# COME GESTIRE I BITCOIN PER PRINCIPIANTI

BITCOIN E CRIPTOVALUTE: INVESTIRE E COMMERCIALIZZARE

ALAN T. NORMAN

Alan T.  Norman

# Come Gestire I Bitcoin – Per Principianti

«Tektime S.r.l.s.»

**Norman A.**

Come Gestire I Bitcoin – Per Principianti / A. Norman — «Tektime S.r.l.s.»,

ISBN 978-8-83-540134-6

Bitcoin non è solo una nuova parola nell'era di Internet o un progresso tecnologico e finanziario, è l'inizio di una nuova era sulla Terra! Solo 10 anni fa non potevamo nemmeno immaginare di sognare il denaro digitale: non puoi toccarli fisicamente ma puoi possederli e spenderli. Oggi questa è una realtà! La rivoluzione dei Bitcoin ha coperto il mondo intero come un'enorme ondata, sempre più persone interessate a questo ”oro digitale”. Bitcoin non è solo una nuova parola nell'era di Internet o un progresso tecnologico e finanziario, è l'inizio di una nuova era sulla Terra! Solo 10 anni fa non potevamo nemmeno immaginare di sognare il denaro digitale: non puoi toccarli fisicamente ma puoi possederli e spenderli. Oggi questa è una realtà! La rivoluzione dei Bitcoin ha coperto il mondo intero come un'enorme ondata, sempre più persone interessate a questo ”oro digitale”.Negli ultimi anni, i Bitcoin sono nati come valuta rivoluzionaria da pochi nerd tecnologici selezionati ed hanno rapidamente cambiato il modo in cui pensiamo al concetto di moneta. Non c'è dubbio che ora vedi i pagamenti con i Bitcoin accettati in tutti i luoghi, ma, se puoi crederci, un tempo era una procedura abbastanza complicata ed era difficile trovare luoghi che ti permettessero di pagare in Bitcoin. Ad ogni modo, per gestire quel mondo devi sapere tutto. Non possiamo garantire che saprai TUTTO da questo libro, ma possiamo garantire che capirai cosa sono i Bitcoin. Che cos'è? Da dove proviene? Come lo usi? È davvero solo denaro falso su Internet creato dagli spacciatori? Questo è esattamente ciò a cui risponderemo in questo libro. Ti forniremo tutte le informazioni che devi sapere per iniziare con i Bitcoin: comprendere le transazioni Blockchain e i Bitcoin, dove conservare i tuoi Bitcoin (come scegliere un portafoglio sicuro), acquistare i Bitcoin, investire nei Bitcoin, come iniziare ad accettare e utilizzare i Bitcoin nella tua azienda, come essere sicuri con i Bitcoin, ecc. Inoltre, l'autore condividerà con te fatti interessanti su i Bitcoin e ti fornirà consigli professionali per inserirti nella famiglia dei Bitcoin! Pronto

ancora ad affrontare il mondo dei Bitcoin? Lo spero. Vorrei essere il primo ad accoglierti ufficialmente nel mondo dei Bitcoin!

ISBN 978-8-83-540134-6

# Содержание

# Alan T. Norman
# Come Gestire i Bitcoin – Per Principianti

**Come gestire i *Bitcoin***

**-**

**per PRINCIPIANTI**

**Bitcoin e criptovalute: investire e commercializzare**

**Alan T. Norman**

**Traduttore: Monja Areniello**

**Ottieni gratis il libro omaggio *Bitcoin* Whales:**
**I ragazzi che hanno ingannato il mondo**

**(Dettagli alla fine del libro)**

# Capitolo 1. Cosa sono i *Bitcoin*?

Se hai comprato questo libro, è probabile che tu abbia sentito parlare dei *Bitcoin*:

- forse ne hai sentito parlare nei circoli finanziari, poiché il valore dei *Bitcoin* è aumentato rapidamente;
- forse ne hai sentito parlare in un contesto tecnologico, poiché i *Bitcoin* sono basati su una nuova tecnologia chiamata *Blockchain*;
- oppure, come molti, potresti aver sentito parlare dei *Bitcoin* sulla stampa specializzata per la quantità di nuovi utenti, celebrità famose e uomini d'affari di successo che hanno iniziato a utilizzare i *Bitcoin* l'anno scorso.

Negli ultimi anni, i *Bitcoin* sono nati come valuta rivoluzionaria da pochi nerd tecnologici selezionati ed hanno rapidamente cambiato il modo in cui pensiamo al concetto di moneta.

Ecco la sinossi di base: i *Bitcoin* sono una valuta digitale. In molti modi, funzionano come dollari, euro o yen, permettendoci di trasferire valore. Ma il punto di forza dei *Bitcoin* è la sua rete. La tecnologia *Blockchain* consente di decentralizzare i *Bitcoin*, il che significa che chiunque può accedere e commercializzare sul libro mastro pubblico dei *Bitcoin*. Utilizzando i *Bitcoin*, puoi inviare fondi a chiunque nel mondo, senza la necessità di grandi istituzioni come banche, convertitori di valuta e processori di pagamento.

