

Introduzione

Bitcoin è una nuova valuta davvero innovativa. Per il fatto che si basa su una rete aperta di computer, esiste unicamente su Internet. Chiunque abbia accesso a Internet può quindi inviare e ricevere denaro con la stessa facilità con cui può inviare un messaggio di posta elettronica. Grazie a questa nuova forma di denaro digitale, possiamo intravedere l'alba di una nuova era nel mondo della finanza.

Bitcoin è stata lanciata nel gennaio 2009, appena pochi mesi dopo la crisi finanziaria del 2008. Trattandosi di una valuta completamente *peer-to-peer*, può essere utilizzata in qualunque Paese del mondo, con la possibilità di trasferirla a chiunque altro. La sua stessa struttura garantisce che nessuno possa vedersi sottratti o bloccati i propri fondi. Gli effetti di questa innovativa valuta sono davvero sorprendenti. Abbiamo già assistito a un incremento di valore della valuta che, risalendo da meno di un centesimo di dollaro è balzata fino a oltre il migliaio di dollari. Fin dal suo lancio, Bitcoin si è trovata a sfidare il mondo della finanza “mainstream”. Originariamente concepita come “oro digitale”, la limitata disponibilità e la resistenza alla manipolazione di bitcoin hanno portato all'esplosione di nuove idee e progetti che hanno grandi potenzialità in grado di sovvertire e rivoluzionare campi importanti dell'economia e della finanza.

Il suo creatore anonimo, Satoshi Nakamoto, è noto solo per i suoi contributi, in particolare il whitepaper Bitcoin, e per i suoi post sui forum, che avevano lo scopo di guidare gli sviluppatori nelle loro attività di supporto e manutenzione del codice sorgente. Anche se nessuno può confermare la sua identità, il valore del suo lavoro è evidente per il fatto che il codice sorgente Bitcoin è stato collaudato e messo alla prova senza che siano stati rilevati bug o falle. Questa è una caratteristica davvero importante per una valuta.

Questo libro spiega la tecnologia Bitcoin da un punto di vista pratico. Inizieremo con un'introduzione semplice e alla portata di tutti, che comprende l'acquisto e la vendita di Bitcoin. Nella parte centrale del libro esamineremo i dettagli interni di Bitcoin, per mostrare il funzionamento delle sue varie parti. Nella parte finale esploreremo quindi vari modi in cui Bitcoin può essere impiegata come “valuta programmabile”.

Argomenti trattati

Il Capitolo 1, *Configurazione di un portafoglio*, introduce l'argomento Bitcoin, spiegando in termini semplici anche le specifiche attività di acquisto di bitcoin. Inoltre affronta gli

elementi che formano le basi della tecnologia Bitcoin, compresi gli indirizzi, le chiavi e i portafogli.

Il Capitolo 2, *Acquisto e vendita di bitcoin*, fa un passo in più e si occupa dell'acquisto e della vendita di bitcoin. Vengono introdotti anche i mercati e gli strumenti utili per gestire un portafoglio Bitcoin.

Il Capitolo 3, *Proteggere i bitcoin*, spiega come diventare *la propria banca*. Vengono introdotti e discussi vari approcci alla protezione dei bitcoin.

Il Capitolo 4, *Parliamo di blockchain*, alza letteralmente il “cofano” sulla tecnologia Bitcoin per mostrarne il funzionamento. Qui vengono illustrati e descritti gli algoritmi e le tecnologie su cui si basa Bitcoin.

Il Capitolo 5, *Installazione di un nodo Bitcoin*, è una guida dettagliata alla configurazione di un nodo Bitcoin, che consente di entrare a far parte della rete. Vengono inoltre introdotti alcuni elementi di base della programmazione Bitcoin.

Il Capitolo 6, *Le attività di mining*, guida attraverso le varie possibilità di mining di Bitcoin. Il capitolo si concentra sulle spese da affrontare per eseguire il mining e aiuta a valutare le possibilità di profitto.

