Bitcoin

Para leigos

Tradução da 2ª Edição

Peter Kent e Tyler Bain

ALTA BOOKS
GRUPO EDITORIAL
Rio de Janeiro, 2023

Sumário Resumido

NESTE CAPÍTULO

- **Descobrindo a história das moedas digitais**
- **Aprendendo sobre o início do Bitcoin e seu criador**
- **Entendendo o que o dinheiro (e o Bitcoin) é e não é**
- **Explorando os benefícios do Bitcoin**

Capítulo 1
Bitcoin em Resumo

Para um mero adolescente, a rede Bitcoin certamente teve um grande impacto no mundo, movimentando mais de US$12,4 trilhões somente em 2021. Ao escrevermos estas palavras, o Bitcoin tem uma *capitalização de mercado* (valor total) de US$918.705.395.133, o que é quase um trilhão de dólares. (A capitalização de mercado é o número total de Bitcoins em "circulação" multiplicado pelo preço de mercado atual de um único Bitcoin.)

Mas esse é um preço atualmente baixo; apenas algumas semanas antes, ele tinha um valor combinado de quase US$1,3 trilhão. Quando você estiver lendo este livro, o valor pode ser maior, menor ou o mesmo. Essa é uma das coisas sobre Bitcoin: seu preço de mercado pode ser muito volátil, como você logo aprenderá se passar um pouco de tempo observando os mercados.

Mas o impacto do qual estamos falando não se refere apenas ao valor de mercado atual do Bitcoin. Na verdade, o valor de mercado da Apple, Inc. é mais de três vezes maior do que o da rede Bitcoin. No entanto, uma comparação com a Apple pode ser apropriada no momento. A Figura 1-1 mostra quanto Bitcoin seria necessário para comprar uma única ação da Apple, de 2010 até 2021. O valor de um único Bitcoin tem aumentado em relação às ações da Apple (assim como, naturalmente, em relação ao dólar norte-americano e outras moedas governamentais).

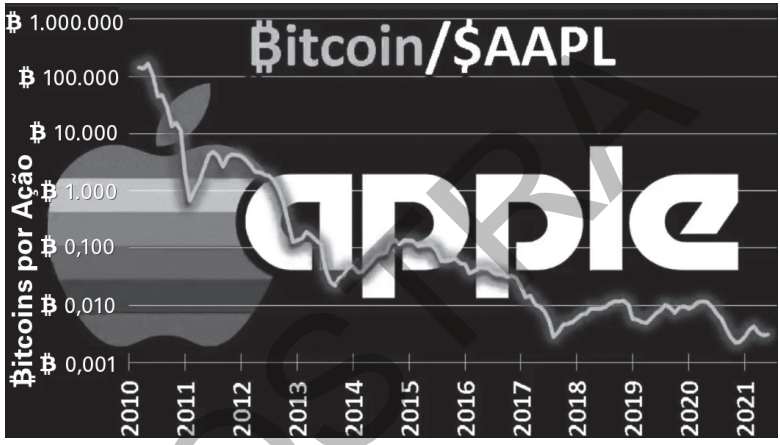

FIGURA 1-1: Quanto Bitcoin é necessário para comprar uma ação da Apple?

O lançamento do Bitcoin desencadeou uma revolução no blockchain e nas criptomoedas. Existem agora mais de 13 mil criptomoedas. (A maioria, fique avisado, é essencialmente sem valor e continuará assim.) No momento de redação deste livro, as cinco principais criptomoedas têm uma capitalização de mercado combinada de quase US$1,7 trilhão de dólares, e diversas criptomoedas têm funções genuinamente úteis além de serem usadas meramente como dinheiro ou uma reserva de valor. É provável que algumas delas perdurem, mesmo que a maioria não o faça.

Porém, estamos aqui para falar do Bitcoin, então vamos começar com um pouco de história. De onde ele veio e como se desenvolveu?

No Princípio, Havia... Moedas Digitais?

As criptomoedas baseadas em blockchain são bem novas, mas as moedas digitais projetadas para uso online já existem há bastante tempo. (Não se preocupe por enquanto com essa coisa da *blockchain*; explicaremos isso em detalhes não tão estarrecedores no Capítulo 2. Por ora, basta entender que um blockchain é um tipo especial de banco de dados, um armazenamento de dados digitais.)

Quando as pessoas começaram a encher os espaços online — o processo começou no início dos anos 1980, mas realmente decolou em 1994 com o advento da internet comercial —, ficou claro que elas precisariam de alguma forma para gastar dinheiro no ciberespaço (as primeiras lojas virtuais abriram naquele ano). É claro que a maioria das transações online hoje em dia usa cartões de crédito e débito — até mesmo PayPal e PagSeguro estão essencialmente permitindo tais transações, juntamente com transferências bancárias —, mas isso não era o caso nos primeiros dias. Muitas pessoas estavam preocupadas com o roubo de cartões de crédito e, portanto, desconfiadas de usar seus números online, por exemplo. (Quando o coautor Peter abriu uma loja online em 1997, ele tinha um gateway de cartão de crédito funcional, mas muitos clientes imprimiam um formulário de pedido em papel e enviavam um cheque pelo correio!)