Tutto succede sulla rete pubblica dei *Bitcoin*.

Oltre ai pagamenti da persona a persona, i pagamenti con i *Bitcoin* sono ora accettati in tutti i tipi di attività. Solo pochi anni fa, trovare luoghi che ti permettessero di pagare con i *Bitcoin* era una sfida. Ad essere sincero, all'inizio, avremmo potuto riempire una sola pagina con i luoghi che accettavano i *Bitcoin*. Ora, l'accettazione dei *Bitcoin* è salita alle stelle.

Un altro uso dei *Bitcoin* è emerso negli ultimi anni: negli investimenti. Mentre sempre più persone hanno iniziato a utilizzare i *Bitcoin*, il loro prezzo è aumentato in modo drammatico. Come vedremo più avanti in questo libro, molte persone acquistano i *Bitcoin* come risorsa che poi sperano aumenti di valore nel tempo.

Naturalmente, i *Bitcoin* hanno ancora problemi e nuove sfide da affrontare nel futuro. Daremo un'occhiata ad alcune di queste sfide nelle seguenti pagine.

In questo libro, tratteremo tutto ciò che devi sapere per iniziare ad usare i *Bitcoin*, quindi cominciamo da dove vengono.

Pronto a tuffarti? Andiamo!

# L’inizio

Ritorniamo a qualche anno indietro. Nel 2008 la crisi finanziaria era in pieno svolgimento e le persone di tutto il mondo avvertivano gli effetti del disastro economico americano. Questa è stata una di quelle volte nella storia in cui le valute nazionali hanno mostrato la loro debolezza. La crisi finanziaria americana ha svalutato il dollaro e le sfide economiche negli Stati Uniti hanno colpito tutto il mondo.

Si pensava si sarebbe arrivati ad un completo collasso economico. Dov'erano tutte quelle persone che avrebbero dovuto assicurarsi che nulla di simile dovesse mai succedere? Hanno fatto un casino alla grande. Questo è per dirla alla leggera, per non dire altro.

## Risposte centralizzate

Le persone più importanti nel settore economico hanno deciso di dare una risposta che solo una banca centralizzata poteva offrire. Per combattere il rapido crollo dei mercati finanziari, i governi di tutto il mondo hanno deciso su quello che viene chiamato "allentamento quantitativo", in cui hanno stampato più denaro e lo hanno pompato nelle loro economie in modo che i loro cittadini avrebbero avuto i fondi necessari per evitare un'altra Grande Depressione.

Questo tipo di rapidi cambiamenti porta a "guerre valutarie" e presto i governi avrebbero lottato per essere quelli con i prezzi competitivi più bassi. Quando poi le banche hanno avuto problemi a causa del basso valore della valuta e hanno ridotto i tassi di interesse, i governi sono stati costretti a salvarle con il denaro dei contribuenti. Come puoi immaginare, questo ha ulteriormente svalutato ulteriormente l'offerta di moneta esistente.

Mentre questa è una visione molto semplificata di un momento complesso della storia economica, la lezione rimane. Le banche centrali che manipolavano l'offerta di moneta hanno svalutato le valute di tutto il mondo.

Alla fine, con i tassi di interesse bassi e i salvataggi dei contribuenti, le stesse banche, che sono state responsabili dei problemi finanziari, sono state quelle che hanno beneficiato della congiuntura prossima al collasso. Fu durante questo periodo che un uomo noto come Satoshi Nakamoto venne ispirato.

## Chi è Satoshi?

Prima di spiegare esattamente come sono nati i *Bitcoin*, vale la pena sapere chi è Satoshi Nakamoto. La sua storia è la storia dei *Bitcoin*.

La vera identità di Satoshi rimane ancora sconosciuta ad oggi. Secondo le sue stesse dichiarazioni del 2012, era un uomo di 37 anni che viveva da qualche parte in Giappone, anche se ci sono molti dubbi al riguardo. Scrive in un inglese fluente e il software *Bitcoin* non è documentato in giapponese, portando molti a pensare di non essere, in effetti, giapponese, anche se potrebbe aver vissuto lì in un dato momento.

Secondo un’indagine investigativa, un programmatore svizzero ha stabilito che Satoshi potrebbe vivere in Nord America, dato l’orario del giorno in cui pubblica sui forum *Bitcoin*. Il programmatore lo ha fatto analizzando i tempi di pubblicazione più comuni e scoprendo che si allineavano con il programma di sonno medio di qualcuno che viveva nel continente.

Sapremo mai chi è il creatore dei *Bitcoin*? È davvero una squadra di persone? Forse non lo sapremo mai, ma una cosa è certa: questa persona controlla circa un milione di *Bitcoin*. A giugno

2017, ciò equivale a quasi $3 miliardi di dollari! Con una fortuna del genere, lui potrebbe comprarsi il diritto alla privacy.

