledger di XRP è collegata al mondo reale tramite i **Gateway**, che permettono al denaro e ad altre forme di valore di entrare e uscire dal network. I Gateway sono inoltre responsabili del rispetto di tutte le normative locali (KYC, AML, CFT ecc.) e di riportare alle autorità eventuali casi sospetti.

Tabella 10.1 – I punti chiave di XRP.

	XRP
Creato da	Ripple Labs
Anno creazione	2012

Protocollo di consenso	Ripple Protocol Consensus Algorithm
Quantità massima	100 miliardi
Quantità circolante	≃ 40 miliardi
Tempo conferma transazione	≃ 3–5 secondi
1 XRP	10^6 drop

Bitcoin Cash (BCH)

Bitcoin Cash è una criptovaluta nata ad agosto 2017, in seguito a una hard fork del Bitcoin (fork eseguita al blocco #478558 della blockchain del Bitcoin). Infatti una parte della community di sviluppatori e miner sosteneva che il Bitcoin non rispecchiasse più l'ideale originale di Satoshi Nakamoto (ovvero

quello di essere una valuta digitale peer-to-peer) a causa dei problemi di scalabilità che ne rendevano estremamente scomodo l'utilizzo per piccoli pagamenti. La fork è stata decisa dopo che le soluzioni proposte per risolvere questo problema, in particolare BIP 91 (SegWit), non sono state ritenute sufficienti, in quanto mancava l'aumento della dimensione del blocco, aspetto considerato fondamentale dai sostenitori del Bitcoin Cash.

Politica monetaria

BCH è una criptovaluta minabile con una quantità massima di 21 milioni, una

quantità circolante di circa 17 milioni. Il prezzo unitario più alto è stato raggiunto a dicembre 2017, con oltre $3.000 per BCH e un market cap di circa $60 miliardi.

Il problema che risolve

Bitcoin Cash punta principalmente a risolvere i problemi di scalabilità del Bitcoin senza ricorrere a soluzioni off-chain come il Lightning Network.

Tecnologia

Da un punto di vista tecnologico Bitcoin Cash è molto simile al Bitcoin. L'unica sostanziale differenza risiede nella

dimensione massima del blocco, attualmente 32 MB per il Bitcoin Cash. In futuro BCH punta ad aggiungere diverse funzionalità come, per esempio il supporto agli smart contract.

Tabella 10.2 – I punti chiave di BCH.

	BCH
Fork da	Bitcoin
Anno creazione	2017
Protocollo di consenso	Proof of Work
Quantità massima	≃ 21 milioni
Quantità circolante	≃ 17 milioni
Tempo di blocco	≃ 10 minuti
1 BCH	10^8 satoshi

Stellar Lumen (XLM)

XLM è la criptovaluta nativa utilizzata nel network Stellar, un protocollo open source per il trasferimento di valore in maniera decentralizzata. Stellar è il competitor principale di Ripple, nonostante entrambi i progetti siano stati co-fondati da Jed McCaleb. Stellar e Ripple, seppur concettualmente simili, hanno come obiettivo due mercati differenti: Ripple è interessato principalmente alle istituzioni finanziarie come le banche, mentre Stellar è più incentrato su mercati emergenti e realtà commerciali, con un approccio meno istituzionale e open source. Tra le partnership di Stellar

troviamo Ibm, che insieme a KlickEx sta sviluppando un sistema blockchain per facilitare le riconciliazioni bancarie nei pagamenti cross-border[55].

Il problema che risolve

Come Ripple, anche Stellar punta a interconnettere istituti finanziari per ridurre i costi dovuti al trasferimento di denaro, in particolare nei pagamenti internazionali.

Politica monetaria

Il numero iniziale di XML (lumen) creati col blocco genesi è di 100 miliardi. Il tasso di inflazione annuale è pari all'1%

e attualmente ci sono circa 19 miliardi di lumen in circolazione. A gennaio 2018, il market cap di XML ha toccato il suo massimo, superando i 15 miliardi di dollari.

Tecnologia

Stellar utilizza un network decentralizzato di nodi che condividono una ledger distribuita aggiornata ogni 2–5 secondi. Il protocollo di consenso utilizzato è lo Stellar Consensus Protocol, che si basa sulla validazione delle transazioni da parte di specifici gruppi di nodi del network (FBA, Federated Byzantine Agreement). In pratica, ogni nodo sceglie altri nodi

considerati affidabili andando a formare diversi gruppi all'interno del network. Nel momento in cui una transazione viene considerata valida da un gruppo, viene convalidata. Questo protocollo permette a Stellar di essere estremamente performante, riuscendo a processare fino a 1.000 tps.

Tabella 10.3 – I punti chiave di XLM.

	XLM
Creato da	Stellar Development Foundation
Anno creazione	2014
Protocollo di consenso	Stellar Consensus Protocol
Quantità massima	Non fissata. 100 miliardi iniziali + 1% di inflazione annuale

Quantità circolante	≃ 19 miliardi
Tempo conferma transazione	≃ 2-5 secondi
1 XLM	10^7 stroop

Litecoin (LTC)

Litecoin è una criptovaluta che permette di effettuare pagamenti globali peer-to-peer, creata nel 2011 da Charlie Lee[56].

Il problema che risolve

La motivazione che ha portato alla creazione del Litecoin è stata quella di migliorare alcuni aspetti del Bitcoin, in particolare di rendere i trasferimenti di valore più veloci ed economici.

Litecoin non va però visto come un rivale del Bitcoin, ma piuttosto come un network complementare, più adatto ai pagamenti di tutti i giorni e, per esempio, a negozi e commercianti.

Politica monetaria

LTC è una criptovaluta minabile con una quantità massima di 84 milioni, una quantità circolante di circa 60 milioni. Attualmente la ricompensa per la creazione di un blocco è pari a 25 LTC, e viene dimezzata ogni 4 anni (esattamente come nel Bitcoin). A dicembre 2017 il market cap di LTC ha toccato il suo massimo, superando i 15 miliardi di dollari, con un prezzo

unitario di oltre 300 dollari.

Tecnologia

Litecoin utilizza un algoritmo Proof of Work nel processo di consenso distribuito. A differenza del Bitcoin (che utilizza un algoritmo basato su SHA-256), Litecoin utilizza un algoritmo chiamato scrypt. Scrypt inizialmente era progettato per essere ASIC-resistant, ovvero con l'obiettivo di minimizzare i vantaggi di utilizzare un hardware specializzato nel processo di mining, come ASIC o FPGA (attualmente esistono macchine ASIC progettate apposta per gli algoritmi scrypt).

I blocchi nel Litecoin vengono

generati più velocemente: 2,5 minuti rispetto ai 10 minuti del Bitcoin, permettendo alle transazioni di essere confermate più velocemente.

Tabella 10.4 – I punti chiave di LTC.

	Litecoin
Creato da	Charlie Lee
Anno creazione	2011
Protocollo di consenso	Proof of Work (scrypt)
Quantità massima	84 milioni
Quantità circolante (2018)	≃ 60 milioni
Tempo di blocco	2,5 minuti
1 LTC	10^8 spark

Tether (USDT)

Tether è una criptovaluta basata sul valore del dollaro americano: 1 USDT è sempre uguale a $1. È la più popolare tra le criptovalute che rientrano sotto la definizione di **stable coin**, cioè quelle criptovalute pensate per mantenere un valore stabile nel tempo, basandosi sul valore di altre valute o commodity come per esempio dollari, euro, oro ecc.

Il valore del Tether è garantito da un collaterale che eguaglia il numero di USDT in circolazione, in questo caso dei dollari americani.

Politica monetaria

Ogni USDT in circolazione ha un corrispettivo USD su dei conti bancari.

Non esiste un numero massimo di tether e questi vengono creati su richiesta (per esempio da parte dei cripto-exchange).

Il problema che risolve

Tether è utilizzata principalmente dai cripto-exchange per simulare l'utilizzo di monete fiat come USD ed EUR, evitando al contempo tutti i problemi legati alla loro gestione (Know Your Customer, antiriciclaggio, bonifici ecc.).

Tecnologia

Tether utilizza un protocollo chiamato "Omni Layer" che permette di creare e scambiare asset digitali utilizzando la

blockchain del Bitcoin.

Monero (XMR)

Monero è una criptovaluta creata nel 2014 incentrata sulla privacy delle transazioni e degli utenti. Monero utilizza speciali protocolli crittografici per garantire che tutte le sue transazioni rimangano non tracciabili. Viene utilizzata una ledger pubblica offuscata, in maniera tale da non permettere a terze parti di sapere il mittente, il destinatario o l'importo della transazione.

Dash (DASH)

Dash nasce nel 2014 dallo stesso codice sorgente del Litecoin (a sua volta basato sul codice sorgente del Bitcoin). Le informazioni di pagamento sulla blockchain di Dash possono essere tenute private, impedendo qualsiasi forma di analisi che tenti di ricondurre un pagamento a uno specifico utente.

Dash è inoltre un esempio di DAO (Decentralized Autonomous Organization), nella quale gli shareholder (chiamati masternode) governano l'organizzazione, decidendo per esempio come spendere i fondi. Il 10% di tutti i nuovi Dash generati viene infatti tenuto come riserva e i masternode hanno la possibilità di

votare su come utilizzare tali fondi.

Dogecoin (DOGE)

Dogecoin è una criptovaluta creata da Jackson Palmer nel 2013 come scherzo (ha come simbolo il meme Doge). Dogecoin ha però iniziato a guadagnare popolarità come valuta di tipping (mancia) nei progetti open source e su piattaforme come Reddit, arrivando a superare il miliardo di dollari di capitalizzazione nel 2017.

Figura 10.2 – Il simbolo del Dogecoin.

Piattaforme smart contract

EOS (EOS)

EOS è un ecosistema basato su blockchain per lo sviluppo di applicazioni decentralizzate, concettualmente simile a Ethereum. È stato co-fondato da Dan Larimer, già creatore di altri progetti come Bitshares e Steem. L'ecosistema EOS è composto da due elementi: il token EOS e la piattaforma EOS.IO.

EOS.IO è una blockchain che utilizza il token EOS come criptovaluta nativa. Il

token EOS garantisce al possessore una determinata porzione di risorse sul network, le quali se non utilizzate possono essere affittate ad altri utenti.

EOS viene spesso considerato come il competitor principale di Ethereum.

Il problema che risolve

Ethereum è attualmente il progetto più conosciuto e utilizzato per la creazione di applicazioni decentralizzate, però, come abbiamo già visto, soffre di diversi problemi come i limiti di scalabilità, un basso throughput e costi di transazione elevati, che ne stanno frenando l'adozione.

EOS.IO ha come obiettivo quello di

concentrare in un'unica piattaforma tutte le migliori caratteristiche di diverse blockchain, come la sicurezza del Bitcoin e la versatilità dell'Ethereum.

Politica monetaria

Al lancio di EOS sono stati generati 1 miliardo di token. Ogni anno la quantità totale viene incrementata del 5%. I nuovi token generati vengono utilizzati per esempio per ricompensare i nodi che contribuiscono alla verifica delle transazioni e alla produzione dei blocchi. Il token EOS ha superato i $15 miliardi di market cap a maggio 2018.

Tecnologia

EOS utilizza una variazione del Proof of Stake come protocollo di consenso, chiamato Delegated Proof of Stake (DPoS). In questo modello non ci sono miner, ma 21 block producer (produttori di blocchi), eletti dai possessori di token EOS e ricompensati con dei token EOS. Si può pensare al DPoS come una democrazia rappresentativa, mentre il PoS sarebbe una democrazia diretta.

I block producer sono sottoposti a un continuo processo di voto da parte di tutti i possessori di token EOS, che possono eventualmente rimuovere uno specifico nodo se si comporta in maniera scorretta.

Questo sistema permette la generazione di nuovi blocchi in maniera estremamente rapida, risolvendo gran parte dei problemi di scalabilità.

Come però già discusso nel trilemma della scalabilità (nel Capitolo 6), non è possibile avere contemporaneamente sicurezza, scalabilità e decentralizzazione, ma bisogna trovare un compromesso.

Ethereum ha scelto sicurezza e decentralizzazione, a costo di una scalabilità ridotta. EOS riduce la decentralizzazione, incaricando 21 rappresentanti dell'intero processo di consenso, e permettendo di ottenere una scalabilità superiore. Attualmente un

nuovo blocco viene generato ogni 0,5 secondi con un throughput finale di circa 3.000 tps in media.

Tabella 10.5 – I punti chiave di EOS.

	EOS
Creato da	Daniel Larimer, Brendan Blumer
Anno creazione	2018
Protocollo di consenso	DPoS
Quantità massima	Non fissata. 1 miliardo iniziale +5% di inflazione annuale
Quantità circolante	≃ 900 milioni
Block time	≃ 0,5 secondi

Cardano (ADA)

Cardano è una piattaforma per l'esecuzione di smart contract rilasciata nel 2017, concettualmente simile a Ethereum ma strutturata su diversi livelli, ognuno incentrato su particolari caratteristiche come scalabilità o sicurezza. Cardano è sviluppato da IOHK, una società che si occupa dello sviluppo di tecnologie peer-to-peer diretta da Charles Hoskinson, già membro fondatore di Ethereum.

Per il design della propria piattaforma, Cardano ha utilizzato un approccio scientifico, sottoponendo le diverse componenti del sistema a ricerches accademiche peer-reviewed.

Può essere quindi visto come un progetto guidato da un rigoroso approccio scientifico.

Il problema che risolve

Cardano si inserisce tra i progetti che cercano di risolvere alcuni problemi intrinsechi alla prima generazione di blockchain, come per esempio la scalabilità e la velocità delle transazioni. Il focus è quindi quello di costruire un ecosistema blockchain più sostenibile e bilanciato.

Politica monetaria

ADA è una criptovaluta minabile con

una quantità massima di 45 miliardi, una quantità circolante di circa 31 miliardi. A gennaio 2018 il market cap di cardano ha superato i $30 miliardi.

Tecnologia

Cardano è composto principalmente da due livelli: il Cardano Settlement Layer (CSL), utilizzato per regolare le transazioni che usano ADA, e il Control Layer, utilizzato per eseguire gli smart contract.

Il protocollo di consenso utilizzato si chiama Ouroboros ed è basato sul Proof of Stake.

Tabella 10.6 – I punti chiave di ADA.

	ADA
Creato da	IOHK
Anno creazione	2017
Protocollo di consenso	PoS (Ouroboros)
Quantità massima	45 miliardi
Quantità circolante	≃ 26 miliardi
Tempo di blocco	≃ 20 secondi

NEO (NEO)

NEO è una piattaforma per lo sviluppo di applicazioni decentralizzate (Dapp), creata nel 2014 con il nome di AntShares e rebranded nel 2017 come NEO.

NEO si definisce come un network

distribuito per la smart economy, ovvero un ecosistema dove vengono integrati asset digitali (digital asset), identità digitali (digital identity) e smart contract.

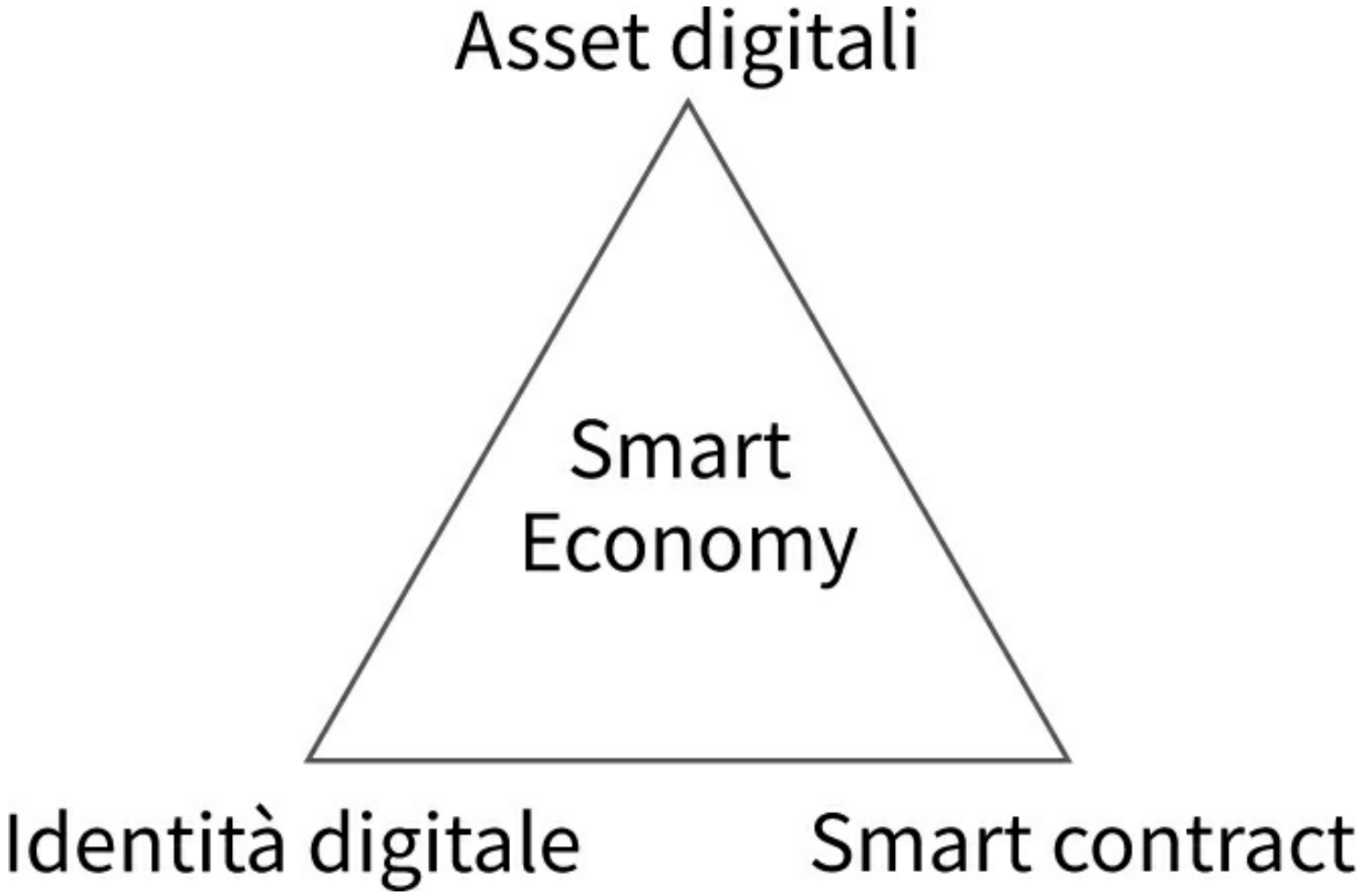


Figura 10.3 – NEO smart economy.

Il problema che risolve

NEO fornisce una soluzione per la digitalizzazione e la gestione dei beni fisici in maniera decentralizzata, permettendo la creazione di un vero e

proprio sistema finanziario digitale collegato al mondo reale. NEO inoltre fornisce alcune soluzioni integrate, come KYC e AML, in modo da essere conforme alle normative di gran parte dei governi mondiali.

Politica monetaria

Il token NEO è una criptovaluta pre-mined, con una quantità massima di 100 milioni, una quantità circolante di 65 milioni.

Il token NEO può essere pensato come una share all'interno dell'ecosistema, che dà diritto per esempio all'elezione dei validatori nel processo di consenso (un protocollo

quindi “delegated”).

I token NEO generano dei dividendi sotto forma di token GAS, i quali sono usati a loro volta per pagare le transazioni sul network.

Ogni token NEO genera 1 GAS ogni 22 anni. Il numero massimo di token GAS che potrà esistere è 100 milioni, che verrà raggiunto nel 2038. GAS ha una quantità circolante di circa 10 milioni.

Tecnologia

NEO utilizza un protocollo di consenso chiamato delegated Byzantine Fault Tolerance (dBFT).

In questo protocollo ci sono dei nodi

speciali, chiamati **book keeper** o **delegati,** responsabili di verificare la validità delle transazioni.

Tra tutti i nodi delegati viene scelto un nodo specifico in maniera randomica, responsabile di creare il nuovo blocco. Una volta creato, il blocco viene inoltrato a tutti i restanti delegati. Il 66% di questi nodi deve essere d'accordo sulla validità di ogni nuovo blocco, prima che questo possa essere aggiunto alla blockchain.

I possessori dei token NEO delegano quindi ai book keeper la gestione del processo di consenso.

Tabella 10.7 – I punti chiave di NEO.

	NEO
Anno creazione	2014
Protocollo di consenso	dBFT
Quantità massima	100 milioni
Quantità circolante	65 milioni
Tempo di blocco	≃ 20 secondi

Altre criptovalute

IOTA (IOT)

IOTA è una criptovaluta creata nel 2015 e concepita per essere utilizzata nel processo di comunicazione e nei pagamenti tra macchine (transazioni machine-to-machine, m2m) nell'ambito

della cosiddetta “Internet of Things”.

L’idea di IOTA è quella di creare un sistema pubblico e aperto che ponga le fondamenta per uno standard di interoperabilità tra dispositivi IoT, abilitando le transazioni tra i dispositivi stessi.

IOTA ha siglato diverse partnership con numerose società di rilevanza internazionale, tra le quali Bosch, Volkswagen, Fujitsu, Microsoft e Accenture.

Il problema che risolve

La domanda di micropagamenti sta crescendo esponenzialmente, e questo è in gran parte dovuto all’esplosione del

settore IoT. Sistemi come Bitcoin non sono attualmente in grado di garantire un volume di transazioni elevato e possiedono evidenti limiti di scalabilità per un'applicazione in questo settore. Nel 2035 sono previsti 1 trilione di dispositivi IoT interconnessi, e l'intenzione di IOTA è quella di sviluppare una piattaforma per permettere alle macchine di comunicare autonomamente tra loro, che sia anche scalabile e in grado di supportare la crescita esponenziale nel numero dei dispositivi.

Politica monetaria

IOTA è una criptovaluta non minabile.

La quantità massima è pari alla quantità circolante, ovvero 2.779.530.283.000.000 IOTA. La quantità massima è così grande proprio perché è stata pensata per effettuare micropagamenti. Per questo motivo solitamente quando ci si riferisce a IOTA si fa riferimento all'unità MIOTA (Mega IOTA), ovvero 1 milione di IOTA. IOTA ha superato i $14 miliardi di market cap a dicembre 2017.

Tecnologia

IOTA non usa una blockchain tradizionale, ma si basa su una tecnologia DLT chiamata **tangle** (ne abbiamo parlato nel Capitolo 6). Le

transazioni sono gratuite e non esistono né miner e né blocchi. Ogni utente per poter creare una transazione deve validare altre due transazioni. Questo genera un sistema estremamente scalabile, con costi di transazione potenzialmente nulli.

Tabella 10.8 – I punti chiave di IOTA.

	IOTA
Tipologia ledger	Tangle
Anno creazione	2015
Quantità massima	2.779.530.283.000.000
Quantità attuale	2.779.530.283.000.000
1 MOTA	10^6 IOTA

Ethereum Classic (ETC)

Ethereum Classic è la criptovaluta nata da una fork della blockchain di Ethereum nel 2016, in seguito a un hack di The DAO (ne abbiamo già accennato nel Capitolo 5). L'hack ha generato uno spaccamento all'interno della community, nella quale una parte aveva intenzione di annullare l'attacco e risarcire i token persi dagli utenti (Ethereum) mentre l'altra riteneva che una blockchain per essere coerente con la sua ideologia dovesse rimanere sempre immutabile anche in situazioni estremamente negative (Ethereum Classic).

Sebbene tra le due blockchain quella

con più rilevanza nel panorama delle criptovalute sia sicuramente Ethereum (per via dei continui miglioramenti e della presenza di esponenti importanti che trascinano la community come Vitalik Buterin), Ethereum Classic rimane comunque un progetto di rilievo (da agosto 2018 ETC è stata la quinta criptovaluta a essere aggiunta all'Exchange Coinbase).

Tronix (TRX)

Tron è una piattaforma decentralizzata, fondata nel 2017, con l'obiettivo di creare un network gratuito per l'intrattenimento e la condivisione di

contenuti digitali, eliminando gli intermediari tra i creatori di contenuti e i consumatori finali, riducendo quindi i costi per gli utenti e aumentando i guadagni per i creatori. Utilizzando il network di Tron chiunque può creare dei contenuti digitali e condividerli senza dover passare per piattaforme centralizzate come Netflix o YouTube. Per facilitare questa condivisione peer-to-peer, Tron ha recentemente acquistato BitTorrent, società dietro lo sviluppo dell'omonimo protocollo p2p. Nel network di Tron viene utilizzata la criptovaluta Tronix (TRX), utilizzata per effettuare pagamenti sulla piattaforma. TRX ha superato i $10 miliardi di market cap a gennaio 2018.

Binance Coin (BNB)

Binance Coin è un token ERC 20 creato dall'exchange Binance e distribuito nel 2017 durante la propria ICO, che ricopre vari ruoli all'interno dell'ecosistema Binance.

Può essere utilizzato, per esempio, per pagare le commissioni di transazione ricevendo degli sconti sulle stesse (50% di sconto il primo anno, 25% il secondo ecc.) o per partecipare alle ICO presenti sull'exchange. In futuro BNB diventerà la criptovaluta nativa nell'exchange decentralizzato di Binance, attualmente in fase di sviluppo.

OmiseGo (OMG)

OmiseGo è un network decentralizzato di servizi finanziari costruito su Ethereum. Il motto di OmiseGo è "Unbank the banked", a rappresentare il suo tentativo di ridurre l'attuale dipendenza dai servizi bancari tradizionali creando un network peer-to-peer per effettuare operazioni finanziare. Tra i servizi offerti da OmiseGo sono presenti, per esempio, un exchange decentralizzato, un sistema che fornisce liquidità, un sistema di pagamenti interbancari (simile a CHIPS, Clearing House Interbank Payments System) e un asset-backed blockchain gateway.

OmiseGo utilizza il token ERC 20

OMG, il cui scopo è quello di verificare la sicurezza del network tramite un processo di consenso basato su PoS.

OmiseGo inoltre ha proposto la prima implementazione di Plasma, una soluzione ai problemi di scalabilità di Ethereum basata sulla creazione di child-chain collegate alla blockchain principale (main chain), sulle quali poter spostare gran parte delle computazioni lasciando alla main chain il compito di garantire la sicurezza del sistema. OMG ha i $2 miliardi di market cap a gennaio 2018.

Augur (REP)

Augur è una piattaforma decentralizzata per il mercato delle previsioni, costruita sulla blockchain di Ethereum. Permette a chiunque di creare delle scommesse su eventi sportivi, politici, meteorologici, economici ecc. Invece di avere dei bookmaker che creano gli eventi e le quote, chiunque può creare i propri eventi in modo decentralizzato con i pagamenti gestiti tramite smart contract.

Augur utilizza la criptovaluta Reputation (REP) come incentivo per ricompensare gli utenti che riportano il risultato esatto di un evento, o aiutano a correggere dei risultati errati. Riportare un risultato sbagliato comporta al contrario la perdita di token REP.

Augur ha superato il miliardo di dollari di market cap a gennaio 2018.

0x (ZRX)

0x è un protocollo open source per lo scambio decentralizzato di token ERC 20 costruito sulla blockchain di Ethereum. Questo protocollo permette a chiunque di creare il proprio exchange decentralizzato. In futuro, infatti, ci saranno migliaia di token diversi e diventa quindi necessario un modo per poterli scambiare in maniera efficiente. Il mercato attualmente offre principalmente delle soluzioni di scambio centralizzato (Coinbase,

Binance ecc.), che non si sposano con la filosofia blockchain e possiedono numerosi problemi (*in primis* la sicurezza). D'altro canto, però, gli exchange decentralizzati sono poco usati e ciò comporta dei volumi ridotti che rendono operativamente difficili gli scambi. 0x punta a risolvere molti dei problemi degli exchange decentralizzati tramite la creazione di un protocollo standard che combina i vantaggi di entrambe le soluzioni.

L'idea alla base di 0x è quella di gestire l'order-book off-chain e risolvere gli ordini on-chain, in maniera da aumentare la scalabilità e ridurre i costi. Il creatore di un exchange viene chiamato **Relayer**, ed è responsabile

della gestione degli ordini di quel particolare exchange.

0x utilizza il token ERC 20 ZRX, che ha lo scopo di pagare i Relayer e funge inoltre da share nella governance del protocollo stesso, permettendo ai possessori di token di votare su eventuali modifiche al protocollo in maniera proporzionale ai token posseduti.

ZRX ha superato il miliardo di dollari di market cap a gennaio 2018.

Golem (GNT)

Golem è un supercomputer globale decentralizzato, che utilizza la potenza

di calcolo di tutte le macchine partecipanti al network per eseguire computazioni intensive.

Golem permette a chiunque di affittare parte della potenza di calcolo del proprio computer ed essere ricompensato tramite dei token, in maniera concettualmente simile a Uber o Airbnb. In particolare Golem utilizza il token ERC 20 GNT. Attualmente Golem si sta focalizzando sul rendering grafico, ma in futuro ci sarà la possibilità di usare il network per altre computazioni, come il training di modelli di machine learning.

GNT ha superato i $900 milioni di market cap a gennaio 2018.

WaltonChain (WTC)

WaltonChain è un progetto che combina la tecnologia blockchain con l'IoT per una gestione più efficiente della supply chain. In particolare, WaltonChain utilizza la tecnologia RFID (Radio Frequency IDentification), ovvero dei tag che usano dei campi elettromagnetici per identificare degli oggetti. In un mercato sempre più globale, infatti, logistica e supply chain stanno diventando dei processi sempre più complessi e distribuiti, che coinvolgono decine o centinaia di attori. Una gestione verticale di queste tipologie di processi diventa spesso inefficiente e costosa.

Una volta che il bene reale viene

digitalizzato tramite l'utilizzo di RFID, l'identità digitale viene trasferita su blockchain, andando a salvare ogni passo del processo produttivo in maniera immutabile.

Questa soluzione introduce il concetto di valore nell'IoT, che WaltonChain definisce come VIoT (Value Internet of Things) e permette lo scambio di informazioni e di valore tra dispositivi IoT.

WaltonChain utilizza una criptovaluta nativa chiamata WaltonCoin (WTC) che viene utilizzata come mezzo di pagamento all'interno del network. WTC ha raggiunto il miliardo di dollari di market cap a gennaio 2018.

Il principale competitor di

WaltonChain in ambito blockchain può essere considerato VeChain.

Vechain (VET)

VeChain è una Blockchain-as-a-Service che punta a fornire una soluzione per il monitoraggio dei prodotti lungo la supply chain e l'anticontraffazione. Tramite l'utilizzo di tecnologie come RFID, NFC o QR code, unite agli smart contract, VeChain è in grado di digitalizzare dei prodotti fisici (beni di lusso, alimentari, farmaci ecc.), e tenerne traccia lungo tutta la filiera produttiva. In questo modo aziende e consumatori finali hanno accesso alle

informazioni aggiornate di ogni prodotto, avendo la garanzia dell'autenticità del prodotto e del rispetto di tutte le norme produttive (per esempio nel settore alimentare si potrà controllare che un prodotto sia sempre stato conservato alla temperatura adeguata).

Nel 2018 passa a essere una vera e propria piattaforma Dapp (come Ethereum) sviluppando la propria blockchain e cambiando il nome in VeChain Thor.

Decentraland (MANA)

Decentraland è una piattaforma di realtà

virtuale distribuita che si appoggia alla blockchain di Ethereum. Gli utenti possono comprare parti di un mondo virtuale, chiamati LAND, e inserire contenuti su di essi. I LAND sono dei token ERC 721 (token non fungibili), identificati da coordinate cartesiane. La loro proprietà è garantita da uno smart contract. Decentraland utilizza inoltre una valuta nativa chiamata MANA, che implementa lo standard ERC 20 ed è utilizzata per comprare i LAND e altri servizi all'interno della piattaforma.

---

52. Il termine altcoin deriva dalla

combinazione della parola “alternative” (alternativo) e “coin” (moneta).

53. Tra i fondatori di Ripple Labs c’è Jed McCaleb, co-founder di eDonkey, Mt. Gox e Stellar.

54. SWIFT è una rete di pagamenti tramite la quale le banche aderenti possono effettuare trasferimenti internazionali. È il sistema attualmente più utilizzato.

55. https://www.klickex.co/klickex-partners-with-ibm.

56. Charlie Lee, ex Google e Coinbase, è attualmente una delle personalità più in vista nel mondo della blockchain.

11

Exchange

Ci sono diversi modi per entrare in possesso di criptovalute. Per esempio partecipare ad una ICO, diventare dei miner, riceverle da qualcuno ecc.

Se però non si rientra in nessuna di queste casistiche, o se si vuole scambiare delle criptovalute con altri asset, è necessario utilizzare un exchange. Chiunque sia interessato a comprare o vendere criptovalute prima o poi si troverà nella situazione di dover

utilizzare queste piattaforme. È quindi fondamentale conoscerne i meccanismi di base.

Nella prima parte di questo capitolo introdurremo i concetti base del trading che aiuteranno a comprendere meglio la differenza fra i diversi tipi di exchange (chi avesse già molta familiarità con questi concetti può saltare qualche pagina e andare direttamente al paragrafo sulla "Manipolazione del mercato").

Un exchange di criptovalute (cripto-exchange, o cryptocurrency exchange) segue gli stessi concetti base (e solitamente la stessa terminologia) di altri exchange come per esempio il Nasdaq o la Borsa italiana. Un cripto-

exchange può inoltre essere centralizzato, e quindi gestire i fondi degli utenti agendo come intermediario nelle transazioni, oppure decentralizzato, appoggiandosi a una struttura peer-to-peer.

Un cripto-exchange è una piattaforma che permette agli utenti di scambiare criptovalute con altre criptovalute o denaro fiat, seguendo le leggi della domanda e dell'offerta. L'esecuzione di un ordine viene chiamato trade.

Ogni exchange può contenere diversi **mercati** (per esempio il mercato dove si scambiano bitcoin e dollari, il mercato dove si scambiano ether e bitcoin ecc.) (Figura 11.1).

