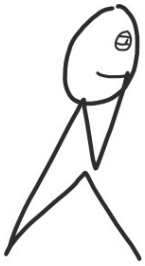
Come funziona Bitcoin?



Bitcoin è un sistema di pagamento elettronico creato nel 2009. Ti permette di inviare denaro a chiunque nel mondo, e non hai bisogno di chiedere il permesso a nessuno per creare un conto.

È stato creato come soluzione al sistema finanziario moderno, dove abbiamo un piccolo numero di grandi banche che controllano chi ottiene un conto e quali transazioni vengono elaborate. In questo sistema il controllo del denaro è centralizzato, e dobbiamo fidarci delle banche, supponendo che agiscano in modo responsabile.

> *“ Le banche devono avere la fiducia di detenere il nostro denaro e trasferirlo elettronicamente, ma lo prestano in ondate di bolle di credito con appena una frazione in riserva in controvalore - Satoshi Nakamoto*

La centralizzazione delle banche e la conseguente crisi finanziaria del 2008 hanno ispirato lo sviluppo di Bitcoin. È un sistema di pagamento, e funziona senza un controllo centrale. È stato progettato anonimamente da Satoshi Nakamoto, divulgato il 31 ottobre 2008, ed è stato avviato ufficialmente nel gennaio 2009.

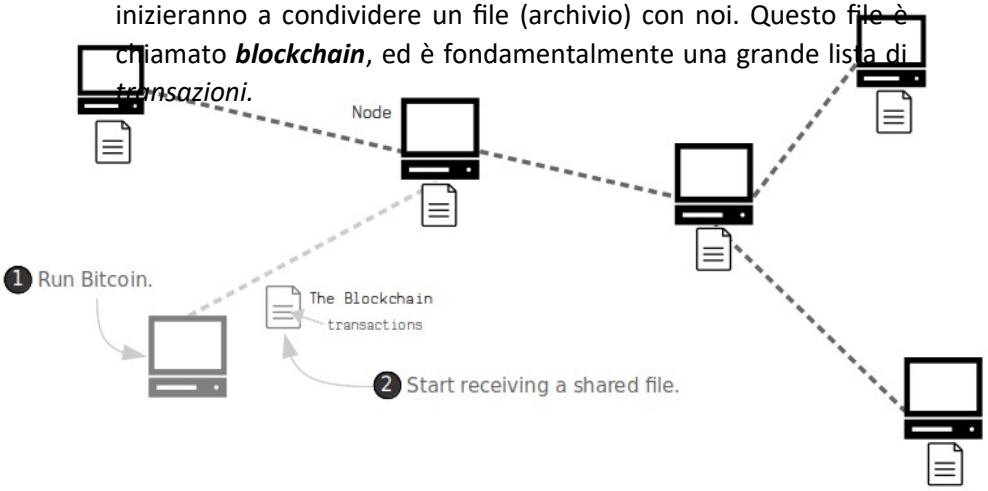
Chiunque può eseguire il programma o utilizzare il sistema.

Quella che segue è una semplice spiegazione di come funziona

Che cos’è Bitcoin?

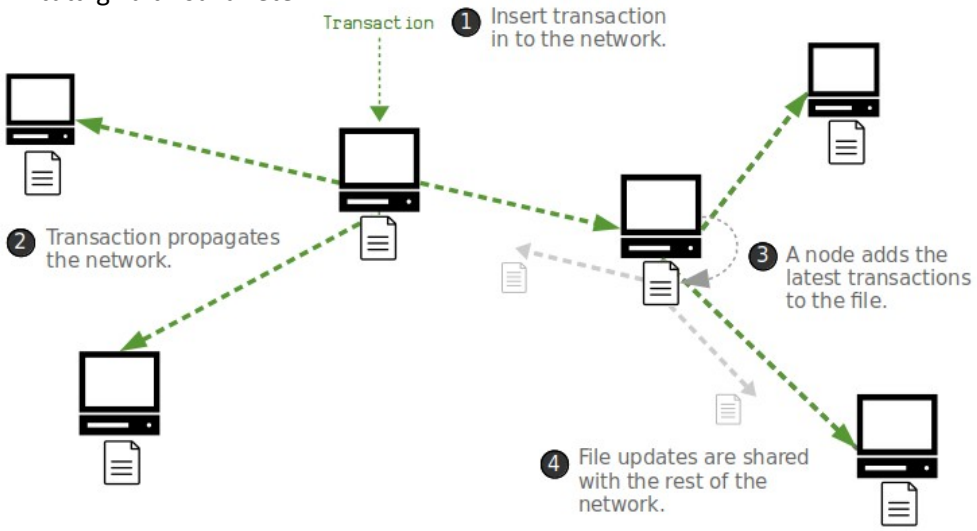
Bitcoin è solo un programma per computer. Puoi scaricarlo ed eseguirlo sul tuo computer.

Quando si lancia il software, il nostro PC si connette ad altri computer che stanno eseguendo lo stesso programma e che inizieranno a condividere un file (archivio) con noi. Questo file è chiamato ***blockchain***, ed è fondamentalmente una grande lista di *transazioni.*



Quando una nuova transazione entra nella rete, viene trasmessa da un computer all'altro fino a quando tutti hanno una stessa copia della transazione.

Le transazioni vengono inserite in blocchi e scritte sulla blockchain dai miner, che secondo il protocollo Bitcoin convalidano i blocchi a intervalli di circa 10 minuti, condividendo gli aggiornamenti con tutti gli altri sulla rete.

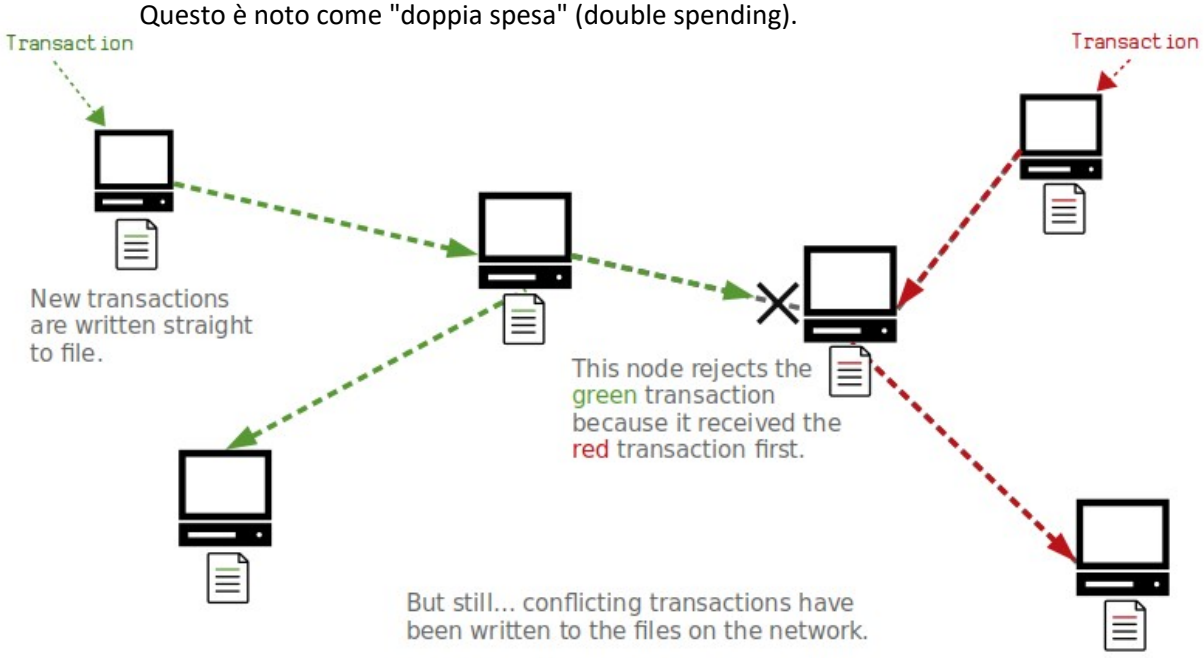


Come risultato, il programma Bitcoin (oggi Bitcoin Core e altri) crea una grande rete di computer che comunicano tra loro per condividere un file e aggiornarlo con nuove transazioni.

Quale problema risolve Bitcoin?

Questo sistema non è una novità, era possibile trasmettere transazioni attraverso una rete di computer prima di Bitcoin. Tuttavia, il problema è che si possono inserire transazioni in conflitto in una rete di computer. Per esempio**, si potrebbero creare due transazioni separate che spendono la stessa moneta digitale**, e inviare entrambe queste transazioni nella rete allo stesso tempo.

Questo è noto come "doppia spesa" (double spending).



Quindi, se state creando un sistema di pagamento elettronico senza un punto centrale di controllo, avete il problema di capire quale di queste transazioni è arrivata "prima", e questa è una cosa difficile da fare quando avete una rete di computer che agiscono tutti indipendentemente. Alcuni computer riceveranno prima la transazione verde e altri computer riceveranno prima la transazione rossa.