## La creazione

Quindi, questo programmatore anonimo ha esaminato lo stato del mondo finanziario e ha riscontrato molti problemi. I metodi tradizionali per risolvere quella crisi erano stati testati e, sebbene funzionassero, in quel momento vide che si faceva poco per prevenire futuri disastri. Cosa si poteva fare al riguardo? Qualsiasi tipo di soluzione centralizzata avrebbe risolto mai problemi come questo per sempre?

Decise che era necessaria una forza dirompente. Qualcosa che avrebbe potuto potenzialmente cambiare il modo in cui pensiamo alla valuta. La risposta è stata una forma di valuta completamente decentralizzata e aperta a tutti. Nessuna banca centrale che la controlla, nessuna catena di trasferimenti con un unico sorvegliante. Nessun gruppo d'élite di persone che prende decisioni che potrebbero influenzare ogni singola persona usando le proprie valute.

## Decentramento

> Decentramento: lo spostamento di dipartimenti di una grande organizzazione da un unico centro amministrativo verso altre posizioni.

Il decentramento era la principale forza trainante del lavoro di Satoshi. In sostanza, decentramento significa che tutti fanno parte dell'economia dei *Bitcoin* e tutti noi stiamo contribuendo in qualche modo. NOI siamo la forza trainante, piuttosto che una banca centrale che controlla quanto vale la nostra valuta e quanto ne abbiamo a disposizione nella nostra economia. Ancora meglio, allo stesso tempo, nessuno di noi ne ha il controllo.

Non esiste governo, banca o intermediario che possa dirci come usare i *Bitcoin*, dal momento che appartengono letteralmente a tutti coloro che lo usano. Detto questo, più persone li usano, meglio funzionano e più diventa fattibile. Ecco come funziona la tecnologia *peer-to-peer*. È gestita direttamente dagli utenti.

Nel vero senso della parola, è un libero mercato. Nel corso degli anni abbiamo sentito molto parlare dei mercati liberi, ma nessun mercato può essere veramente libero quando c'è una forza trainante che lo guida.

## Come ha fatto Satoshi?

Satoshi non è stato il primo a lavorare sul problema della valuta digitale decentralizzata. Crittografi e programmatori avevano lavorato al problema per anni prima del 2008.

La sfida del decentramento è mantenere un registro delle transazioni. Normalmente, quando paghi qualcuno, la banca sottrae i soldi dal tuo conto e li aggiunge al conto del destinatario. Detenere il registro delle transazioni è la funzione principale di una banca.

In un sistema decentralizzato non esiste una banca. Chiunque può inviare una richiesta di transazione alla rete decentralizzata. Ciò rende il libro mastro decentralizzato molto vulnerabile agli attacchi. Gli utenti malintenzionati potrebbero cambiare il libro mastro o spendere una moneta digitale più volte prima che la rete lo noti.

L'innovazione di Satoshi è stata la tecnologia che ora chiamiamo *Blockchain*. Lui ha trovato un modo per proteggere il libro mastro usando la datazione, molta potenza di elaborazione decentralizzata e la crittografia. I *Bitcoin* – la primissima *Blockchain* – utilizzano ancora oggi l'architettura di Satoshi per proteggere i pagamenti.

# E’ una valuta allora?

Una delle principali domande che le persone fanno sui *Bitcoin* è "È una valuta"?

La risposta si trova in una zona grigia. I *Bitcoin* sono un mezzo di pagamento e un modo per trasferire fondi. Puoi usare i *Bitcoin* per effettuare acquisti o inviare pagamenti. È possibile convertire i *Bitcoin* in dollari, euro, sterline, yen o qualsiasi altra valuta, ma non sono supportati da alcuna istituzione. Non esiste un governo centrale a cui puoi chiedere e non ci sono garanzie quando si possiedono i *Bitcoin*. Hanno valore solo nei luoghi e tra le persone che li accettano.

*I Bitcoin* sono ciò che ora chiamiamo valuta digitale nella sua forma più pura, o meglio nota come criptovaluta. I *Bitcoin* sono stati la prima criptovaluta, ma ora ce ne sono molte. Le criptovalute funzionano diversamente dalle valute tradizionali, poiché sono basate sul codice, non sulle decisioni di una banca centrale. Questa differenza li rende attraenti ma anche più volatili.

# Sul costo

Una delle principali caratteristiche di una valuta reale è il valore stabile. Molte persone sostengono che i *Bitcoin* non sono una valuta dato il suo valore volatile. Il prezzo dei *Bitcoin* oscilla notevolmente e occasionalmente raddoppia di valore in breve tempo.

Ad esempio, nel luglio del 2010, il prezzo era $0,08 per *Bitcoin*. Nel dicembre del 2017 i *Bitcoin* hanno raggiunto $20.000. In media, cambia circa il 2% al giorno. Questo è qualcosa che non vedi con le valute tradizionali, portando molti a dire che è inutile. Un prezzo stabile è ciò che convincerà gli investimenti tradizionali e porterà a una crescita sostenuta.