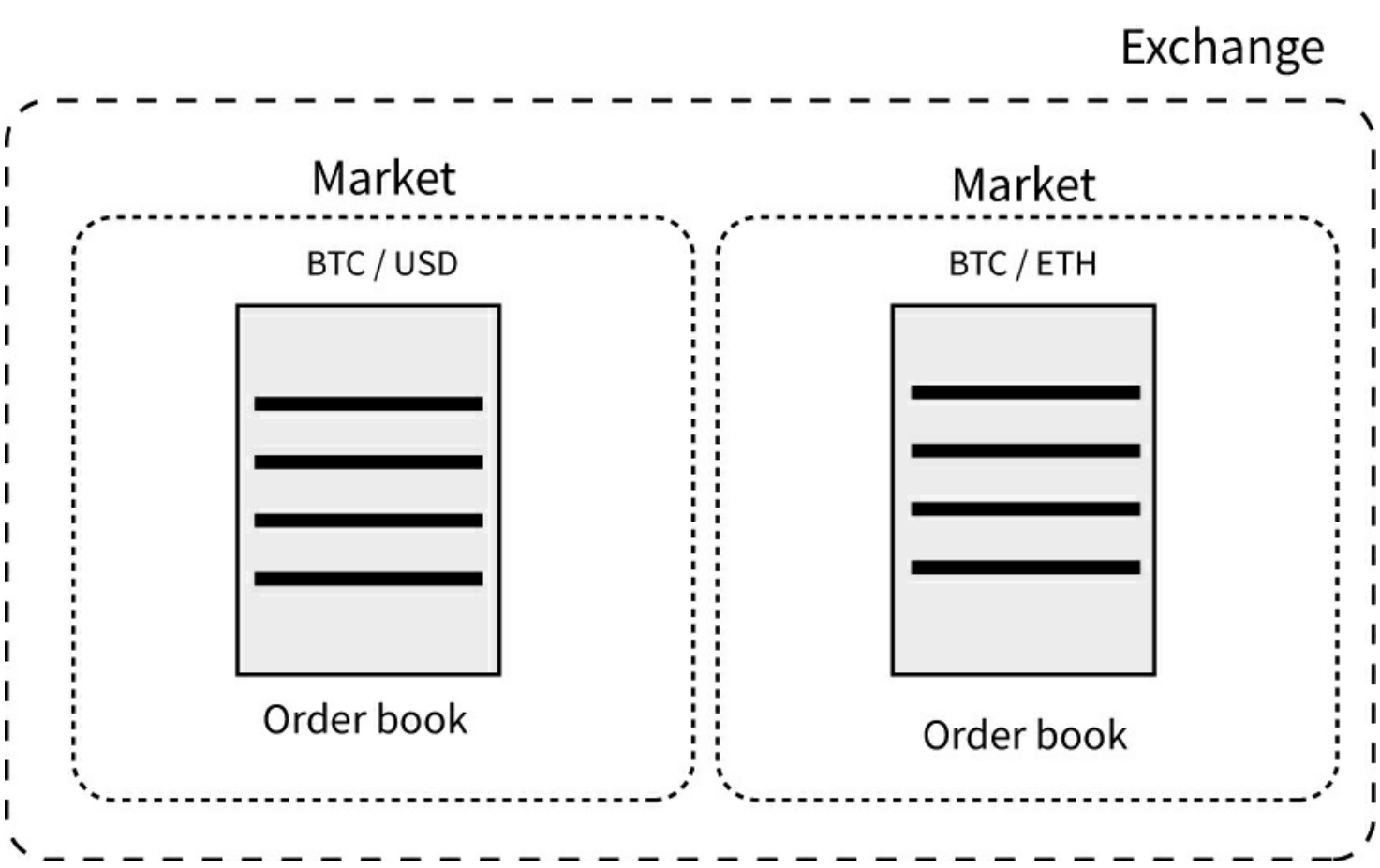


Figura 11.1 – La struttura di un exchange.

Ogni mercato è un'entità indipendente che segue le proprie regole della domanda e dell'offerta, espresse nella forma di ordini d'acquisto (**bid**) o di vendita (**ask**). Tutti gli ordini di uno specifico mercato vengono raggruppati in una lista digitale chiamata **order book**

(libro degli ordini).

Mercato

Un mercato (market) è un luogo dove avviene uno scambio di beni, in questo caso di criptovalute.

Un mercato è composto da una coppia di asset (pair) come per esempio bitcoin e dollari (BTC/USD), o bitcoin ed ether (BTC/ETH).

Solitamente i mercati vengono

raggruppati per **valuta base** (base currency). Si parla quindi di mercati basati sul bitcoin per indicare l'insieme di tutti i mercati dove è possibile scambiare bitcoin (BTC/USDT, BTC/USD, BTC/EUR, BTC/ETH ecc.).

Un exchange ha quindi diversi mercati e ogni mercato ha il proprio order book (Figura 11.2).

Coppia	Ultimo prezzo	Coppia	Ultimo prezzo
BCC/BTC	0.068631 / $453.72	BTC/USDT	6,610.60 / $6,610.60
ETH/BTC	0.031324 / $207.08	BCC/USDT	453.81 / $453.81
DASH/BTC	0.024258 / $160.37	ETH/USDT	207.16 / $207.16
ZEC/BTC	0.019275 / $127.43	LTC/USDT	53.71 / $53.71
XMR/BTC	0.016616 / $109.85	NEO/USDT	17.024 / $17.02

Figura 11.2 – Una porzione dei mercati basati su USDT e BTC sull'exchange Binance. © Binance.

Order book e order matching

Ogni mercato è governato dal suo order book che definisce in tempo reale la domanda (bid) e l'offerta (ask) per quel mercato.

> Un order book mostra in tempo reale tutti gli ordini **aperti** di acquisto e vendita, disposti in base al prezzo.

L'order book viene utilizzato per

accoppiare (match) ordini di acquisto e vendita compatibili. Per esempio, un ordine di acquisto di 1 BTC a $6.000 è compatibile a un ordine di vendita di 1 BTC a $6.000 (d'ora in avanti useremo la forma 1 BTC @ $6.000).

L'order book definisce anche i prezzi d'acquisto e di vendita di un asset, chiamati **bid price** e **ask price**. Il prezzo di un asset in un mercato è definito dal prezzo a cui è avvenuto l'ultimo trade, ovvero dall'ultimo incontro tra domanda e offerta.

Se non è presente alcun ordine di acquisto che sia compatibile con un ordine di vendita (o viceversa) non è possibile eseguire alcun trade (Figura 11.3).

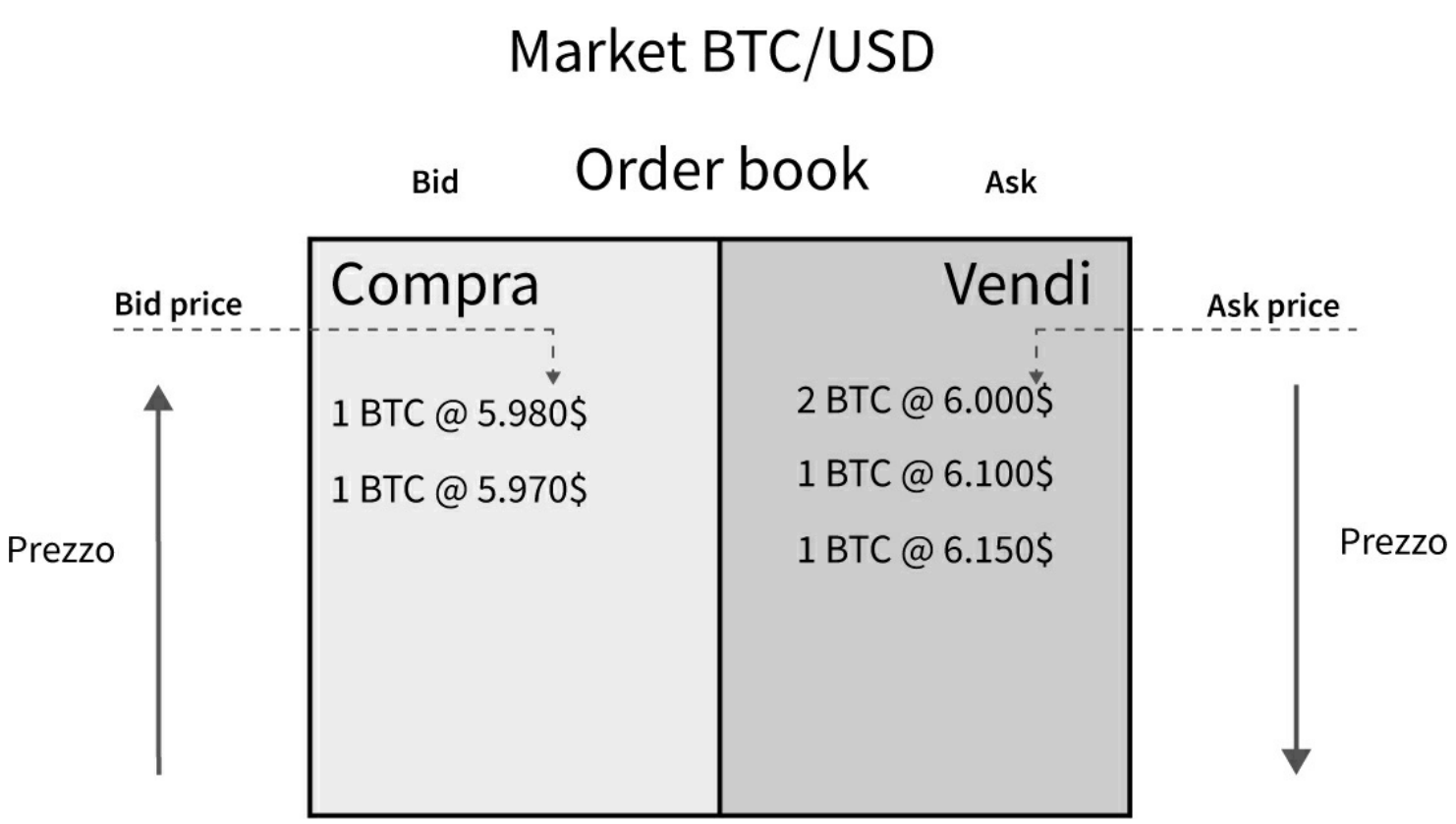


Figura 11.3 – Un esempio di order book.

Successivamente viene creato un ordine di acquisto di 1 BTC @ $6.000 che viene aggiunto all'order book, e dal momento che domanda e offerta si incontrano, è possibile eseguire un trade (Figura 11.4).

Una volta che il trade è avvenuto, l'order book viene aggiornato

rimuovendo gli ordini che sono stati soddisfatti (Figura 11.5).

Viene inoltre aggiornato il prezzo dell'asset, che diventa il prezzo (unitario) a cui è avvenuto l'ultimo trade, in questo caso $6.000 per BTC.

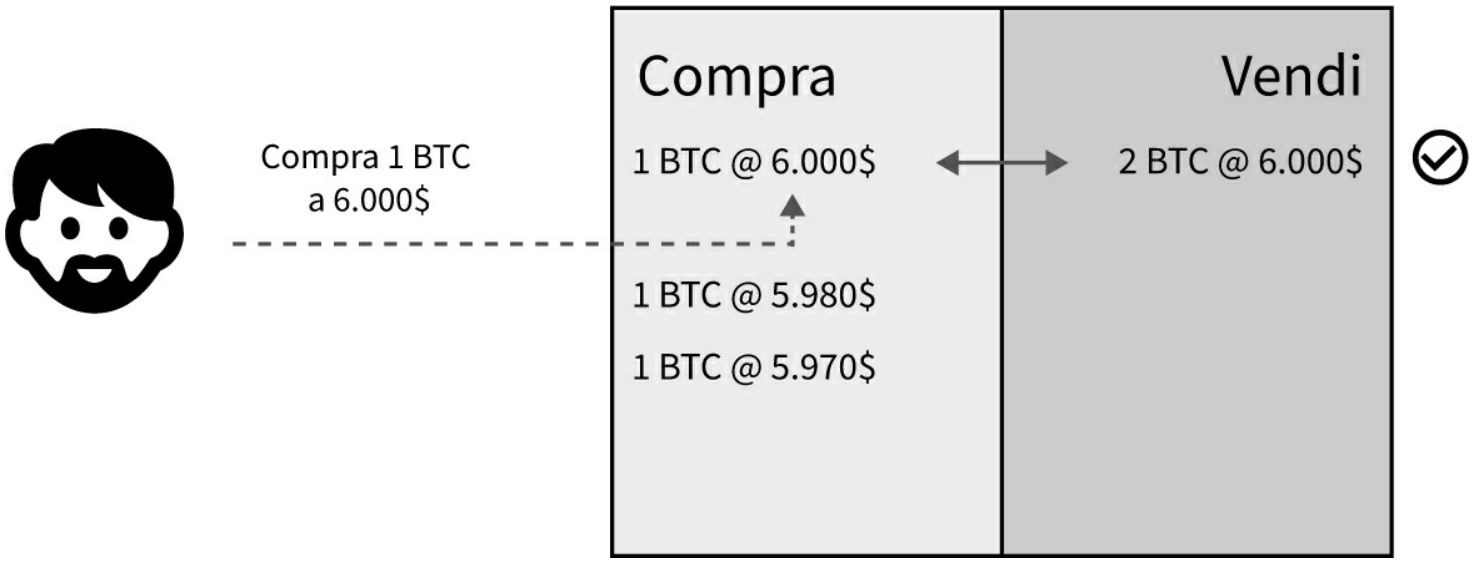


Figura 11.4 – Inserimento di un ordine nell'order book.

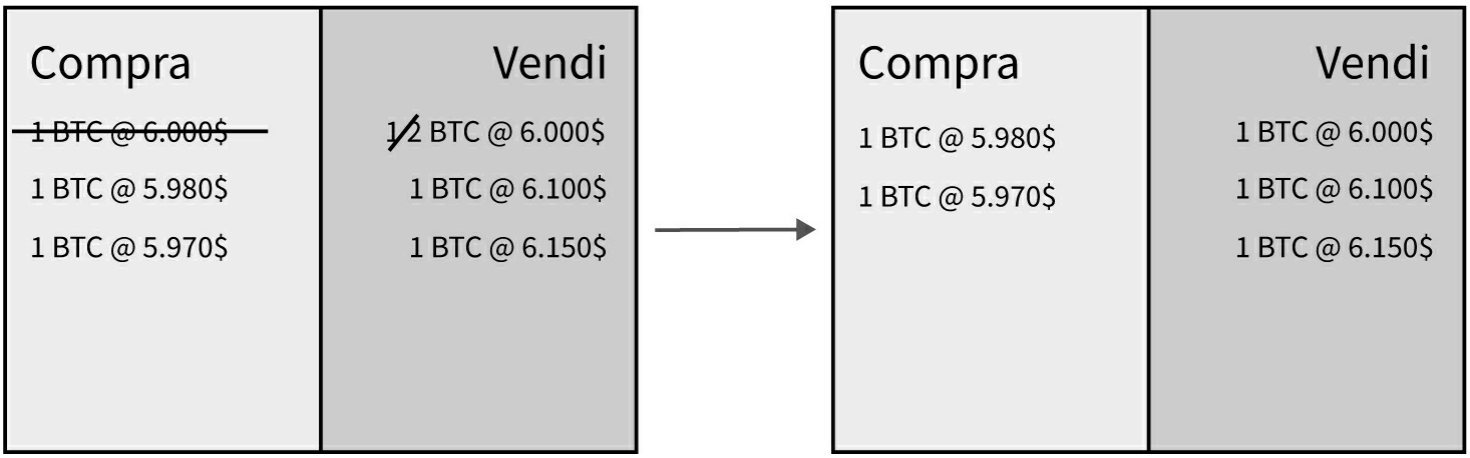


Figura 11.5 – L'aggiornamento dell'order book dopo un trade.

Ordini parziali

Può succedere che nonostante ci sia un match tra due ordini, questi non possano venire eseguiti completamente ma solo in parte. In questo caso di solito l'ordine viene eseguito parzialmente (Figura 11.6).

Nella Figura 11.6 vediamo come ci sia un incontro tra domanda e offerta, ma

in questo caso l'offerta (0,5 BTC) non è sufficiente a soddisfare la domanda (1 BTC). L'ordine viene quindi eseguito parzialmente per un valore di 0,5 BTC e l'order book viene aggiornato in attesa di un altro ordine.

Bid-ask Spread

Quando non c'è un punto di incontro da domanda e offerta, non è possibile alcuno scambio. Bisogna aspettare che:

- un compratore sia disposto ad aumentare l'offerta;
- un venditore sia disposto ad abbassare la domanda;

- vengano create nuove offerte.

In una situazione del genere si parla di spread (divario) tra domanda (bid) e offerta (ask).

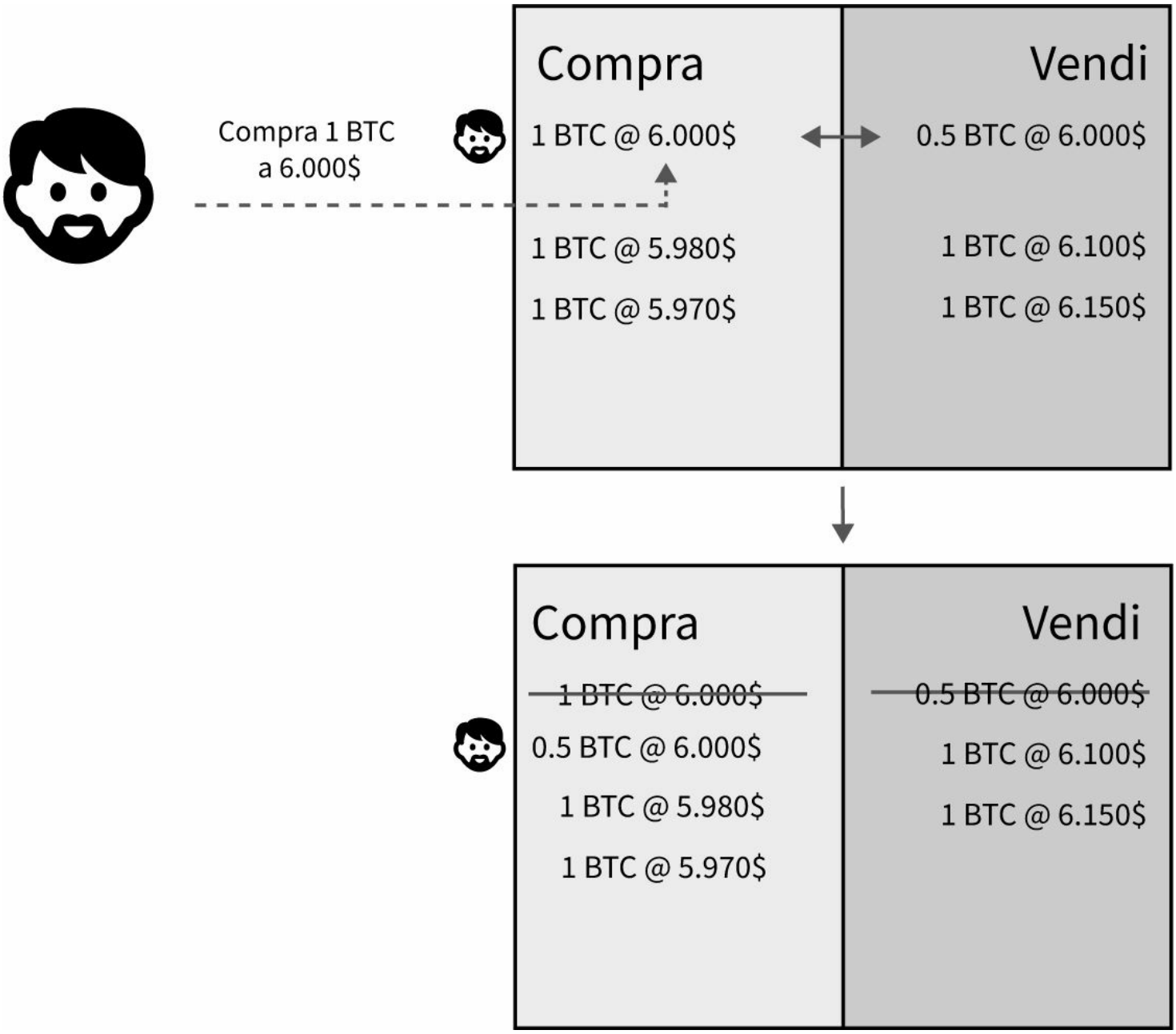


Figura 11.6 – Risoluzione parziale di un ordine.

Il bid-ask spread è un valore che esprime la differenza di

prezzo tra domanda e offerta. Rappresenta la differenza tra il prezzo più alto che un compratore è disposto a pagare e il prezzo più basso che un venditore è disposto ad accettare.

Nella Figura 11.7 il prezzo più alto che un compratore è disposto a pagare per 1 BTC è di $5.980, mentre il prezzo più basso che un venditore è disposto ad accettare è $6.000. Il bid-ask spread è in questo caso di $20 (5.980 - 6.000) e viene solitamente espresso in forma percentuale (0,3%).

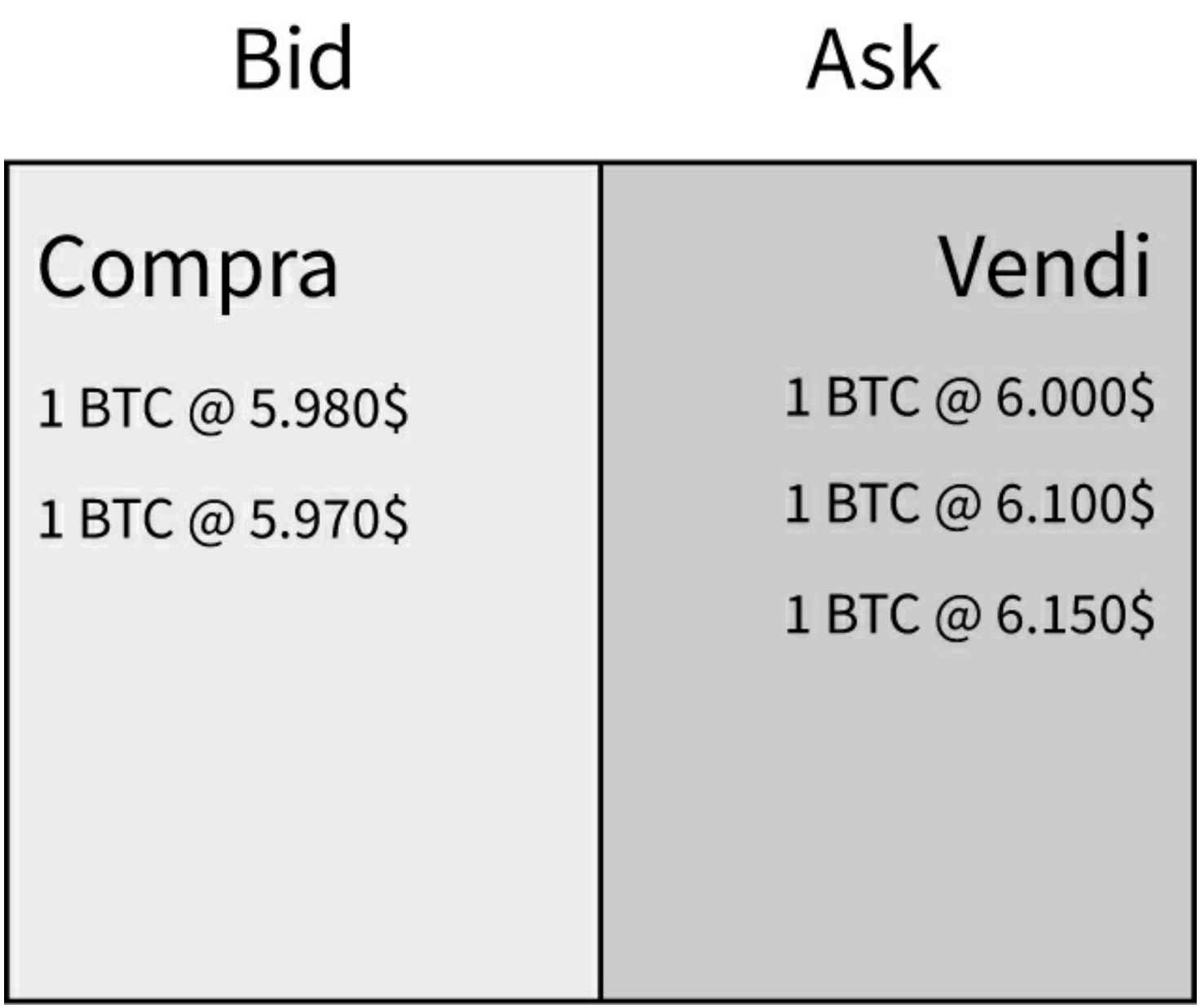


Figura 11.7 – Bid-ask spread di $20 (0,3%).

Interpretazione del bid-ask spread

Il bid-ask spread è un

indicatore dell'attuale stato di domanda e offerta in un particolare mercato.

Per la legge di domanda e offerta, un asset avrà un trend positivo quando i compratori sono in numero maggiore dei venditori (la domanda supera l'offerta) e avrà un trend negativo nel caso opposto (l'offerta supera la domanda).

Il bid-ask spread di un mercato è associato inoltre al concetto di **liquidità**. Un mercato si dice essere liquido se è facile eseguire dei trade in maniera rapida e al prezzo desiderato, in quanto ci sono molti compratori e venditori. Il termine liquido deriva dal fatto che è

facile “liquidare” (vendere) i propri asset.

> In un mercato liquido, il bid-ask spread è basso.

Per mercati poco liquidi, al contrario, lo spread tende ad aumentare, a conferma della lontananza tra domanda e offerta.

Profondità di un mercato (market depth)

Un concetto strettamente legato alla liquidità è la profondità di un mercato.

Per profondità di un mercato si

intende la capacità di uno specifico mercato di soddisfare ordini (anche molto grandi) senza che il prezzo dell'asset venga alterato in maniera considerevole (Figura 11.8).

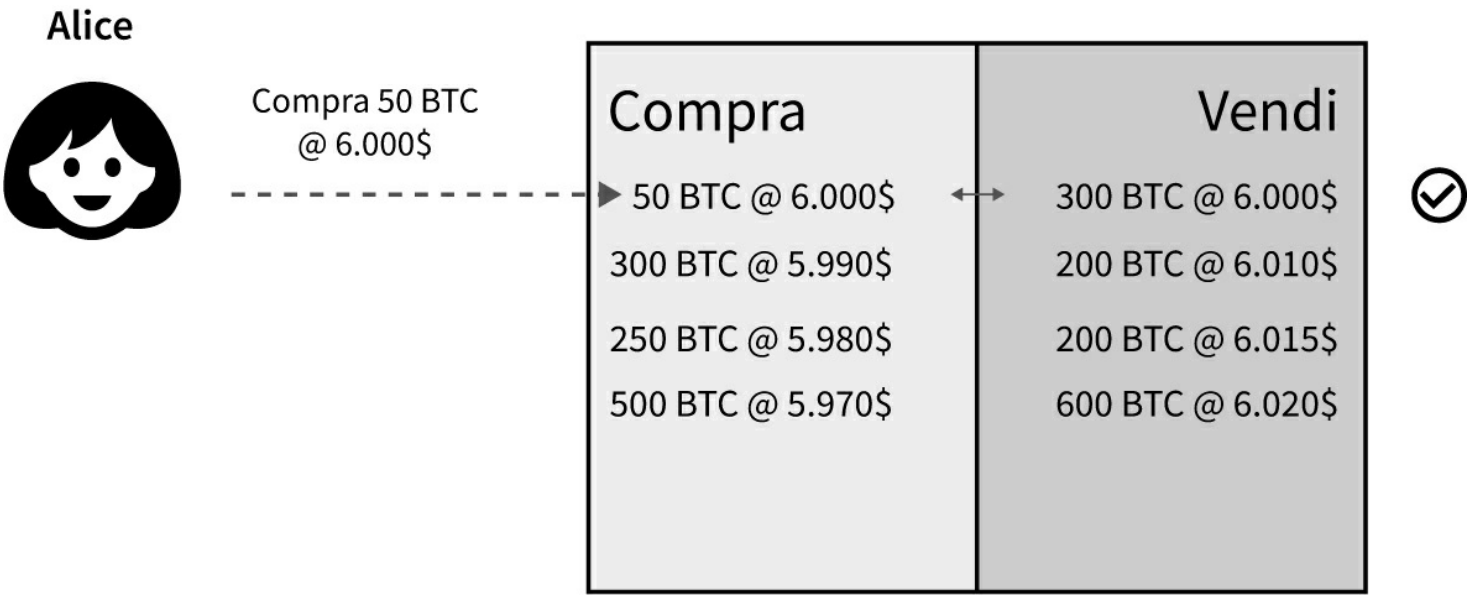


Figura 11.8 – Order book di un mercato profondo.

Se Alice effettua un ordine di acquisto di 50 BTC @ $6.000 non modifica il prezzo del bitcoin in questo mercato. Dopo questa operazione, infatti, restano ancora 250 BTC @ $6.000, quindi il prezzo del bitcoin rimane $6.000.

Interpretazione della profondità del

mercato

La profondità indica quanti ordini possono essere soddisfatti per ogni fascia di prezzo, senza causare una modifica del prezzo stesso. Nel caso precedente, è possibile comprare fino a 300 BTC senza influenzarne il prezzo. Solitamente un mercato molto profondo permette di eseguire grossi ordini senza influenzare il prezzo dell'asset.

La profondità di un mercato viene solitamente rappresentata in maniera cumulativa, aggregando tutti gli ordini allo stesso prezzo (Figura 11.9).

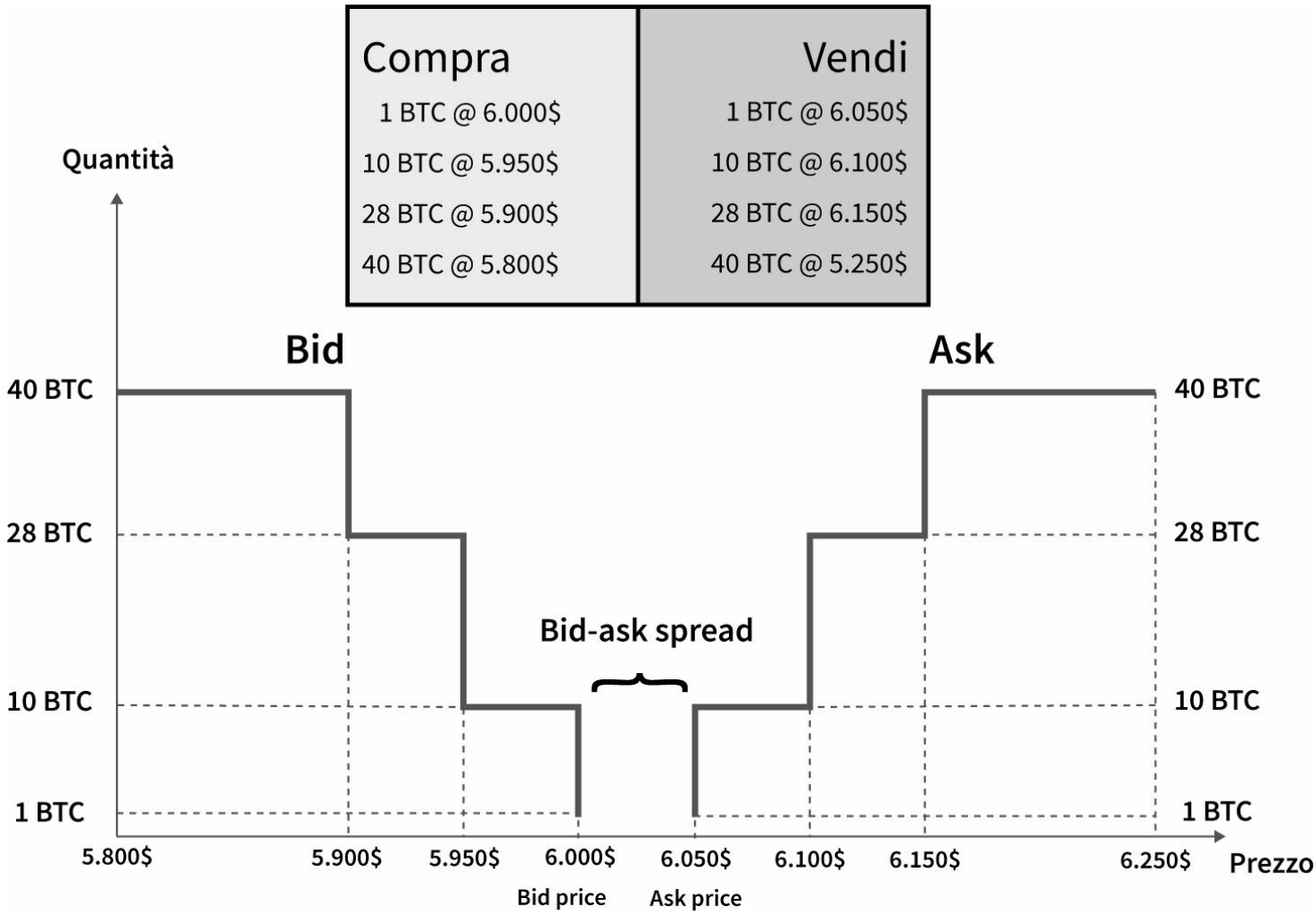


Figura 11.9 – Profondità del mercato BTC/USD.

Su questi grafici si possono spesso notare delle grosse concentrazioni di ordini a particolari livelli di prezzo. In gergo ci si riferisce a queste concentrazioni con il termine **buy wall**

(muro di acquisti) o **sell wall** (muro di vendite), a causa della particolare forma con cui dei grossi ordini vengono rappresentati (Figura 11.10). I buy wall e i sell wall sono spesso il risultato di bot che reagiscono in maniera simile, oppure, come vedremo in seguito, possono essere tecniche di manipolazione di mercato.

Figura 11.10 – Un grafico della profondità del mercato BTC/USD che raffigura un sell wall a circa $6.600, su Binance. © Binance.

Volume

Il volume indica il numero di asset scambiati in un determinato periodo di tempo (solitamente 24 ore) e viene

misurato utilizzando la valuta base del mercato. Nella Figura 11.11, per esempio, sono riportati alcuni mercati con valuta base USDT, in cui il volume è espresso in Tether, e BTC, in cui il volume è espresso in bitcoin.

Coppia	Volume 24h	Coppia	Volume 24h
BCC/BTC	960.66577794	BTC/USDT	82,761,151.18090884
ETH/BTC	4,133.42284683	BCC/USDT	4,027,684.38906250
DASH/BTC	274.87977398	ETH/USDT	20,093,086.35788120
ZEC/BTC	172.05004882	LTC/USDT	2,696,949.89892940
XMR/BTC	306.88378012	NEO/USDT	3,954,156.42874400

Figura 11.11 – Il volume 24h di mercati con base USDT (a sinistra) e BTC (destra). © Binance.

Il volume può far riferimento a un singolo mercato oppure indicare il volume cumulativo di più mercati. Si può quindi parlare del volume nel mercato BTC/USD o del volume dell'intero mercato delle criptovalute. Nel secondo caso si andrà a sommare il volume di tutti i mercati dove vengono scambiare criptovalute.

Ogni transazione contribuisce ad aumentare il volume. Se, per esempio, nelle ultime 24 ore, nel mercato BTC/USD sono stati scambiati 1.000 BTC, il volume di questo mercato è di $6 milioni (1 BTC = $6.000). Il volume (24 ore) del mercato delle criptovalute ha toccato picchi di 60 miliardi a

dicembre 2017[57].

Volatilità

Spesso ci si riferisce alle criptovalute come asset molto volatili.

> La volatilità misura quanto il prezzo di un determinato asset tenda a variare nel tempo.
>
> Maggiore è la volatilità, maggiore saranno le variazioni di prezzo.
>
> La volatilità è strettamente collegata al concetto di rischio: più alta è la volatilità maggiore è il rischio di un

investimento.

Analizzare la volatilità di un asset, e quindi il suo rischio, è fondamentale nella scelta di un investimento e nella creazione di un portafoglio[58].

La volatilità è legata anche al concetto di liquidità: maggiore è la volatilità, minore è la liquidità (la possibilità di effettuare un ordine al prezzo desiderato).