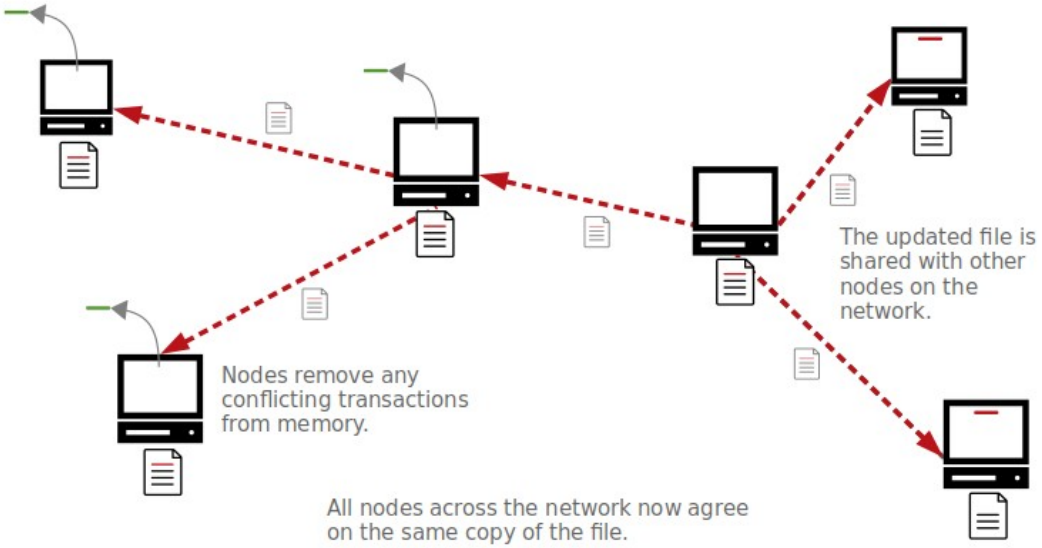
Chi deve decidere quale è arrivata "prima" e dovrebbe essere l'unica scritta nel file?

Bitcoin risolve questo problema obbligando i nodi a tenere in memoria tutte le transazioni che ricevono prima di scriverle in un file, costantemente aggiornato con le nuove transazioni.

Il registro così aggiornato viene condiviso con la rete e i nodi accetteranno le nuove transazioni come "corrette", rimuovendo ogni transazione in conflitto dalla loro memoria. Di conseguenza,

nessuna transazione *double-spent* sarà mai scritta nel file, e tutti i nodi possono aggiornare i loro file in accordo tra loro.

Questo continuo aggiornamento costituisce uno dei punti di forza del progetto di Natoshi Nakamoto, perché crea il famoso consenso della rete.

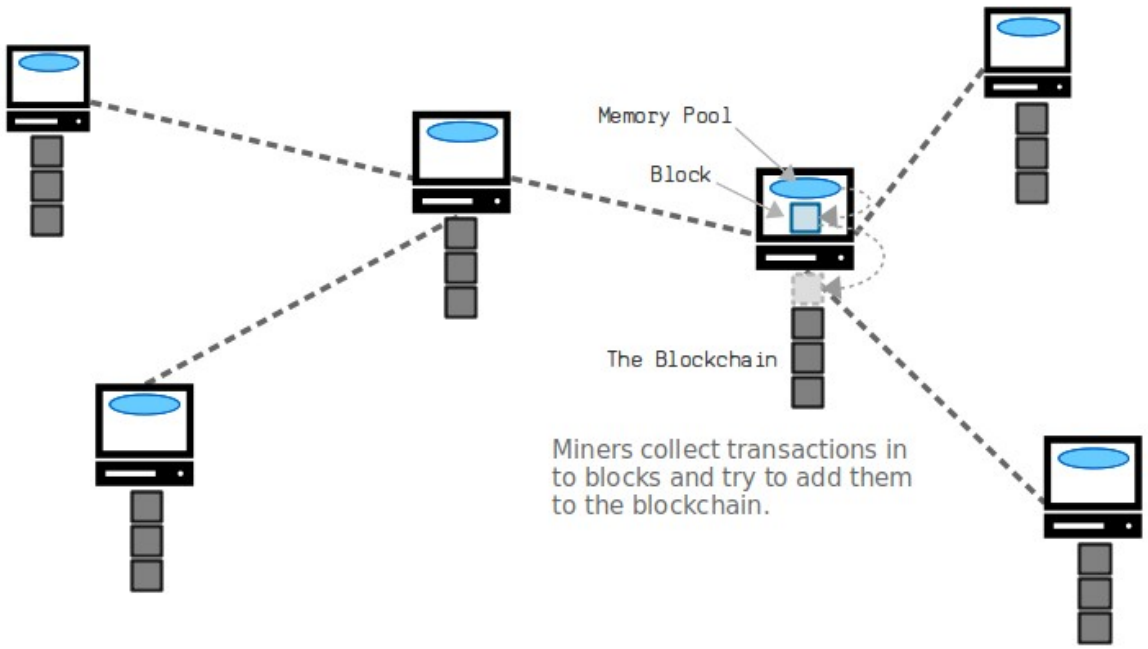


Il processo che aggiunge transazioni al file è chiamato mining, ed è fondamentalmente una competizione a livello di rete che non può essere controllata da un singolo nodo della rete.

Come funziona il mining?

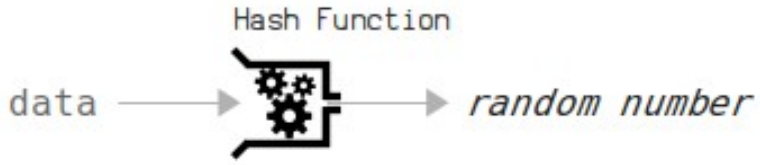
Per cominciare, ogni nodo memorizza le ultime transazioni che ha ricevuto nella sua mem-pool, che è solo una memoria temporanea del proprio computer. Ogni nodo può quindi cercare di estrarre le transazioni dalla mem-pool e scriverla sul file (la blockchain).

Per fare questo, un nodo raccoglierà le transazioni dalla sua mempool in un contenitore chiamato blocco, e poi userà la potenza di calcolo per cercare di aggiungere questo blocco di transazioni alla blockchain.

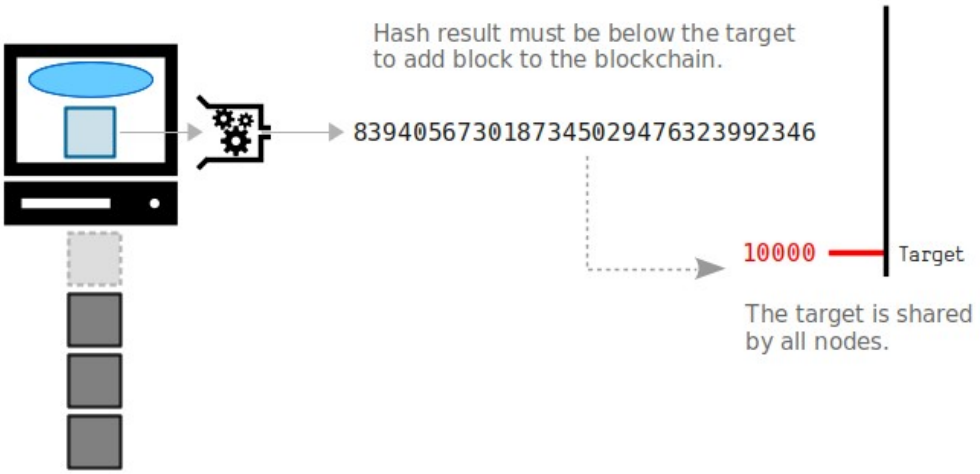


Dove entra in gioco questa potenza di elaborazione? Per aggiungere questo blocco alla blockchain, si deve elaborare il blocco di transazioni con una funzione di hash.

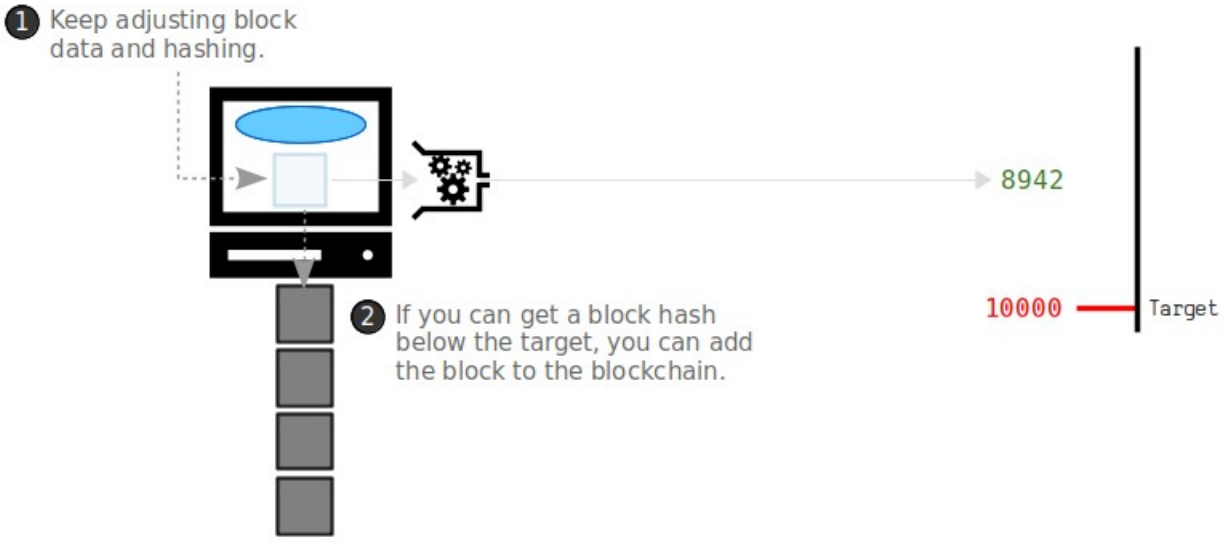
Una funzione di hash è fondamentalmente un mini programma per computer che prende qualsiasi quantità di dati, li rimescola e restituisce come risultato un numero completamente casuale (ma unico).



Affinché il blocco, così elaborato, sia aggiunto con successo alla blockchain, questo numero (l'hash del blocco) deve essere inferiore al target, che è un numero di soglia su cui tutti nella rete sono d'accordo.



Se il vostro hash di blocco risultante non è al di sotto del target, potete fare un piccolo aggiustamento ai dati all'interno del blocco e metterlo di nuovo attraverso la funzione hash. Questo produrrà un numero completamente diverso che si spera sia sotto l'obiettivo. In caso contrario, si aggiusta il blocco e si riprova.