Il Capitolo 7, *Programmazione Bitcoin*, approfondisce le potenzialità di Bitcoin come “valuta programmabile”. Il capitolo descrive la realizzazione di un semplice servizio di garanzia Bitcoin utilizzando JavaScript.

Il Capitolo 8, *Valute alternative*, presenta una panoramica di quattro valute alternative che si basano sul codice sorgente originale Bitcoin. Si conclude con un esempio riguardante la configurazione di un sistema di votazione, reso sicuro da una prova crittografica.

Prerequisiti per la lettura

Per seguire gli esempi di questo libro, avete bisogno solamente di un browser web aggiornato e di una connessione a Internet. Molti dei servizi Bitcoin menzionati nel libro possono essere gestiti via Web e possono operare solo potendo contare su un ambiente di connettività aggiornato. Per alcune operazioni e per l'autenticazione delle operazioni può essere necessario impiegare uno smartphone iOS o Android.

Per poter configurare e installare un nodo Bitcoin, è necessaria una connessione rapida a Internet e un computer dotato di un microprocessore di buona velocità. Il disco rigido deve avere almeno 50 GB di spazio libero, tenendo però presente che, con l'andar del tempo, la blockchain crescerà notevolmente di dimensioni.

Per i vari aspetti che riguardano la programmazione, è necessario dotarsi di un computer che dia accesso alla finestra Terminale. Apple OS X, Windows e Linux offrono questa possibilità. Vi sono anche alcuni strumenti aggiuntivi necessari per la configurazione, come Node.js, per poter seguire tutti gli esempi. In ogni caso, insieme agli esempi, vengono presentati gli strumenti richiesti.

Se siete interessati alla configurazione di una struttura di mining Bitcoin, dovrete dotarvi di apparecchiature molto specifiche. Alcune di queste possono essere difficili da reperire e il loro acquisto è tutt'altro che economico. Trattandosi di un mercato ancora agli esordi, ci si può però aspettare una notevole escursione in termini di prezzi e disponibilità. In ogni caso si consiglia di controllare sui forum e i mercati online, come eBay e Craigslist, per trovare informazioni sull'acquisto delle apparecchiature necessarie.

A chi è rivolto questo libro

Questo libro ha lo scopo di introdurre l'argomento Bitcoin a tutti coloro che hanno almeno un'esperienza di base in termini di home banking. In particolare la prima parte è rivolta a chi è completamente a digiuno di finanza digitale.

La seconda parte è rivolta a chi vuole conoscere tutte le potenzialità di Bitcoin.

Non è strettamente necessario essere programmatori o tecnici hardware per poter seguire gli ultimi capitoli, in quanto vengono sempre fornite spiegazioni semplici, corredate da utili illustrazioni. Per i lettori dotati di un maggiore background tecnico, vengono forniti script e note di installazione, utili per approfondire l'argomento Bitcoin.

Convenzioni

In questo libro troverete diversi stili di testo per distinguere i vari tipi di informazioni. Ecco alcuni esempi.

- Gli esempi di codice nel testo, i nomi di database, i nomi di cartelle, i nomi di file, le estensioni di file, i percorsi, gli indirizzi URL, gli input dell'utente e così via vengono presentati con un carattere monospaziato.
- Un blocco di codice ha il seguente aspetto:

```
// convert 'satoshi' to bitcoin value
var satoshiToBTC = function(value) {
    return value * 0.00000001
}
```

- I comandi da inserire alla riga di comando del Terminale e il relativo output è scritto nel seguente modo:

```
~ npm install bitcoinjs-lib -g
```

- I nuovi termini e le parole chiave vengono presentati in *corsivo*. Sempre in corsivo vengono presentati i comandi da selezionare nel software o nelle pagine web.