In generale, tutti i mercati di criptovalute si possono considerare volatili.

Posizioni

Una posizione identifica una particolare strategia con cui si decide di entrare in un mercato. Esistono due modalità di ingresso in un mercato: **long** e **short**.

Una posizione long (long position) indica una situazione nella quale si punta a trarre profitto da un mercato in trend positivo (bull market).

Una posizione short (short position) punta a trarre profitto da un mercato in trend negativo (bear market).

Long position

Una posizione long è il metodo tradizionale di investimento: si compra un asset e si spera che il suo valore aumenti nel tempo.

Per esempio, si compra un BTC sperando che il prezzo salga. Tutti i criptoexchange supportano questo tipo di operazioni.

Una posizione long è caratterizzata da profitti teoricamente illimitati e perdite limitate. Se infatti si compra un BTC a $6.000, il massimo che si potrà perdere sono $6.000 se il prezzo del BTC va a $0, ma non essendoci un prezzo massimo, il profitto teoricamente è illimitato.

Short position

Nella definizione più semplice, una posizione short è l'opposto di una posizione long. Se quindi nel mercato BTC/USD andare long sul BTC significa comprare BTC sperando che il prezzo del BTC aumenti rispetto al dollaro, andare short sul BTC comporta una vendita dello stesso, sperando che il prezzo del BTC scenda rispetto al dollaro. Questo in quanto in un mercato generico A/B, se il prezzo di A sale rispetto a B, per forza di cose il prezzo di B scende rispetto ad A.

Il termine "short" è inoltre spesso utilizzato in ambito margin trading, una pratica in cui si utilizzano fondi presi in

prestito per eseguire i trade (che spiegheremo nel prossimo paragrafo).

In seguito useremo il termine "posizione short" sempre nell'ambito del margin trading, in quanto è il contesto a cui si fa riferimento nei cripto-exchange.

> Una short position implica la vendita di un asset senza possederlo (apertura di una posizione short), seguita in un secondo momento dall'acquisto dell'asset stesso (chiusura della posizione short).

Vendere un asset senza possederlo significa vendere qualcosa che ci è stato prestato. Quindi con una posizione short stiamo di fatto vendendo degli asset presi in prestito da qualcuno, nella speranza di poter saldare il debito ricomprando lo stesso asset a un prezzo più basso.

> Una posizione short permette di trarre profitto anche in un mercato con un trend negativo.

Se, per esempio, apriamo una posizione short nel mercato BTC/USD di 1 BTC quando il bitcoin è a $6.000, stiamo di fatto vendendo 1 bitcoin (prestato per

esempio dall'exchange) a $6.000 nella speranza di poterlo ricomprare a un prezzo inferiore. Se il prezzo del bitcoin scende a $5.000 possiamo chiudere la posizione short con un profitto di $1.000.

Non tutti i cripto-exchange supportano le posizioni short e solitamente viene richiesto un account abilitato al **margin trading**.

Al contrario di una posizione long, dove le perdite possibili sono limitate, nel caso di una posizione short le potenziali perdite sono illimitate.

Margin trading e leva

finanziaria

Nel mercato delle criptovalute è sconsigliato utilizzare il margin trading e la leva finanziaria, in quanto la volatilità del mercato è estremamente elevata e può portare a una rapida perdita dei propri averi.

> Il margin trading fa riferimento a una pratica nella quale si utilizzano fondi presi in prestito per eseguire dei trade.

Nel nostro caso saranno i cripto-exchange a effettuare il prestito,

utilizzando i fondi dell'utente come garanzia (collaterale).

> Nel margin trading i fondi dell'utente diventano il collaterale del prestito.

Lo scopo principale del margin trading è quello di permettere l'utilizzo della **leva finanziaria**, uno strumento che permette di moltiplicare il valore di una posizione, andando ad amplificare i guadagni (e le perdite) di un trade. Solitamente gli exchange richiedono un collaterale che copra dal 30% al 50% del valore del prestito di una particolare posizione.

Se per esempio l'exchange ci richiede che il collaterale copra almeno il 30% della posizione e abbiamo $1.000 nel nostro account, possiamo di fatto aprire una posizione per un valore di 1.000 × (1/0,3) = $3333,33. Quindi la massima leva che possiamo usare è **3,33 : 1** (la leva finanziaria viene solitamente espressa come proporzione).

Se siamo in una posizione long da $100 con leva 3:1 e il valore dell'asset aumenta del 10%, avremo guadagnato (300 × 0,1) = $30. Se invece il valore dell'asset scende, avremo perso $30 (Figura 11.12).

Bisogna quindi fare molta attenzione se si decide di eseguire trade utilizzando

la leva. Può succedere infatti che il collaterale non sia più sufficiente a coprire il valore del trade e quindi la posizione venga chiusa (liquidata) in automatico. Nel mercato delle criptovalute, a causa della grande volatilità, questo evento è abbastanza comune.

Per questo motivo è fondamentale quando si fa trading (e ancora di più quando si utilizza margin trading) utilizzare delle tipologie di ordine che ci riparino da eventuali movimenti bruschi del mercato in una direzione sfavorevole rispetto alla nostra posizione.

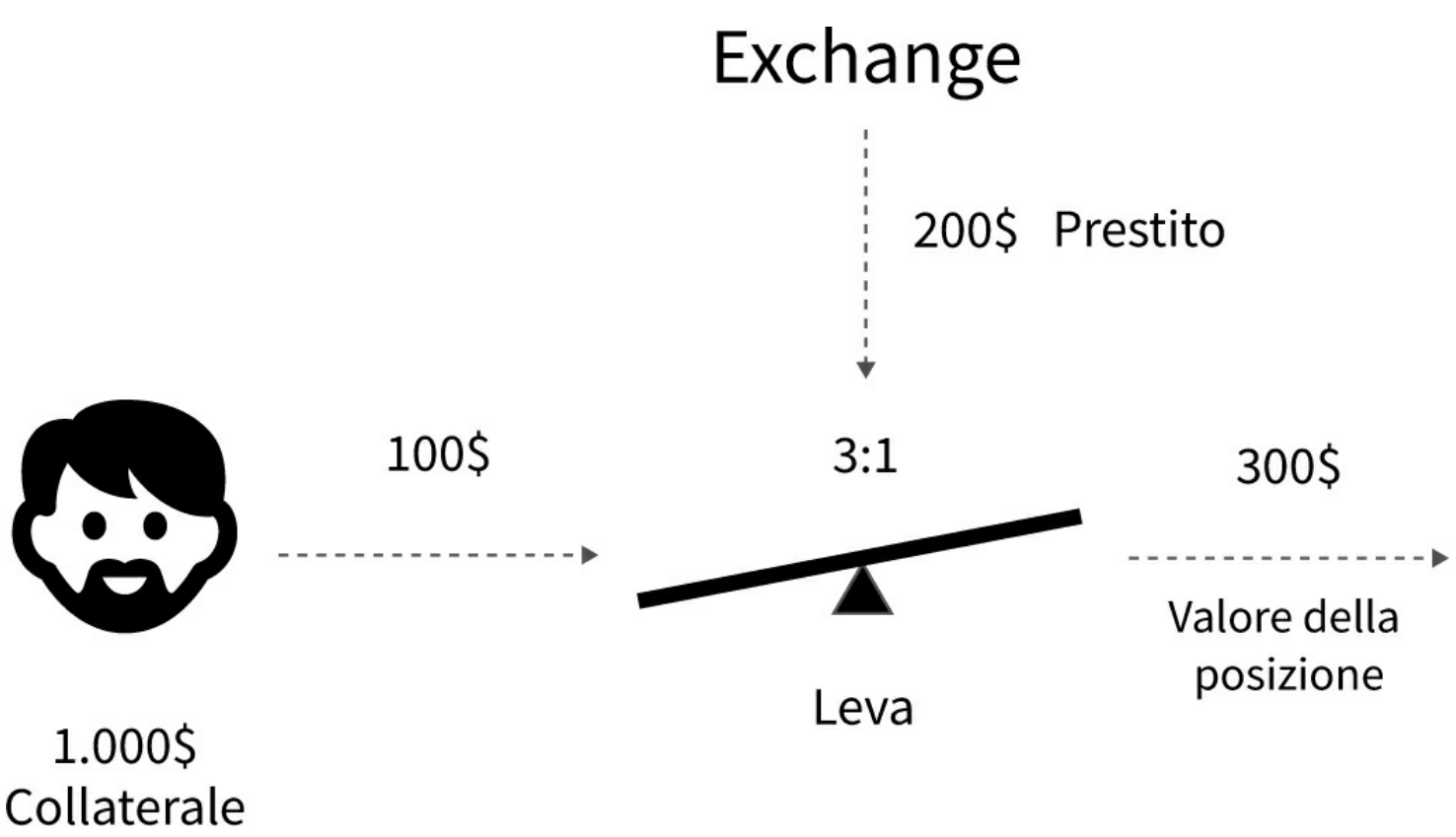


Figura 11.12 – La leva nel margin trading.

Tipologie di ordine

Finora abbiamo visto solo degli ordini di acquisto o vendita a dei prezzi specifici, per esempio un ordine di acquisto di 1 BTC @ $6.000. Solitamente, però, gli exchange offrono

diverse tipologie di ordini che possono tornare estremamente utili in particolari scenari e sono fondamentali nella gestione del rischio.

Market order

Un market order è la tipologia più semplice di ordine e quella comunemente più utilizzata. Un market order è l'ordine di acquisto o di vendita al miglior prezzo possibile, chiamato **market price** (prezzo di mercato). Nel caso di un acquisto, il miglior prezzo è il più basso tra gli ordini di vendita. Nel caso di una vendita, è il più alto tra gli ordini di acquisto. Se è presente almeno

una controparte, un market order verrà sempre eseguito.

Un market order dà la priorità all'esecuzione dell'ordine piuttosto che al prezzo al quale verrà eseguito. Sebbene l'esecuzione venga garantita, non avviene nessun controllo sul prezzo. In mercati molto volatili come quello delle criptovalute il prezzo di esecuzione di un market order può differire notevolmente rispetto al prezzo corrente (Figura 11.13).

Indicheremo un market order nella forma 1 BTC @ * (Figura 11.14).

Il simbolo star, *, viene utilizzato per esprimere il concetto "qualsiasi valore". Poiché i market order vengono sempre eseguiti finché c'è una

controparte, è necessario stare particolarmente attenti in mercati poco profondi, in quanto si potrebbe finire per eseguire un trade a un prezzo molto diverso da quello che si aveva in mente.

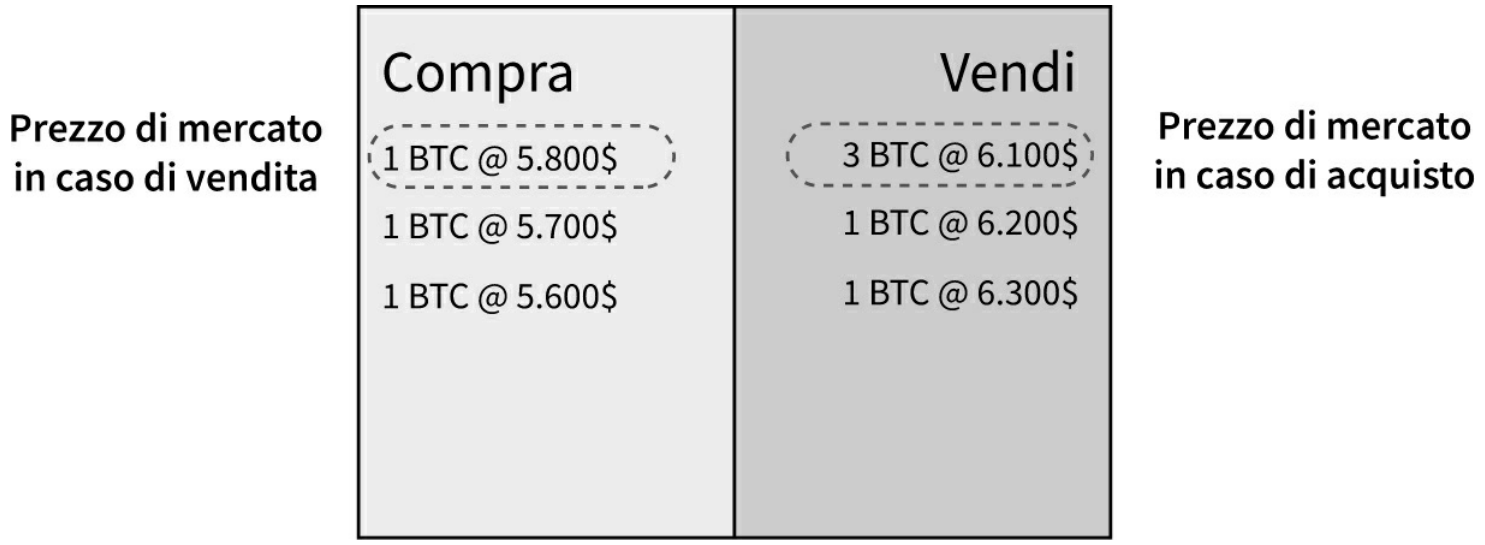


Figura 11.13 – I prezzi di mercato in un order book.

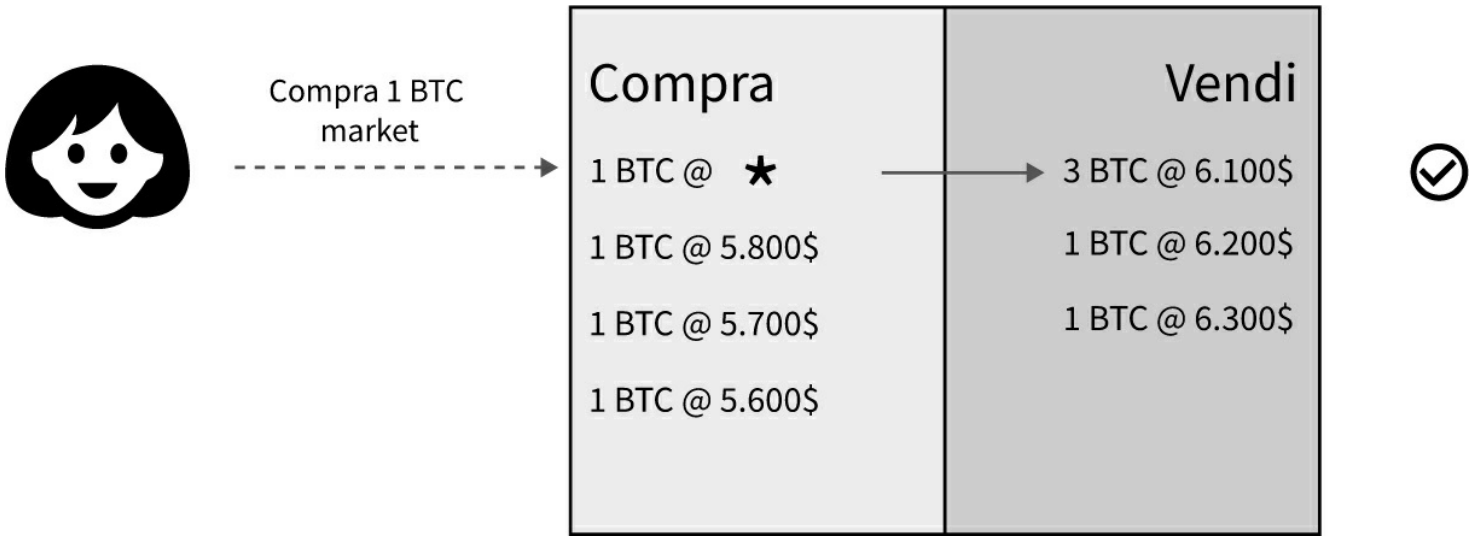


Figura 11.14 – L'esecuzione di un market order.

Prendiamo per esempio il caso di un mercato BTC/USD nel quale l'ultimo trade è stato fatto a un prezzo unitario del bitcoin di $6.000. L'exchange, quindi, ci comunicherà che il prezzo di mercato del bitcoin è $6.000. Vedendo il bitcoin a un buon prezzo, Marco decide di comprare 50 BTC, e crea un market buy order per 50 BTC, senza

accorgersi di quanto il mercato sia poco profondo (Figura 11.15).

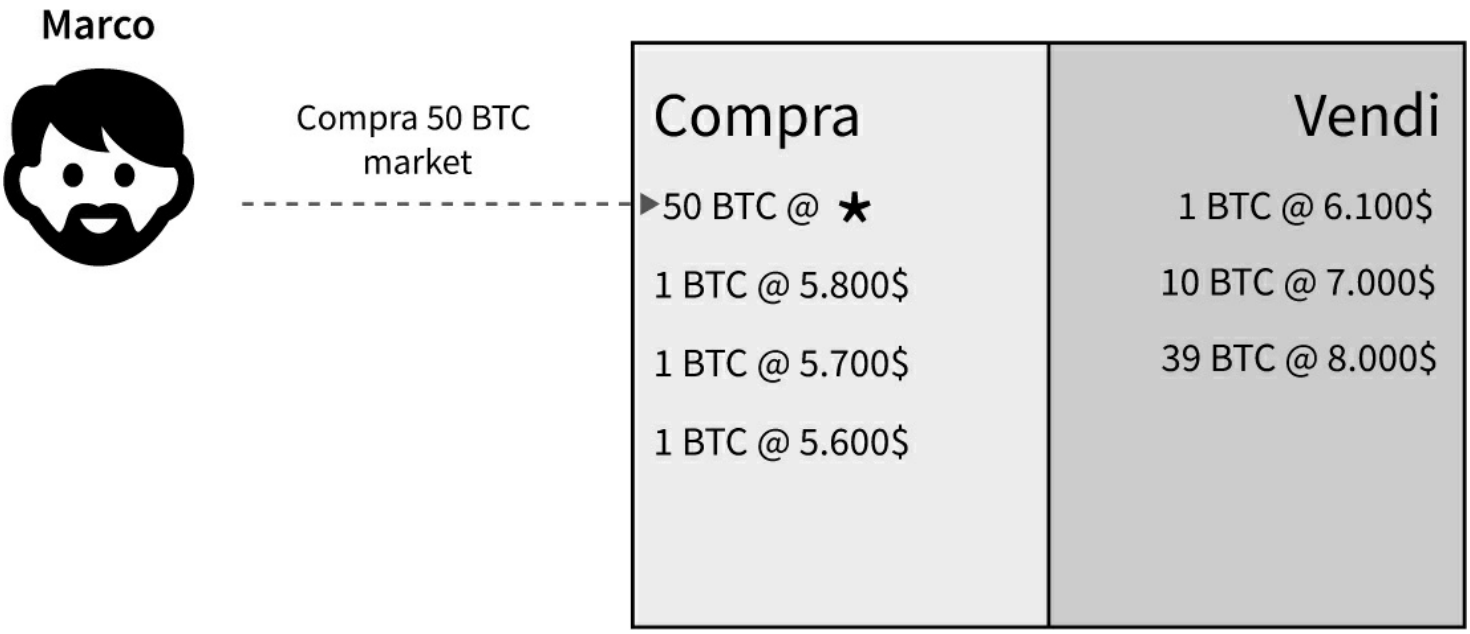


Figura 11.15 – La creazione di un grosso market order in un mercato poco profondo.

L'ordine di acquisto viene eseguito, partendo dal prezzo migliore e continuando finché l'ordine non viene soddisfatto. Essendo un market order, infatti, non c'è alcun controllo o limitazione sul prezzo (Figura 11.16).

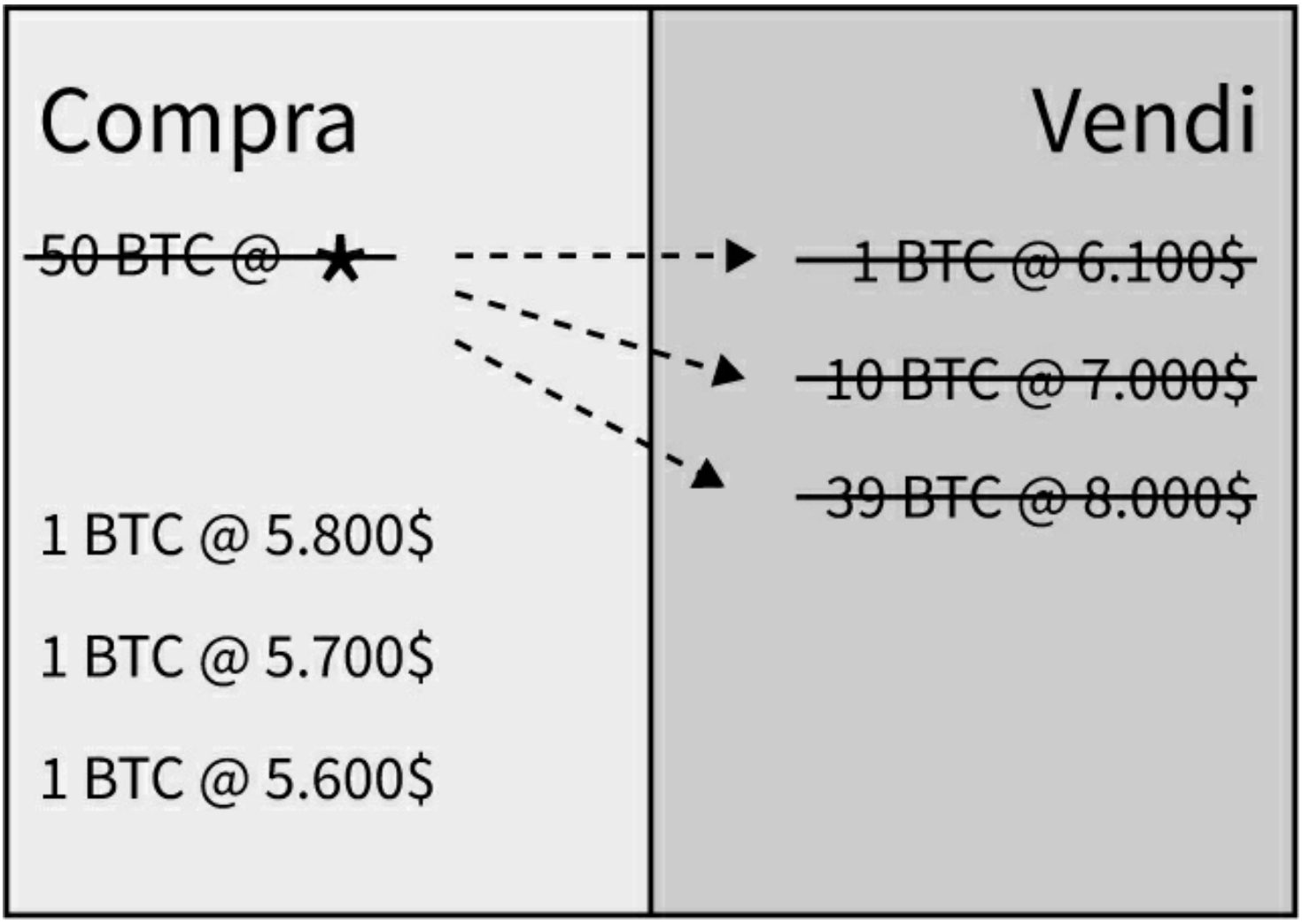


Figura 11.16 – L'esecuzione di un market order in un mercato poco profondo.

Il prezzo finale medio a cui Marco ha comprato i bitcoin è stato quindi $7.762, oltre il 20% in più rispetto al prezzo di mercato a cui aveva intenzione di comprarli. In più, questo singolo ordine

ha fatto aumentare di oltre il 20% il prezzo del bitcoin.

Graficamente, il risultato apparirà simile a quello in Figura 11.17.

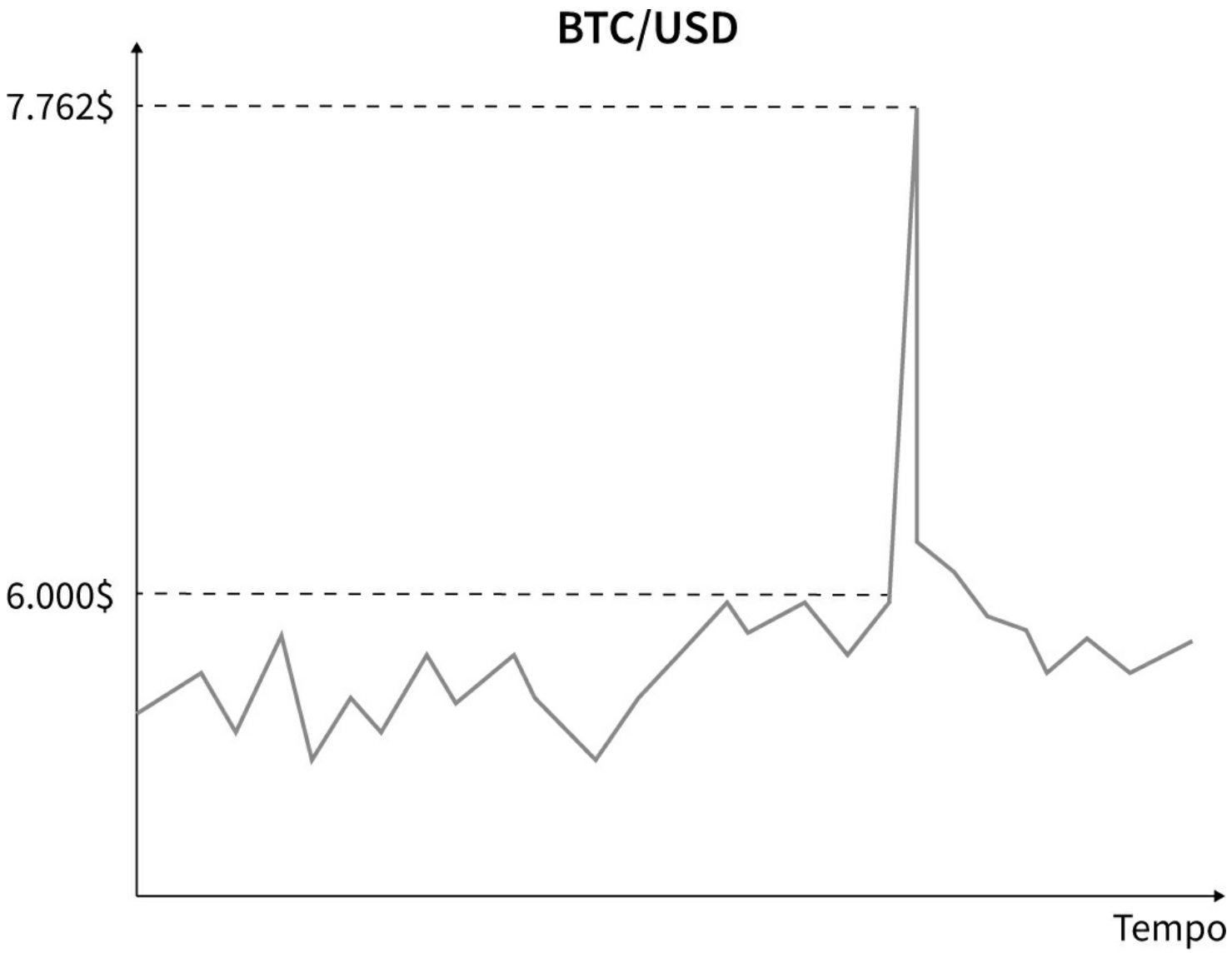


Figura 11.17 – L'oscillazione di prezzo dovuta a un grosso acquisto in un mercato poco profondo.

Una situazione come quella appena descritta potrebbe essere un errore di trading, oppure potrebbe nascondere una

strategia mirata. Come vedremo in seguito, infatti, questi movimenti importanti di prezzo, se volontari, sono una strategia che punta a far scattare gli ordini automatici e i bot (**stop hunting**).

Limit order

> Un limit order è un ordine di acquisto (buy limit order) o di vendita (sell limit order) di un asset a un determinato prezzo, o eventualmente a un prezzo migliore.

A differenza di un market order, un limit

order potrebbe non venir mai eseguito, ma garantisce il rispetto del prezzo imposto.

Se per esempio un utente crea un limit buy order per 1 BTC @ $6.000 significa che vuole comprare un bitcoin *esattamente* a $6.000, o eventualmente a un prezzo inferiore. Similmente, un limit sell order per 1 BTC @ $6.000 significa che l'utente vuole vendere 1 bitcoin *esattamente* a $6.000, o eventualmente un prezzo superiore (Figura 11.18).

Figura 11.18 – Esempi di limit order.

Un limit order viene utilizzato quando la garanzia del prezzo è più importante della garanzia di esecuzione.

Stop loss

Uno stop loss è un ordine di acquisto o vendita che viene attivato nel momento in cui un asset raggiunge un determinato prezzo, chiamato **stop**. Quando il prezzo

di stop è raggiunto, viene creato un market order.

Un **buy stop** crea un market buy order nel momento in cui l'asset raggiunge il prezzo di stop. Un **sell stop** funziona nel modo opposto.

Se, per esempio, un utente crea un sell stop order di 1 BTC @ $6.000 (Figura 11.19), nel momento in cui il bitcoin raggiungerà lo stop verrà creato un ordine di mercato. Nella figura 11.19 il sell market order viene chiuso a $5.950.

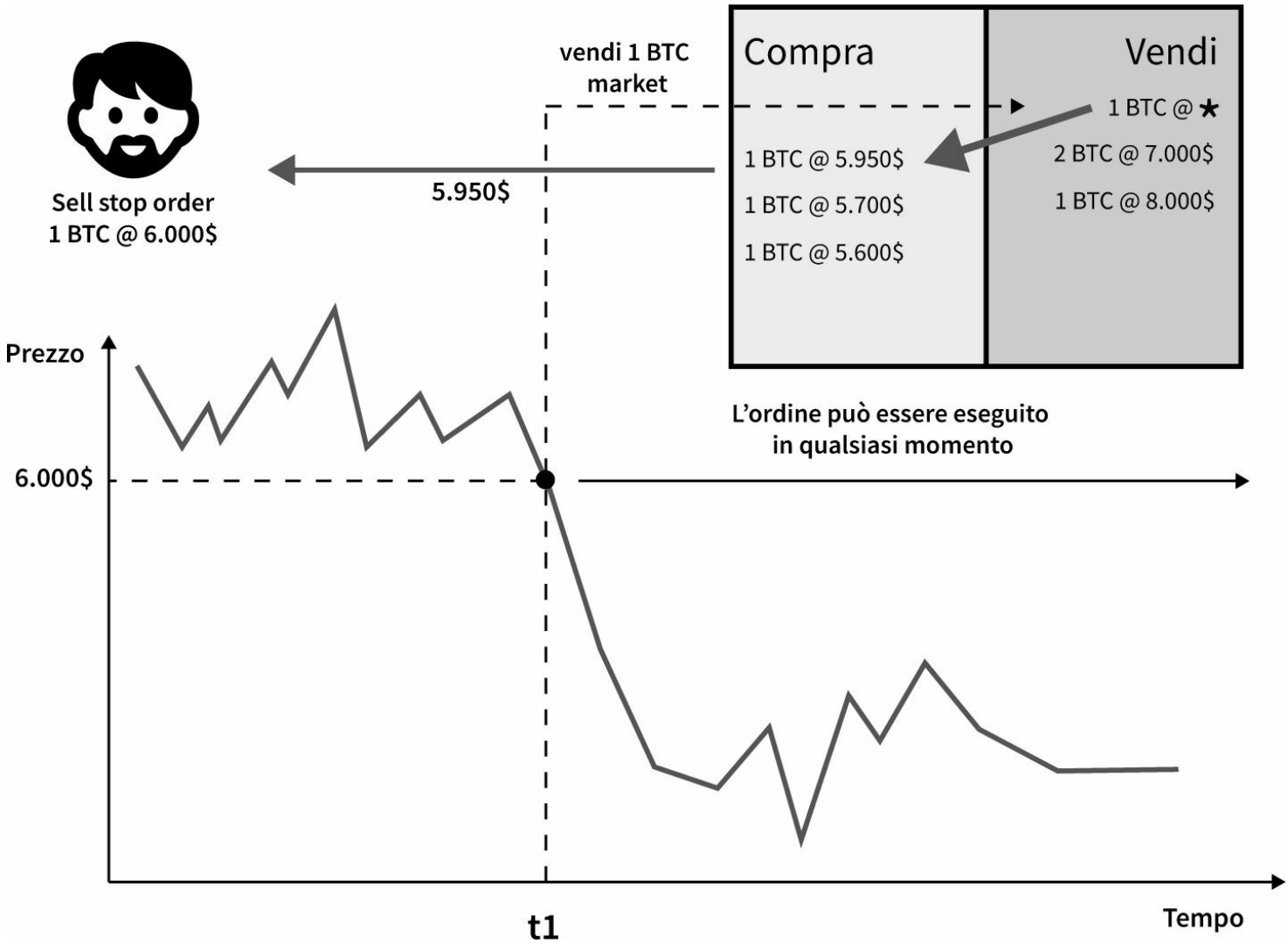


Figura 11.19 – L'esecuzione di un sell stop order.

In mercati molto volatili il prezzo di esecuzione di un ordine stop loss potrebbe spostarsi significativamente dal prezzo di stop.

Stop hunting

Gli stop loss sono a tutti gli effetti una versione molto basilare di trading automatico, in quanto vengono creati degli ordini in maniera automatica, senza la supervisione umana. Questo ha portato alcuni trader a sfruttare questa situazione, utilizzando una tecnica chiamata stop hunting (o stop fishing: andare a caccia/pesca degli stop).

L'idea dello stop hunting è quella di causare una modifica del prezzo sufficiente a far scattare gli stop loss. Gli stop loss sono infatti solitamente concentrati su livelli di prezzo (più o meno) prevedibili, chiamati supporto e resistenza (Figura 11.20).

Se un trader con sufficiente disponibilità economica riuscisse a influenzare il prezzo di mercato e a far scattare gli stop loss, si andrebbe a creare un effetto valanga, come possiamo vedere in Figura 11.21. In questo esempio, un trader prevede che ci siano molti sell stop a $5.800. Prova quindi a far scendere il prezzo fino a $5.800 vendendo 100 BTC.