Havia também a questão das *microtransações*. Certamente, no mundo digital, deveria ser possível pagar a alguém, digamos, cinco ou dez centavos por algo, como o acesso a um vídeo ou artigo. O problema das microtransações ainda não foi resolvido em muitos lugares (embora seja possível argumentar que a rede Bitcoin Lightning, que discutimos no Capítulo 4, quase nos leva até lá), mas, no entanto, essa é uma das ideias que impulsionaram o desenvolvimento das moedas digitais.

E elas se desenvolveram. Em 1983, David Chaum escreveu um artigo de pesquisa sobre o conceito das moedas digitais (*Blind Signatures for Untraceable Payments — Assinaturas Cegas para Pagamentos não Rastreáveis*), sugerindo o uso de criptografia para criar e gerenciar uma moeda digital. Assim, mesmo naquela época, a criptografia tinha um papel nas moedas digitais, embora não fossem conhecidas como criptomoedas então. Quando você ouve as pessoas falando sobre criptomoedas, elas

geralmente estão falando dessa nova geração de criptomoedas baseadas em blockchain que começaram com o Bitcoin. (Explicamos mais sobre criptografia e como ela se relaciona com as criptomoedas no Capítulo 2.)

Chaum de fato lançou uma moeda digital baseada em criptografia em 1990, conhecida como *DigiCash*, mas eram dias ainda muito iniciais. Pouquíssimas pessoas estavam online em 1990, e a moeda morreu por volta de 1998. O que provavelmente prejudicou as moedas digitais no fim dos anos 1990 foi que as empresas de cartões de crédito queriam participar da ação online e, assim, se esforçaram para amenizar o medo dos consumidores de usar cartões de crédito na internet.

Ainda outras moedas digitais apareceram. Havia o e-gold, uma moeda apoiada por ouro real, e o Millicent, uma moeda criada por uma grande empresa de computação, a Digital Equipment Corporation (DEC). (Se você é mais jovem do que, digamos, 30 e poucos anos, provavelmente não se lembrará da DEC, mas ela era muito importante. Na verdade, até mesmo a IBM tinha uma divisão de micropagamentos trabalhando com moedas digitais na época.)

Depois, houve o NetBill, um projeto da Universidade Carnegie Mellon que mais tarde foi fundido em outro sistema, o CyberCash, que acabou ficando nas garras do PayPal. Houve o Beenz, que tinha uma parceria com a MasterCard a certa altura, o First Virtual, o CyberCoin, o Flooz (promovido por Whoopi Goldberg, não menos!), e vários outros.

Mas nada *durou* muito. Diversas grandes ideias, mas ninguém conseguiu fazer tudo *funcionar*. No início dos anos 2000, a maioria desses esforços era moribunda (algo provavelmente desencadeado pelo crash das pontocom no fim de 2000). Havia exceções. A Liberty Reserve, com sede na Costa Rica, funcionou de 2006 até 2013, mas foi fechada após acusações de que estava sendo usada para lavar bilhões de dólares de lucros criminosos. E sistemas fechados que funcionam em redes particulares, como as Moedas QQ da China, são usados principalmente no serviço de mensagens Tencent QQ Messaging.

Mas então, havia Satoshi Nakamoto e seu mágico blockchain.

O Nascimento do Bitcoin

No dia 1º de novembro de 2008, alguém chamado Satoshi Nakamoto postou uma mensagem em um fórum sobre criptografia intitulada *Bitcoin P2P e-cash paper* (arquivada em `https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html`). Nela, Nakamoto anunciava que "vinha trabalhando em um novo sistema de dinheiro eletrônico que é totalmente peer-to-peer, sem autoridade central".

Em outras palavras, ele havia criado um sistema monetário que funcionava em uma rede de pares — computadores trabalhando em conjunto, sendo cada um igual ao outro. Sem poder central, nenhum banco ou governo para agir como uma "autoridade central" era necessário.

Um comentário que ele fez no post explicou sua visão do problema com as criptomoedas anteriores. "Muitas pessoas descartam automaticamente a moeda eletrônica como causa perdida por causa de todas as empresas que fracassaram desde os anos 1990", escreveu. Ele acreditava que esses outros sistemas de dinheiro digital tinham uma fraqueza crucial, um calcanhar de Aquiles. "Espero que seja óbvio que foi apenas a natureza controlada central desses sistemas que os condenou. Acredito que esta é a primeira vez que estamos tentando um sistema descentralizado, não baseado em confiança."