NOTA

Gli avvertimenti, le annotazioni importanti, i trucchi e i suggerimenti vengono presentati, nel testo, nel seguente modo.

Scarica i file degli esempi

Sul sito dell'editore originale inglese, Packt Publishing, potete scaricare i file degli esempi presentati del testo. Per farlo è necessario registrarsi gratuitamente all'indirizzo <https://www.packtpub.com/register>. Quindi andate sulla scheda del libro all'indirizzo <https://www.packtpub.com/hardware-and-creative/learning-bitcoin> (o per comodità <http://bit.ly/packt-bitcoin>) e fate clic su *Code Files*.

In caso di problemi potete anche scaricare una copia dei file dal nostro sito, ma ricordate che potrebbe non essere aggiornata a eventuali update o rettifiche implementati dall'autore dopo la prima pubblicazione del volume: l'indirizzo è <http://bit.ly/apo-bitcoin>.

L'autore

Richard Caetano è un imprenditore e sviluppatore software attivo a Parigi ma nato e cresciuto in una fattoria in California. Ha maturato un forte interesse nello sviluppo software fin dalla più tenera età. Nel corso degli anni ha progettato sistemi che vanno dall'automazione delle attività agricole alla contabilità, alla sicurezza, alla musica digitale e ai videogiochi per smartphone.

Nel 2011, Richard ha scoperto il whitepaper Bitcoin e questo ha completamente cambiato la sua vita. Dopo aver compreso le potenzialità di questa tecnologia, ha cambiato strada e da allora sta lavorando per far conoscere Bitcoin in tutto il mondo.

Ha lanciato una prima applicazione, chiamata *btcReport*, che sfruttava la propria struttura per fornire notizie e informazioni a coloro che fossero interessati a Bitcoin. Da allora ha tenuto ovunque conferenze e meeting sul tema.

Nel 2015 ha lanciato *Stratumn*, una società che si occupa di aiutare gli sviluppatori a realizzare applicazioni trasparenti, facili da verificare e sicure basate su blockchain, la tecnologia su cui si fonda la valuta bitcoin.

I revisori

Francesco Canessa è uno sviluppatore software esperto in Bitcoin e tecnologie blockchain. I suoi strumenti di lavoro preferiti con Bitcoin sono Bitcoin Core tramite la sua API JSON, per la sua solidità e semplicità, e la libreria JavaScript Bitcore per creare agili software per portafogli lato client.

Poiché crede che Bitcoin e blockchain siano innovazioni importanti per i nostri tempi, realizza progetti open-source (per esempio *BitNFC* – <http://bitnfc.org>) per ricercare e dimostrare le vere potenzialità di queste tecnologie e trovare nuovi modi per spingere l'adozione di Bitcoin.

Ha lavorato come traduttore principale dell'edizione italiana di *Mastering Bitcoin*, O'Reilly Media, scritta da Andreas M. Antonopoulos.

Il suo linguaggio di programmazione preferito è Ruby e i suoi hobby sono l'Internet delle Cose e la creazione di stampanti 3D.

Jose Celano ha iniziato a lavorare con i computer all'età di 10 anni, con un Commodore 64. Si è laureato in Ingegneria Tecnica su Sistemi Informatici presso l'Università de Las Palmas de Gran Canaria.

Ha creato una società IT (*iQ ingenieros*) nel 2004 dopo aver terminato gli studi e vi ha lavorato per 10 anni, principalmente sviluppando applicazioni web. È sempre stato interessato ai sistemi di pagamento via Internet e allo sviluppo web.

Nel settembre 2013 ha iniziato a studiare l'argomento Bitcoin. Nel febbraio 2014 è diventato free-lance e ha iniziato a lavorare su progetti Bitcoin. Da qualche tempo Jose lavora come consulente PHP per BlockCypher, una startup di San Francisco che fornisce servizi web blockchain, per consentire agli sviluppatori di realizzare con facilità applicazioni blockchain affidabili.