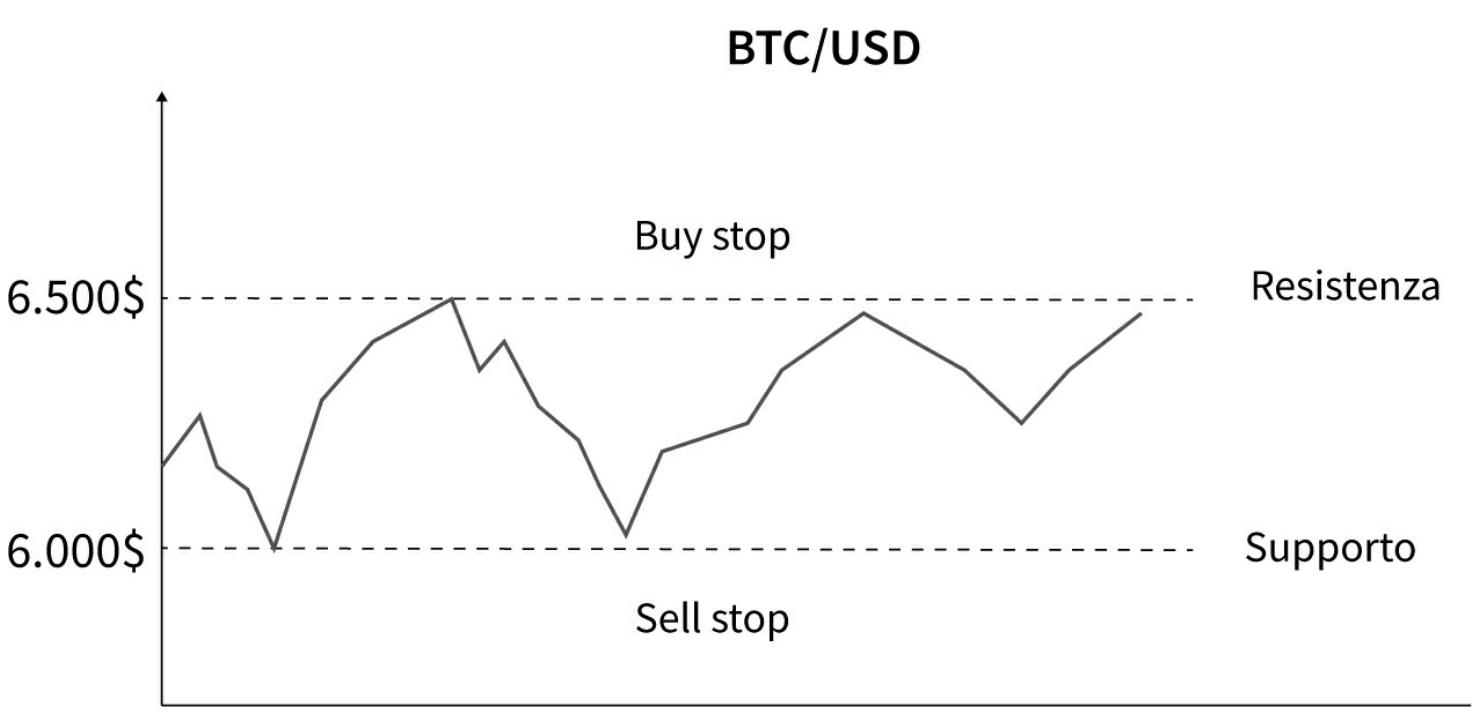


Figura 11.20 – Supporto e resistenza.

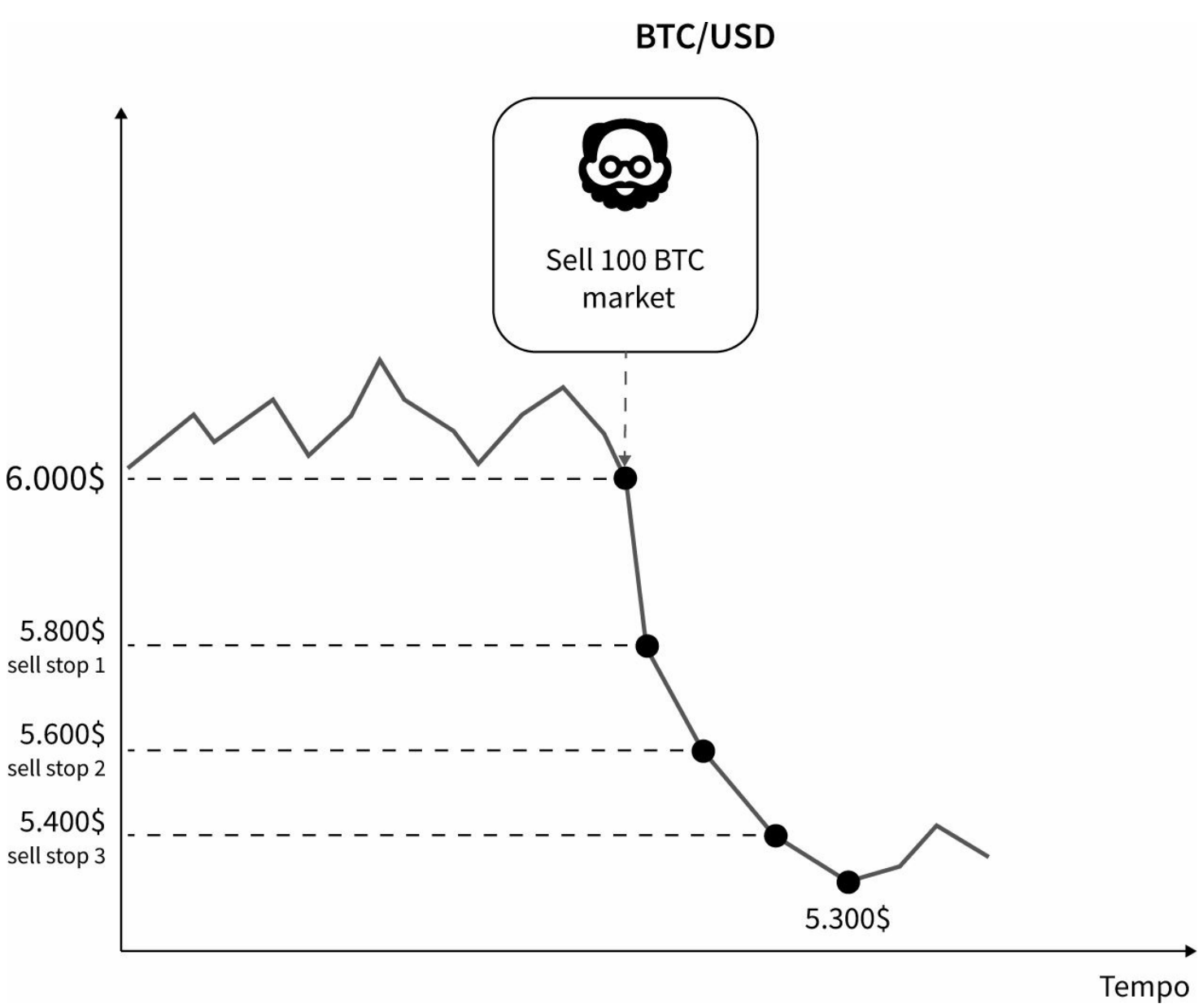


Figura 11.21 – L'effetto dello stop hunting e degli stop loss sul prezzo di mercato.

Se il trader ha fatto bene i calcoli e riesce a far scendere il prezzo fino a $5.800, tutti gli stop loss su quel livello

verranno azionati, creando numerosi market sell order. A loro volta questi faranno scendere ulteriormente il prezzo, generando un effetto a catena fino ad arrivare a $5.300.

A quel punto il trader che aveva innescato questa valanga ricompra i BTC che aveva venduto a un prezzo molto più basso, aspettando che il mercato risalga.

Tutto questo solitamente succede in pochi minuti, o addirittura pochi secondi, ed è un fenomeno noto come **flash crash**.

Ovviamente affinché una strategia del genere funzioni sono necessari:

- una grande disponibilità

economica da parte del trader;

- un mercato con pochi volumi e poca liquidità, quindi facilmente manipolabile;
- una grande propensione al rischio.

Tutte queste condizioni sono spesso presenti negli exchange di criptovalute, e infatti non sono rari casi del genere. Esploreremo alcune casistiche simili nel paragrafo successivo sulle manipolazioni del mercato[59].

Manipolazione del

mercato

Gli exchange di criptovalute sono ancora poco regolamentati dal punto di vista legale. Questo fatto, unito a mercati con poca liquidità e bassi volumi, apre alla possibilità di manipolare facilmente il prezzo delle criptovalute.

> La manipolazione del mercato è un tentativo di interferire nel libero ed equo processo di domanda e offerta con lo scopo di creare un'immagine non veritiera di un mercato, e trarre profitto da essa.

C’è chi sostiene addirittura che gran parte del boom nel prezzo delle criptovalute del 2017 sia dovuto a fenomeni di manipolazione.

In questo paragrafo esploreremo alcune delle tecniche più comuni usate per manipolare il prezzo delle criptovalute.

Pump and dump

Il pump and dump è una delle tecniche concettualmente più semplici e immediate per manipolare il prezzo di un asset. L’idea alla base di un pump and dump è la seguente:

1. si compra un asset;

2. lo si fa salire di prezzo in maniera artificiale in modo da attirare nuovi investitori che spingano ulteriormente il prezzo (pump);
3. si vende l'asset scaricando sugli ultimi entrati le perdite (dump).

Al centro del processo di pump and dump c'è un gruppo di persone molto organizzato. Queste persone scelgono un mercato che reputano manipolabile (per esempio il mercato BTC/XYZ), e iniziano a comprare il token (fittizio) XYZ su tale mercato.

Successivamente vengono create delle news false (come per esempio una partnership tra XYZ e una grossa

azienda).

In seguito, il gruppo inizia a comprare grossi volumi di XYZ, creando nel mercato un sentimento di FOMO (Fear of missing out, paura di perdere un'opportunità), con lo scopo di rendere l'aumento di prezzo più credibile.

Le persone esterne al gruppo, vedendo l'aumento di prezzo e le news, pensano che sia un buon investimento e comprano anche loro il token XYZ, facendone salire ulteriormente il prezzo. Una volta che il target prefissato è stato raggiunto, i creatori del pump vendono i token, scaricando sui nuovi entrati le perdite (Figura 11.22).

I pump and dump, sebbene siano

stati quasi del tutto eliminati nei mercati regolamentati, sono decisamente comuni nei mercati di criptovalute, in quanto:

- molti mercati hanno poco volume e sono facilmente manipolabili;
- gli exchange non sono regolamentati;
- molti degli investitori sono inesperti (non conoscono le basi della tecnologia blockchain e del token) e non sono in grado di distinguere un aumento di prezzo reale da uno artificiale.

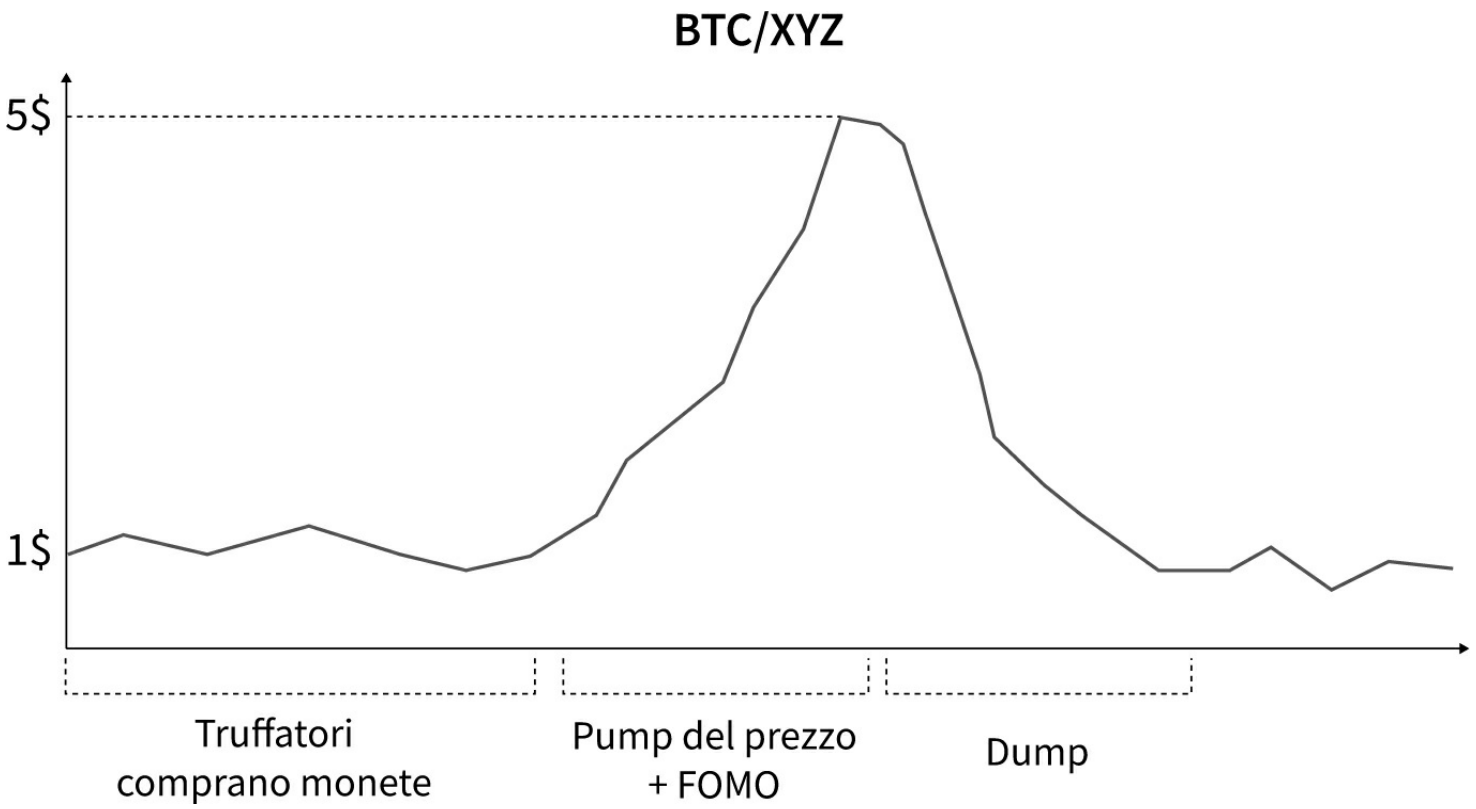


Figura 11.22 – Esempio di variazione di prezzo dovuto al pump and dump.

Wash trading

Il wash trading è un processo nel quale si compra e si vende un asset (criptovalute) con lo scopo di generare delle false informazioni, come per esempio creare del volume fittizio.

Sebbene sia una tecnica illegale negli exchange tradizionali, attualmente non c'è nessuna regolamentazione sul wash trade nei criptoexchange[60].

Nella pratica, questo avviene effettuando un grande numero di buy e sell order (sullo stesso asset) quasi istantaneamente, dando l'impressione che ci sia molto movimento nel mercato quando in realtà non è così.

Uno studio del Blockchain Transparency Institute[61] stima che oltre il 60% del volume (circa 6 miliardi di dollari) generato dai cripto-exchange sia in realtà dovuto a wash trading. Molto spesso sono gli exchange stessi a fare wash trading per far risultare un volume

maggiore e dare quindi l'impressione di essere molto utilizzati. Può essere visto come l'equivalente dei click/like finti nell'ambito exchange.

Un altro dei motivi alla base del wash trade è quello di rendere più credibile un movimento di prezzo artificiale. L'analisi del volume gioca infatti un ruolo fondamentale nei bot e nei trader per valutare la credibilità di un movimento di prezzo.

Spoofing

Lo spoofing è una forma di manipolazione del mercato nella quale vengono creati degli ordini finti (ovvero

senza alcuna intenzione di essere eseguiti, per esempio cancellandoli poco prima della possibile esecuzione) con lo scopo di manipolare il sentiment (opinione) di un mercato, influenzando la percezione della reale domanda e offerta. Lo spoofing è solitamente eseguito insieme al wash trading, in modo da aumentare la credibilità della manipolazione.

Creando grossi ordini di acquisto o di vendita si può infatti dare l'impressione di ottimismo o pessimismo su un mercato. Se sul mercato BTC/USD, per esempio, comparisse un grosso ordine di vendita di BTC, questo potrebbe creare panico e spingere altri trader a vendere. Poco

prima della possibile esecuzione dell'ordine, questo verrebbe cancellato, per poi essere ricreato poco dopo.

Si andrebbero così a creare dei sell wall o buy wall che compaiono e scompaiono velocemente (caratteristica appunto dello spoofing) generando un sentimento di FOMO (Fear of of missing out) o FUD (Fear, uncertainty and doubt). Un sell wall imponente è infatti un chiaro segno di pessimismo sul mercato, che viene interpretato da trader e bot come qualcuno in procinto di vendere un'enorme quantità di criptovalute. Per mettersi al riparo, trader e bot anticipano il sell wall vendendo le loro criptovalute.

Quello che a prima vista potrebbe sembrare spoofing in realtà può anche essere frutto dei trading bot che seguono regole simili e quindi reagiscono in maniera simile[62]. È quindi possibile che i sell/buy wall siano in realtà dovuti a numerosi bot che reagendo allo stesso modo creano ordini di acquisto o vendita molto simili.

Quando il panico dovuto a questi sell wall (o buy wall) porta i trader a vendere le criptovalute, lo spoofer le compra a un prezzo basso e cancella tutti gli ordini creati in precedenza.

Il prezzo di una

criptovaluta

Gli exchange sono indipendenti l'uno dall'altro, ognuno con i propri mercati e i propri order book. La stessa criptovaluta potrebbe avere prezzi notevolmente differenti su diversi exchange o addirittura su diversi mercati dello stesso exchange (il bitcoin nel mercato BTC/USD potrebbe avere un prezzo diverso dal bitcoin nel mercato BTC/ETH). Ogni mercato, infatti, calcola il prezzo di un asset basandosi sui propri trade. Non esiste quindi un prezzo "ufficiale" di una criptovaluta, ma piuttosto una media pesata (solitamente in base al volume) dei

prezzi di quella criptovaluta su tutti i mercati dei diversi exchange.

Se quindi si volesse calcolare il prezzo attuale del bitcoin in USD bisognerebbe considerare tutti i mercati su tutti gli exchange dove si scambiano bitcoin e fare una media pesata sul volume dei prezzi dopo averli convertiti in dollari (Figura 11.23). Il prezzo del bitcoin su Coinmarketcap, per esempio, è la media pesata di oltre 400 mercati distribuiti su oltre 100 exchange.

Wash trading e spoofing possono cambiare significativamente l'influenza di un exchange nella determinazione del prezzo finale di una criptovaluta. Immaginiamo infatti che un trader voglia far alzare il prezzo del bitcoin. Questo

trader decide quindi di manipolare il mercato BTC/USD sull'exchange 2, in quanto risulta essere il più manipolabile. Essendo un mercato con poco volume riesce a far alzare il prezzo del BTC fino a $7.000, e tramite wash trading riesce a far arrivare il volume fino a $300 milioni (Figura 11.24).

Il prezzo finale del bitcoin quindi aumenta di oltre quasi il 10% in poche ore, dando l'impressione di un notevole ottimismo nel mercato. Questo porta quindi altri trader a comprare bitcoin, facendo salire ulteriormente il prezzo.

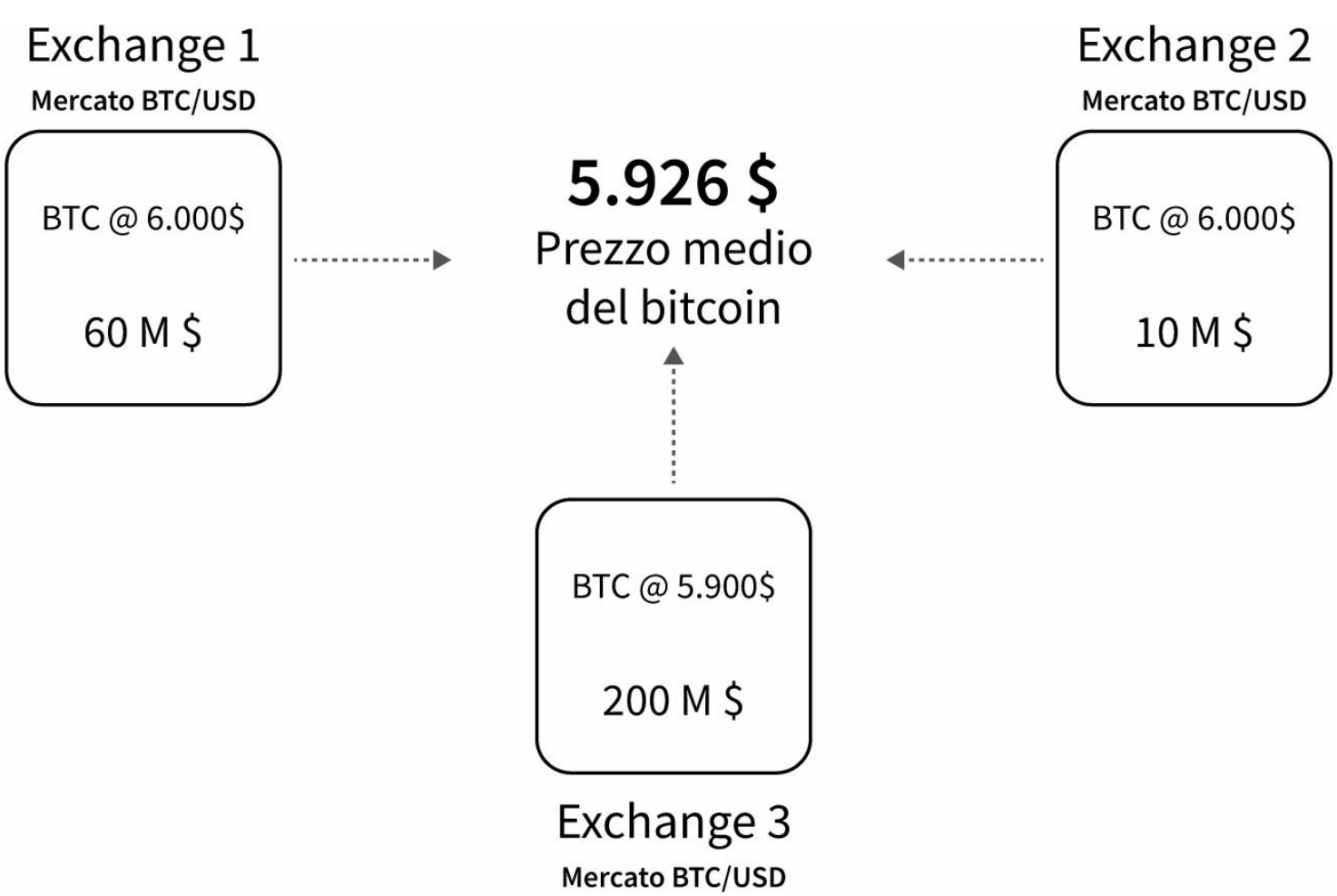


Figura 11.23 – Esempio di calcolo del prezzo medio del bitcoin.

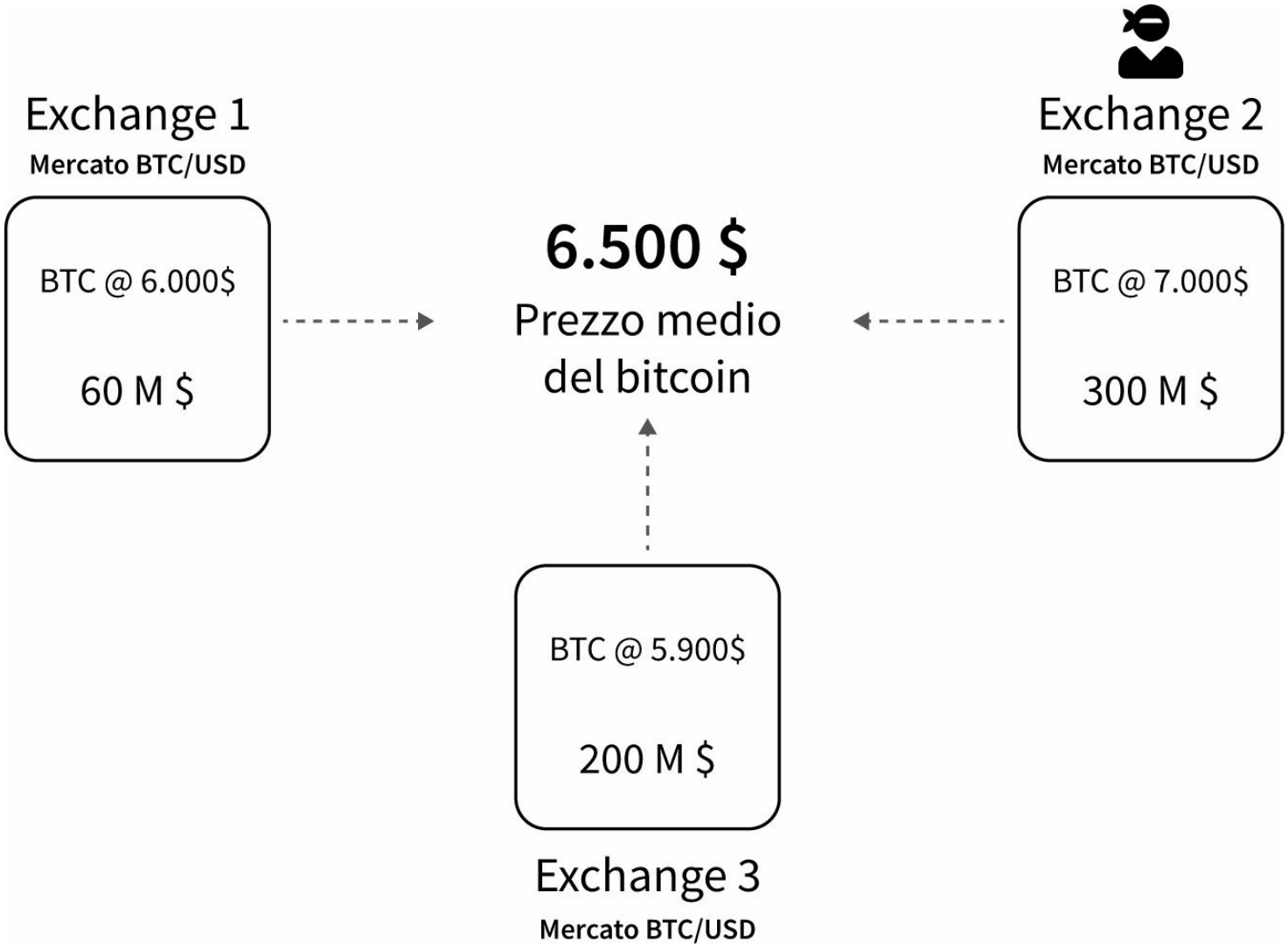


Figura 11.24 – L'effetto della manipolazione del mercato sul prezzo medio del bitcoin.

Arbitraggio

L'arbitraggio fa riferimento all'acquisto e vendita contemporanea dello stesso

asset su diversi mercati, guadagnando dalle differenze di prezzo sui mercati (Figura 11.25).

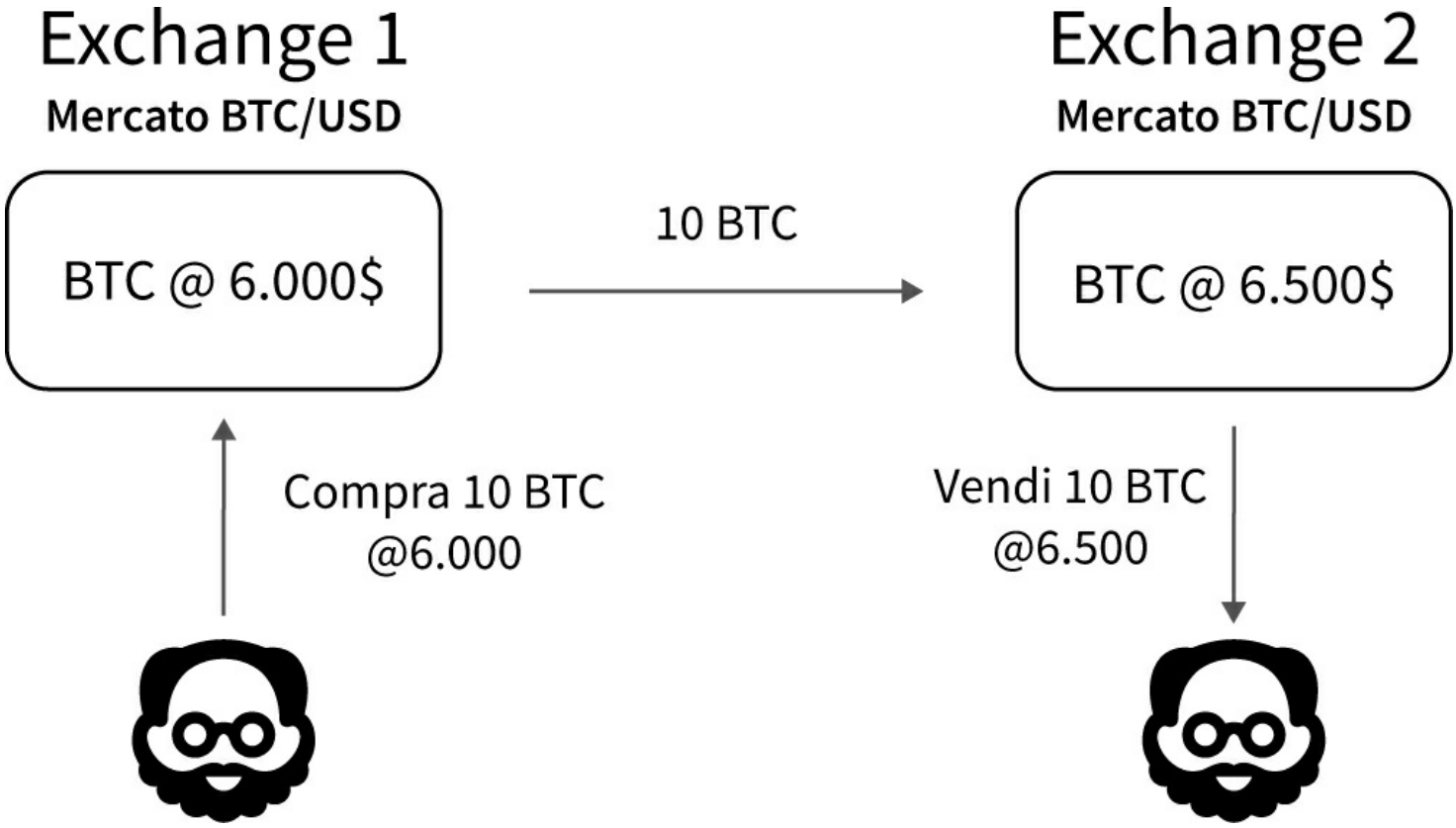


Figura 11.25 – L'arbitraggio per guadagnare dalle differenze di prezzo tra gli exchange.

È possibile utilizzare tecniche di arbitraggio anche sullo stesso exchange, sfruttando le differenze di prezzo tra diversi mercati (Figura 11.26).

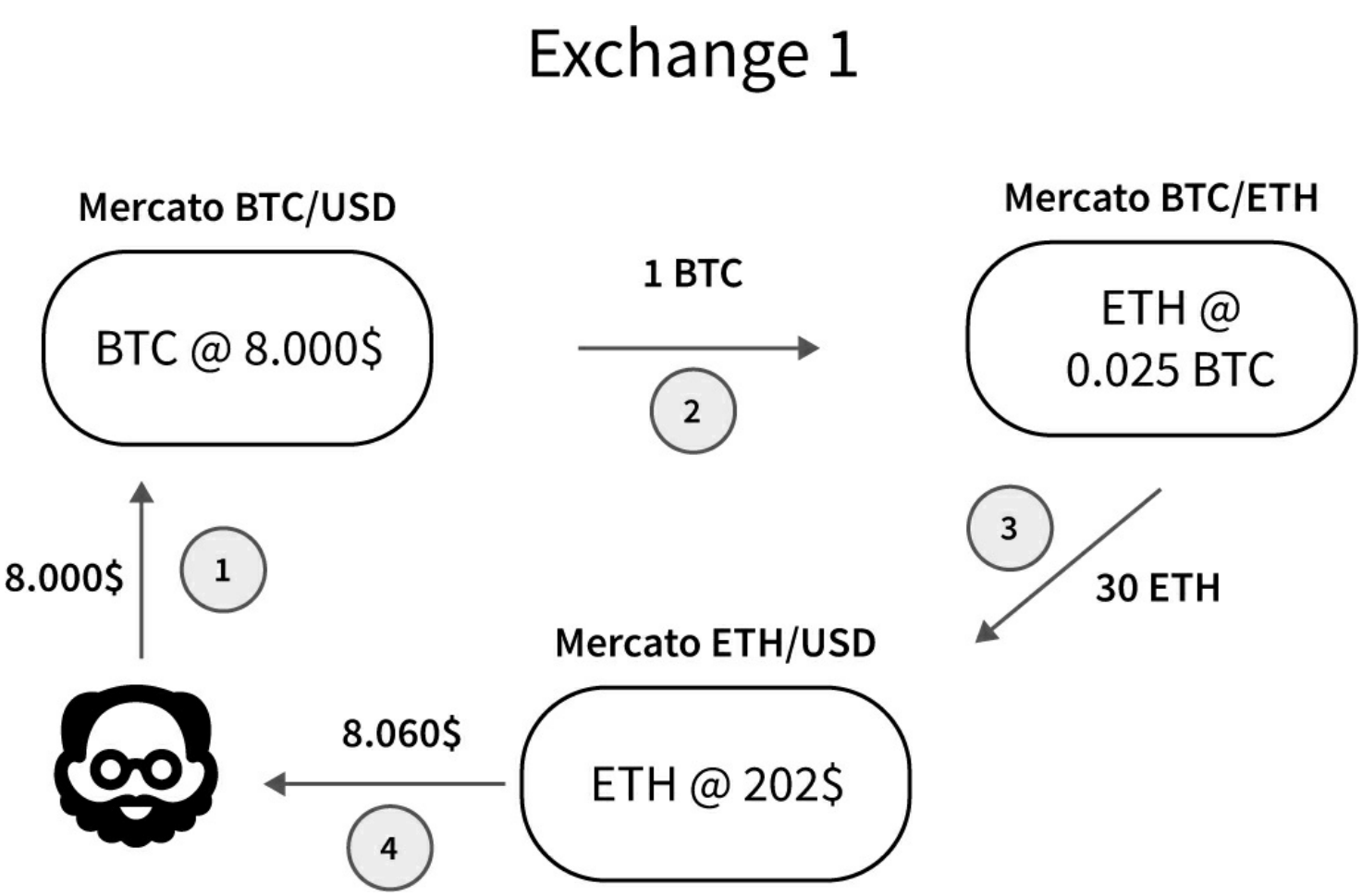


Figura 11.26 – L'arbitraggio su diversi mercati nello stesso exchange.

È possibile ripetere questo processo numerose volte, e solitamente è fatto in automatico dai bot. Bisogna inoltre considerare le commissioni trattenute dall'exchange per ogni operazione.

Exchange centralizzati

Sebbene le criptovalute siano nate come soluzione per rimuovere gli intermediari dai processi di scambio, attualmente la quasi totalità delle transazioni avviene tramite exchange centralizzati.

> Gli exchange centralizzati sono il punto di incontro tra il mondo decentralizzato della blockchain e il mondo centralizzato dei tradizionali servizi web.

Un exchange centralizzato è un exchange in cui è presente un'autorità centrale.

Rientrano in questa categoria Coinbase, Binance, Bittrex, Bitfinex, Kraken ecc. Questi exchange gestiscono il capitale degli utenti e le chiavi private di tutti wallet. Questa tipologia di exchange è soggetta a pesanti critiche per diversi motivi, dovuti principalmente al fatto che si stia adottando un modello centralizzato per interagire con una tecnologia naturalmente decentralizzata [25].