Questo è importante per i *Bitcoin*? Dipende da come li guardi. A breve termine, la volatilità del prezzo può avere un impatto enorme sulla fiducia delle persone. Quando si tenta di attirare nuove persone nel mondo delle criptovalute, il prezzo in rapida evoluzione può sicuramente essere un problema.

La chiave è guardare il quadro generale. Se sei qualcuno che è interessato a far parte di un cambiamento economico veramente rivoluzionario, il piano a lungo termine è ciò che interessa maggiormente.

Con questo in mente, molte ricerche hanno dimostrato che i *Bitcoin* dovrebbero stabilizzarsi ad un certo punto in futuro e fluttuare molto meno. I tipici alti e i bassi possono essere ampiamente valutati da quanta pubblicità stanno ottenendo i *Bitcoin* in un determinato momento.

C'è anche un'alta probabilità che i governi inizieranno a regolare le criptovalute nei prossimi anni. Mentre la regolamentazione non sarà in grado di bloccare le valute decentralizzate, essa avrà invece un forte effetto moderatore in che misura e quanto velocemente cambieranno le valutazioni.

# Cos’è una criptovaluta?

> "Criptovaluta: una valuta digitale in cui vengono utilizzate tecniche di crittografia per regolare la generazione di unità di valuta e verificare il trasferimento di fondi, operando indipendentemente da una banca centrale".

Definire le criptovalute richiede molte informazioni tecniche che tratteremo più approfonditamente nel prosieguo del libro, ma vale la pena introdurle qui in modo da poter capire di cosa stiamo parlando.

In parole povere, una criptovaluta è formata da linee di codici che hanno valore monetario. Usando la crittografia, la rete decentralizzata crea nuove monete e protegge le transazioni. Alcuni membri della rete decentralizzata installano computer che elaborano il codice. In cambio, questi nodi – conosciuti come minatori – ricevono un premio per la sicurezza delle transazioni sulla *Blockchain*.

# Perché i *Bitcoin*?

*I Bitcoin* non sono l'unica criptovaluta, ma hanno costantemente mantenuto il loro dominio come la criptovaluta numero uno al mondo negli ultimi dieci anni.

C'è da dire che i *Bitcoin* non sono la migliore criptovaluta al mondo. Nuovi progetti sono stati accompagnati da scalabilità, velocità e privacy delle transazioni molto superiori. Ma queste nuove monete non sono state in grado di rovesciare i *Bitcoin* dal suo trono.

Parte del motivo per cui i *Bitcoin* hanno mantenuto il loro vantaggio è perché sono stati i primi. I *Bitcoin* sono stati la prima *Blockchain* di sempre. Tutto l'interesse iniziale per *Blockchain*, dal 2008 al 2013, si è concentrato sui *Bitcoin*. Questo significa che i *Bitcoin* avevano la più grande base di utenti e di grandi sviluppatori per costruire il sistema.

Questo processo è un ciclo virtuoso per i *Bitcoin*. Poiché sono supportati dalla più grande rete, hanno riscosso ampia accettazione. Effetto principale di questa grande rete significa che più persone usano una tecnologia, più diventa utile.

Prendi ad esempio l'e-mail. Non sarebbe affatto utile se tu fossi l'unica persona al mondo con un indirizzo e-mail. Sarebbe in qualche modo utile se tu e poche altre persone aveste la posta elettronica. Ma è estremamente utile quando quasi tutti hanno un indirizzo e-mail. L'adozione dei *Bitcoin* ha lo stesso effetto. Diventa più utile quando più persone li accettano.

I *Bitcoin* hanno ancora oggi la maggior attenzione di qualsiasi criptovaluta, principalmente perché sono ancora i più utilizzati. La sua lunga storia conferisce loro anche una certa legittimità.

Nel corso di un decennio, i *Bitcoin* hanno affrontato e superato molti ostacoli e sfide tecniche, risalendo sempre. Il loro comprovato record di sicurezza li rende anche più sicuri per i principianti.

Mentre altre criptovalute possono concentrarsi su funzioni specifiche, i *Bitcoin* sono una valuta digitale versatile che è disponibile in quasi tutti gli scambi di monete alternative. In questa fase, è la valuta che ha dietro di sé gli investimenti, una base di utenti, la sicurezza e le registrazioni tracciate.

# Conoscere i *Bitcoin*

Questo è solo l'inizio. In questo libro, tratteremo ogni aspetto dei *Bitcoin* e ti daremo consigli sul mondo reale e su come iniziare.

C'è molto da imparare. È facile impantanarsi nelle particolarità dei *Bitcoin* e come funziona la tecnologia, ma per iniziare, hai solo bisogno di capire le fondamenta. Questo è esattamente ciò che leggerai nelle prossime pagine.