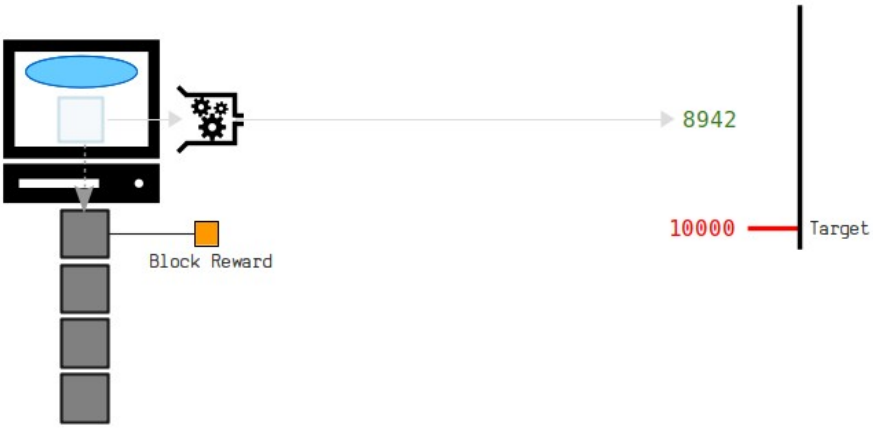


In sintesi il processo di mining utilizza la potenza di elaborazione per eseguire i calcoli di hash il più velocemente possibile per cercare di essere il primo computer della rete a ottenere un hash di blocco inferiore al target. Se si ha successo, si può aggiungere il blocco di transazioni alla blockchain e condividerlo con il resto della rete.

NOTA: anche se è ancora possibile per chiunque provare a minare i blocchi, non è più competitivo farlo su un computer di casa. Ora c'è un hardware specializzato che è stato progettato per eseguire i calcoli di hash il più velocemente e nel modo più efficiente possibile, il che significa che il mining è ora eseguito per lo più da coloro che hanno accesso a hardware specializzato ed elettricità a buon mercato

Da dove vengono i Bitcoin?

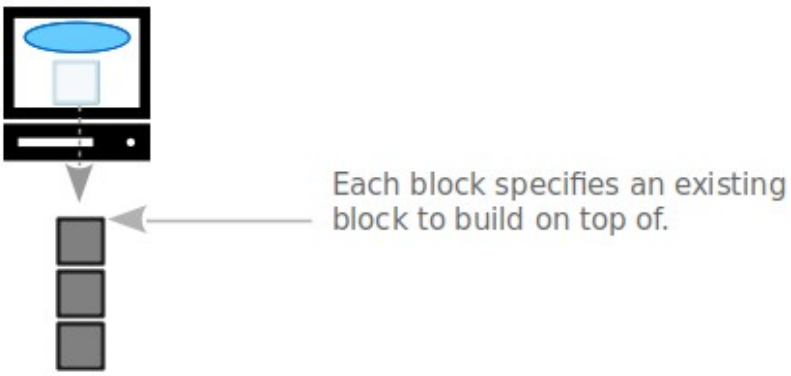
Come incentivo a usare la potenza di elaborazione per cercare di aggiungere nuovi blocchi di transazioni alla blockchain, ogni nuovo blocco rende disponibile una quantità fissa di bitcoin che non esisteva prima. Pertanto, se si è in grado di estrarre con successo un blocco, si è in grado di "inviare" questi nuovi bitcoin come ricompensa per il proprio sforzo.



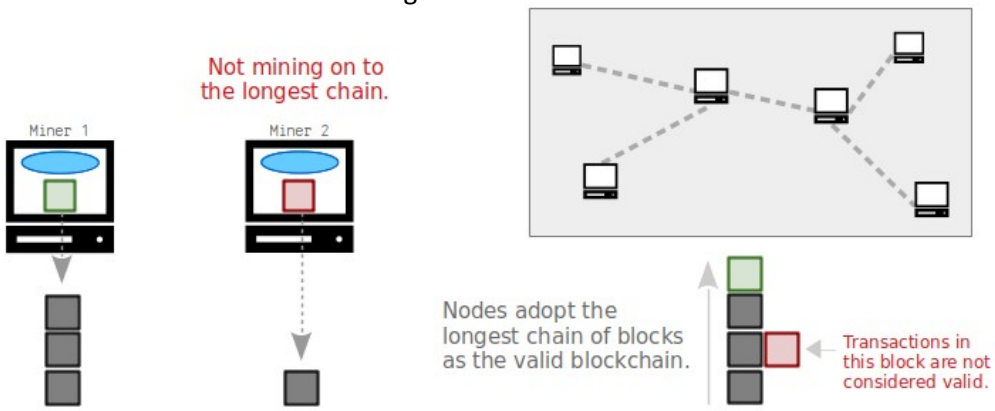
Questa ricompensa di nuovi bitcoin è chiamata ricompensa di blocco, ed è la ragione per cui il processo è chiamato "mining".

Perché il registro viene chiamato blockchain?

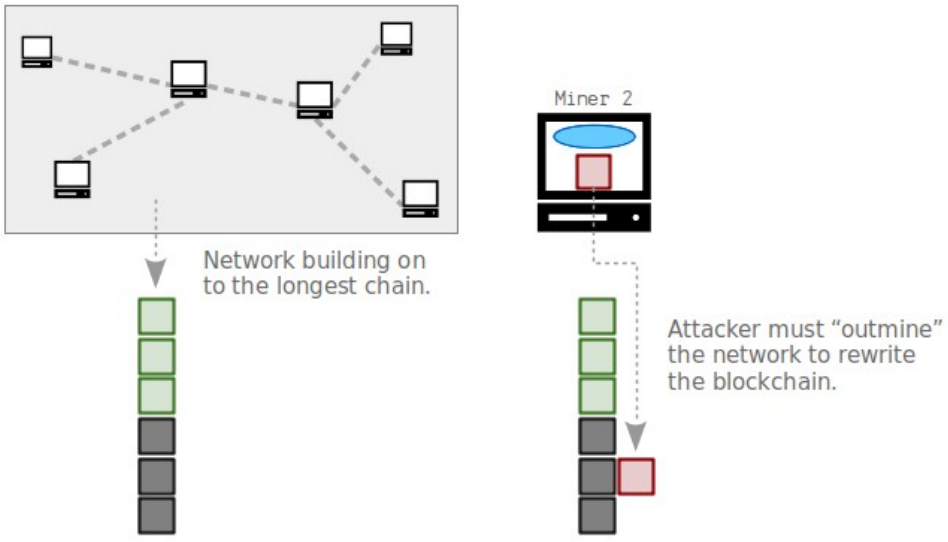
Come abbiamo visto, le transazioni non sono aggiunte al file individualmente - sono raccolte insieme e aggiunte in blocchi. Ognuno di questi nuovi blocchi si posiziona sopra uno già esistente, e così il file è costituito da una catena di blocchi; da qui, blockchain.



Inoltre, ogni nodo della rete adotterà sempre la catena di blocchi più lunga che riceve come versione "ufficiale" della blockchain. Questo significa che i miner cercheranno sempre di costruire sopra la "cima" della catena di blocchi più lunga conosciuta, pertanto qualsiasi blocco che non fa parte della catena più lunga non sarà considerato valido dagli altri nodi.



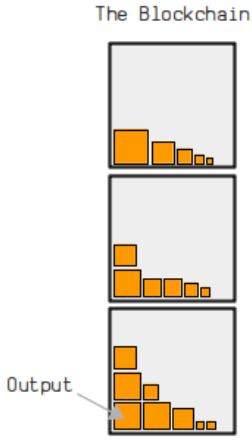
Pertanto, se qualcuno volesse riscrivere la storia delle transazioni, avrebbe bisogno di ricostruire una catena più lunga di blocchi per creare una nuova catena più lunga da far adottare agli altri nodi. Tuttavia, per ottenere questo, un singolo minatore avrebbe bisogno di avere più potenza di calcolo del resto della rete messa insieme.



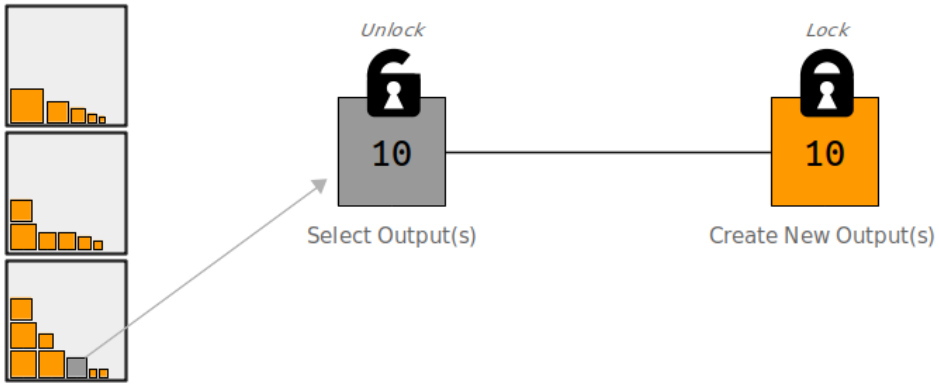
Di conseguenza, lo sforzo combinato della rete rende difficile per qualsiasi individuo "superare" la rete e riscrivere la blockchain.

Come funziona una transazione?

Si può pensare alla blockchain come a un deposito di cassette di sicurezza, che noi chiamiamo output. Questi output sono solo contenitori che contengono una certa quantità di bitcoin.