Tra le maggiori critiche agli exchange centralizzati, possiamo citare:

- La necessità di riporre fiducia nell'exchange: gli exchange centralizzati si basano su degli IOU, che necessitano un'enorme

quantità di fiducia. Ci sono stati numerosi casi di blocco degli account non giustificati, blocco dei prelievi dovuti a scarsa liquidità o situazioni poco trasparenti.

- Gli utenti non possiedono le chiavi private: in un exchange centralizzato un utente non possiede realmente le criptovalute, in quanto l'exchange non dà accesso alle chiavi private dei wallet. L'utente quindi delega la gestione dei propri fondi all'exchange.
- Sicurezza: gli exchange

centralizzati sono dei target perfetti per gli hacker.

- Privacy: per poter utilizzare un cripto-exchange centralizzato è solitamente necessario passare attraverso processi di identificazione come per esempio il KYC.
- Gli order book sono facilmente manipolabili.

Ovviamente, però, ci sono anche molti punti a favore degli exchange centralizzati. Non per niente attualmente dominano il mercato degli exchange. Tra i punti a favore di un exchange centralizzato possiamo citare:

- Facilità di utilizzo: gli exchange centralizzati sono estremamente facili da usare, offrendo una user interface intuitiva e ottimizzata. Attualmente il mondo delle criptovalute non è user friendly. Per molti, gestire un wallet o addirittura comprendere il concetto di chiavi private non è banale. Un exchange nasconde questa complessità, dando la possibilità a utenti inesperti di comprare o vendere criptovalute in modo estremamente semplice.
- Tipologie di ordini più avanzate: gli exchange centralizzati offrono numerose tipologie di ordine,

come gli stop loss o altre forme di trading automatico.

- Margin trading: questa modalità di trading richiede una controparte che presti i fondi. Nel caso di exchange centralizzati è molto facile, in quanto si può esporre l'exchange in prima persona per effettuare il prestito.
- Velocità: attualmente le blockchain non si avvicinano alle velocità raggiungibili tramite sistemi centralizzati.
- Sicurezza: la questione sulla sicurezza è state elencata

precedentemente tra gli svantaggi. Bisogna però riconoscere che alcuni exchange come Coinbase offrono delle garanzie di sicurezza superiori a quelle utilizzate da gran parte degli utenti. Coinbase dichiara che il 98% dei fondi sono salvati offline[63] e i fondi online sono coperti da assicurazioni[64] che proteggono gli utenti in caso di hackeraggio.

Scenari

Ogni exchange è strutturato in modo differente dagli altri, e con

l'aggiornamento continuo delle tecniche di sicurezza e l'evoluzione delle blockchain alcuni scenari possono cambiare.

Deposito criptovalute

Il primo scenario che andiamo ad analizzare è quello del deposito di criptovalute sull'exchange centralizzato (Figura 11.27).

L'exchange comunica all'utente l'indirizzo dove poter depositare le criptovalute. L'indirizzo solitamente è gestito da un hot wallet in possesso dell'exchange (un wallet può gestire numerosi indirizzi) (1). Ogni indirizzo è mappato in maniera univoca con un

utente, così da poter sapere a chi accreditare le criptovalute.

Una volta che il deposito è stato ricevuto, vengono aggiornati i profili utente salvati nel database per riflettere le nuove quantità (2). Questo equivale all'exchange che consegna all'utente degli IOU.

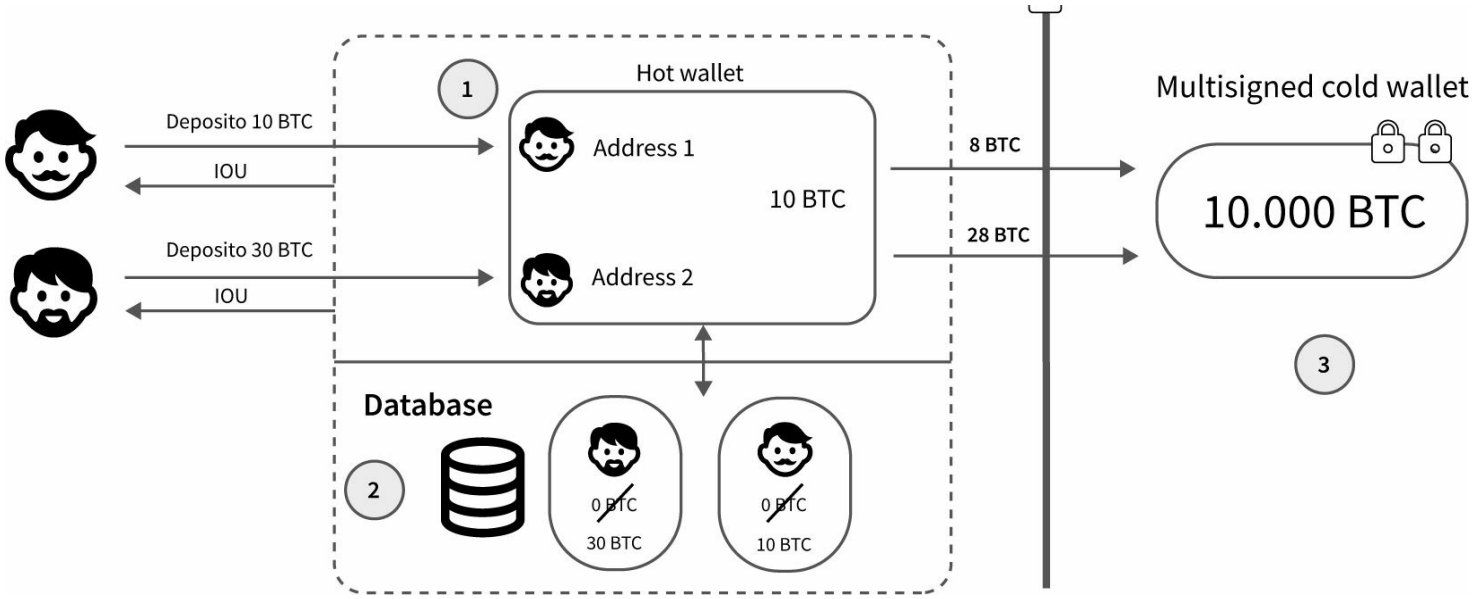


Figura 11.27 – Il deposito di criptovalute su un exchange centralizzato.

Per ragioni di sicurezza, solitamente sugli hot wallet non vengono lasciate molte criptovalute, o addirittura non ne viene lasciata nessuna. La quantità di criptovalute che eccede i limiti di sicurezza viene spostata in un cold wallet, lasciando nell'hot wallet solo un piccola percentuale per coprire piccoli prelievi (3).

Il cold storage di bitcoin di Bitfinex, per esempio, utilizza un indirizzo multisignature 3-of-6 (3D2oetdNuZUqQHPJmcMDDHYoqkyN e oggi contiene circa 130.000 BTC.

Esecuzione di un ordine

In questo scenario illustriamo come viene gestito un trade da parte di un exchange (Figura 11.28).

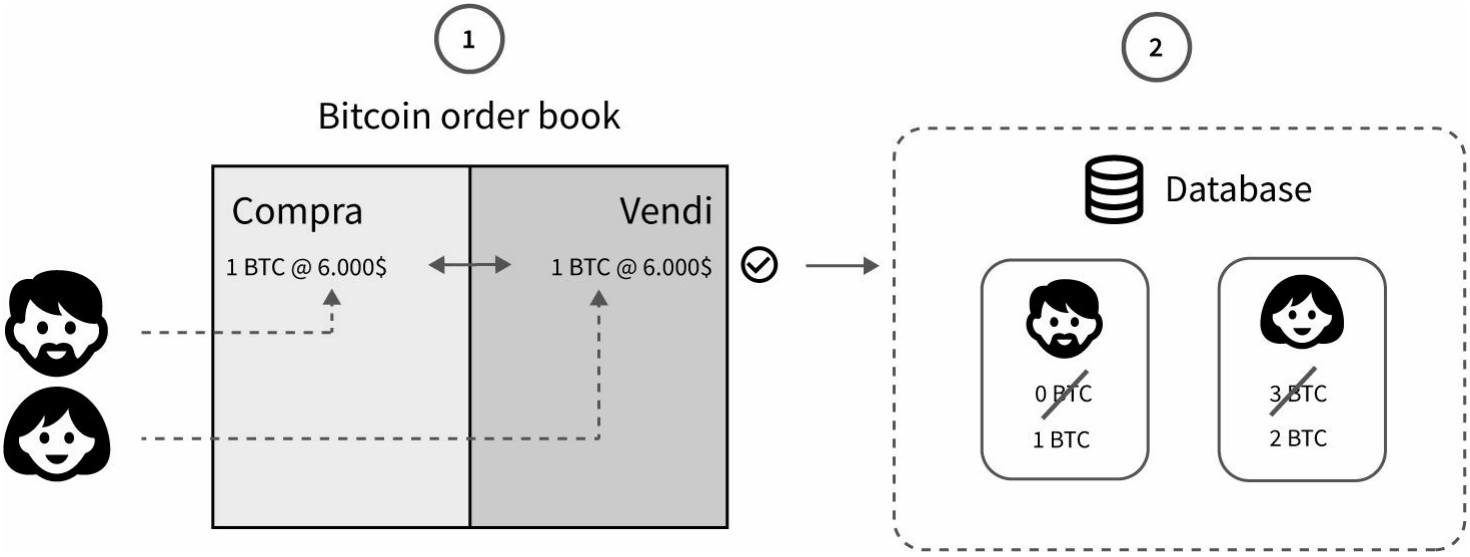


Figura 11.28 – L'esecuzione di un ordine su un exchange.

Due utenti creano rispettivamente un limit buy order e un limit sell order, che vengono salvati nell'order book (1). Una volta eseguito l'ordine vengono aggiornati i rispettivi profili utente (2).

In un exchange centralizzato, quando viene effettuato un trade non c'è alcun movimento

di criptovalute, tutto viene gestito a livello applicativo.

Prelievo

Nel caso di un prelievo, l'utente deve specificare un indirizzo sul quale mandare le criptovalute. Se la quantità richiesta è contenuta nell'hot wallet, il prelievo può essere relativamente rapido. Se, al contrario, il prelievo è di dimensioni rilevanti, l'exchange deve prelevare criptovalute dal cold wallet per poi trasferirle all'indirizzo specificato dall'utente. Successivamente hot wallet e cold wallet vengono ribilanciati secondo le politiche dell'exchange (Figura 11.29).

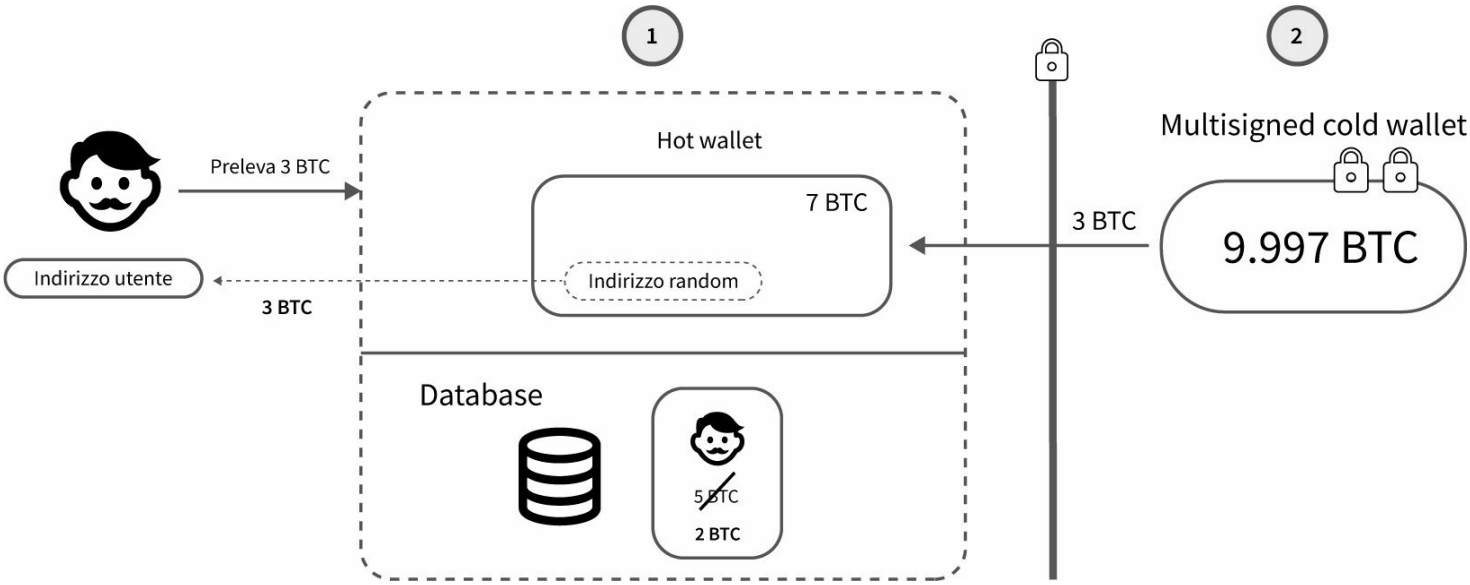


Figura 11.29 – Il prelievo di bitcoin da un exchange.

L'indirizzo dal quale riceviamo le criptovalute che abbiamo prelevato può essere un indirizzo qualsiasi tra quelli utilizzati dall'exchange. Per questo motivo viene sempre specificato di non usare gli indirizzi degli exchange per partecipare alle ICO.

Commissioni di prelievo

Quando si prelevano alcune criptovalute da un exchange possono venir richieste delle commissioni di prelievo. Queste vengono solitamente utilizzate per pagare i miner e ribilanciare hot wallet e cold wallet.

Dark pool e OTC market

Alcuni cripto-exchange centralizzati offrono dei servizi di trading pensati appositamente per i grossi investitori (in gergo **whales**, balene). I grossi investitori infatti non utilizzano gli order book pubblici quando devono effettuare delle operazioni, ma piuttosto degli

order book privati (dark pool[65]) o delle forme di trading peer-to-peer (OTC market[66]), principalmente per due motivi:

- **Privacy:** mantenendo le proprie transazioni confidenziali non vengono rivelate eventuali strategie finanziarie.
- **Liquidità:** gli order book pubblici spesso non hanno sufficiente liquidità per coprire dei grossi ordini. Questo andrebbe a influenzare enormemente i prezzi.

Hacking

Da quando i primi cripto-exchange hanno fatto la loro comparsa, sono stati vittime di numerosi casi di hacking, alcuni anche eclatanti, che hanno portato al furto di centinaia di milioni di dollari in criptovalute. In questo paragrafo riportiamo brevemente alcuni degli hack più famosi.

Mt. Gox

Data: 2011-2014.
Quantità rubata: circa 850.000 BTC ($450 milioni al tempo).
Mt. Gox è nato inizialmente nel 2007 da Jed McCaleb (uno dei co-founder di eDonkey, Ripple e Stellar) come luogo per lo scambio di carte del gioco Magic

(Mt. Gox sta infatti per "Magic: The Gathering Online eXchange"). Nel 2010 è diventato un exchange di bitcoin con sede in Giappone. Al momento di massimo successo, Mt. Gox gestiva oltre il 70% di tutte le transazioni di bitcoin.

Questo è stato senza dubbio l'hack più famoso nell'ambito delle criptovalute, sia per la quantità di criptovalute rubata sia per le ripercussioni che ha avuto e ancora oggi sta avendo. Non si è trattato di un attacco singolo, ma di numerosi attacchi diluiti in un periodo di circa tre anni, dal 2011 fino al 2014, senza essere mai scoperti dall'exchange, portando al furto di circa 800.000 BTC. Il 7 febbraio 2014 Mt. Gox bloccò tutti i prelievi di

bitcoin, citando un problema tecnico. Pochi giorni dopo il sito venne chiuso e Mt. Gox dichiarò bancarotta.

200.000 BTC furono recuperati, ma a oggi nessun investitore ha ancora ricevuto un risarcimento.

Bitfinex

Data: agosto 2016.
Quantità rubata: 120.000 BTC ($72 milioni al tempo).
Gli hacker sono riusciti a sfruttare una vulnerabilità nel wallet multisig usato da Bitfinex. Per sopperire alla perdita, Bitfinex ha ridotto tutti i fondi degli utenti del 36%, emettendo un token (BFX token) con la funzione di IOU.

Bitfinex ha progressivamente rimborsato tutti gli utenti. Dopo l'hack, l'exchange ha aumentato notevolmente le misure di sicurezza. Attualmente è uno degli exchange più utilizzati.

CoinCheck

Data: gennaio 2018.
Quantità rubata: 523.000.000 NEM (oltre 500 milioni di dollari al tempo). L'hacker è riuscito a prendere possesso di un hot wallet (!) dell'exchange dove erano custoditi oltre $500 milioni di dollari in token NEM. CoinCheck ha dichiarato che rimborserà completamente gli utenti.

BitGrail

Data: febbraio 2018.
Quantità rubata: 17.000.000 NANO (195.000.000 dollari al tempo).
Riportiamo questo hack in quanto effettuato ai danni di un exchange italiano, portando al furto di oltre $195 milioni di dollari in NANO. Le dinamiche che hanno portato all'hackeraggio non sono molto chiare, con accuse reciproche tra l'exchange, il team NANO e diversi analisti che hanno dato la responsabilità all'exchange [26].

Questi sono solo alcuni degli hack avvenuti negli ultimi anni. Potete trovare diverse liste costantemente aggiornate online.

Exchange decentralizzati

Un exchange decentralizzato (DEX) è un cripto-exchange dove tutte le operazioni tipiche di un exchange vengono eseguite in maniera decentralizzata. Un DEX rimuove tutti gli intermediari, creando un ambiente dove è possibile scambiare criptovalute in maniera sicura tramite l'utilizzo di smart contract che fungono da garanti, senza la necessità di un'autorità centrale a vigilare e gestire i processi.

Si può quindi dire che i DEX siano fondamentali affinché le criptovalute possano realmente diventare un sistema

di scambio decentralizzato.

Un exchange decentralizzato permette lo scambio peer-to-peer di criptovalute senza dover gestire i fondi degli utenti.

Pro e contro

Molti dei vantaggi degli exchange decentralizzati sono gli stessi che si hanno nell'utilizzo della tecnologia blockchain al posto di una centralizzata, in particolare:

- Vengono rimossi gli intermediari: uno dei principali benefici di un exchange decentralizzato è la rimozione

degli intermediari, in allineamento con i principi della tecnologia blockchain. Viene quindi creata un'applicazione trustless senza punti di controllo centrale e quindi senza possibilità di censura o controllo sui fondi degli utenti. In un exchange decentralizzato non c'è molto spazio per regolamentazioni e controlli.

- Sicurezza: viene ridotto notevolmente il rischio di hackeraggi, in quanto l'exchange non possiede i fondi degli utenti, che rimangono sotto il controllo degli utenti durante tutto il

processo di scambio. Gli hot wallet degli exchange centralizzati restano infatti un enorme punto debole. Un exchange decentralizzato gode inoltre della sicurezza derivante dai protocolli della blockchain.

- Sono più resistenti a tecniche di manipolazione del mercato: la blockchain, infatti, può garantire dei livelli di trasparenza molto superiori rispetto alla controparte centralizzata.
- Privacy: gli utenti non devono comunicare i propri dati personali per poter accedere ai servizi dell'exchange.

- Assenza di downtime: non essendoci server centrali, l'exchange è sempre attivo. Non sono quindi possibili attacchi come DDoS o altre forme.

Per quanto riguarda i contro, possiamo citare:

- Gli exchange decentralizzati sono più complessi da usare: bisogna gestire i propri wallet e le operazioni sono spesso lente e macchinose.
- Poco utilizzati: attualmente i volumi degli exchange decentralizzati non sono comparabili ai volumi di quelli

centralizzati. Questo spesso crea problemi di volume e liquidità che portano ad avere spread molto alti, rendendo i trade difficoltosi.

- Mancanza di funzionalità avanzate: le tecnologie attualmente utilizzate negli exchange decentralizzati non offrono i presupposti per la gestione di tipologie di ordini più avanzate, come per esempio gli stop loss o altre forme di trading automatico. È inoltre assente il margin trading, dal momento che questa modalità richiede una controparte che

presti i fondi. Nel caso di exchange centralizzati è molto semplice da gestire, ma nel caso di exchange decentralizzati bisogna appoggiarsi a protocolli di prestito decentralizzati.

- Mancanza di supporto per il denaro fiat: non rispettando regolamentazioni come KYC e AML, non possono integrare denaro fiat.
- Problemi di regolamentazione: la mancanza di regolamentazione o l'identificazione degli utenti potrebbe portare a problemi di evasione fiscale o di riciclaggio di denaro (anche se attualmente

casi di riciclaggio si verificano anche in exchange centralizzati, come per esempio BTC-e, chiuso nel 2017 proprio per riciclaggio).

- Alcuni exchange che dichiarano di essere decentralizzati non lo sono veramente: per esempio, a seguito di un hackeraggio, Bancor (un exchange decentralizzato) ha bloccato la sua piattaforma, dimostrando di avere un controllo centralizzato sugli smart contract che gestivano gli scambi. Charlie Lee, il creatore di Litecoin, ha dichiarato che “un exchange non

è decentralizzato se può perdere o bloccare i fondi degli utenti. Bancor può fare entrambe le cose. È un falso senso di decentralizzazione."

- Gli smart contract usati nella gestione degli scambi possono avere vulnerabilità.

Atomic swap

Un atomic swap è una tecnica per scambiare criptovalute in maniera peer-topeer senza che vi sia fiducia nella controparte. Il termine **atomic** (atomico) indica la modalità con cui avviene lo

scambio: un'operazione atomica è infatti un'operazione che o viene eseguita completamente o non viene eseguita affatto.

Gli atomic swap sono possibili grazie all'utilizzo di uno smart contract, che ricopre la funzione di garante. In particolare questo contratto implementa una tecnica chiamata HTLC (Hash Timelock Contract, un concetto simile a quello usato nel Lightning Network) che definisce uno smart contract limitato temporalmente tra le due parti coinvolte nella transazione. Se quindi una delle parti non conferma la transazione entro i termini, dopo uno specifico tempo, lo scambio non avverrà e le criptovalute saranno restituite ai proprietari,

rimuovendo così il rischio di controparte.

Gli atomic swap possono essere utilizzati per scambiare token di due blockchain diverse (cross-chain swap). Facciamo un esempio: Alice e Marco vogliono scambiare bitcoin e litecoin utilizzando un atomic swap. Dopo aver deciso il tasso di cambio, entrambi affidano le loro criptovalute a uno smart contract e aspettano che la controparte dia l'ok (Figura 11.30).

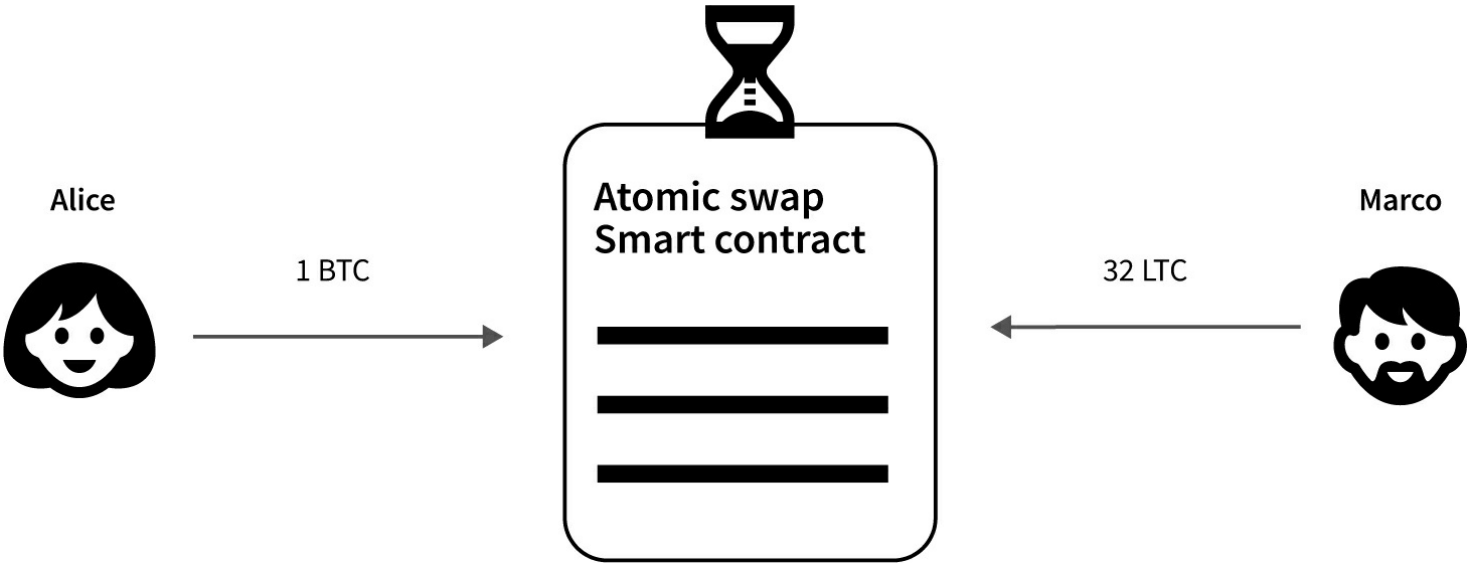


Figura 11.30 – Un esempio di scambio usando un atomic swap.

Se allo scadere del tempo Marco ha confermato l'arrivo dei bitcoin ma Alice non ha ancora confermato l'arrivo dei litecoin, lo smart contract annulla l'operazione e restituisce ai proprietari le rispettive criptovalute (Figura 11.31).

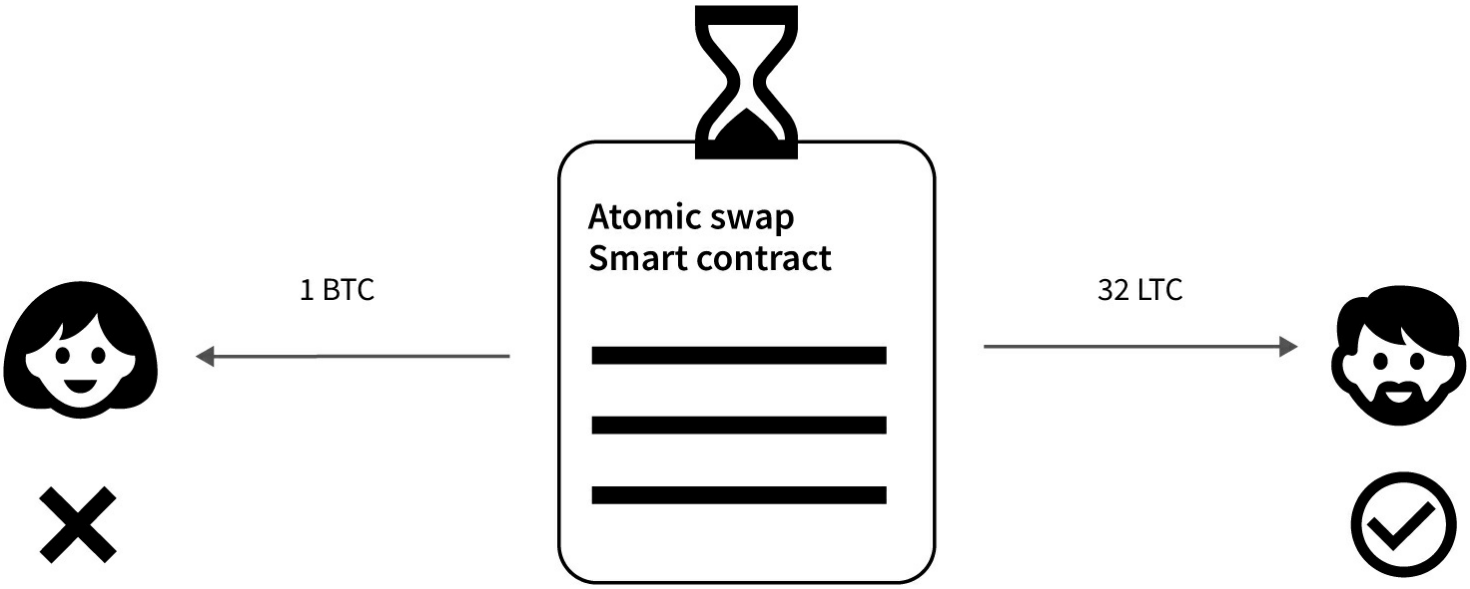


Figura 11.31 – La risoluzione di uno scambio non riuscito usando un atomic swap.

---

57. https://coinmarketcap.com/charts.
58. https://en.wikipedia.org/wiki/Modern_portfolio
59. Lo stop hunting è legale quindi non è stato inserito tra le tecniche di manipolazione del mercato.
60. https://business.nasdaq.com/media/98477_wash

trading-faq-_tcm5044-18334.pdf.
61. https://www.blockchaintransparency.org.
62. Uno di questi indicatori è per esempio la death cross: https://www.investopedia.com/terms/d/deathcro
63. https://www.coinbase.com/security.
64. https://support.coinbase.com/customer/portal/a how-is-coinbase-insured-.
65. https://blog.kraken.com/post/259/introducing-the-kraken-dark-pool.
66. https://www.bitfinex.com/posts/181.

12

La rivoluzione economico-sociale

Storicamente, quando la società si è trovata di fronte a una tecnologia rivoluzionaria, la prima reazione è stata sempre quella della diffidenza. È accaduto per l'automobile, per l'elettricità e per Internet.

Gli imprenditori che hanno avuto successo sono stati quei pionieri che sono riusciti a perseguire la propria idea

rivoluzionaria nonostante la resistenza al cambiamento da parte della società.

I problemi affrontati dalle nuove tecnologie sono molteplici, come per esempio uno sviluppo non ancora completo, un ecosistema di infrastrutture non adatto, una legislazione spesso avversa.

Le prime automobili erano tutt'altro che user friendly. I motori erano poco potenti e rumorosi, non avevano freni efficienti, invece del volante si doveva usare un timone, mancavano i più comuni standard di sicurezza ecc. Queste automobili inoltre utilizzavano infrastrutture che erano pensate per i cavalli. Le strade non erano asfaltate, non c'era segnaletica né illuminazione,

mancavano totalmente le stazioni di rifornimento e i parcheggi, non esistevano meccanici. A questo vanno inoltre aggiunti i legislatori, che non capendo la nuova tecnologia crearono leggi che, riviste anni dopo, appaiono assurde. Nel caso delle automobili, nel 1865, il limite di velocità era di 5 km/h nelle zone extraurbane e 3 km/h in città, ma soprattutto ogni veicolo doveva avere a bordo un guidatore e un fuochista, e la macchina doveva essere preceduta da una persona che sventolava una bandiera rossa o una lanterna[67]. Sicuramente una legislazione che non ha aiutato la diffusione dell'automobile.

In un mondo fatto per i cavalli, le

prime automobili sono risultate sicuramente delle invenzioni senza futuro.

> Guidare una macchina su una strada non asfaltata, senza semafori, senza parcheggi, non permette di apprezzare i reali benefici di questa tecnologia.

Per aiutare la diffusione delle automobili, oltre al naturale sviluppo tecnologico è stato necessario costruire un'infrastruttura che fosse pensata per loro. Sono state costruite strade asfaltate, stazioni di servizio, segnaletica ecc. Si è dovuto quindi

creare un'infrastruttura completamente nuova affinché le automobili potessero portare dei reali benefici.

> Questo è un pattern tipico dell'innovazione.
> L'innovazione si scontra con un'infrastruttura non adeguata e con una legislazione che non ha capito a fondo le potenzialità della nuova tecnologia.

Una storia simile è successa anche per l'elettricità. I giornali l'avevano etichettata come un capriccio da ricchi, che avrebbe incendiato le case e che

sarebbe stata impossibile da usare. In un mondo che non era pensato per l'elettricità, questa nuova tecnologia risultava inservibile. Mancavano le infrastrutture per portare la corrente elettrica in casa e gli strumenti per utilizzarla. Per illuminare strade e abitazioni, si diceva, era molto più comodo bruciare olio o kerosene.

Anche in questo caso è stato necessario costruire una nuova infrastruttura che fosse di supporto alla tecnologia stessa. L'evoluzione tecnologica espande le possibilità rispetto alla tecnologia precedente e apre campi di applicazione fino a quel momento nemmeno immaginati.

La tecnologia blockchain rientra

perfettamente in questo paradigma. Esiste una tecnologia che permette di rimuovere intermediari e scambiare valore senza autorità centrali. Manca però l'infrastruttura necessaria affinché la tecnologia blockchain possa proliferare.

Smart economy

Con il termine smart economy identifichiamo l'applicazione della tecnologia blockchain e degli smart contract ai processi economici. Tra le componenti fondamentali della smart economy troviamo:

- **smart contract**, che vanno a definire l'insieme di regole che governa gli accordi commerciali e societari.
- **smart property**, che permette la digitalizzazione degli asset e ne sposta la gestione su blockchain tramite l'utilizzo di smart contract;
- **digital identity**, che permette la digitalizzazione dell'identità di una persona o di un'istituzione e ne sposta la gestione su blockchain;
- **token model**, un modello economico basato sull'utilizzo

delle criptovalute nelle transazioni monetarie.

La smart economy può essere quindi vista come un tentativo di applicazione dei principi della tecnologia blockchain a un sistema economico. Un esempio concreto in questo senso sono le DAO.

DAO, Decentralized Autonomous Organization

Decentralized Organization indica una realtà dove la governance è decentralizzata e appartiene agli shareholder che esercitano i propri diritti decisionali tramite votazioni. **Autonomous** implica un sistema in

grado di eseguire azioni in autonomia, sulla base di regole espresse sotto forma di smart contract.

Una DAO è quindi un'organizzazione senza una struttura gerarchica tradizionale, ma con un sistema di regole che definisce in maniera decentralizzata quali azioni saranno intraprese, basandosi sul parere dei propri shareholder. I profitti dell'organizzazione sono infine distribuiti agli shareholder tramite criptovalute.

> Una DAO può essere definita come un'organizzazione di persone che, interagendo

tramite un protocollo di regole definite in precedenza, raggiungono un consenso sulle azioni da intraprendere ed eseguono tali azioni.

Tabella 12.1 – Le differenze tra un'impresa tradizionale e una DAO.

Azienda tradizionale	**DAO**
Struttura societaria gerarchica	Struttura societaria decentralizzata controllata dagli shareholder
Appoggiata a un sistema legale tradizionale	Basata su smart contract
La proprietà degli asset è gestita tramite contratti	La proprietà degli asset è gestita tramite smart property

L’identità degli shareholder è gestita attraverso un sistema tradizionale	L’identità degli shareholder è gestita tramite smart identity

Alla base di una DAO c’è un sistema di smart contract che definisce le regole a cui tutti i partecipanti devono sottostare. Tutte le transazioni sono salvate sulla blockchain insieme alla proprietà di eventuali asset digitalizzati, mentre il consenso distribuito garantisce la sicurezza e la correttezza delle operazioni (Figura 12.1).