# Capitolo 2. Capire la *Blockchain* & le transazioni in *Bitcoin*

Prima di conoscere le basi per acquistare e detenere il tuo primo *Bitcoin*, esaminiamo i fondamenti della tecnologia che fa funzionare *Bitcoin*: la *Blockchain*. Recentemente, '*Blockchain*' ha guadagnato lo status di parola d'ordine per le nuove startup. Molte persone che usano il termine non hanno un'idea chiara di come la *Blockchain* protegge una rete decentralizzata. Entro la fine di questo capitolo, capirai le basi della *Blockchain* meglio di molti appassionati di criptovaluta.

# *Blockchain* e *Bitcoin*

Se ti ricordi, è stato nel 2008 che Satoshi Nakamoto ha pubblicato per la prima volta un libro bianco sulla tecnologia dei *Bitcoin* e ha dettagliato il sistema *peer-to-peer* che esegue le transazioni dei *Bitcoin*. La stessa valuta *Bitcoin* è un'idea rivoluzionaria, ma la tecnologia che la alimenta è la vera innovazione. La *Blockchain* di Satoshi consente di creare registri decentralizzati sicuri per qualsiasi cosa, non solo per la criptovaluta.

La *Blockchain* dei *Bitcoin* è il libro mastro pubblico contenente tutte le transazioni che sono state fatte nella storia dei *Bitcoin*. Poiché non esiste un organo di governo centrale o un database, il libro mastro si trova su una rete composta da tanti computer che eseguono il software dei *Bitcoin*. Tutti lavorano insieme per costruire la rete.

Tutto questo accade pubblicamente e chiunque può visualizzare il traffico mentre sta accadendo. Questo livello di trasparenza è inaudito in qualsiasi altro sistema finanziario. Questa trasparenza è ciò che rende uniche le criptovalute.

Più in generale, la *Blockchain* può potenzialmente influire sulla nostra vita, laddove, ad esempio, è necessario verificare l'identità, condurre una transazione o sottoscrivere un contratto. Il registro pubblico sulla *Blockchain* può essere più veloce, più economico e più sicuro di molte istituzioni di cui ci fidiamo oggi.

# Come funzionano le transazioni in *Bitcoin*?

I *Bitcoin* non esistono fisicamente. Non c'è un deposito di *Bitcoin* da qualche parte. Se ci pensi, non è troppo diverso dai nostri soldi moderni. I soldi che vedi quando accedi al tuo conto bancario non significano che ci sia una scatola con i tuoi fondi al suo interno. Allo stesso modo, non c'è nulla che puoi definire e dire "questo è un *Bitcoin*".

Invece, quando si avvia una transazione, si invia la richiesta di transazione all'intera rete. I minatori sulla rete aggiungeranno la tua transazione al libro mastro pubblico insieme ad altre richieste di transazione attualmente sulla rete. Questo libro mastro viene quindi timbrato con marca temporale, collegato all'ultimo libro mastro prodotto e bloccato con una chiave crittografica. Un libro mastro timbrato, collegato e bloccato si chiama blocco.

## I blocchi

I blocchi delle transazioni contengono tutto ciò di cui hanno bisogno sia per aggiungere nuove transazioni sia per connettere il blocco ai precedenti. Ci sono quattro cose incluse in ogni blocco: un riferimento al blocco precedente nella catena, tutte le transazioni aggiunte, un marca temporale e la prova crittografica che mostra come è stato creato il blocco.

Questa combinazione di timbratura, collegamento e blocchi chiusi è stata l'innovazione di Satoshi che ha permesso la creazione dei *Bitcoin*. Essa risolve i problemi di creazione di un libro mastro nel quale chiunque può aggiungere:

- la marca temporale che mostra la posizione del blocco, garantendo che i blocchi non vengano confusi o che più blocchi non vengano onorati contemporaneamente dalla rete;
- il collegamento che è un riferimento al blocco precedente incorporato nel contenuto del blocco corrente. Ciò protegge il posto del blocco in una lunga catena di blocchi. La *Blockchain*!;
- il blocco crittografico è noto come *hash*. I minatori della rete usano la loro potenza di calcolo per calcolare questo *hash*. Per i *Bitcoin*, questo è un puzzle incredibilmente difficile che necessita dei processori più veloci del mondo per risolverli in una media di 10 minuti.

Ospitando tutte queste informazioni in un unico blocco, il sistema *Blockchain* è in grado di regolarsi da solo e non richiede un occhio attento per supervisionare. Non è necessario che qualcuno controlli manualmente le transazioni. Una volta eseguito l'*hashing*, è quasi impossibile modificare il contenuto di un blocco.

La modifica del contenuto di un blocco richiede la modifica del libro mastro, la ricostruzione del blocco e la risoluzione del puzzle crittografico. Spero che il tuo computer sia più veloce di tutti gli altri computer della rete, perché dovrai vincere la gara per completare il puzzle se vuoi che il tuo blocco venga aggiunto. Questo è altamente improbabile, data l'enorme potenza di calcolo sulla rete dei *Bitcoin*.