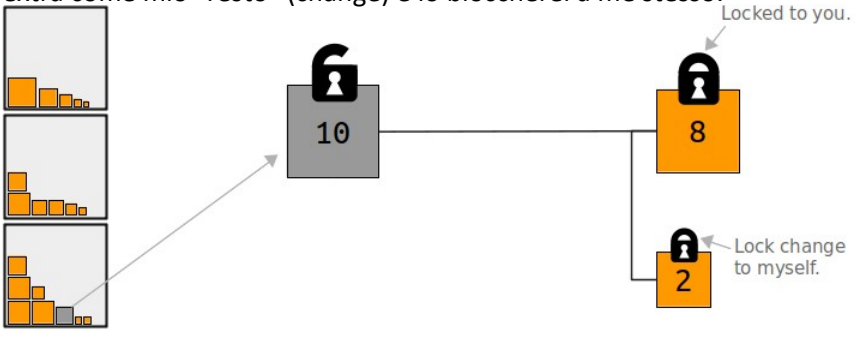


Quando ci si appresta a fare una transazione in bitcoin, vengono selezionati alcuni output e sbloccati e si creano nuovi output che vengono a loro volta bloccati.

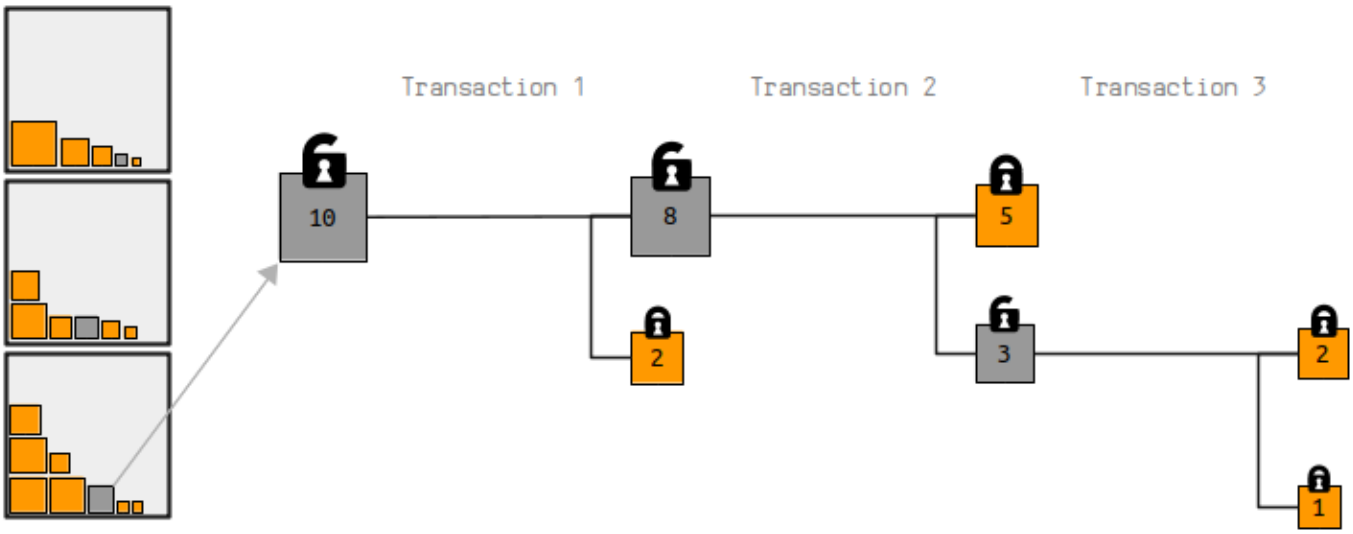


Così, quando si inviano bitcoin a qualcuno, si sta effettivamente mettendo una quantità di fondi in una nuova cassetta di sicurezza mettendo un lucchetto su di essa, che solo la persona che riceve i bitcoin può sbloccare (sempre con la sua chiave privata, firmando digitalmente).

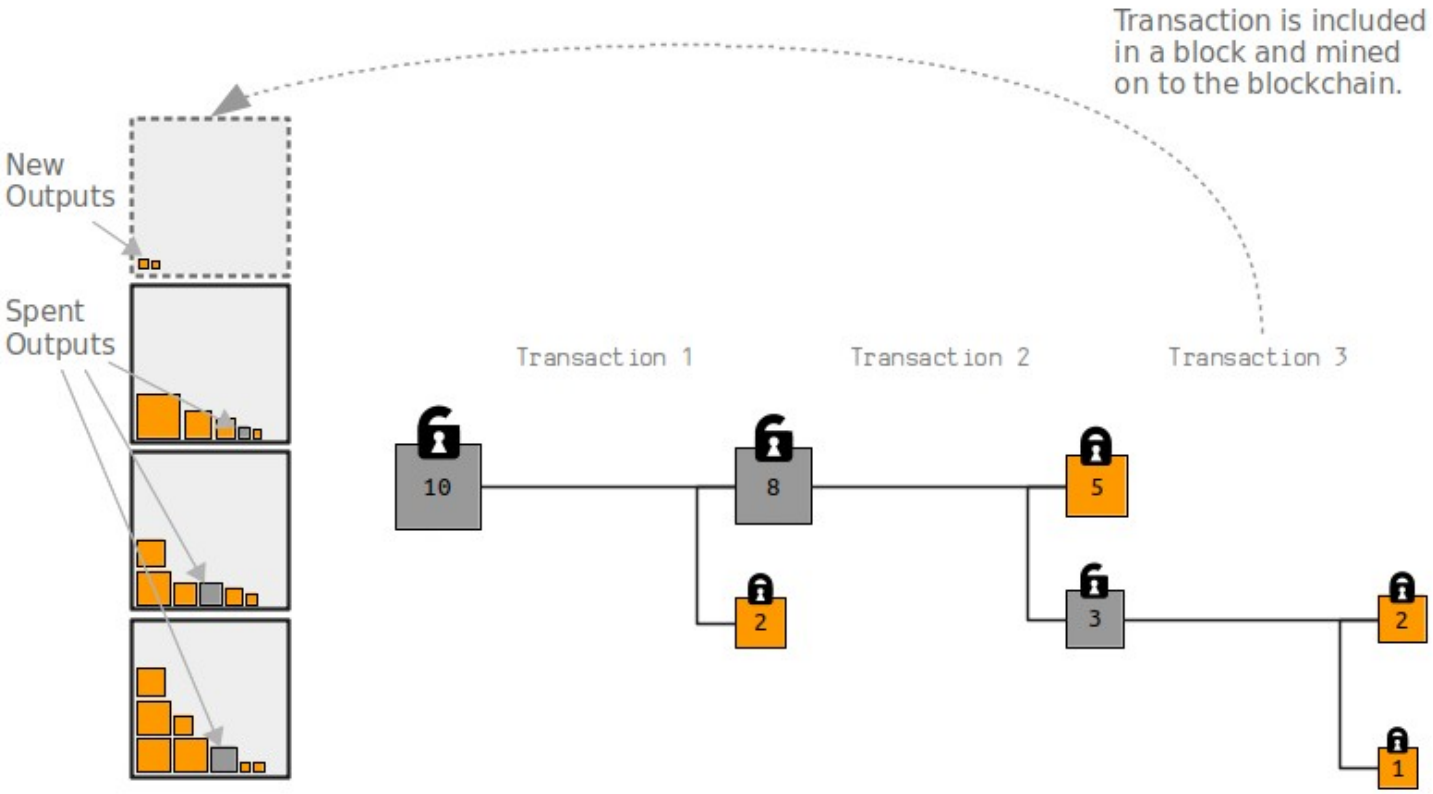
Per esempio, se volessi mandare dei bitcoin, selezionerei alcuni input dalla blockchain che posso sbloccare, e creerei una nuovo output che solo il destinatario può sbloccare. Inoltre, se non volessi mandare tutti i bitcoin che ho sbloccato, creerei un output extra come mio "resto" (change) e lo bloccherei a me stesso.



Andando avanti, se volete inviare i vostri bitcoin a qualcun altro, dovreste ripetere il processo di selezione degli output esistenti (che potete sbloccare con la vostra password) e creare nuovi output da queste. Di conseguenza, le transazioni bitcoin formano una struttura a grafo, dove il movimento dei bitcoin è collegato da una serie di transazioni.



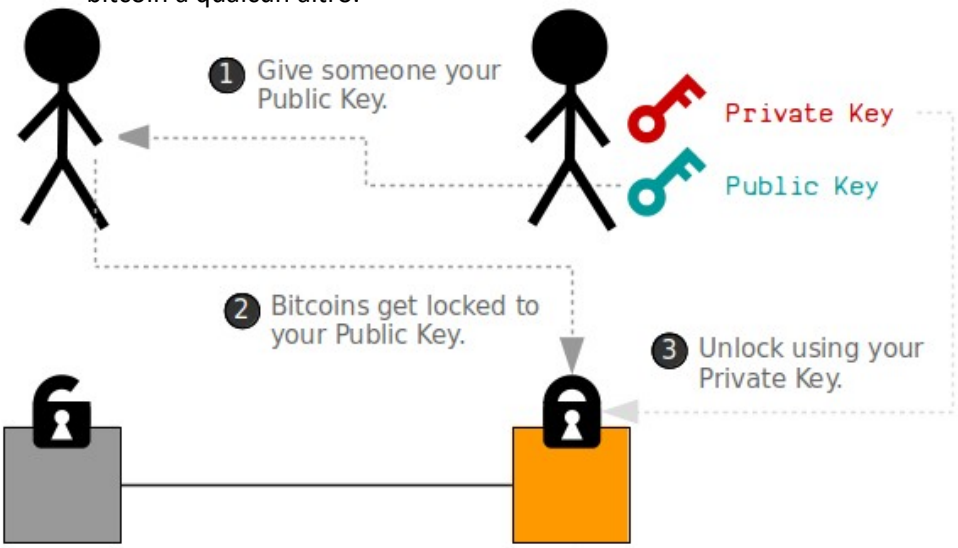
Infine, quando una transazione viene minata sulla blockchain, gli output che sono stati utilizzati (spesi) nella transazione non possono essere utilizzati in un'altra transazione, e gli output appena creati saranno disponibili per essere spostati in una transazione futura.



Come si fa a possedere bitcoin?