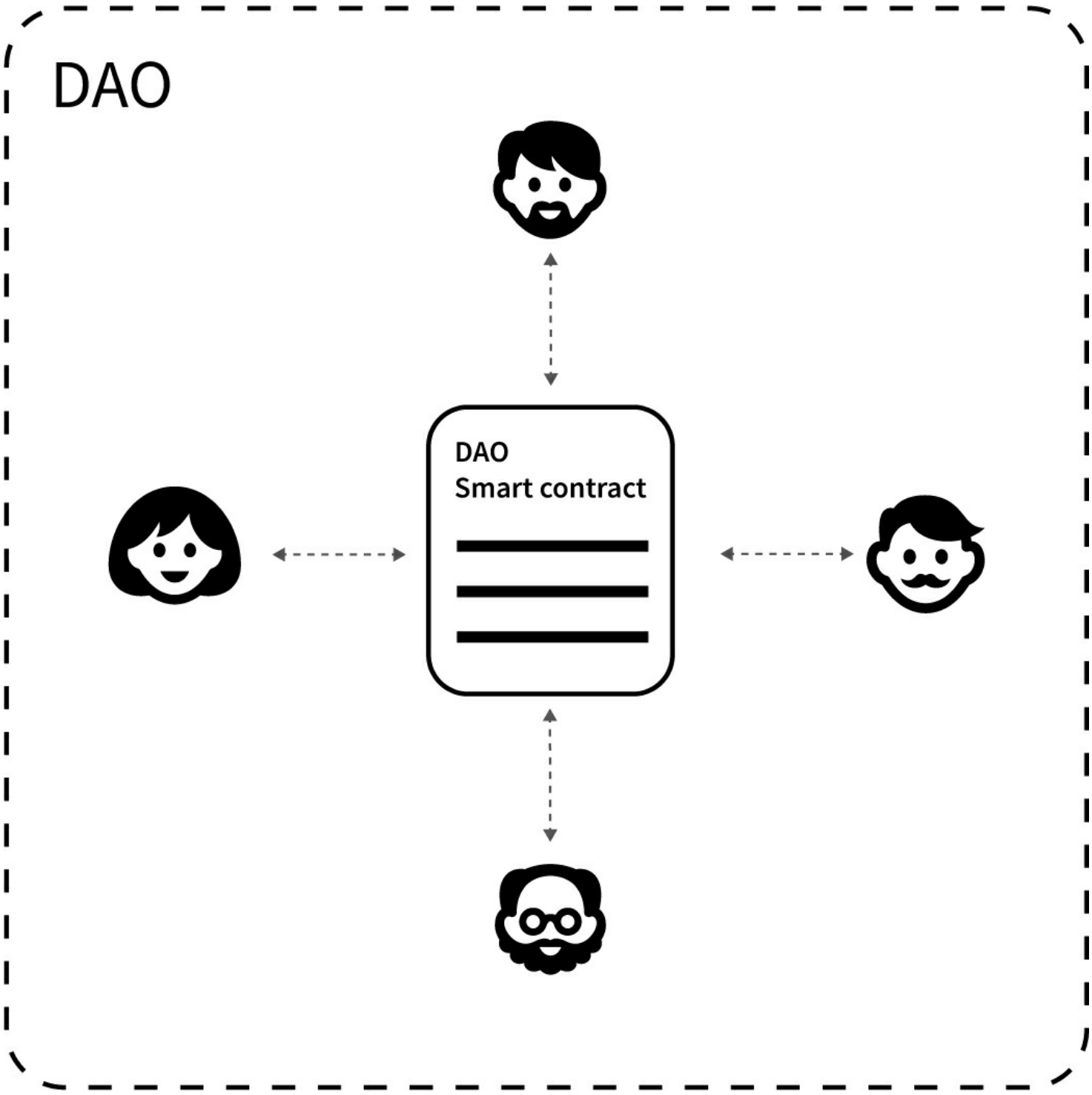


Figura 12.1 – La struttura di una DAO.

Il Bitcoin può essere considerata un esempio molto semplice di DAO nel

quale gli shareholder sono i miner. Il protocollo che seguono è quello del Bitcoin e le regole sono definite dal consenso del network.

DASH

Oltre a essere una criptovaluta, DASH può essere considerato un esempio di DAO nella quale le decisioni sono prese da un gruppo di utenti chiamati **masternode**. I masternode, oltre a eseguire tutta una serie di operazioni che garantiscono il funzionamento e la sicurezza del network, hanno anche il ruolo di shareholder e con esso il potere di votare sulle proposte riguardanti tutto l'ecosistema DASH, per esempio votare

su come utilizzare i fondi. Chiunque abbia almeno 1.000 DASH può diventare un masternode.

The DAO

The DAO è stato un progetto con l'obiettivo di creare una Decentralized Autonomous Organization per il finanziamento di progetti. L'idea era quella di delegare la gestione completa dei fondi agli shareholder, ovvero a tutti quelli che possedevano dei token DAO. Questi fondi sarebbero stati utilizzati per finanziare altri progetti. I progetti da finanziare venivano decisi tramite una votazione degli shareholder. I profitti degli investimenti sarebbero stati

distribuiti tra tutti gli shareholder.

Durante la ICO (maggio 2016), The DAO ha raccolto oltre 150 milioni di dollari (il 14% di tutti gli ETH in circolazione all'epoca, a testimonianza dell'enorme rilevanza che aveva raggiunto questo progetto). Tuttavia, un mese dopo l'inizio della ICO, degli hacker hanno sfruttato una vulnerabilità nel codice del progetto riuscendo a rubare gran parte dei fondi raccolti durante la ICO [10]. Oltre a segnare la fine di The DAO, questo hack ha causato la fork tra Ethereum ed Ethereum Classic.

La rivoluzione del web

"Ho immaginato il web come una piattaforma aperta
che avrebbe consentito a tutti, ovunque, di condividere
informazioni, accedere a opportunità e collaborare
andando oltre i confini geografici e culturali.
In molti modi, il web ha tenuto fede a questa visione,
anche se è stata necessaria una battaglia continua
per tenerlo libero."

—**Tim Berners-Lee**, creatore del World Wide Web

A partire dalla sua nascita, il web ha continuato a evolversi senza sosta diventando una risorsa fondamentale in ogni aspetto della nostra vita. Molti, però, sostengono che la direzione di questa evoluzione stia andando a scalfire i principi di libertà e neutralità che avevano in origine portato alla nascita del web. Qui parleremo di come il web si sia evoluto, analizzando i problemi attuali ed esplorando come la blockchain potrà avere un ruolo fondamentale nell'aiutare a risolverli.

Web 1.0

La prima versione del web, il Web 1.0,

era caratterizzata da contenuti statici read-only. Il primo esempio di World Wide Web non era altro che una serie di pagine web dove venivano presentate delle informazioni senza alcuna possibile interazione.

Il fulcro su cui si basava il Web 1.0 era la comunicazione di informazioni. Chiunque, pubblicando un sito web, rendeva le informazioni accessibili a chiunque. Per la prima volta venivano realmente abbattuti i limiti geografici e si gettavano le fondamenta per un sistema globale di informazioni. Il Web 1.0 segna la nascita di una prima generazione di aziende della New Economy, che iniziano a intuire il potenziale rivoluzionario di questa

nuova tecnologia.

Web 2.0

Il Web 2.0 viene definito come web di lettura e scrittura (read-write). Grazie a connessioni più veloci e software più funzionali diventa infatti possibile per gli utenti creare e condividere contenuti, ottenendo così un web social che sposta l'attenzione sugli utenti. I contenuti iniziano a diventare personalizzabili e le piattaforme sono in grado di creare un'esperienza su misura dell'utente.

In questa fase nascono piattaforme e servizi come YouTube, Wikipedia, Facebook, Amazon, Airbnb, Uber ecc., e

molte altre applicazioni che hanno migliorato la qualità della vita di milioni di persone in tutto il mondo.

Web 3.0

> "Internet is broken."
>
> —**Joseph Lubin**, co-fondatore di Ethereum

I numerosi problemi legati al Web 2.0 hanno portato molte persone a ritenere necessaria una rivoluzione strutturale del web, per riportarlo alla sua idea iniziale di piattaforma decentralizzata, aperta e universale. Tra i principali problemi del Web 2.0 possiamo citare i

seguenti:

- **Monopolio dei dati**. Non c'è possibilità di competizione con i giganti del web. Google, Microsoft, Facebook, Amazon ecc. possiedono enormi risorse economiche, la quasi totalità del traffico web e una potenza di calcolo pressoché illimitata. È impossibile per qualsiasi startup pensare di poter competere con queste aziende sotto questi aspetti.
- **Modello economico**. L'attuale modello economico basato sulla pubblicità (attention economy) sta iniziando a mostrare alcuni

problemi. Nonostante ci sia una diffusione senza precedenti di contenuti, i guadagni dei creator (come per esempio gli youtuber) sono diminuiti nel tempo.

- **Non-possesso dei dati**. Gli utenti non sono in possesso dei propri dati, che vengono ceduti gratuitamente in cambio di servizi gratuiti. Inoltre, come questi dati vengano utilizzati è molto spesso poco trasparente.
- **Non-persistenza dei dati**. Fino a quando i dati restano salvati in database centralizzati rimarrà sempre la possibilità che vengano persi, cancellati o

censurati.

Alla luce di quanto detto, sta nascendo la consapevolezza di dover re-decentralizzare i servizi web. Questa idea è diffusa da molto tempo, ma adesso finalmente esistono le tecnologie che permettono questa transizione, come la blockchain. Così si potrebbero ottenere numerosi vantaggi, tra i quali:

- **Decentralizzazione**. Nessun punto di controllo centrale. Non è necessario alcun permesso da parte di un'autorità centrale per caricare qualcosa sul web. Questo garantisce una protezione contro qualsiasi forma di censura e controllo. Il web tornerebbe a

essere un sistema neutrale, senza possibilità di censura.

- **Democratizzazione degli accessi**. È possibile offrire un accesso a chiunque abbia una connessione Internet, senza discriminazioni su età, sesso, religione, posizione geografica o fascia di reddito.
- **Uptime dei servizi**. Non essendoci alcun nodo centrale, non c'è nessun singolo punto di fallimento dell'infrastruttura, che rimane quindi sempre operativa.
- **Possesso dei dati**. Gli utenti riprenderebbero possesso dei

propri dati potendo decidere con chi condividerli e in che modo, venendo eventualmente remunerati. I giganti del web hanno tantissime informazioni sugli utenti: dai dati anagrafici ai loro principali interessi e alle loro carte di credito. Gli advertiser pagano milioni per questi dati, ma gran parte del profitto viene trattenuto dai fornitori dei servizi.

- **Persistenza dei dati**. I dati verranno archiviati in maniera ridondante su diversi nodi distribuiti indipendenti, eliminando la possibilità che

vadano persi.

Molti progetti stanno già lavorando in questa direzione e qui riportiamo alcuni esempi di attuali servizi web con il loro corrispettivo decentralizzato.

Tabella 12.2 – Confronto tra alcuni servizi Web 2.0 e i loro analoghi nel Web 3.0.

	Web 2.0	**Web 3.0**
Cloud computing	Google Cloud, Amazon EC2	Ethereum, EOS, Golem
Cloud storage	Dropbox, Google Drive, Amazon S3	Filecoin, Storj, IPFS
Modello di revenue	Pubblicità, analisi dati	Token model
Pagamenti	Stripe, PayPal, Visa	Criptovalute

Attualmente questi nuovi progetti non sono paragonabili ai loro analoghi centralizzati. C'è ancora una differenza molto marcata in termini di velocità, scalabilità, costi e user experience rispetto ai modelli centralizzati. Questi sono solo alcuni dei fattori che dovranno essere migliorati prima di poter pensare a una effettiva adozione delle applicazioni decentralizzate (Figura 12.2).

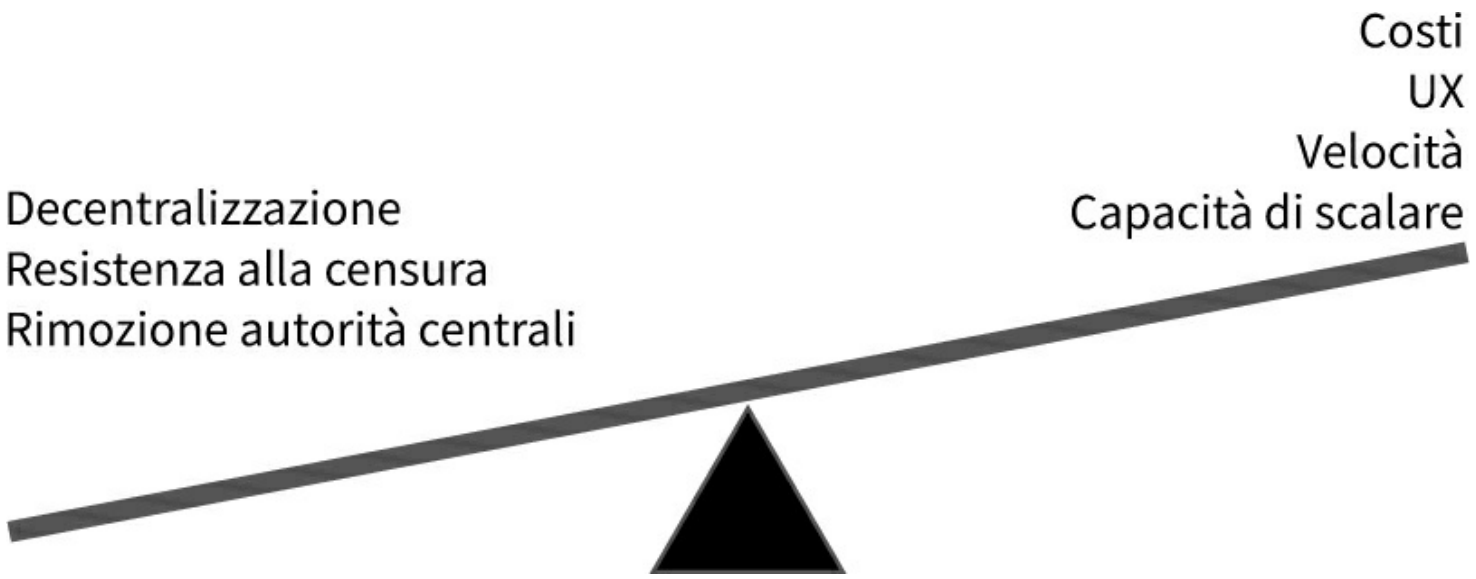


Figura 12.2 – Il trade-off tra sistemi centralizzati e decentralizzati.

Le blockchain private nell'industria

È opportuno a questo punto identificare il ruolo delle blockchain private nel panorama attuale e approfondire la ragione per cui siano viste in maniera particolarmente positiva da aziende e istituzioni finanziarie.

A differenza delle blockchain pubbliche, completamente aperte e senza censure, quelle private possiedono un livello di controllo degli accessi, e per

questa ragione vengono anche chiamate **permissioned**: questo significa che richiedono un'autorizzazione per potervi accedere o partecipare. Quindi alcuni attori hanno il controllo su chi può entrare a far parte del network, su chi può scrivere sulla blockchain e su chi può prendere parte al processo di consenso.

In pratica, per poter accedere a una blockchain privata è solitamente necessario un invito da parte di chi ha creato la blockchain. Oltre al controllo degli accessi, una blockchain permissioned implica che ci possono essere delle restrizioni in lettura (visualizzare dati o transazioni) o in scrittura (scrivere dei dati, creare nuove

transazioni).

Questo sistema è in netto contrasto con l'ideologia delle blockchain pubbliche, nate per essere accessibili da parte di chiunque e resistenti a qualsiasi tipo di censura.

Blockchain private vs blockchain pubbliche

Come accennato precedentemente nel Capitolo 3, le blockchain private possono essere distinte in due modelli strutturali:

- **Blockchain completamente private**, nelle quali una sola autorità ha il permesso di

scrivere sulla blockchain e detiene praticamente il controllo del sistema distribuito.

- **Blockchain consortium**, nelle quali il processo di consenso è controllato da dei nodi definiti a priori sui quali viene distribuita l'autorità.

Se il primo si può descrivere come un sistema tradizionale (centralizzato) unito a un grado di verifica crittografica (molto simile a un classico database distribuito), il modello di blockchain consortium può essere visto come un sistema ibrido tra una blockchain pubblica e un modello ad autorità centralizzata. D'ora in avanti quando

parleremo di blockchain private, ci riferiremo alle blockchain consortium.

Un esempio potrebbe essere un consorzio di 30 istituzioni, ognuna in controllo di un nodo, e con un consenso che reputa un blocco valido solo se convalidato da almeno 20 nodi.

Questo apre la tecnologia blockchain a scenari differenti, ed è perciò ritenuto da molti un modello particolarmente vantaggioso in alcune specifiche applicazioni, per esempio in ambito industriale e più in generale in processi che richiedono la collaborazione tra più istituzioni.

Si può per esempio pensare al miglioramento dell'efficienza nel processo della supply chain, nel quale

un prodotto per passare dal produttore al consumatore richiede il coordinamento di molti enti di natura differente, oppure all'Unione Europea, che potrebbe utilizzare la blockchain sia come ledger che come sistema di votazione, permettendo a ogni Paese di rappresentare un nodo.

> "L'idea che esista un solo modo di utilizzare la blockchain è completamente sbagliata, ed entrambe le categorie hanno i loro vantaggi e svantaggi."
>
> —**Vitalik Buterin**, creatore di Ethereum

Alcuni vantaggi delle blockchain private

rispetto a quelle pubbliche:

- Il consorzio o la società che possiede il controllo della blockchain privata, potrebbe cambiare le regole della blockchain, invertire transazioni, modificare bilanci ecc. Sebbene questo renda una blockchain lontana dall'essere immutabile, può essere una funzione necessaria in alcuni casi specifici. Per esempio, nel catasto il governo ha bisogno di avere il controllo sul registro dei possessori dei terreni, mentre un catasto non controllato dal governo finirebbe per renderlo

non riconosciuto dal governo stesso e di conseguenza inutile.

- I nodi validatori sono fidati (trusted), perciò si riduce il rischio di un attacco da parte dei miner o di altri partecipanti al network. Tuttavia, la sicurezza di un tale sistema è direttamente collegata all'onestà e alla correttezza delle parti incaricate del processo di validazione.
- Il processo di validazione è più veloce, dal momento che le transazioni e i blocchi devono essere verificati da pochi nodi e non da decine di migliaia di macchine.

- Avendo il controllo della blockchain, si può intervenire manualmente per risolvere eventuali problemi.
- Tramite la possibilità di restringere la lettura dei dati contenuti al loro interno, le blockchain private permettono di mantenere un elevato grado di confidenzialità, difficilmente ottenibile con una blockchain pubblica.

Al contrario, nelle blockchain pubbliche gli utenti sono protetti da un eventuale abuso di potere da parte degli sviluppatori o dei miner, dal momento che nessuno può modificare

autonomamente il protocollo. Questo rende le blockchain pubbliche "censorship resistant".

Infine, la possibilità di creare smart contract amministrati privatamente su blockchain pubbliche (o l'utilizzo di canali tra blockchain private e pubbliche) permette di ottenere varie combinazioni ibride tra i due sistemi.

In generale, in alcuni casi la blockchain pubblica è la soluzione ideale, in altri un certo grado di controllo è semplicemente necessario [27].

Blockchain private vs database

distribuiti

I database distribuiti sono dei sistemi nei quali i dati non sono memorizzati sullo stesso computer ma vengono distribuiti su più nodi, e quindi potenzialmente distribuiti tra diverse entità. Si possono notare quindi diverse analogie tra database distribuiti e blockchain private. Infatti, se nelle blockchain pubbliche la struttura decentralizzata crea una netta separazione con il concetto di database distribuito, quando si parla di blockchain private la linea diventa più sottile.

Uno dei dibattiti più ricorrenti nella community a questo proposito è

senz'altro il confronto tra blockchain private e database distribuiti, con alcuni che li ritengono indistinguibili [28], e altri che sostengono che una soluzione su blockchain abbia in ogni caso dei vantaggi in termini di disintermediazione e robustezza [29].

> In sostanza, le blockchain private forniscono livelli più alti di controllo degli errori e di validità delle transazioni rispetto ai normali database distribuiti.

I database distribuiti in passato hanno sofferto il problema di non poter

prevenire attività malevole. Per esempio, nel caso in cui una delle istituzioni partecipanti venisse compromessa o hackerata e scrivesse dati corrotti nel database, avrebbe invalidato l'intero database per tutti gli altri partecipanti.

Inoltre, in un database distribuito tra diverse entità, stabilire chi detiene l'autorità del sistema, come avviene la gestione del controllo degli accessi, come vengono validate le transazioni, o definire come viene ripartita la potenza di calcolo tra i diversi nodi, non è facile a causa della vastità dei possibili scenari. La struttura della blockchain, al contrario, fornisce una soluzione immediata e condivisibile, riducendo

drasticamente gli eventuali dissensi fra le parti coinvolte.

Per questa stessa ragione, le blockchain private rendono semplice la collaborazione tra più entità e aiutano a costruire in modo trasparente un rapporto di fiducia tra di esse, abbattendo le barriere psicologiche o strategiche che spesso ostacolano l'aumento di efficienza e lo sviluppo di nuovi metodi innovativi derivanti dalla collaborazione tra diverse entità.

Perché le aziende stanno scommettendo sulle blockchain private

Tra le numerose caratteristiche delle blockchain private che le rendono appetibili ad aziende e istituzioni ci sono quindi:

- la riservatezza dei dati;
- l'accesso selettivo dei partecipanti al network;
- una piattaforma con regole condivise che aiutano all'instaurazione di fiducia tra le parti;
- l'immediato riconoscimento di chi effettua una transazione sulla blockchain.

Dal punto di vista della scalabilità della

tecnologia, le caratteristiche principali riguardano:

- la minima potenza computazionale richiesta;
- le migliori performance in termini di throughput rispetto alle blockchain pubbliche;
- i costi di transazione e di mantenimento molto ridotti e definiti a priori.

La possibilità di avere il controllo (distribuito) della blockchain e di rimediare a potenziali errori sono caratteristiche che possono essere desiderabili se non addirittura necessarie in alcune applicazioni.

Il fatto inoltre di poter effettuare un processo di controllo (due diligence) nei confronti di chi intende partecipare a una blockchain privata, può essere per esempio una funzione indispensabile per istituzioni come le banche per poter aderire alle regolamentazioni in merito.

Sono diversi i progetti che offrono soluzioni specifiche per le imprese, tra cui citiamo:

- **Ethereum**: Ethereum è attivamente coinvolto nella definizione di uno standard della tecnologia blockchain per le imprese, avendo costituito la Enterprise Ethereum Alliance (EEA)[68].

- **Quorum**: sviluppata da JP Morgan, Quorum è una blockchain privata progettata per processare transazioni finanziarie. Come la blockchain di Ethereum, è basata sull'utilizzo di smart contract.
- **R3 Corda Enterprise**: sviluppata da R3, Corda vuole essere una soluzione alle inefficienze e ai rischi derivanti dalle tecnologie legacy (obsolete), tuttora utilizzate da molte istituzioni nel mondo della finanza e del commercio, le quali rendono estremamente difficile instaurare collaborazioni

aziendali o sviluppare soluzioni innovative.

Infine, una delle iniziative senz'altro più interessanti è Hyperledger, nata grazie alla Linux Foundation e che già coinvolge numerose realtà industriali in tutto il mondo.

Hyperledger

Hyperledger non è propriamente una blockchain ma piuttosto un "incubatore" di progetti basati sulla tecnologia blockchain. È un'iniziativa globale e open source, della quale fanno parte i leader mondiali della finanza e dell'industria[69]. La Hyperledger

Foundation è supportata da un folto numero di leader di mercato nei più svariati settori[70], tra cui Ibm, Intel, Daimler, Fujitsu, JP Morgan e Cisco.

Il suo obiettivo è quello di instaurare una collaborazione cross-industry per lo sviluppo di tecnologie blockchain e DLT, concentrandosi sul miglioramento delle performance e l'affidabilità di questi sistemi per supportare transazioni globali e soluzioni innovative nel mondo del business [30].

A ottobre 2018, Hyperledger Foundation ha inoltre stretto una collaborazione con la Ethereum Enterprise Alliance (EEA), unendo così due delle principali realtà in ambito

blockchain con la comune volontà di accelerare il più possibile l'integrazione della tecnologia in ambito enterprise [31].

La famiglia di progetti Hyperledger è molto ampia, perciò ci limiteremo a descrivere brevemente alcuni dei servizi più noti.

Hyperledger Fabric

Il primo progetto a essere sviluppato all'interno della Hyperledger Foundation, con il contributo di Digital Asset e Ibm, è anche quello più versatile e utilizzato. Hyperledger Fabric consente di sviluppare applicazioni e soluzioni in ambito blockchain con

un'architettura modulare, in quanto molte delle sue caratteristiche possono essere attivate o disattivate, incluso il protocollo di consenso della blockchain.

La principale novità introdotta è la suddivisione dei peer in 3 diverse categorie: endorser, committer e consenter. La loro funzione è quella di permettere la condivisione di informazioni solo con specifici partecipanti al network – un evento comune a molte attività in cui sono coinvolte diverse organizzazioni.

Si può pensare a Hyperledger Fabric come a una blockchain privata, con la differenza che possono esistere più ledger contemporaneamente. Questi ledger prendono il nome di channel

(canali) e fungono appunto da canali di comunicazione tra due o più membri del network con lo scopo di condurre transazioni private o confidenziali senza coinvolgere gli altri partecipanti, ottenendo una flessibilità non possibile con le blockchain tradizionali.

Uno dei progetti in fase di sperimentazione in Italia che sfrutta Hyperledger Fabric riguarda lo sviluppo di una piattaforma per l'emissione di quote nelle società italiane, in collaborazione con il London Stock Exchange Group e Ibm [32].

Hyperledger Sawtooth

Inizialmente sviluppato con il contributo

di Intel, Hyperledger Sawtooth è il secondo progetto a entrare a far parte dei servizi Hyperledger e introduce un innovativo protocollo di consenso chiamato **Proof of Elapsed Time** (PoET), un processo che elegge il miner vincitore del nuovo blocco in modo simile a quello di una lotteria – il funzionamento è a sua volta basato sul Software Guard Extension di Intel (SGX) [33].

Altre proprietà uniche di Sawtooth sono il supporto agli smart contract e la possibilità di implementare un **consenso dinamico**, cioè modificabile in un secondo momento in base ai requisiti del network [34].

Uno dei casi di applicazione

principali è nella supply chain, in quanto consente di unire l'utilizzo di sensori (IoT) per ottenere informazioni sul tracciamento e la qualità dei prodotti, con i vantaggi di immutabilità e trasparenza offerti dalla tecnologia blockchain.

Oltre alla supply chain, Sawtooth viene anche applicato per scambiare beni digitali[71].

Hyperledger Quilt

Tra gli strumenti (tool) offerti da Hyperledger, Quilt nasce nel 2018 grazie al contributo di NTT Data e Ripple, e permette di costruire applicazioni basandosi sul protocollo

Interledger (ILP), un rivoluzionario protocollo di pagamenti cross-blockchain, ovvero che permette di scambiare criptovalute tra blockchain diverse e di ampliare enormemente la flessibilità delle applicazioni che si basano sulla tecnologia blockchain.

Interledger, il protocollo per l'Internet del valore

Nel Capitolo 7 abbiamo visto come la blockchain abbia posto le basi per la creazione di un Internet del valore,

rendendo possibile lo scambio di asset digitali in maniera decentralizzata, abbattendo di fatto confini geografici e politici.

Tuttavia, i pagamenti nel mondo blockchain sono lontani dall'essere ideali, dal momento che le reti stesse sono disconnesse l'una dall'altra. Lo scambio di valore è relativamente semplice solo se chi invia e chi riceve il denaro si trovano sullo stesso network (per esempio sulla stessa blockchain), una condizione non sempre soddisfatta. Quando il trasferimento di valore coinvolge più di una rete, le procedure da seguire diventano complesse, lunghe e costose.

Il potere di Internet come

piattaforma di scambio di informazioni deriva dalla possibilità di connettere chiunque. Questo accade proprio perché Internet non è una singola rete, ma è un network che collega altri network: un **Internetwork**.

> È possibile creare un network universale per trasferire valore, indipendente da ogni società o valuta?

Inventato nel 2015 da Stefan Thomas ed Evan Schwartz e avviato nel 2018, Interledger vuole essere per lo scambio di valore quello che Internet è per lo scambio di informazioni: un protocollo

aperto per effettuare pagamenti attraverso ledger di qualsiasi tipo: da wallet digitali a sistemi di pagamento nazionali, a blockchain e oltre.

L'architettura aperta e il protocollo minimale permettono a Interledger di connettere qualsiasi sistema di scambio di valore, senza essere collegato ad alcuna società, blockchain o valuta[72].

Nella pratica, questo viene ottenuto tramite i cosiddetti **connector** (connettori), operatori indipendenti che agiscono come exchange decentralizzati per criptovalute, valute fiat o altri asset digitali (Figura 12.3).

Con Interledger, per esempio, un utente può mandare BTC e il

destinatario potrà ricevere ETH o qualsiasi altra criptovaluta (o valuta fiat) che preferisce. Gli asset sono scambiati automaticamente nel corso della transazione senza che nessuna delle parti sia coinvolta nel processo di trasformazione, rendendo il processo estremamente semplice e veloce.

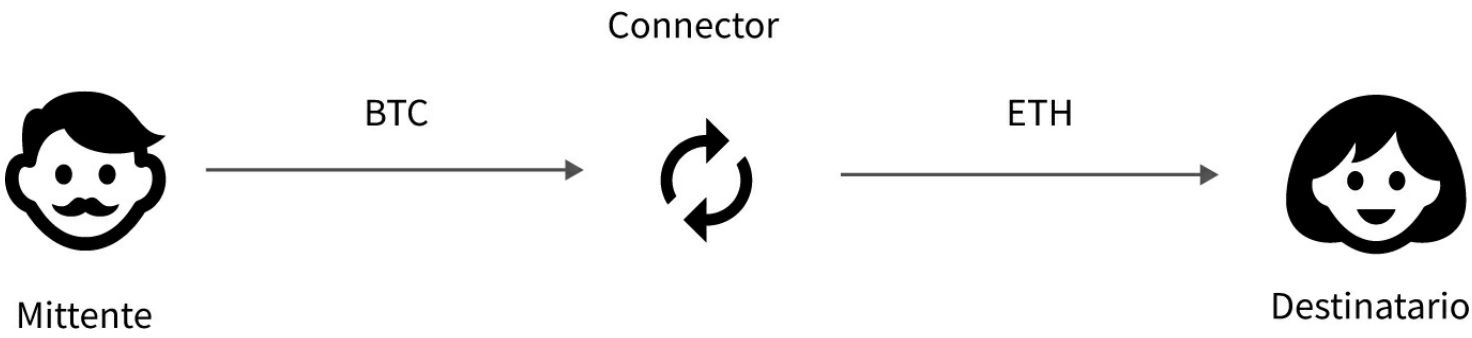


Figura 12.3 – Il trasferimento di denaro con Interledger.

Il progetto viene attualmente portato avanti dalla Interledger Community di

W3C (World Wide Web Consortium, la community internazionale che sviluppa gli standard del web e condotta dal fondatore del World Wide Web Tim-Berners Lee) ed è in gran parte influenzato dai protocolli che oggi costituiscono Internet. Bill Gates e la sua fondazione umanitaria sono anche stati recentemente coinvolti nella startup Coil, fondata dall'ex CTO di Ripple, in un progetto che utilizza Interledger per fornire servizi finanziari a Paesi meno sviluppati [35].

Interledger è quindi un progetto che permette di creare nuove soluzioni e modelli di business, contribuendo enormemente all'intera infrastruttura digitale, specialmente nel caso della

blockchain. Le applicazioni rese possibili da questo protocollo sono innumerevoli, ed è l'ennesima conferma che ci troviamo ancora all'alba di una nuova era digitale [36].

---

67. https://it.wikipedia.org/wiki/Locomotive_Act.
68. https://entethalliance.org.
69. https://www.hyperledger.org/about/leadership.
70. https://www.hyperledger.org/members.
71. https://sawtooth.hyperledger.org/examples/inde
72. https://interledger.org

13

Le applicazioni blockchain

In questo capitolo analizzeremo gli impatti della tecnologia blockchain nel mondo dell'industria. Ogni paragrafo conterrà un'analisi preliminare sul settore considerato e alcuni casi reali di utilizzo. La trattazione vuole dare al lettore degli spunti su come la blockchain possa essere utilizzata in varie situazioni, e la possibilità di

approfondire tramite le risorse suggerite. L'obiettivo del capitolo, dunque, è quello di essere una fonte d'ispirazione per il lettore.

Servizi finanziari

La blockchain e più in generale le DLT possono sicuramente aumentare l'efficienza in diversi aspetti dei servizi finanziari come i pagamenti, la custodia degli asset o il trading. Dal punto di visto tecnologico, questi sono tra i servizi più lenti ad adattarsi alle nuove tecnologie, in quanto spesso restano legati a sistemi legacy (obsoleti) che

ostacolano enormemente l'innovazione. Per fare un esempio, molte banche e aziende nel 2013 utilizzavano ancora COBOL, un linguaggio di programmazione nato nei primi anni '60 e che sopravvive solo in questi sistemi poiché troppo costoso da aggiornare.

Le innovazioni tecnologiche hanno però portato gli utenti ad avere aspettative più alte sulla qualità dei servizi. L'estrema difficoltà dei servizi finanziari a rimanere al passo coi tempi è uno dei motivi che ha causato la nascita di numerose startup fintech negli ultimi anni. *Harvard Business Review* assicura che la blockchain sarà per i servizi finanziari quello che Internet è stata per i media [37].

Ci troviamo in un periodo storico nel quale il mondo finanziario sta progressivamente aumentando i costi e diminuendo l'efficienza. Una regolamentazione incerta, i tassi di interesse ai minimi storici e le nuove banche digitali stanno portando notevole competizione nel mondo bancario tradizionale.

Diventa quindi fondamentale per una banca riuscire a ridurre le voci di costo principali per ottimizzare le risorse a disposizione. Alcuni esempi possono essere i costi per il trasferimento internazionale di fondi, la sicurezza e l'antiriciclaggio. McKinsey & Co stima che nei prossimi 5 anni le banche

mondiali potrebbero perdere circa 100 miliardi di dollari di profitto per colpa di inefficienze di gestione [38]. E un report di Santander stima un risparmio complessivo per le banche di 20 miliardi di dollari l'anno grazie all'implementazione di tecnologie blockchain [39].

Transazioni e pagamenti

Il trasferimento di valore è sempre stato un processo lento e costoso, soprattutto per i pagamenti cross-border. Per trasferire denaro, per esempio, dall'Italia al Sudafrica, bisogna passare attraverso numerose banche in un

processo che può richiedere giorni o addirittura settimane, con costi che arrivano anche a superare il 10% del valore della transazione. La tecnologia blockchain è in grado di semplificare questo processo rimuovendo tutti gli intermediari, aumentando drasticamente la velocità e diminuendo i costi. Accenture ha stimato che l'utilizzo della blockchain potrà portare alle banche risparmi complessivi per oltre 8 miliardi di dollari l'anno (su una spesa di 30 miliardi dollari) [40].