I blocchi sono disposti in una catena e se si desidera modificare una transazione precedente, è necessario modificare quel blocco e risolvere il nuovo puzzle. Ma la risposta al vecchio puzzle originale è incorporata nel blocco successivo della catena. Dovresti aggiornare anche il blocco successivo, questa volta con la nuova risposta del puzzle! Ogni volta che modifichi un blocco, dovrai risolvere nuovamente il puzzle per ogni blocco successivo. Più puzzle a blocchi devi risolvere, meno è probabile che tu attui con successo il tuo attacco. Le transazioni in *Bitcoin* eseguite da più di un'ora sono statisticamente quasi impossibili da modificare.

Dopo che una transazione è stata aggiunta alla *Blockchain*, è lì per sempre e registrata su ogni computer nella rete. In questo modo, *Blockchain* è uno dei database più sicuri che si possano immaginare.

## Conferme

Le transazioni effettuate devono essere confermate per assicurarsi che siano corrette. I minatori, che creano un nuovo blocco e lo aggiungono alla *Blockchain* ogni dieci minuti, fanno questo. I minatori verificano le transazioni, le registrano nel libro mastro pubblico e le aggiungono al blocco successivo. Una volta risolto il blocco, la transazione viene considerata verificata e le modifiche sono improbabili.

Come descritto sopra, diventa sempre più difficile cambiare una transazione vecchia nella catena del blocco. Per questo motivo, alcune persone preferiscono attendere diversi blocchi prima di dire “transazione confermata”.

Quando si utilizzano i *Bitcoin* in un negozio, alcuni commercianti potrebbero non costringerti ad aspettare affatto. Ciò significa che stanno aspettando che tu venga a conoscenza del pagamento. Questo è in genere più comune con le transazioni di basso valore in quanto vi è un minor rischio di frode.

## Commissioni

Come con tutti i sistemi transazionali, i *Bitcoin* sono soggetti a commissioni per ogni trasferimento. Vi è però una distinzione importante: le commissioni non sono richieste e possono essere determinate dalla persona che invia i fondi.

In cambio di conferme più rapide, i minatori raccolgono ed elaborano le commissioni. Se paghi abbastanza, il minatore sposterà la tua transazione in cima alla pila per essere aggiunto al blocco successivo. Una volta che loro hanno creato con successo un nuovo blocco dei *Bitcoin*, raccolgono le commissioni per tutte le transazioni incluse in quel particolare blocco.

Le commissioni sono interamente volontarie e la persona che avvia la transazione può decidere se desidera o meno includere una commissione. Includendo una commissione, invece, puoi assicurarti che i minatori abbiano un incentivo per elaborare la tua transazione. Se scegli di non includere una commissione, i minatori elaboreranno altre transazioni prima delle tue. Potresti aspettare ore (o addirittura giorni) prima che la tua transazione gratuita venga inclusa in un blocco.

Alcuni portafogli (dove conservi e gestisci i tuoi *Bitcoin*) decideranno la commissione di transazione per te. Diremo di più sui portafogli a breve.

# La *Blockchain* e le transazioni

La *Blockchain* ti sembra un po' meno misteriosa ora? Questo è solo l'inizio di questa incredibile invenzione. Ho scritto un intero libro sulla tecnologia *Blockchain* (Tutto sulla tecnologia *Blockchain*). Se sei interessato, questo libro te la spiegherà in modo più approfondito.

In seguito, tratteremo di più sui minatori, ma per ora passiamo ad alcune informazioni utili su come ottenere e spendere i *Bitcoin*.

# Capitolo 3. Iniziamo a trattare i *Bitcoin*

Con una criptovaluta come i *Bitcoin*, la cosa più importante è ottenere ottime informazioni e comprendere il sistema prima di immergersi. I *Bitcoin* non hanno un'autorità centrale, quindi le transazioni non possono essere annullate. Se commetti un errore con i tuoi *Bitcoin*, esso sarà permanente. Detto questo, fai attenzione, investi solo un po' alla volta e fai le tue ricerche.

Questo libro è una buona introduzione, ma probabilmente non è esaustivo per tutto ciò che scoprirai nel mondo dei *Bitcoin*. Il miglior consiglio che posso darti è leggere il più possibile.

I *Bitcoin* possono sembrare spaventosi o complicati. L'obiettivo di questo capitolo è metterti a tuo agio con i concetti di base e le regole di base per iniziare. Tieni presente che nel libro ci saranno spiegazioni più approfondite, quindi non rimarrai sprovvisto di informazioni.

# Sicurezza personale sui *Bitcoin*

Prima di dare qualche consiglio su come acquistare, detenere, vendere e negoziare in *Bitcoin*, dobbiamo parlare di sicurezza. La stessa rete dei *Bitcoin* è altamente sicura. La rete *Bitcoin* non è mai stata hackerata ed è estremamente improbabile che qualcuno possa modificare una transazione sul libro mastro pubblico dei *Bitcoin*.

Il rischio per la sicurezza derivante dal possesso dei *Bitcoin* deriva dalla disattenzione personale o dai rapporti con fornitori di servizi di terze parti. Ecco alcuni consigli.