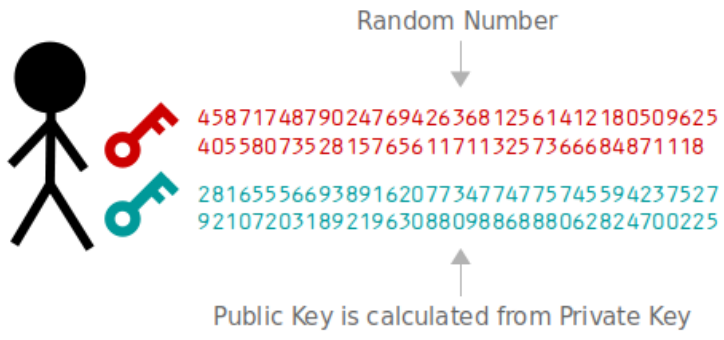
Per essere in grado di "ricevere" bitcoin, è necessario avere il proprio set (coppia) di chiavi. Questo set di chiavi è come il tuo indirizzo email e la tua password, solo che nel protocollo Bitcoin si chiamano chiave pubblica e chiave privata.

Per esempio, se volessi mandarti dei bitcoin, tu dovresti prima darmi la tua chiave pubblica (o meglio l'indirizzo che è ricavato dalla chiave pubblica). Quando creo la transazione, metterei la tua chiave pubblica dentro il lock dell'output. Tu useresti poi la tua chiave privata per sbloccare questo output quando vuoi inviare i bitcoin a qualcun altro.



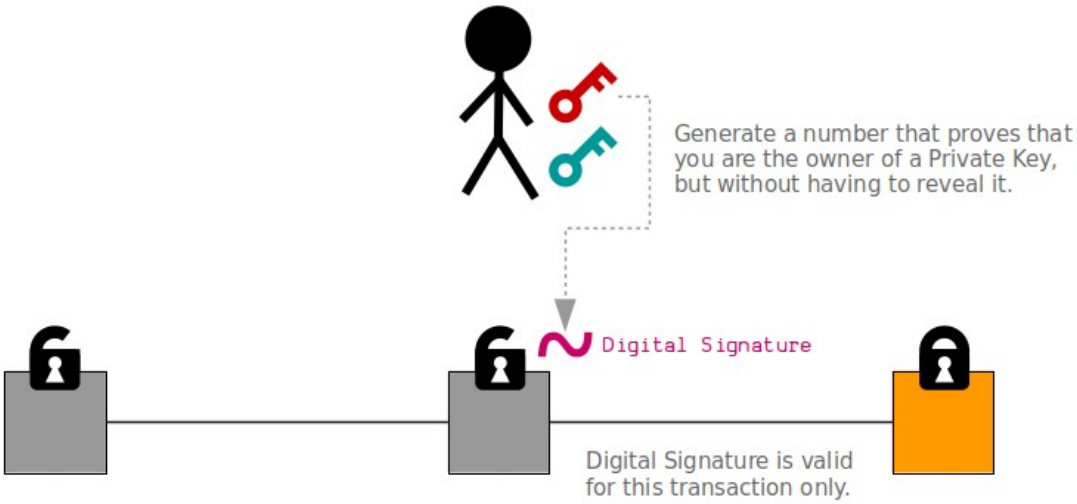
Quindi dove si possono ottenere una chiave pubblica e una chiave privata? Si possono generare con l'aiuto della crittografia.

In breve, la tua chiave privata è solo un grande numero casuale, e la tua chiave pubblica è un numero calcolato da questa chiave privata. Ma la parte intelligente è che puoi dare la tua chiave pubblica (o meglio l'indirizzo che è una rappresentazione di essa) a qualcun altro, ma non può ricavarne la chiave privata.



Ora, quando vuoi sbloccare i bitcoin che sono assegnati alla tua chiave pubblica, usi la tua chiave privata per creare quella che si chiama una firma digitale. Questa firma digitale prova che sei il proprietario della chiave pubblica (e quindi puoi sbloccare i bitcoin), senza dover rivelare la tua chiave privata.

Questa firma digitale è anche valida solo per la transazione per cui è stata creata, quindi non può essere usata per sbloccare altri bitcoin bloccati alla stessa chiave pubblica.



Questo sistema è noto come "crittografia a chiave pubblica", ed è disponibile dal 1978. Bitcoin fa uso di questo sistema per consentire a chiunque di creare chiavi per inviare e ricevere bitcoin in modo sicuro, senza la necessità di un'autorità centrale per emettere conti e password.

Riassumendo

Per iniziare con bitcoin, si genera una chiave privata e una chiave pubblica. La chiave privata è solo un numero casuale molto grande, e la chiave pubblica è calcolata da essa. Queste chiavi possono essere facilmente generate da un computer, o anche da qualcosa di semplice come una calcolatrice. La maggior parte delle persone usa un wallet bitcoin per generare e gestire le chiavi.

Per ricevere bitcoin, bisogna fornire l'indirizzo bitcoin ricavato dalla propria chiave pubblica a qualcuno che vuole inviare dei fondi'. Il mittente crea una transazione in cui sblocca i bitcoin che possiede, e crea una nuova "cassetta di sicurezza" di bitcoin su cui viene applicata la chiave pubblica del destinatario, come lock e dimostrazione della proprietà.

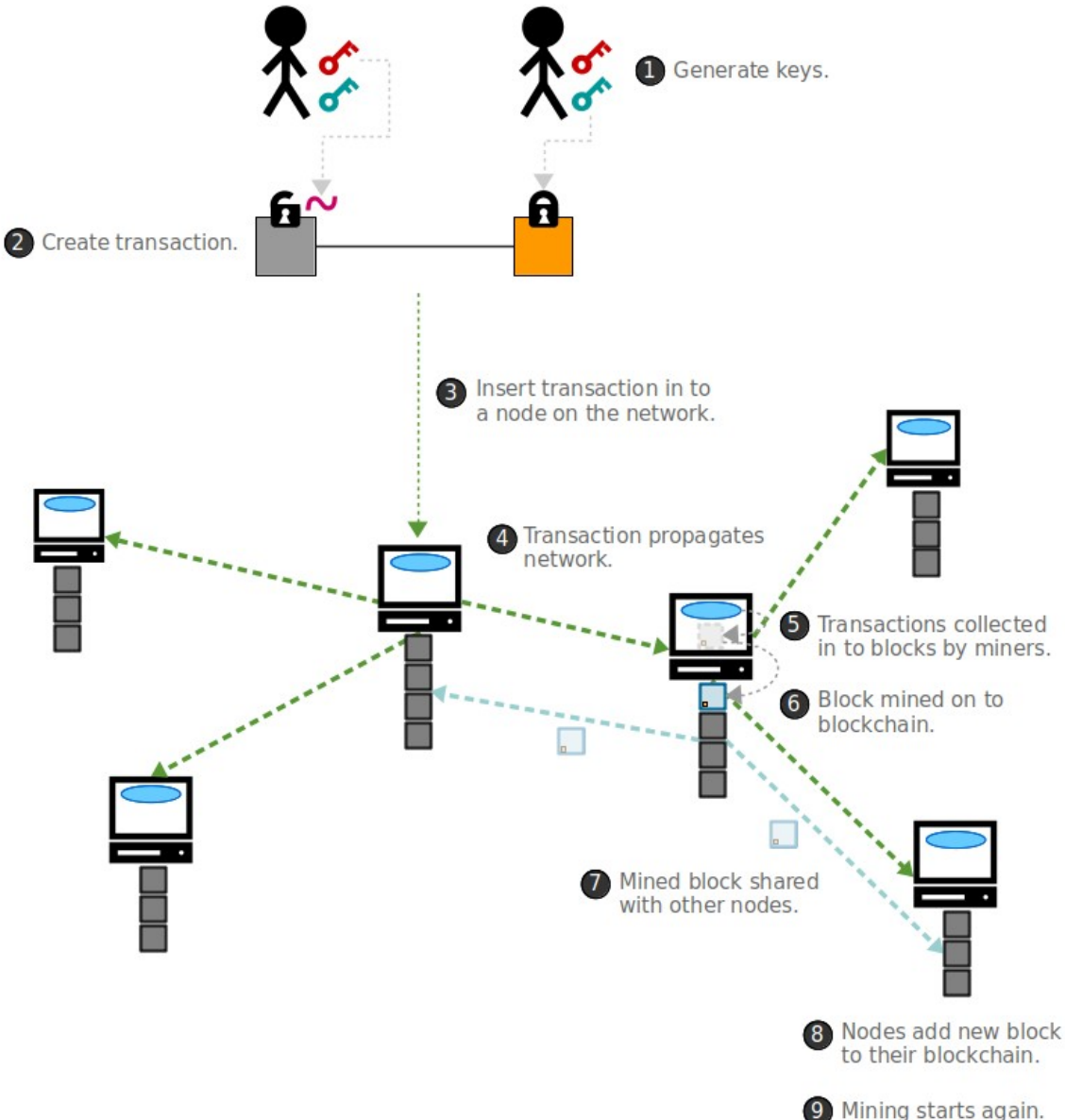
Questa transazione viene poi inviata a tutti i della rete bitcoin, dove viene trasmessa da computer a computer fino a quando ogni nodo della rete ha una copia della transazione. Da qui, ogni nodo

ha l'opportunità di provare a minare le ultime transazioni che ha ricevuto sulla blockchain.

Questo processo di mining implica che un nodo prelevi le transazioni dalla mempool per metterle in un blocco, e metta ripetutamente i dati del blocco attraverso una funzione di hash (con un piccolo aggiustamento ogni volta) per cercare di ottenere un hash del blocco inferiore al target value.

Il primo miner che trova un hash di blocco al di sotto del target value aggiungerà il blocco alla sua blockchain e lo trasmetterà agli altri nodi della rete. Ogni nodo aggiungerà anche questo blocco alla propria copia della blockchain (rimuovendo qualsiasi transazione in conflitto dala propria mempool), e riavvierà il processo di mining per cercare di continuare sopra questo nuovo blocco nella catena.