Ripple

Ripple, da non confondere con il token XRP, è una società focalizzata sullo

sviluppo di soluzioni blockchain per il trasferimento globale di denaro. A differenza di altri progetti come Bitcoin e Litecoin, pensati per un utilizzo mainstream, i clienti di Ripple sono principalmente banche e fornitori di servizi di pagamento. Uno dei prodotti di Ripple è RippleNet, ovvero un network di banche e servizi di pagamento interconnesso attraverso la tecnologia blockchain.

Nella pratica, RippleNet trasforma qualsiasi asset (da valute fiat a prodotti finanziari) in token scambiabili all'interno di un ledger distribuito (per un'analisi più dettagliata rimandiamo al Capitolo 10).

Ripple ha siglato partnership con

società come Unicredit, Ubs e Santander, e sta aumentando notevolmente la sua rete [41]. Il competitor più vicino a Ripple può essere considerato SWIFT, che in risposta a RippleNet ha lanciato di recente GPII, ancora però molto lontano dagli standard di velocità e sicurezza di Ripple[73].

SALT: prestiti peer-to-peer

SALT (Secured Automated Lending Technology) è una piattaforma di prestiti peer-to-peer basata su Ethereum. Questa piattaforma permette di usare criptovalute come collaterale per un prestito in contanti. Questi asset sono

ideali in quanto economici da trasferire, immagazzinare o liquidare, se confrontati, per esempio, con proprietà immobiliari o stock.

La blockchain inoltre, tramite l'utilizzo di smart contract, garantisce una gestione altamente efficiente e trasparente dei prestiti, permettendo di eliminare le frodi e ridurre enormemente i costi.

TenX

TenX è un progetto che ha lo scopo di creare un wallet mobile e delle carte di credito fisiche per spendere criptovalute nei negozi in maniera semplice e trasparente, anche se questi negozi non

accettano direttamente criptovalute. L'idea di TenX è quella di rendere ogni asset su blockchain spendibile istantaneamente. Come altri progetti simili, TenX è stato rallentato notevolmente dalle legislazioni, ancora incerte su temi come il pagamento in criptovalute.

Verifica dell'identità

Secondo una ricerca di Thomson Reuters, le banche spendono dai 50 ai 600 milioni di dollari l'anno solo per politiche di sicurezza riguardanti l'identità digitale, come il KYC (Know Your Customer, le procedure per

verificare dell'identità di una persona) o l'AML (Anti Money Laundering) [42]. Le attività sono volte prevalentemente a evitare problematiche inerenti al riciclaggio di denaro o al terrorismo.

La blockchain si inserisce in questo contesto eliminando tutti gli intermediari e instaurandosi come "sorgente unica di verità" per l'identità digitale, certificando l'autenticità dei dati e l'immutabilità delle informazioni. Spostando la gestione dell'identità digitale su blockchain, gli utenti saranno in grado di creare una propria identità su cui hanno il pieno controllo. Una volta verificata l'identità, gli utenti potranno consentire l'accesso a queste informazioni a terze parti, mantenendo

sempre il controllo sui propri dati.

Trading e finanza

> "C'è una possibilità molto concreta che tutte le transazioni societarie verranno spostate su blockchain."
>
> —**Johan Toll**, Nasdaq, Head of Blockchain Product Management

La tecnologia blockchain, e in particolare gli smart contract, sono destinati a rivoluzionare molti degli aspetti legati ai meccanismi che regolano il trading.

Attualmente uno degli scenari più

problematici in questo ambito è la liquidazione dei titoli azionari. I broker per eseguire questo tipo di operazioni devono passare attraverso un processo di verifiche e burocrazia che può richiedere diversi giorni a causa delle regolamentazioni e dei numerosi intermediari. La blockchain può rendere questi processi più veloci, sicuri e meno costosi.

Nasdaq

Nasdaq, il secondo più grande stock exchange al mondo per market cap, è convinto che esista un grande potenziale nell'ambito dei servizi finanziari per poter sfruttare la tecnologia blockchain,

in particolare nelle aree che richiedono il tracciamento e il trasferimento di asset digitalizzati in maniera peer-to-peer [43]. Sfruttando l'immutabilità delle transazioni su blockchain è possibile creare un sistema molto più efficiente per la liquidazione di asset, il trasferimento di denaro o di security, la gestione dei collaterali e la condivisione di informazioni, il tutto in maniera trasparente e verificabile.

Come caso pratico, Nasdaq ha creato una piattaforma sperimentale basata su blockchain (chiamata Linq) per la gestione delle share di compagnie private all'interno del Nasdaq Private Market, permettendo a queste di emettere security digitali salvate sulla

blockchain [44]. Le società possono così trasferire queste security in maniera estremamente semplice e veloce, eliminando completamente la necessità di documenti cartacei.

Iconomi

Iconomi è una piattaforma per la gestione di asset digitali che permette agli utenti di investire in Digital Asset Array (DAA), una combinazione di diversi asset digitali. Ogni manager può creare i propri DAA e permettere a chiunque di investire in maniera trasparente grazie all'utilizzo di smart contract. Iconomi offre agli utenti una varietà di investimenti con diversi

livelli di rischio. Il DAA più popolare, al momento, è il Blockchain Index, un indice basato sulle principali criptovalute.

Industria 4.0

Supply chain

La supply chain (o catena di distribuzione) è la filiera logistico-produttiva che porta un prodotto da un'organizzazione a un cliente. Nella supply chain è compreso il reperimento delle materie prime e dei componenti necessari all'ottenimento del prodotto

finito.

In un mercato sempre più globale questi processi sono diventati estremamente complessi, includendo talvolta decine o centinaia di fasi distribuite in altrettante location.

In una supply chain intervengono pagamenti, burocrazia, lavoro e una complessità tale che spesso comporta un notevole aumento di prezzo per i consumatori finali o una diminuzione della qualità del prodotto.

I problemi che intercorrono in questi innumerevoli passaggi sono di varia natura, come la perdita o la manipolazione delle informazioni, la complessa gestione delle diverse parti coinvolte nel processo logistico e i

ritardi dovuti alla burocrazia. La tecnologia blockchain può aiutare questo insieme di processi portando trasparenza, tracciabilità dei prodotti e riduzione della fiducia necessaria tra le parti.

Attraverso l'immutabilità e la sicurezza dei dati è possibile salvare ogni singolo passaggio di produzione o lavorazione all'interno di una blockchain rendendolo chiaro, visibile e accessibile a tutte le parti autorizzate.

In questo modo, il produttore può tracciare molto più efficacemente costi e tempi di produzione. Il trasportatore allo stesso modo può pianificare tempi, capacità e costi con la conseguenza di

aumentare enormemente l'efficienza di tutta la catena distributiva. Il consumatore, infine, è in grado di verificare la provenienza (e in alcuni casi la qualità) del prodotto acquistato e può beneficiare dei risparmi.

Il caso pratico: Carrefour e Walmart

La nota catena francese di supermercati Carrefour ha annunciato di recente di avere iniziato a implementare la blockchain Ibm per la tracciabilità dei suoi prodotti. Il progetto inizialmente si occuperà di monitorare la distribuzione di polli, uova e pomodori freschi dai produttori stessi fino all'arrivo nei negozi.

L'utilizzo della tecnologia blockchain ha lo scopo di far sì che ciascun componente della supply chain possa fornire informazioni relative al suo particolare ruolo nella filiera, potendo così identificare nel dettaglio ciascun lotto (date, luoghi, trattamenti, canali di distribuzione ecc.).

In termini concreti, nell'etichetta di ciascuno dei prodotti di Carrefour sarà presente un codice QR che i consumatori potranno scannerizzare con il loro smartphone. Le etichette forniranno informazioni sul prodotto e sul viaggio da esso intrapreso fino all'arrivo sugli scaffali. Il consumatore sarà quindi in grado di conoscere il luogo e il modo di

allevamento, il nome dell'allevatore, il cibo somministrato, i trattamenti, le etichette e il luogo del macello.

I benefici sono chiari per tutta la filiera: i produttori possono ricevere continuamente dati per migliorare la produzione e ottimizzare la distribuzione, il consumatore può sapere in trasparenza le informazioni di prodotto, il brand fornisce un servizio migliore ai propri clienti [45].

Un altro caso interessante di implementazione è quello di Walmart, che negli Stati Uniti ha implementato la stessa tecnologia per tracciare la provenienza di carne e frutta. In questo caso si è potuto evidenziare un risparmio considerevole del tempo

necessario a tracciare un prodotto, passando da diversi giorni a qualche secondo.

Il caso pratico: Walmart e Alibaba

I giganti mondiali Walmart e Alibaba si stanno muovendo verso l'adozione di tecnologie blockchain per rendere più efficiente l'intero sistema retail.

Walmart ha siglato una partnership con Ibm per il tracciamento del cibo in Cina, iniziando due progetti pilota sulla carne di maiale e sul mango [46]. Il sistema permette di tracciare il prodotto dalla sua nascita fino allo scaffale, riducendo il tempo di verifica d'origine da settimane a minuti, e aiutando a

gestire velocemente i casi di prodotti da richiamare.

Alibaba ha siglato una partnership con Cainiao, una sua controllata nel settore logistica, per un progetto pilota che comprende 50 Paesi e oltre 30.000 merci tracciate nel proprio ciclo di vita e in comunicazione con gli e-commerce del gruppo [47].

Il caso pratico: My Story

La tracciabilità della filiera produttiva è un tema di grande rilevanza anche in Italia, per esempio, nel settore vitivinicolo. DNV GL, società di servizi assicurativi e gestione del rischio, ha sviluppato una soluzione che attraverso

la scansione di un QR code, posto direttamente sull'etichetta della bottiglia, permette ai consumatori di conoscere la storia del vino che si apprestano a consumare.

My Story fornisce informazioni specifiche – verificate e certificate da un soggetto terzo indipendente – sulle caratteristiche e sui processi di produzione, per fornire un quadro completo e sicuro del prodotto.

Attraverso tale applicazione i brand, i rivenditori, gli attori intermedi della filiera produttiva nonché i clienti finali potranno contare su dati non modificabili verificati da una parte terza indipendente, in modo da avere piena visibilità, trasparenza e controllo sui

vari stadi di lavorazione lungo la supply chain. Per ora sono quattro le aziende vinicole che utilizzano l'applicazione [48].

Maersk

A.P. Moller-Maersk, società integrata di trasporti e logistica con più marchi, leader mondiale nel trasporto di container e nella loro gestione in ambito portuale, ha dato avvio a una joint venture con Ibm al fine di creare una piattaforma per accelerare il commercio.

Questa piattaforma, basata sulla tecnologia blockchain, aiuterà a gestire e rintracciare decine di milioni di

container a livello globale, digitalizzando il processo della supply chain.

L'obiettivo è di offrire al mercato una piattaforma digitale pensata per essere impiegata dall'intero ecosistema logistico, creando maggior trasparenza e semplicità nello spostamento delle merci (le qualità che attualmente mancano al sistema). L'unico ostacolo da superare per realizzare questo progetto è riuscire a convincere tutte le parti coinvolte nel processo [49].

De Beers

Il Gruppo De Beers, leader mondiale nell'estrazione, lavorazione e

commercializzazione di diamanti, ha da poco terminato la fase sperimentale di una propria piattaforma su blockchain. Lo scopo è garantire la tracciabilità dei diamanti dal momento dell'estrazione fino a quello della vendita. Il prototipo è stato lanciato su un piccolo campione e servirà a sviluppare ulteriormente la piattaforma rendendola inclusiva e user-friendly. I punti chiave su cui gli sviluppatori si concentreranno sono la protezione dei dati sensibili, la velocizzazione dei processi e la garanzia di una maggiore sicurezza per gli investitori.

Lo scopo è quello di sviluppare una piattaforma blockchain aperta, su cui poter costruire applicazioni che

apportino ulteriori benefici al settore. L'utilizzo della tecnologia blockchain, permettendo totale tracciabilità e trasparenza, non solo garantirebbe la provenienza naturale ed etica dei diamanti, ma creerebbe anche un registro unico e permanente, a prova di contraffazione, per tutti i diamanti su di esso registrati [50].

Anti-contraffazione

VeChain

VeChain è una piattaforma basata su blockchain fondata nel 2015, focalizzata su gestione della supply chain, tracciamento di prodotti e

anticontraffazione. Inizialmente costruita su Ethereum, nel 2018 ha lanciato la propria blockchain chiamata VeChain Thor [51]. Le partnership includono Pwc e Bmw [52].

L'idea di base di VeChain è quella di fornire gli strumenti (QR, NFC, RFID, sensori) per permettere la digitalizzazione del prodotto e il trasferimento dell'identità digitale su blockchain. Tutte le informazioni vengono aggiornate in tempo reale seguendo l'evoluzione del prodotto lungo la supply chain, andando a ridurre enormemente il rischio di contraffazione.

Considerando il caso precedentemente descritto per la

tracciatura della filiera nel settore vitivinicolo, VeChain offre una piattaforma di autenticazione e tracciamento delle bottiglie dove ogni parte del processo produttivo e logistico viene salvata sulla blockchain.

IoT

La tecnologia blockchain si candida a tutti gli effetti come supporto ideale per l'industria IoT.

Per IoT si intende il network di dispositivi fisici (automobili, sensori, elettrodomestici ecc.) dotati di connettività e in grado di comunicare o

scambiare dati tra loro. Dai circa 9 miliardi di dispositivi connessi nel 2017, si pensa che nel 2025 ce ne saranno più di 55 miliardi, assieme a un valore di investimenti nel settore intorno ai 15 triliardi di dollari nello stesso periodo [53].

Una crescita così massiva di dispositivi e dati raccolti nasconde insidie non indifferenti, dalla sicurezza alle integrazioni, dalla velocità alla connettività.

Alcuni di questi punti possono essere risolti grazie all'utilizzo di sistemi blockchain, e nel successivo paragrafo esploreremo alcune delle applicazioni più interessanti.

Smart home

Quando parliamo di smart home (home automation o domotica) ci riferiamo a quelle abitazioni che utilizzano tecnologie interconnesse per creare automazioni nella gestione dei processi interni di un'abitazione.

Alcuni esempi potrebbero essere la gestione automatica del riscaldamento o dell'illuminazione basata su sensori. Oppure il controllo da remoto delle telecamere di sicurezza, o ancora l'utilizzo di smart lock al posto delle serrature tradizionali. Questa realtà, seppur in rapida espansione, soffre di una mancanza di standard definiti che potrebbero causare problemi riguardanti

sicurezza e privacy. In questo ecosistema così ricco di sfide e rischi, la tecnologia blockchain può sicuramente inserirsi fornendo proprietà come:

- **Decentralizzazione:** grazie alla distribuzione delle informazioni e alla mancanza di un unico punto di controllo centrale, è possibile rendere più efficiente il network di dispositivi.
- **Sicurezza:** permettendo al network di device di scambiare dati senza il bisogno che vi sia fiducia tra le parti.

È quindi fondamentale scegliere il

protocollo blockchain più corretto, poiché scalabilità, velocità e privacy ricoprono un ruolo fondamentale.

IOTA

Quando si parla di IoT nel mondo DLT non si può fare a meno di citare IOTA, attualmente il più conosciuto progetto in ambito IoT per transazioni m2m (machine-to-machine).

Nel Capitolo 6 abbiamo visto come questa particolare tecnologia sia in grado di offrire transazioni gratuite e potenzialmente scalabili all'infinito.

Di questo se ne sono accorte grandi aziende come Bosch, Volkswagen e

Microsoft, che hanno siglato partnership per integrare IOTA nei propri prodotti IoT. Uno dei progetti più interessanti riguarda una partnership non formale con Microsoft e Fujitsu che prevede la costruzione di un marketplace di dati su IoT sicuro e distribuito, accessibile e monetizzabile dalle aziende [54].

Un altro caso d'uso è TIOTA, la Trusted-IoT-Alliance tra Cisco, Bosch e altri grandi aziende per portare avanti progetti di integrazione IoT con sistemi di ledger decentralizzati.

Self driving car

L'industria dell'automotive è coinvolta

da più lati nell'innovazione portata dalla tecnologia blockchain. Non solo le automobili stanno diventando device sempre più connessi, ma si stanno trasformando in veri e propri veicoli autonomi, in grado di trasportare merci o persone senza l'aiuto umano alla guida. Sono le self driving car o driverless car, letteralmente "auto a guida autonoma", che tanto stanno facendo parlare di sé dopo i vari test di Tesla, Google, Apple, Uber e altri grandi player del mondo automotive.

Smart car

La possibilità di integrare un'auto a guida autonoma con la tecnologia

blockchain potrebbe portare il concetto di autonomia a un livello superiore. Tramite questa tecnologia è possibile infatti dotare l'automobile di una propria identità digitale e un proprio wallet di criptovalute, rendendola di fatto un'entità autonoma sia dal punto di vista giuridico che finanziario.

Utilizzando i concetti di smart property, diventa possibile collegare l'identità digitale della macchina all'identità digitale di una persona, semplificando enormemente procedure come il trasferimento della proprietà o il noleggio.

L'auto potrebbe, per esempio, pagare in autonomia l'assicurazione, effettuando microtransazioni a ogni

chilometro percorso. L'assicurazione potrebbe inoltre essere integrata direttamente con uno smart contract che in caso di incidenti controlla diversi parametri come la velocità o il rispetto della segnaletica e provvede a calcolare e rendere immediatamente disponibili i fondi per il risarcimento.

Prioritizzazione degli itinerari

Una delle prospettive più affascinanti nel mondo delle self driving car è l'integrazione di IoT, machine learning e blockchain.

Un brevetto recentemente registrato da Ford, apre uno scenario nuovo nell'utilizzo di queste tecnologie per

risolvere il problema del traffico [55].

La tecnologia è stata chiamata "Cooperatively Managed Merge and Pass (CMMP) System" e permette una cooperazione diretta tra automobili per stabilire velocità e priorità tra i diversi veicoli. Le persone che avranno più urgenza potranno pagare quelle meno di fretta per arrivare in tempo, per esempio, a un appuntamento, aumentando la velocità o sfruttando le corsie meno trafficate. Il sistema funziona attraverso un token che viene scambiato in modo decentralizzato tra veicoli e che quindi si autoregola in base a domanda e offerta.

Il sistema permetterebbe uno snellimento non indifferente del traffico

urbano grazie all'uso di algoritmi di machine learning capaci di monitorare continuamente strade, veicoli e itinerari.

Energia

Negli ultimi anni il mercato dei pannelli solari domestici e in generale delle energie rinnovabili è cresciuto enormemente, grazie anche alla riduzione dei costi e alle politiche di incentivo per gli investimenti in energia rinnovabile.

L'utilizzo principale della tecnologia blockchain in ambito energetico riguarda la creazione di

piattaforme di scambio peer-to-peer, dove diventa possibile per gli utenti vendere o comprare energia senza dover necessariamente passare per degli intermediari.

Un report di Pwc mostra in modo dettagliato come molte startup stiano lavorando in questo senso [56].

Power Ledger

Power Ledger è una piattaforma globale di trading di energia basata su tecnologia blockchain (Ethereum) in cui è possibile vendere e comprare energia rinnovabile. L'idea è quella di creare un marketplace che permetta agli utenti di

effettuare transazioni di energia in maniera peer-to-peer. L'utilizzo della tecnologia blockchain è ideale, in quanto fornisce un sistema trasparente, verificabile e automatizzato in cui vengono salvate tutte le transazioni avvenute, rimuovendo gran parte degli attori intermedi che solitamente sono in controllo dei meccanismi di scambio e causano un inevitabile aumento dei costi di gestione. Power Ledger permette di effettuare transazioni di energia in tempo reale tra diversi utenti sparsi per il mondo dando alle comunità la possibilità di ottenere l'autosufficienza energetica.

Power Ledger offre diverse soluzioni, tra le quali:

- **µGrid (microgrid)**: la piattaforma peer-to-peer di trading di energia rinnovabile in maniera regolata, che consente, per esempio, di effettuare microtransazioni di energia o di acquisire dati di utilizzo.
- Power port: una piattaforma pensata per la gestione delle stazioni di ricarica per i veicoli elettrici, con la possibilità di pagamenti istantanei e il monitoraggio in tempo reale dei consumi.

Le applicazioni in ambito governativo

Le applicazioni della tecnologia blockchain in ambito governativo e della pubblica amministrazione sono svariate. Negli ultimi tempi si è sentito parlare principalmente di identità digitale e di come sarebbe possibile automatizzare una serie di processi riguardanti, per esempio, sanità, istruzione, pagamento delle imposte e in generale snellire ogni scenario attualmente bloccato da una burocrazia soffocante. Qui analizzeremo quali possono essere gli impatti della tecnologia blockchain sul settore pubblico e come già diversi Paesi nel

mondo abbiano avviato dei test reali sull'utilizzo della tecnologia.

I limiti di questo tipo di applicazione sono principalmente di carattere burocratico e normativo, più che tecnologico.

Identità digitale

Per aprire un conto corrente o stipulare un contratto telefonico è necessario provare la propria residenza e cittadinanza con un documento come una carta d'identità, un passaporto o una patente.

Allo stesso modo, l'accesso a servizi pubblici quali sanità o istruzione

è governato da un riconoscimento di identità rilasciato dal governo del Paese di residenza o provenienza.

Questo tipo di procedimento porta con sé diverse complicazioni, come per esempio l'invalidità di alcuni documenti al di fuori dei confini nazionali. A questo si unisce una burocrazia lenta e complessa, e la difficoltà di accesso a questo tipo di servizi per persone che vivono in Paesi del terzo mondo.

A tale proposito, nel 2017, la Banca Mondiale ha stilato una serie di principi considerati fondamentali per massimizzare i benefici dei sistemi di identificazione [57].

Molti stati forniscono degli ID univoci per riconoscere i propri

cittadini, ma si sente la necessità di un sistema globale di riconoscimento sicuro, non modificabile, privo di censura e facilmente accessibile.

È qui che si inserisce la tecnologia blockchain: un'identità digitale per ogni essere umano, slegata dal controllo governativo e non dipendente dai documenti di identità dei vari Paesi. L'idea si avvicina molto a quella esposta nella parte sugli impatti nel mondo bancario, in particolare sui processi di KYC.

Diverse aziende e organizzazioni hanno iniziato la costruzione di questo ecosistema, con i primi test già attivi in Kenya e in altri Paesi africani.

La blockchain permette di certificare l'esistenza, la data di creazione, l'origine e il contenuto di qualsiasi documento, contratto, licenza, proprietà o evento esistente in forma digitalizzata, in maniera automatica e senza l'intervento di terze parti. È possibile eventualmente mantenere riservate queste informazioni e renderle accessibili solo al proprietario o a terze parti autorizzate senza lunghi processi di identificazione.

Civic

Civic è una piattaforma che si occupa di identità digitale e utilizza la blockchain (Ethereum) per gestire l'identità degli

utenti in maniera decentralizzata, lasciando la proprietà delle informazioni agli utenti stessi, che decidono autonomamente con chi condividerle. Civic quindi è un progetto che punta a ridare agli utenti il controllo dei propri dati. In particolare Civic fornisce un sistema di verifica dell'identità per individui e aziende, più sicuro, economico ed efficiente rispetto ai sistemi tradizionali.

Uno dei casi di applicazione di Civic è il KYC richiesto da banche o piattaforme di investimento. A seconda del servizio utilizzato, una pratica KYC può richiedere giorni o settimane, in quanto l'azienda deve verificare la correttezza di tutte le informazioni in un

processo pieno di burocrazia.

Utilizzando Civic ogni azienda ha la possibilità di verificare le informazioni dell'utente controllando direttamente i dati salvati sulla blockchain senza la necessità di richiedergli di caricare ogni volta le informazioni. L'identità di una persona diventa così facilmente trasferibile da un servizio a un altro.

Il voto digitale

È facilmente intuibile come, avendo un sistema di riconoscimento digitale per ogni singolo cittadino, sia possibile l'ottimizzazione di molti scenari, come il voto tramite sistemi digitali,

riducendo sensibilmente i rischi legati a corruzione, modifica delle schede elettorali e vendita di voti.

Finora, il voto digitale ha portato con sé una serie di dubbi e domande: chi controlla la piattaforma online con la quale si vota? Come è possibile essere sicuri che i voti siano conteggiati senza errori? Queste domande possono trovare una risposta nella tecnologia blockchain, rendendo il voto digitale più sicuro e trasparente.

Un voto digitale diventerebbe una transazione, e come abbiamo già visto il consenso del network impedisce ogni forma di doppia spesa, eliminando il rischio di falsificazione dei voti.

Il conteggio dei voti diventa

immediato e verificabile, garantendo tra le altre cose un notevole risparmio economico.

Il voto digitale è uno scenario applicabile anche da aziende che potrebbero garantire un diritto di voto ai propri shareholder, in una maniera sicuramente più efficiente di quanto avviene attualmente.

Nasdaq eVoting

Nasdaq eVoting è un progetto, nato nel 2016, che ha portato alla creazione di una piattaforma basata su blockchain per la semplificazione dei processi di voto da parte di compagnie e investitori, attualmente complicati da una mancanza

di trasparenza e tracciabilità. Questa piattaforma, oltre a ridurre la complessità delle votazioni, diminuisce drasticamente i costi di gestione [58].

Sanità

Le aziende operanti in ambito sanitario hanno iniziato a intravedere il potenziale di questa tecnologia andando ad applicarla in diversi settori di loro competenza. La blockchain può essere usata per esempio nella gestione delle cartelle cliniche. C'è infatti un'estrema necessità di modernizzare il modo in cui le cartelle cliniche dei pazienti sono gestite.

La blockchain potrebbe rivelarsi incredibilmente utile nella gestione e archiviazione dei documenti tenendo traccia della storia medica di ogni paziente, in modo automatico e sicuro, permettendo la condivisione di queste informazioni con soggetti autorizzati anche oltre i confini nazionali.

Essere ricoverati all'estero non sarebbe più un problema, in quanto le informazioni diventerebbero accessibili senza barriere linguistiche, burocratiche o geografiche.

Un altro utilizzo di questa tecnologia riguarda il settore farmaceutico, dove la blockchain viene utilizzata per il monitoraggio delle forniture di farmaci e

per verificarne l'autenticità (vedi supply chain).

Istruzione

La Comunità Europea ha pubblicato un report sulle possibili applicazioni della blockchain nel campo dell'istruzione [59].

Il report, intitolato "Blockchain in Education", focalizza la sua attenzione sulla possibilità di tracciare in modo digitalizzato le conoscenze e competenze raggiunte dagli studenti in ambito accademico, disegnando quindi un profilo unico e immutabile del percorso di studi di ciascuna persona.

La Commissione ha esposto diversi scenari e sfide, tra i quali il riconoscimento e il trasferimento di crediti formativi, le certificazioni digitali, il riconoscimento multi-step e le transazioni di pagamento degli studenti.

Nonostante sia un campo abbastanza lento in ambito di innovazione, già molti istituti di rilievo a livello mondiale si stanno adoperando per testare i sistemi blockchain. Il MIT e il FSMB hanno iniziato dei progetti pilota in questo ambito [60].

Il caso pratico: Estonia

Tutto ciò che abbiamo trattato in questo paragrafo è già praticamente realtà in

Estonia.

Parliamo di X-Road e di E-Residency, due progetti che hanno visto la luce qualche anno fa e che stanno avendo un ottimo riscontro in un Paese che conta quasi un milione e mezzo di abitanti.

X-Road è una piattaforma basata su un protocollo distribuito che comunica con le varie infrastrutture pubbliche e private per erogare e tracciare l'utilizzo dei servizi da parte di aziende e cittadini, dall'identità digitale fino ai servizi sanitari e all'istruzione. È inoltre implementato un sistema automatico di fondi che si sbloccano in base alla situazione economico-sociale.

E-Residency dà invece la possibilità

a qualsiasi persona nel mondo di richiedere l'identità digitale estone. Questo permette di aprire e gestire una startup in Estonia da remoto, senza burocrazia cartacea e garantendo l'accesso a una serie di servizi a supporto delle aziende.

Nel momento in cui scriviamo, ci sono oltre 45mila cittadini digitali, da 167 Paesi nel mondo, che hanno aperto oltre 5.000 startup.

Grazie a queste iniziative l'Estonia sta riuscendo ad attirare capitali e ottimizzare la gestione del Paese: oltre l'86% dei cittadini hanno un'identità digitale, il 99,6% delle transazioni bancarie vengono effettuate

elettronicamente e il 96,3% fa la dichiarazione dei redditi online[74].

Il tutto è stato possibile grazie alla visione di un Paese innovativo che ha velocemente capito le potenzialità della tecnologia blockchain.

Il retail

Sebbene il settore retail sia strettamente legato alle applicazioni in ambito supply chain, è necessario dedicare un veloce approfondimento sugli impatti paralleli che la tecnologia blockchain può portare in questo settore.

Il primo in assoluto è appunto il

beneficio di tracciare la provenienza di un prodotto: i negozi potranno esporre a scaffale dei prodotti certificati e protetti, con la certezza di ingredienti e allergeni o luoghi di produzione e origine.

Un'altra possibile area di applicazione è legato ai programmi fedeltà: secondo un censimento di Colloquy, sono attive solo negli Stati Uniti oltre 3,3 miliardi di membership legate a programmi di loyalty, con premi che hanno un valore percepito di 50 miliardi di dollari ogni anno [61].

È chiaro come la voce di costo legata a questi programmi sia di miliardi di dollari ogni anno, divisa tra sconti concessi ai clienti e sistemi che riescano a tracciare gli acquisti tra differenti

canali, negozi e dispositivi. La tecnologia blockchain permetterebbe ai retailer di gestire un sistema comune e distribuito per tracciare in modo preciso e immutabile i progressi dei propri clienti, premiandoli automaticamente con coupon o sconti una volta raggiunti determinati livelli di spesa.

Ultimo, ma non certamente meno importante, il tema dei pagamenti. Molto spesso le commissioni di gestione di un sistema di pagamento elettronico sono proibitive per piccoli negozi. Per transazioni ridotte come il pagamento di un caffè, le commissioni bancarie eliminano totalmente il profitto del negoziante. Le criptovalute offrono delle

soluzioni estremamente più economiche degli attuali sistemi di pagamento elettronici.

No-profit

Le organizzazioni no-profit a scopo benefico aiutano ogni anno milioni di persone in tutto il mondo. Solo negli Stati Uniti sono oltre 1,4 milioni e raccolgono circa 370 miliardi di dollari all'anno[75].

Oltre i numerosi progetti che queste compagnie portano avanti con forza e determinazione, ce ne sono purtroppo alcuni poco trasparenti, che utilizzano

parte dei fondi per scopi diversi da quelli pubblicizzati. Negli Usa i continui problemi legati allo scarso controllo di queste attività hanno portato un cittadino su tre a non credere alla beneficenza fatta da queste organizzazioni [62].

Grazie alla blockchain è possibile tracciare in modo trasparente l'utilizzo di questi fondi in tutto il percorso dai donatori ai destinatari. È possibile poi tracciare l'uso di questi fondi in progetti reali, aggiornando il donatore sullo stato di avanzamento dei lavori in termini di infrastrutture e aiuti.

Un altro grosso fattore è la riduzione dei costi dovuti alla rimozione degli intermediari. Nel sistema attuale, i fondi passano tra diverse organizzazioni,

private o governative, che inevitabilmente trattengono percentuali di gestione. Attraverso una blockchain invece si avrebbe un percorso diretto da donatori a progetti no-profit, senza dover remunerare nessun intermediario.

Infine, grazie all'utilizzo delle criptovalute, è possibile raggiungere popolazioni sprovviste di sistemi bancari. Il problema degli unbanked è infatti estremamente diffuso. Secondo i dati del 2017, gli adulti che non hanno accesso a servizi bancari sono circa 1,7 miliardi [63].

Le Nazioni Unite

Intorno alla metà del 2017, si è conclusa una delle prime operazioni umanitarie utilizzando la tecnologia blockchain: le Nazioni Unite hanno aiutato 10.000 rifugiati siriani utilizzando la blockchain di Ethereum. I fondi sono stati regolarmente tracciati e sono serviti a comprare cibo e altri beni di prima necessità [64]. La tecnologia blockchain ha permesso di risparmiare tempo e costi, bypassando di fatto il sistema bancario tradizionale, di difficile accesso per i rifugiati.

Digital advertising

L'Interactive Advertising Bureau (IAB) ha rilasciato il suo primo paper sulla tecnologia blockchain affermando che "rappresenta una soluzione naturale per la catena di fornitura della pubblicità digitale, con un potenziale per aumentare l'efficienza, ridurre i costi ed eliminare le frodi" [65].

A tale proposito, riportiamo di seguito alcuni dati statistici raccolti da Basic Attention Token[76].

- Circa il 50% dell'utilizzo dati su dispositivi mobile è dovuto a pubblicità o tracker che rallentano notevolmente la navigazione e il consumo di batteria. Molti di questi violano

la privacy. E la quantità di pubblicità contenenti malware è aumentata notevolmente.

- Gran parte degli introiti è trattenuta dagli intermediari come Google e Facebook. I profitti per i publisher e i creator sono crollati.
- I bot (robot informatici, utilizzati principalmente per inviare messaggi) hanno causato frodi per oltre 7 miliardi di dollari nel solo 2017.
- Gli advertiser spesso non sanno dove verranno posizionate le proprie pubblicità, rischiando

danni di immagine, click fasulli o un targeting non ideale.

Questa situazione così caotica ha portato gran parte degli utenti a utilizzare delle forme di ad-blocking (programmi o estensioni del browser che bloccano le pubblicità o i tracker).

Un altro tema controverso nell'ambito dell'advertising è il trattamento dei dati sensibili. Gran parte delle informazioni sul reale utilizzo dei dati personali sono tenute segrete o sono estremamente difficili da reperire. Quindi spesso non ci sono garanzie sul fatto che le informazioni raccolte sugli utenti non vengano vendute a terze parti.

Attraverso la tecnologia blockchain

è possibile tracciare l'utilizzo di queste informazioni rendendole accessibili solamente alle figure che ne hanno diritto. Anche la raccolta di questi dati può avvenire in maniera trasparente con il consenso dell'utente, che accetta di condividere informazioni personali come sesso, età o provenienza, ricevendo dei token in cambio. Gli advertiser non dovranno più pagare migliaia di euro per raccogliere informazioni da terze parti (spesso con metodologie al limite della legalità) ma potranno riceverle direttamente dal potenziale cliente, migliorandone l'esperienza online grazie a contenuti personalizzati sui suoi specifici interessi.

Quello del digital advertising è quindi un settore da tenere sotto controllo, soprattutto per i volumi che muove, stimati intorno ai 40 miliardi di dollari solo negli Usa nella prima metà del 2017 [66].

BAT (Basic Attention Token) e browser Brave

BAT è un progetto di digital advertising basato su blockchain (Ethereum) che punta a migliorare radicalmente il settore della pubblicità digitale. Il fulcro

del progetto è il token BAT, che ricopre il ruolo di utility token per la piattaforma, permettendo pagamenti diretti tra utenti, creator e publisher. BAT è inoltre integrato nel web browser Brave.

Brave è un progetto free e open source per un browser che nativamente blocca gli ad invasivi e i tracker. Brave utilizza il token BAT per creare un nuovo sistema di ricompense dei content creator basato sull'attenzione. Il browser, infatti, registra automaticamente l'attenzione dell'utente e provvede a remunerare i publisher in maniera estremamente accurata e trasparente. Brave nel 2018 ha registrato circa 4 milioni di utenti attivi mensili.