## Non condividere mai la chiave privata

Questa è la prima regola della sicurezza dei *Bitcoin* e dovrebbe essere ovvia. Nessuna società o persona legittimata potrà mai richiedere la chiave privata dei tuoi *Bitcoin* (a meno che tu non stia autorizzando una spesa). Gli indirizzi dei *Bitcoin* non sono collegati alla tua identità. Non è necessario fornire l'identificazione durante la creazione della maggior parte dei portafogli e l'unica cosa che distingue il proprietario di un portafoglio è sapere la sua chiave privata.

Quindi, chiunque abbia la tua chiave privata può spendere i tuoi *Bitcoin*. E non c'è modo di annullare le transazioni o segnalare frodi sui *Bitcoin*. Non condividere mai la tua chiave privata.

## Non perdere la tua chiave privata

Un effetto collaterale degli indirizzi anonimi è che non c'è modo di recuperare la chiave privata in caso di smarrimento. L'unico modo per accedere al tuo indirizzo è con la chiave. Se perdi la chiave, i tuoi fondi spariranno per sempre.

La maggior parte dei portafogli si occupa di questo per te e memorizzerà le tue informazioni chiave con una password recuperabile. Assicurati sempre di eseguire il backup di tutte le informazioni sulla chiave privata in più luoghi.

## Avere un portafoglio sicuro

Come puoi immaginare, un portafoglio è ciò che contiene i *Bitcoin* che ricevi. Esistono diverse opzioni di cui discuteremo, alcune gestite sul web, altre su hardware, cellulari e altro ancora. Molte persone conservano i loro *Bitcoin* giornalieri in un normale portafoglio web mentre conservano il resto in un portafoglio più sicuro su cui poter eseguire il backup e proteggerli. In questo modo, anche se qualcuno dovesse hackerare il tuo computer non sarà in grado di toccare i tuoi risparmi. Parleremo di più sui diversi portafogli in seguito.

## Sapere che il prezzo cambierà

Il prezzo dei *Bitcoin* cambia di minuto in minuto. È importante capirlo perché a volte può essere una corsa ad ostacoli. Sono andati costantemente in salita, ma hanno anche avuto periodi di calo di valore. Alcuni anni fa, era quasi incredibile che un *Bitcoin* valesse $100. Al momento della stesura di questo documento, vale oltre $11.000! Anche se si prevede che salirà col passare del tempo, ci saranno giorni in cui il prezzo si abbasserà e fa tutto parte della corsa.

## Non puoi richiedere indietro i pagamenti

I pagamenti in *Bitcoin* non sono come quelli con le carte di credito o con PayPal. Una volta che invii denaro a qualcuno, questa è l'unica persona che può restituirtelo. Con questo in mente, è fondamentale che ti fidi della persona a cui stai inviando fondi e ricontrolla sempre l'indirizzo del portafoglio.

Nel caso in cui invii i *Bitcoin* all'indirizzo sbagliato, è improbabile che lo riavrai. Controlla due, tre volte tutti i dettagli della transazione prima di inviare fondi.

Se succede qualcosa, non esiste una compagnia centrale che possa aiutarti. Questo ha effetti positivi e negativi sull'uso dei *Bitcoin* rispetto ad altri metodi di pagamento, ma ne parleremo un po' più avanti.

## I Bitcoin sono tracciabili

Poiché i *Bitcoin* operano su un libro mastro pubblico, chiunque può vedere la cronologia delle transazioni sulla rete. Le transazioni sono solo un elenco di indirizzi pubblici con i relativi importi. Ma gli investigatori intelligenti possono costruire una rete di transazioni e identificare il mittente. Nel tempo, un investigatore dedicato potrebbe capire quale sia il tuo indirizzo e vedere tutti gli indirizzi con cui hai effettuato i pagamenti con *Bitcoin*.

Ci sono alcuni modi per evitare che siano tracciati i tuoi *Bitcoin*. Puoi utilizzare molti indirizzi o persino un indirizzo per ogni nuova transazione. Puoi anche utilizzare i servizi di miscelazione delle monete che mascherano la fonte dei fondi mescolandoli con altri fondi. Vale comunque la pena sapere, in anticipo, che il libro mastro pubblico è proprio questo: pubblico.

## I problemi potrebbero aumentare

I *Bitcoin* stanno rapidamente crescendo e potrebbero esserci molti cambiamenti in arrivo in futuro. Nuovi aggiornamenti potrebbero far ripensare alcuni fornitori sui loro servizi e prezzi, le conferme potrebbero rallentare, le commissioni potrebbero aumentare o potrebbe verificarsi una moltitudine di altre cose. Non si può dire come cambieranno le cose, ma finché si capisce cosa c'è dietro tutto questo, starai bene.

# Iniziare con i *Bitcoin*

Questo è solo l'inizio. C'è molto da imparare, ma ti guiderò in questo libro per renderti sicuro e abbastanza ben informato per iniziare ad utilizzare questa valuta digitale in rapida crescita!