Infine, il miner che ha minato questo blocco avrà inserito la propria transazione speciale all'interno del blocco, che gli permette di raccogliere una certa quantità di bitcoin che prima non esisteva. Questa ricompensa (block reward) agisce come incentivo per i nodi a continuare a costruire la blockchain, distribuendo contemporaneamente nuove monete in tutta la rete bitcoin.



Conclusioni

Bitcoin è un programma che condivide un file sicuro con altri computer in tutto il mondo. Questo file sicuro è composto da transazioni, e queste transazioni usano la crittografia per permettere alle persone di inviare e ricevere pagamenti (cassette di sicurezza) digitali. Come risultato, questo crea un sistema di pagamento elettronico che può essere usato da chiunque, e funziona senza un punto centrale di controllo.

La rete Bitcoin funziona ininterrottamente dal suo rilascio nel gennaio 2009. Nel 2019, la rete Bitcoin ha elaborato oltre 112 milioni di transazioni, muovendo un totale di 15.577.763.114.629,34 dollari (15,58 trilioni).

Bitcoin stesso è anche in fase di sviluppo attivo, con oltre 600 sviluppatori che contribuiscono al codice dal suo rilascio. Questo è dovuto al fatto che il software è "open source", il che significa che chiunque può vedere il codice e contribuire a migliorarlo.

Perché dovrei fidarmi?

Perché posso verificare tutto e non ho bisogno di fidarmi di nessuno, è tutta matematica e calcolo.

Perché tutte queste informazioni sono gratuite?

Perché:

-Bitcoin è un programma open-source che puoi eseguire gratuitamente.
-Ho imparato tutto quello che so su Bitcoin, programmazione e scrittura gratuitamente.
-Questo sito web (https://learnmeabitcoin.com/) è costruito interamente con strumenti open-source che sono gratuiti.
-Quindi perché non l'istruzione gratuita?

Tuttavia, le donazioni sono molto apprezzate: 3Beer3irc1vgs76ENA4coqsEQpGZeM5CTd

Perché questo sito web?

Perché voglio che anche altre persone capiscano come funziona il bitcoin.

Bitcoin ti permette di trasferire valore a chiunque altro nel mondo, e penso che questo sia importante. Se capisci come funziona il bitcoin, puoi creare il tuo bel software che fa la differenza.

Guida per principianti

Un'introduzione al bitcoin

Come funziona Bitcoin

Ho scritto questa guida nel 2015 mentre stavo imparando Bitcoin per la prima volta. Ho pensato che sarebbe stato utile se avessi dimenticato completamente come funzionava e avessi bisogno di una guida rapida.

Le spiegazioni sono semplicistiche e i disegni sono orrendi, ma è comunque una lettura divertente.

- " Signing & Verifying

Come iniziare

Scaricare il tuo primo portafoglio

> *" Iniziare semplicemente e migliorare è meglio che non iniziare affatto*

Così hai sentito parlare di Bitcoin e vuoi essere coinvolto. Qual è il modo migliore per iniziare?

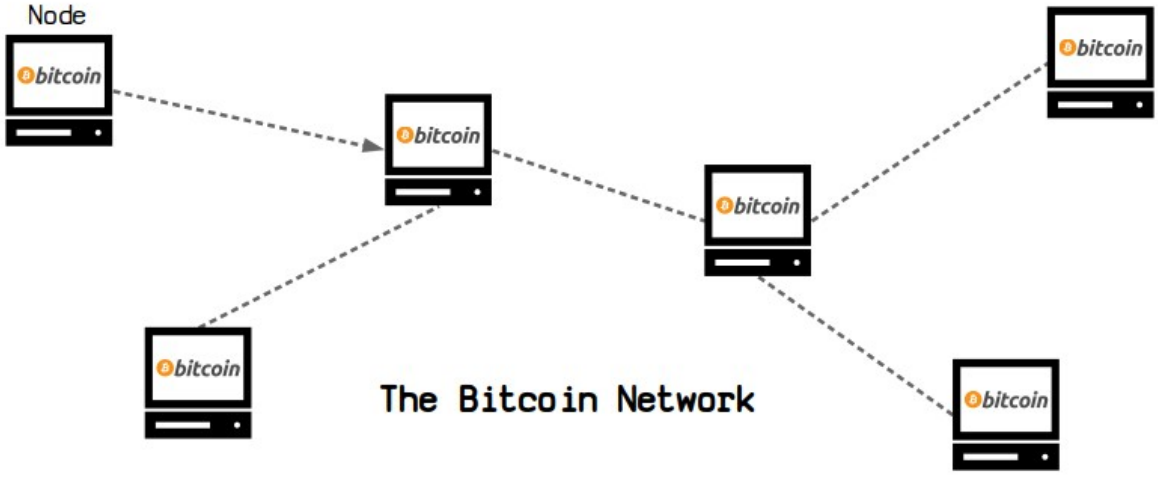
Permettetemi...

Bitcoin Core

Il modo migliore per iniziare veramente con Bitcoin è scaricare Bitcoin Core

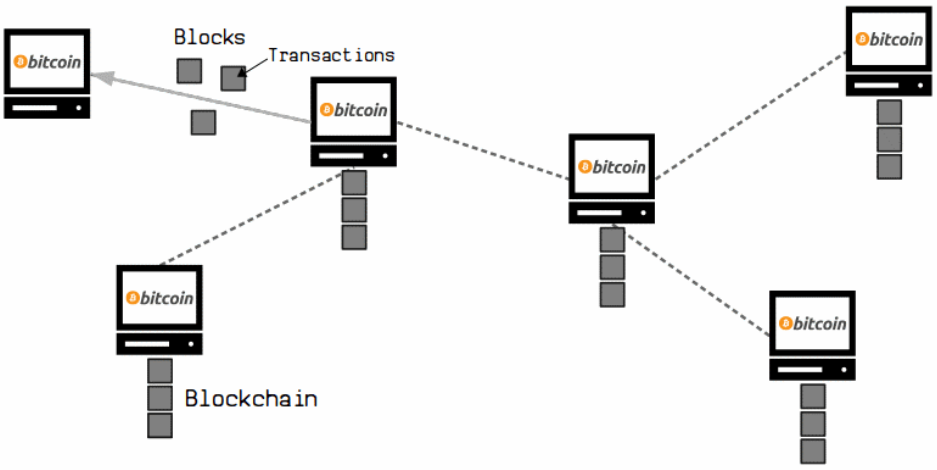
Bitcoin Core è il programma originale creato da Satoshi Nakamoto nel 2009

Quando si esegue Bitcoin Core, questo si connette ad altre persone che eseguono lo stesso programma, creando una rete di computer che comunicano tra loro.



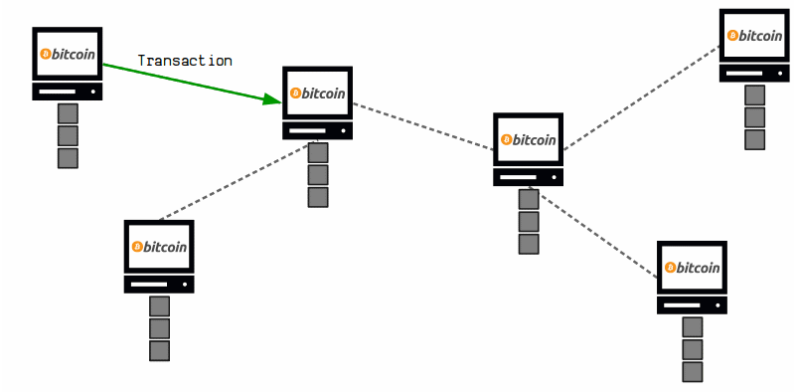
I computer del network sono chiamati nodi

La prima volta che esegui Bitcoin Core, inizierai a scaricare un file dagli altri nodi della rete. Questo file è chiamato blockchain, ed è un grande file contente tutte le transazioni.



Il file è composto da blocchi singoli, e ogni blocco contiene transazioni

Una volta scaricata e verificata l'intera blockchain, si può iniziare a fare transazioni, che si propagano nella rete e vengono scritte nella blockchain sul computer di tutti.



La blockchain è una memoria permanente per le transazioni

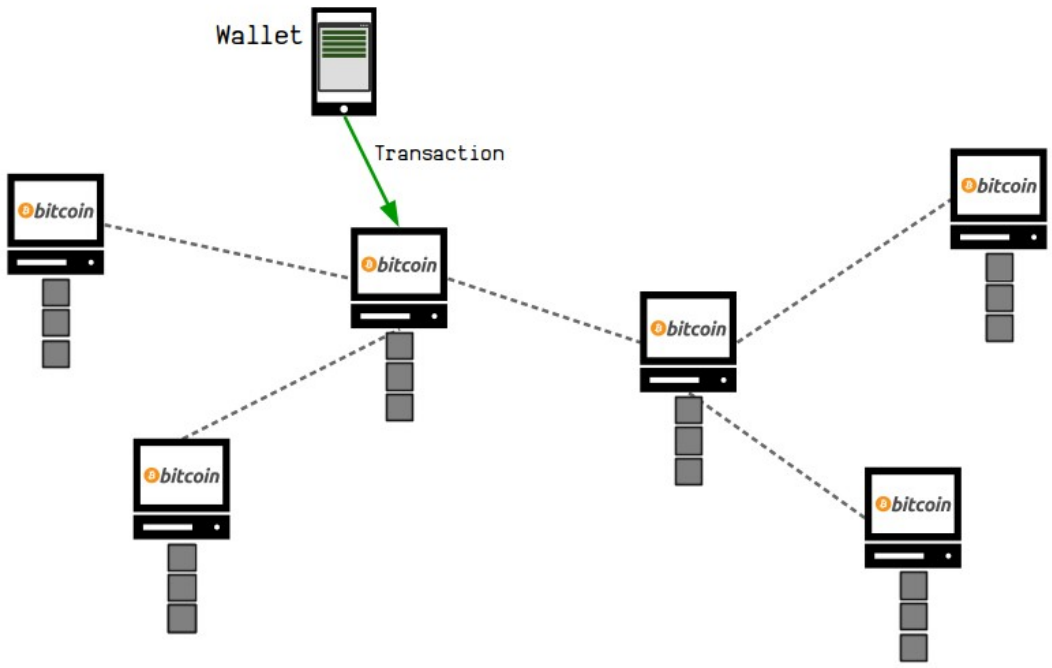
E queste sono le basi del Bitcoin.