Smart property

Smart property è un concetto introdotto da Nick Szabo (un pioniere degli smart contract) nel 1994 e può essere visto come un'estensione dell'idea di smart contract alla proprietà. Per smart property ci riferiamo alla gestione di una proprietà utilizzando degli smart contract. Il bene può essere un oggetto fisico come una macchina o una casa, oppure delle proprietà astratte, come le quote di una società o la proprietà intellettuale di un brevetto o una canzone. La smart property introduce

alcuni notevoli vantaggi, come per esempio la possibilità di scambiare questo bene senza doversi appoggiare a intermediari.

Questo tipo di applicazione incontra però diverse frizioni per questioni legali e fiscali. Prima di poter implementare su larga scala una soluzione del genere, è necessario che l'intero sistema che oggi gestisce gli scambi di proprietà riesca ad adeguarsi agli standard della tecnologia blockchain. Sicuramente gli impatti si estendono anche al mondo del lavoro, con decine di figure professionali oggi fondamentali (per esempio notai e avvocati) che perderebbero la loro funzione centrale di intermediazione e certificazione.

Il progetto Svezia

Il catasto svedese sarà tra le prime istituzioni a testare la tecnologia blockchain. La Lantmateriet, l'autorità governativa che si occupa appunto di mappare e gestire gli immobili in Svezia, prevede di condurre la prima transazione su blockchain nei prossimi mesi e sta selezionando volontari intenzionati ad acquistare o vendere proprietà.

La scelta è in questo momento ricaduta su una blockchain privata e non su un'infrastruttura decentralizzata come

quella di Bitcoin o Ethereum, nello specifico quella di ChromaWay[77].

Mats Snäll, capo dello sviluppo del progetto, ha dichiarato che questo tipo di tecnologia farà risparmiare centinaia di milioni di dollari di spese al governo svedese, ed è fiducioso che i test effettuati in piccola scala verranno presto estesi all'intero sistema.

Le applicazioni del cloud

Cloud storage

La richiesta di cloud storage è destinata a crescere enormemente nei prossimi anni. Ci si aspetta infatti che questo mercato passi dai 30 miliardi di dollari del 2017 a oltre 80 miliardi di dollari nel 2023 [67]. Questa crescita è trainata da diversi fattori come l'esplosione dell'IoT e l'aumento dello spazio richiesto da file video e immagini in alta qualità.

Attualmente il mercato è dominato da grossi provider come Amazon (AWS), Google (Google App Engine), Microsoft (Azure) e Dropbox, che danno la possibilità a chiunque di utilizzare il loro servizi di cloud storage offrendo prezzi competitivi grazie all'economia

di scala. Questo modello centralizzato soffre però di problemi legati soprattutto alla sicurezza e alla privacy dei dati.

Il cloud storage è un settore che può trarre benefici da una soluzione decentralizzata costruita sul supporto offerto dalla tecnologia blockchain.

Decentralizzando il cloud storage, si può dare la possibilità a chiunque di affittare parte del proprio hard disk, proprio come oggi si usa mettere a disposizione il proprio appartamento con Airbnb. Lo storage diventa così una commodity scambiabile in maniera decentralizzata e sicura.

Storj

Storj è un'applicazione di cloud storage decentralizzato che garantisce privacy e sicurezza dei dati promettendo una soluzione finale più veloce, sicura ed economica rispetto ai provider tradizionali. I file vengono divisi, criptati, replicati e distribuiti su diversi nodi della rete. Non essendoci data center da mantenere, il costo finale di questo prodotto è ridotto di circa il 67% rispetto alle soluzioni centralizzate.

Cloud computing

Le stesse considerazioni per il settore del cloud storage valgono anche per il cloud computing, con l'unica differenza

che al posto dello storage viene condivisa la potenza di calcolo della propria macchina.

Golem

Golem è un progetto che punta a creare un network computazionale distribuito (un supercomputer globale), offrendo una piattaforma peer-to-peer che ha la funzione di marketplace dove poter comprare e vendere potenza di calcolo. Golem punta al mercato di applicazioni che richiedono molta potenza di calcolo come il rendering grafico o il machine learning[78].

73. https://www.swift.com/our-solutions/global-financial-messaging/payments-cash-management/swift-gpi.
74. https://e-resident.gov.ee/start-a-company.
75. https://givingusa.org/giving-usa-2016.
76. https://basicattentiontoken.org.
77. https://chromaway.com.
78. https://golem.network.

Conclusione

Abbiamo cercato di racchiudervi tutti i concetti principali, ma questo libro non può essere una spiegazione esaustiva, poiché l'argomento è estremamente vario e complesso. Il libro deve essere quindi un punto di partenza.
Se siamo riusciti nel nostro intento e vi siete appassionati alla tecnologia blockchain, probabilmente vi chiederete: "E ora? Cosa posso fare con quello che ho appreso?". Queste sono senz'altro alcune delle possibilità.

Sarai in grado di valutare quali

criptovalute sono più affini alla tua visione di questo mondo.

Da Bitcoin a Ethereum, da Ripple a Dogecoin, da Stellar a IOTA, da 0x a Omisego, da Golem a Vechain. Il panorama delle criptovalute è immenso e variegato ed esistono numerosi progetti che vale la pena approfondire anche solo per curiosità. È senz'altro questo il modo migliore per rendersi conto di come il mondo stia prendendo una nuova eccitante direzione rispetto al passato.

Sarai in grado di investire autonomamente nelle diverse criptovalute.

Solitamente si inizia sempre da un exchange come Coinbase o Binance, ma potrai ora anche approfondire autonomamente se gestire i tuoi wallet, come farlo e a quali servizi affidarti. Potrai esplorare i fondamenti tecnici delle diverse criptovalute e decidere in maniera autonoma se investire o meno, senza la necessità di fare affidamento sulle opinioni di altre persone.

Sarai in grado di accettare criptovalute per la tua attività.
Tutto ciò di cui hai bisogno è infatti un wallet sul quale ricevere i pagamenti, ma il processo continua a diventare sempre più semplice grazie a servizi

come Coinbase Commerce.

Accettare criptovalute è uno dei modi migliori per esplorare questa tecnologia e allo stesso tempo risultare innovativi aprendosi a nuovi clienti che apprezzano questo genere di opportunità. La flessibilità della tecnologia e delle soluzioni a oggi disponibili rendono possibile utilizzarle in qualsiasi tipo di attività, dagli e-commerce (specialmente se internazionali) alle attività commerciali come bar o negozi.

Qualora si decidesse di accettare criptovalute come forma di pagamento, consigliamo comunque di approfondire il tema con uno specialista con esperienza nel settore per sapere come procedere dal punto di vista legale.

Sarai in grado di valutare le ICO in base alle tue preferenze, e decidere se prenderne parte.

Gran parte dei progetti basati su blockchain nasce tramite ICO. Se ti piace l'idea di investire in progetti innovativi, le ICO fanno per te.

Ricorda, non investire mai solo in base a come il progetto appare, ma guarda soprattutto in che modo intende risolvere i problemi delle soluzioni attuali utilizzando la tecnologia blockchain. Ora sei in grado di farlo.

Sarai in grado di capire come implementare al meglio la blockchain

nei progetti.

Riteniamo che il potenziale di questa tecnologia risieda in primo luogo nelle persone che decideranno di approfondirla, insieme al loro desiderio di voler sperimentare con essa in modo originale. Le innovazioni rese possibili dalla blockchain riguardano ogni settore, e quelle attualmente disponibili sono solo le prime applicazioni che puntano a cambiare il mondo come lo conosciamo oggi. Ricorda: la blockchain è specialmente utile quando usata per risolvere problemi non risolvibili con altre tecnologie. In genere, quindi, il problema dovrebbe richiedere una o più delle seguenti caratteristiche:

decentralizzazione, immutabilità, rimozione degli intermediari, instaurazione di un meccanismo di fiducia tra le parti, trasparenza delle informazioni.

Se invece la tua attività è una startup o se stai pensando di avviare un tuo progetto su blockchain, sarai in grado di ragionare meglio su come applicare la blockchain nel tuo caso specifico. Se il tuo progetto sfrutta le proprietà peculiari della blockchain per risolvere un grosso problema, sei sicuramente sulla buona strada. E sappi che facciamo il tifo per te!

La nostra intenzione è quella di promuovere lo scambio di idee e discussioni sul tema, creando un ambiente in cui appassionati ed esperti si riuniscono per discutere di come questa tecnologia si evolve e influenza la società di oggi.

Puntiamo a essere sempre più coinvolti in questo genere di iniziative e ci auguriamo che anche tu decida di prendere parte alle varie community per sfruttare al meglio quello che hai appreso in questo libro e contribuire alla sana informazione su questa tecnologia.

Se vuoi un consiglio, un parere su un tuo progetto, o anche solo farci sapere

cosa ti è piaciuto di questo libro (o cosa non ti è piaciuto), non esitare a scriverci.

Bibliografia/sitograf

[1] Wolfson R., *Maltese Parliament Passes Laws That Set Regulatory Framework For Blockchain, Cryptocurrency And DLT,* https://www.forbes.com/sites/rachel-wolfson/2018/07/05/maltese-parliament-passes-laws-that-set-regulatory-framework-for-blockchain-cryptocurrency-and-dlt/#7d9ebe8749ed.

[2] *Italy joins European partnership on blockchain supporting the delivery of cross-border digital public services,* https://ec.europa.eu/digital-single-

market/en/news/italy-joins-european-partnership-blockchain-supporting-delivery-cross-border-digital-public.

[3] Lee D., *Nokia: The rise and fall of a mobile giant*, https://www.bbc.com/news/technology-23947212.

[4] Petrini R., *La follia dei tulipani olandesi: così è nata la prima bolla speculativa della storia*, https://www.repubblica.it/economia/finala_tulipani-182608191.

[5] *Bolla delle Dot-Com*, https://it.wikipedia.org/wiki/Bolla_dellecom.

[6] *True scale of Bitcoin ransomware*

extortion revealed, https://www.technolo-gyreview.com/s/610803/true-scale-of-bitcoin-ransomware-extortion-revealed.

[7] Nakamoto S., *Bitcoin: A Peer-to-Peer Electronic Cash System,* https://bitcoin.org/bitcoin.pdf.

[8] Sedgwick K., *Verge Is Forced to Fork After Suffering a 51% Attack,* https://news.bitcoin.com/verge-is-forced-to-fork-after-suffering-a-51-attack.

[9] Antonopoulos A. M., *The Internet of Money,* Createspace Independent Pub, 2016.

[10] Siegel D., *Understanding The DAO*

Attack, https://www.coindesk.com/understanding-dao-hack-journalists.

[11] Mueller B., *What Caused the Accidental Killing of the Parity Multisig Wallet & How to Detect Similar Bugs,* https://hackernoon.com/what-caused-the-latest-100-million-ethereum-bug-and-a-detection-tool-for-similar-bugs-7b80f8ab7279.

[12] Redman J., *80% of the 21 Million Bitcoins Have Been Mined Into Existence,* https://news.bitcoin.com/80-of-the-21-million-bitcoins-have-been-mined-in-to-existence.

[13] Antonopoulos A. M., *Mastering*

Bitcoin, O'Reilly Media, 2014.

[14] Szabo N., *Smart Contracts,* http://www.fon.hum.uva.nl/rob/Courses/I

[15] Shieber J., *SEC says Ether isn't a security, but tokens based on Ether can be,* https://techcrunch.com/2018/06/14/sec-says-ether-isnt-a-security-but-tokens-based-on-ether-can-be.

[16] Williams-Grut O., *The 11 biggest ICO fundraises of 2017,* https://www.busi-nessinsider.com/the-10-biggest-ico-fundraises-of-2017-2017-12?IR=T.

[17] Suberg W., *ICO da record per EOS, 4 mld di dollari raccolti in un*

anno, https://it.cointelegraph.com/news/eos-about-to-secure-a-record-4-bln-in-year-long-ico.

[18] Kasanmascheff M., *Quest'anno il volume delle ICO è già raddoppiato rispetto all'intero 2017, rivela un recente studio,* https://it.cointelegraph.com/news/pwc-report-finds-that-2018-ico-volume-is-already-double-that-of-previous-year.

[19] Kharif O., *Half of ICOs Die Within Four Months After Token Sales Finalized,* https://www.bloomberg.com/news/articl 07-09/half-of-icos-die-within-four-months-after-token-sales-finalized.

[20] Alexandre A., Dal 2017 ad oggi le ICO hanno raccolto 20 miliardi di dollari: lo rivela uno studio di Autonomous Research, https://it.cointelegraph.com/news/researc 20-billion-raised-through-icos-since-2017.

[21] Liao S., *The SEC created its own scammy ICO to teach investors a lesson,* https://www.theverge.com/tldr/2018/5/1 cryptocurrency-ico-investors.

[22] Acheson N., *China's ICO Ban: Understandable, Reasonable and (Probably) Temporary,* https://www.coindesk.com/chinas-ico-ban-understandable-reason-able-

probably-temporary.

[23] Nakamura Y., *World's Biggest Cryptocurrency Exchange Is Heading to Malta*, https://www.bloomberg.com/news/articl 03-23/the-world-s-big-gest-cryptocurrency-exchange-is-moving-to-malta.

[24] Cramer M., *Ethereum Casper Update Expected in 2019, Sharding in 2020*, https://unhashed.com/cryptocurrency-news/ethereum-sharding-update-ex-pected-2020.

[25] Partz H., *Vitalik Buterin si scaglia contro gli exchange centralizzati:*

'Spero brucino all'inferno', https://it.cointelegraph.com/news/ethereus-vitalik-bute-rin-blasts-centralized-crypto-exchanges-i-hope-they-burn-in-hell.

[26] Morris D. Z., *BitGrail Cryptocurrency Exchange Claims $195 Million Lost to Hackers*, http://fortune.com/2018/02/11/bitgrail-cryptocurrency-claims-hack.

[27] Vitalik B., *On Public and Private Blockchains*, https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains.

[28] Narayanan A., *"Private blockchain" is just a confusing name*

for a shared database, https://freedom-to-tinker.com/2015/09/18/private-blockchain-is-just-a-confusing-name-for-a-shared-database.

[29] Greenspan G., *Blockchains vs centralized databases,* https://www.multi-chain.com/blog/2016/03/blockchains-vs-centralized-databases.

[30] *Linux Foundation's Hyperledger Project Announces 30 Founding Members and Code Proposals To Advance Blockchain Technology,* https://www.linuxfoun-dation.org/press-release/2016/02/linux-foundations-hyperledger-project-an-nounces-30-founding-members-and-code-proposals-

to-advance-blockchain-technology.

[31] Allison I., *Two of Blockchain's Biggest Consortiums Just Joined Forces,* https://www.coindesk.com/ethereum-enterprise-alliance-hyperledger-block-chain-consortiums-join-forces.

[32] Suberg W., *Italian Stock Exchange to Develop Hyperledger-Based Blockchain Shares Platform,* https://cointelegraph.com/news/italian-stock-exchange-to-de-velop-hyperledger-based-blockchain-shares-platform.

[33] Rilee K., *Understanding Hyperledger Sawtooth - Proof of*

Elapsed Time, https://medium.com/kokster/understandin hyperledger-sawtooth-proof-of-elapsed-time-e0c303577ec1.

[34] Middleton D., *Announcing Hyperledger Sawtooth 1.0!*, https://www.hy-perledger.org/blog/2018/01/30/announci hyperledger-sawtooth-1-0.

[35] Khatri Y., *Gates Foundation Partners With Former Ripple CTO's Blockchain Project*, https://www.coindesk.com/gates-foundation-partners-with-former-ripple-ctos-blockchain-project.

[36] Schwartz E., *Interledger: How to*

Interconnect All Blockchains and Value Networks, https://medium.com/xpring/interledger-how-to-interconnect-all-blockchains-and-value-networks-74f432e64543.

[37] Ito J., Narula N., Ali R., *The Blockchain Will Do to the Financial System What the Internet Did to Media,* https://hbr.org/2017/03/the-blockchain-will-do-to-banks-and-law-firms-what-the-did-to-media.

[38] Bugrov D., Miklos D., Poppensieker T., *A Brave New World for Global Banking,* https://www.mckinsey.com/industries/fir services/our-insights/a-brave-new-world-for-global-banking.

[39] *Fintech 2.0: rebooting financial services,* https://www.nasdaq.com/article/fintech-20-rebooting-financial-services-cm715877.

[40] *Banking on Blockchain,* https://www.accenture.com/us-en/insight-bank-ing-on-blockchain.

[41] Marquer S., *The World's Biggest Banks Lead the Blockchain Charge,* https://ripple.com/insights/the-worlds-biggest-banks-lead-the-blockchain-charge.

[42] Thomson Reuters, *Thomson Reuters 2016 Know Your Customer Surveys Reveal Escalating Costs and*

Complexity, https://www.thomsonreuters.com/en/pres releases/2016/may/thomson-reuters-2016-know-your-customer-surveys.html.

[43] *Nasdaq Blockchain Strategy - Moving Beyond the POC,* https://business.nasdaq.com/media/Block 61791.pdf.

[44] Bajpai P., *How Stock Exchanges Are Experimenting With Blockchain Technology,* https://www.nasdaq.com/article/how-stock-exchanges-are-experiment-ing-with-blockchain-technology-cm801802.

[45] Wilson T., *Chickens and eggs: Retailer Carrefour adopts blockchain*

to track fresh produce, https://www.reuters.com/article/us-carrefour-blockchain-ibm/chickens-and-eggs-retailer-carrefour-adopts-blockchain-to-track-fresh-pro-duce-idUSKCN1MI162.

[46] Aitken R., *IBM & Walmart Launching Blockchain Food Safety Alliance In China With Fortune 500's JD.com,* https://www.forbes.com/sites/rogeraitken/walmart-launching-blockchain-food-safety-alliance-in-china-with-fortune-500s-jd-com/#e5d34bf7d9c5.

[47] Zhao W., *Alibaba's T-Mall Is Moving Cross-Border E-Commerce to Block-chain,*

https://www.coindesk.com/alibabas-t-mall-moving-cross-border-e-com-merce-blockchai.

[48] *Vino 4.0: tracciato e verificato dalla vite alla bottiglia con la blockchain,* https://www.dnvgl.it/news/vino-4-0-tracciato-e-verificato-dalla-vite-alla-botti-glia-con-la-blockchain--116366.

[49] Maersk e Ibm: nasce la joint venture sulla blockchain per il commercio globale e le filiere digitali, http://www-03.ibm.com/press/it/it/pressrelease/5361

[50] Shabalala Z., *De Beers tracks diamonds through supply chain using*

block-chain, https://www.reuters.com/article/us-anglo-debeers-blockchain/de-beers-tracks-diamonds-through-supply-chain-using-blockchain-idUSKBN1IB1CY.

[51] Milano A., *VeChain Arrives: What to Know About the $1.5 Billion Block-chain for Business,* https://www.coindesk.com/vechain-arrives-know-1-5-bil-lion-blockchain-business.

[52] *A complete list of VeChain partnerships,* https://vechaininsider.com/partnerships/a complete-list-of-vechain-partnerships.

[53] Newman P., There will be more

than 55 billion IoT devices by 2025 — these are the biggest drivers for adoption, https://www.businessinsider.com/interne of-things-report?IR=T.

[54] Ponciano J., *IOTA Foundation Launches Data Marketplace For 'Internet-Of-Things' Industry,* https://www.forbes.com/sites/jonathanpo foundation-launches-data-marketplace-for-internet-of-things-research/#5aed75bbf52b.

[55] *Vehicle-to-vehicle cooperation to marshal traffic,* https://patents.google.com/patent/US992

[56] *Blockchain - an opportunity for*

energy producers and consumers?, http://www.pwc.com/gx/en/industries/as blockchain-opportunity-for-energy-producers-and-consumers.pdf.

[57] Principles on identification for sustainable development: toward the digital age, http://documents.worldbank.org/curated/ REVISED-English-ID4D-IdentificationPrinciples-Folder-web-English-ID4D-IdentificationPrinciples.pdf.

[58] Higgins S., *Nasdaq Declares Blockchain Voting Trial a 'Success'*, https://www.coindesk.com/nasdaq-declares-blockchain-voting-trial-a-success.

[59] Grech A., Camilleri A. F., *Blockchain in Education*, http://publications.jrc.ec.europa.eu/repos

[60] Sundararajan S., *100 Diplomas: MIT Issues Graduate Certificates on a Block-chain App*, https://www.coindesk.com/100-diplomas-mit-issues-graduate-certificates-on-a-blockchain-app.

[61] Berry J., *The 2015 Loyalty Census - Big numbers, big hurdles*, https://www.petrosoftinc.com/wp-content/uploads/2018/03/2015-loyalty-census.pdf.

[62] Perry S., *1 in 3 Americans Lacks Faith in Charities, Chronicle Poll*

Finds, https://www.philanthropy.com/article/1-in-3-Americans-Lacks-Faith/233613.

[63] *The Global Findex database 2017,* http://documents.worldbank.org/curated/en/332881525873182837/The-Global-Findex-Database-2017-Measuring-Fi-nancial-Inclusion-and-the-Fintech-Revolution.

[64] Del Castillo M., *United Nations Sends Aid to 10,000 Syrian Refugees Using Ethereum Blockchain,* https://www.coindesk.com/united-nations-sends-aid-to-10000-syrian-refugees-using-ethereum-blockchain.

[65] *Blockchain for Video Advertising:*

A Market Snapshot of Publisher and Buyer Use Cases, https://www.iab.com/guidelines/blockch video-advertis-ing-market-snapshot-publisher-buyer-use-cases.

[66] *IAB Internet advertising revenue report*, https://www.iab.com/wp-content/uploads/2017/12/IAB-Internet-Ad-Revenue-Report-Half-Year-2017-REPORT.pdf.

[67] *Cloud Infrastructure Services Market: Global Forecast until 2023*, https://www.reportlinker.com/p0558665 Infrastructure-Services-Market-by-Service-Type-Deployment-Model-Organization-Size-Vertical-And-Region-Global-Forecast-to.html.

Glossario

Altcoin

Abbreviazione per “alternative coin”, termine con il quale spesso ci si riferisce alle criptovalute diverse dal bitcoin.

Architettura (di rete)

Identifica l’architettura di una rete. Solitamente si fa distinzione tra architettura client/server e architettura peer-to-peer (vedi **Peer-to-peer**).

ASIC

Acronimo di Application Specific

Integrated Circuit, una macchina progettata esclusivamente per il mining (vedi **Mining**).

Bitcoin

Il Bitcoin (con l'iniziale maiuscola) è un network peer-to-peer per lo scambio di denaro digitale, creato nel 2009. La criptovaluta utilizzata in questo network si chiama bitcoin (con iniziale minuscola, il simbolo è BTC): è la prima criptovaluta a essere stata creata e, a oggi, anche la più conosciuta.

Blocco

I blocchi sono i mattoni che formano una blockchain. Vengono aggiunti sequenzialmente uno alla volta, creando

una struttura dati “a catena” (blockchain).

Blocco genesi

Il nome che solitamente viene conferito al primo blocco di una blockchain.

Blockchain

La blockchain è un ledger digitale, decentralizzato e distribuito, strutturato come una catena di blocchi responsabili dell’archiviazione di dati. La blockchain è un’infrastruttura digitale che garantisce ai dati in essa contenuti specifiche caratteristiche come decentralizzazione, sicurezza e immutabilità.

Bounty

Spesso utilizzati nelle ICO, sono

meccanismi di ricompensa per gli utenti che partecipano allo sviluppo dei progetti delle ICO. La ricompensa consiste in token e viene solitamente data in cambio di una pubblicizzazione del progetto o dell'identificazione di bug nel codice sorgente.

Chain split (divisione di catena)

Divergenza nello stato di una blockchain che risulterà in una divisione temporanea o permanente in due blockchain separate. Avviene quando nodi diversi hanno una diversa cronologia delle transazioni. Un chain split temporaneo avviene in seguito a una fork regolare (vedi **Fork regolare**), mentre un chain split permanente può

avvenire in seguito a una hard fork (vedi **Hard fork**) se non c'è il consenso di tutti i nodi.

Chiave

Un'informazione, solitamente rappresentata da un numero estremamente grande, che viene utilizzato per determinare il risultato di un algoritmo crittografico.

Chiave privata

Una chiave crittografica utilizzata per la generazione di una chiave pubblica negli algoritmi di crittografia a chiave pubblica (public-key cryptography). Un messaggio criptato con una chiave pubblica può essere decifrato solamente

con la rispettiva chiave privata. La chiave privata non deve mai essere condivisa.

Chiave pubblica

Chiave crittografica derivata matematicamente dalla chiave privata e utilizzata nella crittografia a chiave pubblica (public-key cryptography). Può essere condivisa con chiunque.

Cold storage

Nell'ambito blockchain, fa riferimento al salvataggio delle chiavi private su un dispositivo non connesso a Internet.

Consenso

Il consenso è un accordo generale tra i membri di un dato gruppo (in questo

caso i nodi della blockchain), ognuno dei quali ha una parte del potere decisionale.
In una blockchain il consenso è un accordo su ciò che è accaduto e detiene l'unica possibile verità sullo stato attuale della blockchain. Gli algoritmi più utilizzati nel processo per raggiungere il consenso sono il Proof of Work (PoW) e il Proof of Stake (PoS).

Criptazione

Processo di codifica di un messaggio in maniera tale da permettere l'accesso al messaggio originale solo a persone autorizzate.

Cripto-economia

Sistema basato sull'unione di crittografia e incentivi economici per garantire la sicurezza di un sistema.

Criptovalute

Un asset digitale sviluppato su una tecnologia blockchain.

Crittografia

Lo studio delle tecniche di comunicazione sicura in un ambiente ostile (per esempio Internet). Lo scopo della crittografia è quello di costruire dei protocolli che impediscano a terze parti non autorizzate la lettura o la manomissione di informazioni.

Crittografia a chiave pubblica

Un tipo di crittografia largamente

utilizzato su Internet per criptare un messaggio o creare una firma digitale. Utilizza una coppia di chiavi in relazione matematica tra loro (vedi **Chiave pubblica** e **Chiave privata**).

DLT

Acronimo di Distributed Ledger Technology. Identifica tutti i sistemi che utilizzano una tecnologia basata su un ledger distribuito. La blockchain è una DLT dove il ledger assume una forma di catena. Altre DLT, come per esempio il tangle di IOTA (vedi **Tangle**), strutturano il ledger in maniera diversa.

Double spending

Una situazione nella quale esiste più di

una copia digitale di qualcosa che dovrebbe essere unico (soldi, identità, voti ecc.). Il problema del double spending viene risolto dalla blockchain senza dover ricorrere a un'autorità centrale.

Ethereum

Ethereum è una piattaforma decentralizzata pensata per eseguire smart contract. La criptovaluta di Ethereum si chiama Ether, il cui simbolo è ETH.

Fiat currency

In italiano "moneta legale". È una valuta che acquisisce valore poiché riconosciuta da un governo. È la

tipologia di valute correntemente utilizzate, come l'euro, il dollaro, la sterlina ecc.

Firma digitale

La firma digitale è un sistema crittografico utilizzato per dimostrare l'autenticità di un messaggio o di un documento digitale.

FOMO

Acronimo di "Fear of missing out", la paura di perdere un'occasione.

Fork

Una modifica delle regole di consenso di una blockchain. Oltre alla fork regolare (vedi **Fork regolare**), si distingue principalmente tra soft e hard

fork (vedi **Soft fork** e **Hard fork**).

Fork regolare

Si intende una divergenza temporanea di una blockchain. Si verifica quando due o più miner creano un blocco nello stesso momento, causando una situazione temporanea di incertezza su quale sia il blocco da considerare valido. Solitamente la fork regolare si risolve automaticamente alla generazione del blocco successivo.

FUD

Acronimo di "Fear, uncertainty and doubt". In italiano: paura, incertezza e dubbio.

Hard fork

Una modifica delle regole di consenso non retrocompatibile con il sistema esistente.

Hardware wallet

Dispositivo fisico appositamente costruito per custodire le chiavi private in modo sicuro.

Hash

Una funzione che viene usata per mappare dati di lunghezza arbitraria a dati di lunghezza definita.

Hashrate

Numero di hash calcolati al secondo.

Hot storage

Fa riferimento a un wallet collegato in

qualche modo a Internet. Le chiavi private sono state create o memorizzate su una macchina connessa a Internet.

Indirizzo

In una blockchain l'indirizzo può essere considerato l'analogo del codice IBAN in un conto corrente.

Ledger

Un registro dove vengono salvate tutte le transazioni.

Miner

Tutti coloro che partecipano al processo di mining.

Mining

Processo tramite il quale vengono creati

e aggiunti nuovi blocchi a una blockchain.

Mobile wallet

Un wallet software nella forma di applicazione per smartphone.

Network (rete)

Insieme di due o più sistemi informatici interconnessi tra loro.

Nodo

Un partecipante al network. In una blockchain esistono due tipi di nodi: fullnode e light-node.

Un full-node salva localmente l'intera blockchain e può interagire direttamente con essa.

Un light-node, al contrario, ha

bisogno di comunicare con un full-node per eseguire operazioni sulla blockchain.

Nonce

Un valore che serve per variare l'input della funzione di hash utilizzata nel calcolo della PoW (vedi **Hash** e **Proof of Work**).

Paper wallet

Si intende la coppia di chiavi crittografiche (pubblica e privata) stampate su un foglio di carta. È la forma più semplice possibile di cold storage.

Peer-to-peer (P2P)

Un modello di architettura logica di rete

informatica in cui i nodi sono equivalenti o “paritari” (peer), potendo fungere al contempo da client e server verso gli altri nodi terminali (host) della rete.

Proof of Stake (PoS)

Protocollo utilizzato per raggiungere il consenso distribuito dove il potere di voto di ogni partecipante è proporzionale al suo stake.

Proof of Work (PoW)

Protocollo utilizzato per raggiungere il consenso distribuito dove il potere di voto di ogni partecipante è proporzionale al suo **Hashrate** (vedi).

Ransomware

Una virus che rende inutilizzabile un computer (per esempio criptando il contenuto dell'hard disk) e chiede un riscatto (spesso sotto forma di criptovalute) per ridare l'accesso all'utente.

Rete centralizzata

Una rete dove è presente una forma di centralizzazione. Si può parlare di rete centralizzata da un punto di vista dell'architettura, della logica o dell'autorità.

Rete decentralizzata

Una rete dove tutte le risorse sono allocate sui nodi della rete che comunicano tra loro in maniera peer-to-

peer (vedi **Peer-to-peer**).

Ricompensa

Meccanismo di incentivazione usato nel sistema di rewarding di miner e validator (vedi alle voci **Miner** e **Validator**). Tipicamente la ricompensa è data in criptovalute di una specifica blockchain (per esempio BTC sulla blockchain del Bitcoin).

Satoshi

Il nome dell'unità minima in cui può essere suddiviso 1 bitcoin, pari a 10^-8 BTC.

Satoshi Nakamoto

Alias del creatore del Bitcoin, la cui vera identità rimane sconosciuta.

SegWit

Abbreviazione di Segregated Witness. È un esempio particolare di **Soft fork** (vedi) proposta dal team del Bitcoin.

Smart contract

Uno smart contract è un programma in grado di avere tutte le caratteristiche di un contratto del mondo reale, ma che viene salvato ed eseguito all'interno di una blockchain. L'accordo non è vincolato dalla legge ma dal contratto stesso attraverso il consenso del network.

Soft fork

Si intende una modifica retrocompatibile alle regole di consenso di una

blockchain.

Software wallet

Applicazione che gestisce le chiavi di uno o più indirizzi e facilita l'interazione con la blockchain. Può essere installata su un computer o uno smartphone.

Stato (di una blockchain)

Lo stato di una blockchain è il risultato delle azioni avvenute su quella blockchain fino a al momento considerato. Può essere rappresentato da un singolo hash.

Transazione

In generale, una transazione (valida) è tutto ciò che scrive sulla blockchain.

Validator

Equivalente dei miner nella Proof of Stake.

Wallet

Letteralmente “portafoglio”, è un sistema che ha lo scopo di gestire uno o più indirizzi. A seconda dell’ambiente in cui operano, i wallet si distinguono tra hot e cold storage. I wallet inoltre vengono distinti tra hardware wallet, software wallet e paper wallet.

Ringraziamenti

Non saremmo mai stati in grado di scrivere questo libro senza l'aiuto e il supporto di molte persone e amici. Vogliamo ringraziare in modo particolare **Riccardo Secco** per aver messo a disposizione la sua esperienza nel campo delle tecnologie innovative, oltre che per aver contribuito alla scrittura dei Capitoli 11 e 12; **Mattia Marcon e Andrea Fantin** per il loro contributo nella fase di revisione e le indicazioni sulla parte legislativa; **Massimo DeMarchi e Federico Badini** per la revisione dei contenuti tecnici;

Andrea Sparacino, Maurizio Vedovati e tutto il team di Hoepli per aver creduto nelle nostre capacità e averci permesso di pubblicare questo libro; **Annalisa Costa** per il suo contributo nella fase di stesura del libro.

Gli autori

Gianluca Chiap. Full-stack developer e CTO di abitcompany, ingegnere informatico laureato al Politecnico di Milano. Dal 2016 si interessa alla tecnologia blockchain, in particolare in ambito smart contract. @forgiangi

Jacopo Ranalli. Startup entrepreneur specializzato in lean management. Ingegnere dei Materiali e delle Nanotecnologie laureato presso il

Politecnico di Milano e con esperienza di ricerca presso l'Imperial College di Londra.

Membro della commissione "Startup e settori innovativi" dell'Ordine degli Ingegneri della Provincia di Milano, partecipa spesso come relatore a eventi sulla blockchain ed è coinvolto in numerosi progetti e iniziative volti allo sviluppo e incubazione di startup.

Nel 2016 rimane affascinato dal potenziale rivoluzionario della tecnologia blockchain, specialmente nel mondo delle startup e in quello industriale. @jjranalli

Raffaele Bianchi. Consulente strategico a Milano con esperienza nel settore dei financial services. Ingegnere dei Materiali laureato al Politecnico di

Milano e CEO di abitcompany.

Entra in contatto con il mondo della blockchain a partire dal 2016 e si interessa particolarmente delle applicazioni blockchain in ambito Insurance e IoT.

Abitcompany offre servizi di consulenza tecnico-strategica in ambito Blockchain e DLT.

Informazioni sul Libro

L'AVVENTO DELLA BLOCKCHAIN É ORMAI INESORABILE. QUESTA RIVOLUZIONARIA TECNOLOGIA SI STA DIFFONDENDO IN TUTTI I SETTORI APRENDO LE PORTE A SOLUZIONI PRIMA IRREALIZZABILI.

La blockchain segna un cambio netto nel modo in cui le applicazioni digitali vengono pensate e costruite,

permettendo di modificare radicalmente la società e i business di oggi.

Blockchain: Tecnologia e applicazioni per il business offre un percorso a 360 gradi su

La tecnologia blockchain

Il suo potenziale

Le sue applicazioni

Il panorama in Italia e nel mondo

Una guida che vi permette di acquisire una reale comprensione di questa innovativa tecnologia, mettendo in luce benefici e rischi di un mondo

decentralizzato che, inevitabilmente, sembra destinato ad essere sempre più reale.