# Capitolo 4. Dove tenere i tuoi *Bitcoin*

## Il tuo indirizzo dei *Bitcoin*

Hai già inviato un'e-mail a qualcuno prima, giusto? Tale indirizzo specifico consente a quella persona di inviare e ricevere messaggi a chiunque altro sul web con un indirizzo e-mail. Gli indirizzi dei *Bitcoin* funzionano in modo simile anche se c'è una differenza chiave.

### Che cos'è l'indirizzo dei Bitcoin?

L'indirizzo dei *Bitcoin* è la stringa specifica di caratteri che identifica il tuo portafoglio. A differenza dell'indirizzo e-mail, un singolo portafoglio può avere più indirizzi e persino un indirizzo per ogni nuova transazione effettuata.

Nel caso dei *Bitcoin*, l'indirizzo ha una lunghezza compresa tra 26 e 35 caratteri alfanumerici. Ogni indirizzo inizia con 1 o 3 ed è sensibile al maiuscolo / minuscolo. Questa serie di caratteri deve essere esatta o i fondi non possono essere trasferiti, ma ciò non dovrebbe sorprendere chi ha già trasferito fondi con i metodi tradizionali.

Quando vuoi ricevere fondi, condividi il tuo indirizzo dei *Bitcoin* con la persona che paga. Puoi anche elencare il tuo indirizzo pubblicamente. La condivisione del tuo indirizzo non dà accesso al tuo account in nessun modo. Indica solo alla rete dove dirigere i fondi.

> "Ecco un esempio di un indirizzo dei Bitcoin:
> 1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2"

# Indirizzi monouso

Mentre gli indirizzi e-mail, per usare il nostro esempio precedente, non cambiano, la maggior parte degli esperti consiglia di utilizzare un nuovo indirizzo per i tuoi *Bitcoin* per ogni transazione. Poiché l'indirizzo non è lo stesso del tuo portafoglio, questo significa che non stai creando un nuovo portafoglio, ma semplicemente usi un nuovo identificativo per le persone che ti inviano i *Bitcoin*. Ci sono diversi motivi per farlo.

## Anonimato

C'è un grosso problema con il riutilizzo dell'indirizzo dei *Bitcoin*: corri il rischio di perdere l'anonimato che viene fornito dai *Bitcoin*.

Ogni volta che usi l'indirizzo dei *Bitcoin*, condividi pubblicamente le informazioni su dove provengono i *Bitcoin* o dove sono andati. Poiché i *Bitcoin* operano su un libro mastro pubblico, le persone possono vedere il tuo indirizzo quando viene visualizzato sul libro mastro. Nel tempo, l'uso ripetuto dello stesso indirizzo significa che utenti malintenzionati potrebbero mappare le tue relazioni, le tue transazioni e i fondi in entrata. Più usi gli stessi indirizzi, più informazioni qualcuno può ottenere su di te.

> "Questo non è sempre probabile. Questo dovrebbe essere un problema solo se vuoi essere assolutamente sicuro di rimanere anonimo".

Con questo in mente, la creazione di nuovi indirizzi per ogni transazione aiuta a preservare la tua identità e mantenere le tue transazioni più anonime. Anche quando le transazioni sono registrate in pubblico, questo è un modo efficace per mantenere lo scudo dell'anonimato.

La creazione di un nuovo indirizzo è in genere semplice come fare clic su un pulsante nel client del portafoglio. Discuteremo dei portafogli a breve.

## Identificare i pagamenti

Se sei un'azienda o sei qualcuno che desidera tenere traccia delle transazioni, è molto più facile farlo con gli indirizzi monouso.

Essendo le transazioni legate a un indirizzo univoco, puoi sempre verificare di aver ricevuto un pagamento in base all'indirizzo che hai dato. Ciò vale anche se ogni cliente utilizza lo stesso indirizzo assegnato, ma non è il modo consigliato di ricevere fondi.

In questo modo, ogni pagamento avrà il proprio identificatore univoco. Ciò è particolarmente utile se stai gestendo un reparto crediti o debiti di grandi dimensioni.

## Qualche motivo per non farlo?

Potrebbe sembrare una seccatura o irrilevante creare nuovi indirizzi per ogni transazione. Se stai solo effettuando transazioni minime o non sei preoccupato di essere rintracciato, qual è il danno?

Alla fine, è solo una buona abitudine da prendere. Aumentare l'anonimato dei pagamenti aumenta l'anonimato generale della rete. Se tutti creassero nuovi indirizzi, i pagamenti sarebbero difficili da rintracciare, anche su un libro mastro pubblico. Come vedremo in una sezione successiva, questa privacy generale della rete è importante per la fungibilità e l'utilizzo dei *Bitcoin*.

Il consenso schiacciante è che non ci sono praticamente ragioni per non utilizzare un indirizzo nuovo per ogni transazione oltre al fatto di fare clic ogni volta per crearne uno.

# Конец ознакомительного фрагмента.