Bitcoin Wallet

Il requisito per eseguire Bitcoin Core è che devi scaricare e memorizzare l'intera blockchain. Questa è una buona cosa, perché crea una copia extra della blockchain, e stai aiutando a trasmettere le transazioni anche ad altri computer.

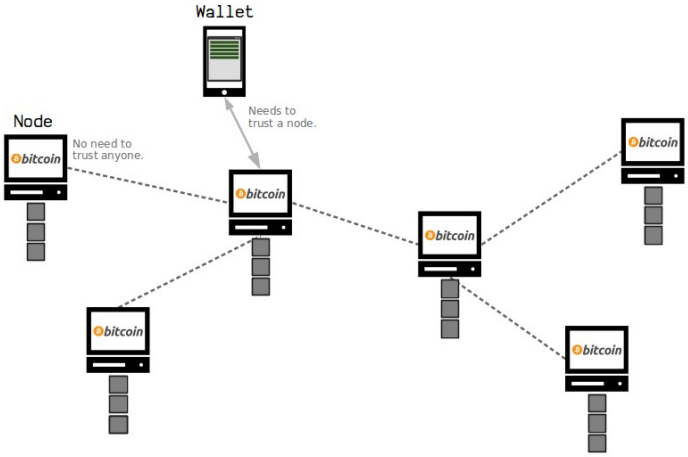
Tuttavia, non tutti hanno lo spazio sul disco rigido per memorizzare la propria copia della blockchain.

Quindi, invece di eseguire Bitcoin Core, si può usare "qualcosa" chiamato wallet o client leggero. I wallet permettono di inviare e ricevere bitcoin, ma senza aver bisogno dell'intera copia della blockchain.

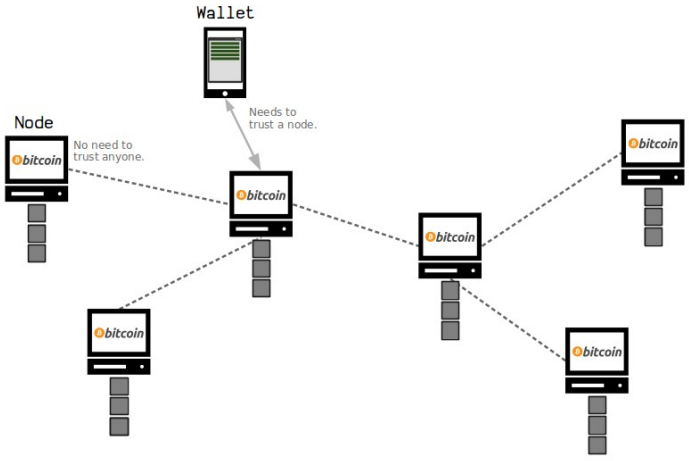


I wallet interagiscono con i nodi

Se si preferisce non eseguire un nodo completo, un portafoglio bitcoin detto anche light client è il modo più semplice per iniziare con i bitcoin



Qual è lo svantaggio di usare un portafoglio invece di Bitcoin Core?

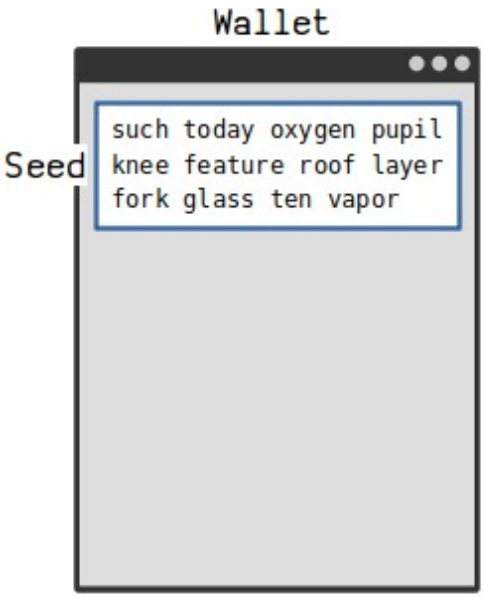


Bitcoin Core - Hai una copia di ogni transazione mai effettuata. Quindi puoi verificare ogni transazione che ricevi e vederle sul tuo computer, senza bisogno di fidarti di nessun altro.
Wallet- Il wallet ha bisogno di connettersi a un nodo per ottenere informazioni sulle transazioni. Ti stai quindi fidando del wallet e del creatore per connetterti ad un nodo onesto per ottenere i dettagli corretti della transazione.
Usare un wallet è il modo più comodo per usare bitcoin (è il modo in cui lo uso io), ma eseguire un nodo completo è il modo per usare bitcoin senza doversi fidare di nessuno (cosa che mi piace anche fare).

La scelta è personale.

Cosa fa un wallet?

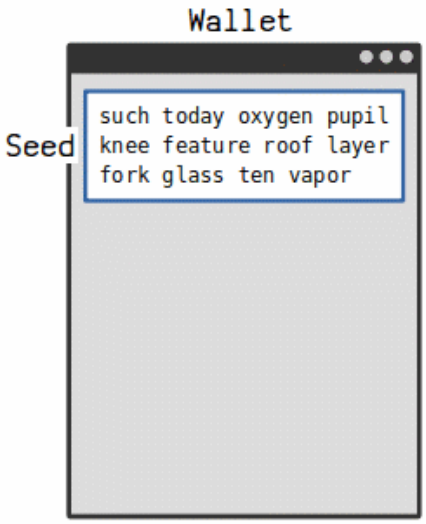
Quando inizi a usare un portafoglio bitcoin per la prima volta, ti verrà dato un seed. Questo seed è una lista generata casualmente di 12-24 parole che nessun altro al mondo ha mai visto.



Il tuo seed è unico, e viene usato per creare ogni indirizzo nel tuo portafoglio.

Un indirizzo è quello che dai alle persone in modo da poter ricevere bitcoin.

Ogni indirizzo ha la sua chiave privata, che viene usata quando invii i tuoi bitcoin a qualcun altro



Quindi, in breve, un portafoglio bitcoin gestisce le tue chiavi e indirizzi in modo che tu possa inviare e ricevere bitcoin.

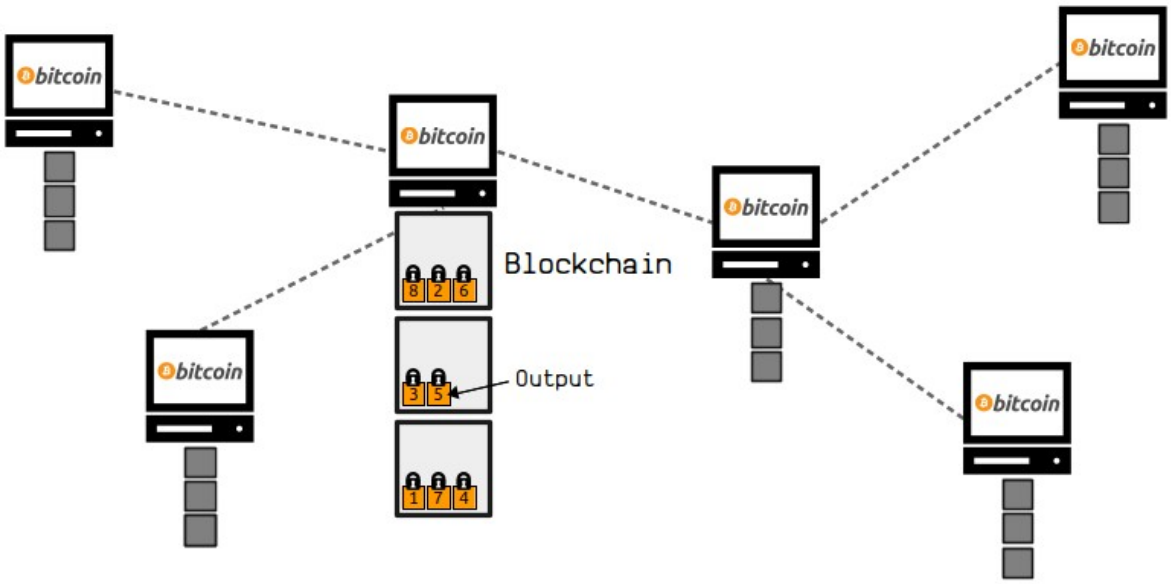
Suggerimento: se perdi il tuo portafoglio, puoi recuperare tutte le tue chiavi (e tutti i tuoi bitcoin) solo con il tuo seed.

Attenzione: Tieni il tuo seed al sicuro e non mostrarlo a nessuno. Se qualcuno ottiene il tuo seed può accedere ai tuoi bitcoin.

Come funziona Bitcoin?

Bitcoin è una rete di computer, e tutti lavorano insieme per condividere un file chiamato blockchain.

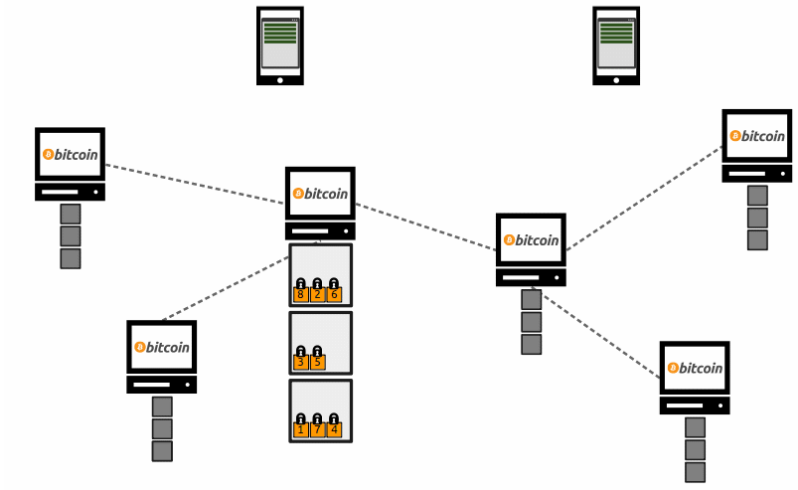
Si può pensare alla blockchain come a una gigantesca stanza di cassette di sicurezza, dove ognuna di queste cassette contiene una quantità di bitcoin e una serratura.



Le cassette sono chiamate output. Possono contenere qualsiasi quantità di bitcoin, e possono essere vincolate ad una varietà di chiusure

Quando fai una transazione, il tuo portafoglio seleziona, grazie alle chiavi private e pubbliche, una quantità di bitcoin dalla blockchain che ti appartiene, e crea una nuova cassetta di bitcoin per la persona a cui vuoi inviarli.

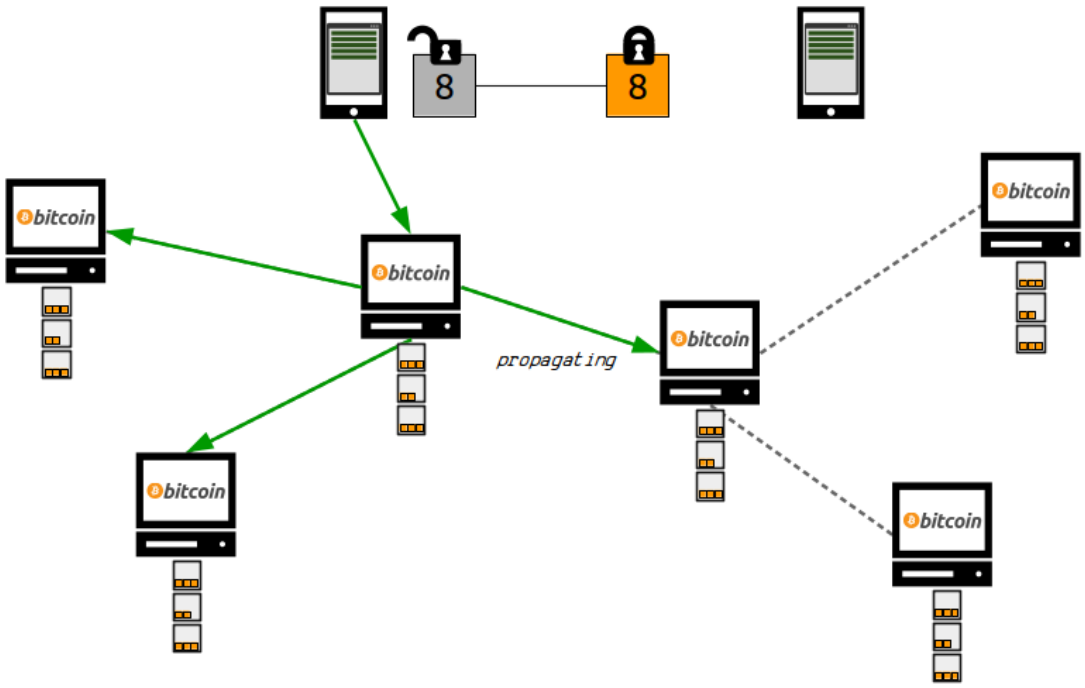
Il tuo portafoglio mette l'indirizzo dell'altra persona dentro il lucchetto della nuova cassetta, e usa la chiave privata necessaria per sbloccare la cassetta di bitcoin che è attualmente lockata al tuo indirizzo.



Le chiavi private e gli indirizzi si occupano dello sblocco e del blocco.

In altre parole, stai sbloccando la tua cassetta di sicurezza e creando una nuova cassetta di sicurezza per qualcun altro.

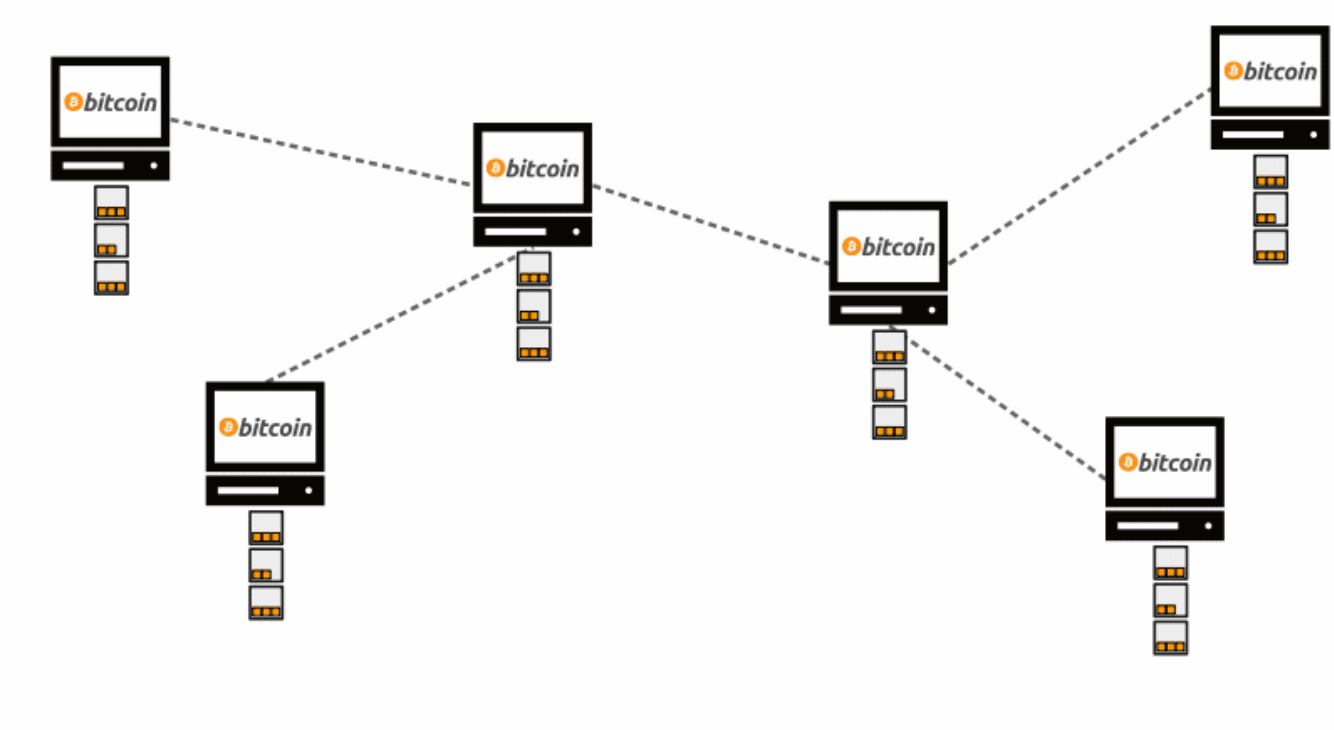
Comunque, questa transazione (che è solo un pacchetto di dati) viene inviata ad uno dei computer della rete, dove viene ritrasmessa da computer a computer fino a quando tutti sulla rete hanno una copia della tua transazione.



I nodi propagano i messaggi nella rete

Alla fine questa transazione si farà strada nelle blockchain di tutti.

Questo accade perché uno dei nodi della rete raccoglie le ultime transazioni che ha ricevuto in un blocco, e poi estrae questo blocco sulla blockchain (il che richiede energia). Poi condivide questo blocco minato con gli altri nodi della rete, che lo aggiungono anche alla loro blockchain.



Quindi, a intervalli regolari (un nuovo blocco di transazioni viene estratto nella blockchain ogni 10 minuti circa), ogni nodo della rete aggiornerà la sua blockchain con le ultime transazioni che sono state inviate alla rete. Questo processo si ripete più e più volte, così la blockchain cresce costantemente con nuove transazioni.

Ad ogni modo, una volta che una transazione entra nella blockchain non può essere rimossa, il che significa che la transazione è completa e i bitcoin sono passati di mano.

Ed è così che funziona il bitcoin.

Conclusioni

Se sei curioso circa Bitcoin come programma e vuoi sostenere la rete, allora scarica ed esegui Bitcoin Core.

Bitcoin Core

D'altra parte, se non sei a conoscenza degli sforzi per eseguire un full node e vuoi solo inviare e ricevere bitcoin, allora procurati un portafoglio.

Quale portafoglio scegliere? Tenersi sempre aggiornati

Personalmente gestisco un nodo sul mio computer di casa (perché mi piace imparare su Bitcoin e voglio sostenere la rete), ma uso un portafoglio per l'invio e la ricezione quotidiana di bitcoin. Raccomando di scaricare un portafoglio per iniziare, poi passare alla gestione di un nodo se si decide che si vuole imparare di più, partecipare alla rete bitcoin favorendone la decentralizzazione, avere più privacy (non si inviano le proprie master public key a sconosciuti) e sicurezza.

Nota: Questo sito web è dedicato all'interazione con un nodo Bitcoin Core e alla comprensione del suo funzionamento, ma per semplicità il resto di questa guida "per principianti" si concentrerà solo sull'uso di un portafoglio.

In ogni caso, il modo migliore per iniziare con Bitcoin è quello di usarlo davvero, e per fare questo avrete bisogno di ottenere i vostri primi bitcoin...