PAPO DE ESPECIALISTA

Nakamoto havia criado um nome de domínio e um site simples, bitcoin.org, onde postou um documento explicando como tudo isso funcionaria: `https://bitcoin.org/bitcoin.pdf` [veja a versão em português aqui: `https://bitcoin.org/files/bitcoin-paper/bitcoin_pt_br.pdf`]. É bom você dar uma olhada, embora não seja essencial para sua compreensão do Bitcoin (há algumas partes bem técnicas no artigo).

O whitepaper que ele publicou descreve como um *blockchain* (uma forma especial de banco de dados) poderia ser usado para gerenciar a moeda. Essencialmente, o blockchain registra um livro-razão, um registro de transações de moeda, e visto que o blockchain é duplicado em diversos computadores (os *pares*, ou *peers*) e que esses pares são todos iguais, não é necessária a confiança em uma parte central. Você pode ouvir descrições do Bitcoin como sendo um sistema "sem confiança". Isso não significa que não podemos confiar nele, mas que uma autoridade central não é necessária. A confiança, de fato, está incorporada no

sistema. A matemática — ou matemágica, como Peter gosta de chamar — que alimenta o sistema significa que *podemos* confiar nas transações do Bitcoin, mesmo sem uma "autoridade" central supervisionando o sistema (veja o porquê disso no Capítulo 2).

LEMBRE-SE

Satoshi Nakamoto (seja lá quem for essa pessoa ou "coisa") não usou as palavras *criptomoeda*, *blockchain* ou *sem confiança* ao longo de seu whitepaper. Esses termos foram aplicados ao sistema posteriormente por outras pessoas.

Na verdade, a ideia da cadeia do blockchain já existia havia algum tempo — pelo menos desde 1991. Lembra-se de David Chaum do famoso DigiCash? Ele vinha trabalhando na ideia de um blockchain desde o início dos anos 1990.

De qualquer forma, Nakamoto não parou por aí. Em janeiro de 2009, ele/ela lançou a rede Bitcoin. Nakamoto lançou cerca de 30 mil linhas de código que definiam os protocolos e processos de rede necessários para operar esse sistema de dinheiro descentralizado e peer-to-peer. E assim, o Bitcoin nasceu.

É claro, em janeiro de 2009, o Bitcoin não tinha essencialmente nenhum valor. Ainda assim, o *bloco gênesis* criado por Nakamoto (o primeiro bloco de dados no blockchain gerando os primeiros 50 Bitcoins), juntamente com os blocos de dados subsequentes "minerados" por Nakamoto (veja o Capítulo 7), compreendem talvez um milhão de Bitcoins: a preços atuais, são US$47.369.000.000. Sim, perto de 50 bilhões de dólares!

Mas Quem É Nakamoto?

Então, quem é esse Satoshi Nakamoto? Ninguém sabe. Bem, alguém deve saber, mas ou não está dizendo ou não conseguiu convencer ninguém. Na verdade, nem mesmo está claro *o que* Satoshi Nakamoto é. Um homem? Uma mulher? Um grupo de colaboradores? Uma organização ou empresa? Não sabemos ao certo, embora a maioria das suposições indique ser um homem ou um grupo de duas ou três pessoas. Talvez não surpreendentemente, os alvos mais citados sejam geralmente criptógrafos e matemáticos.

Há o próprio Satoshi Nakamoto, é claro — essa foi uma escolha óbvia. Um nipo-americano residente na Califórnia que nasceu Satoshi Nakamoto, e agora se chama Dorian Prentice Satoshi Nakamoto, parece ter algumas das habilidades necessárias para ser o Nakamoto, mas ele nega ser o fundador do Bitcoin.

Depois, há Nick Szabo, um entusiasta da moeda digital que foi marcado como Nakamoto, mas nega ser o fundador do Bitcoin. Elon Musk também foi "acusado", mas ele nega (e nós pessoalmente achamos que ele provavelmente estava muito ocupado para encontrar o tempo necessário!). Há o matemático japonês Shinichi Mochizuki (ele nega), o sociólogo econômico finlandês Dr. Vili Lehdonvirta (nega) e o estudante de criptografia irlandês Michael Clear (sim, nega).

Um dos candidatos mais barulhentos é Craig Wright, um cientista da computação australiano. Ele certamente afirma que é Nakamoto, embora seja acusado por muitos de realizar uma fraude elaborada. No momento de redação deste capítulo, um júri declarou Wright culpado, e ele teve que pagar US$100 milhões à família de David Kleiman, um amigo falecido, por uso indevido de fundos em uma joint venture na qual eles trabalharam. Mas separadamente, o júri também considerou que David Kleiman não estava relacionado com a criação do Bitcoin.

No entanto, o júri não descobriu se Craig Wright *é* Nakamoto — apenas que, caso seja, não precisa dividir seus US$50 bilhões com a família de Kleiman. Não é um mau negócio. Na verdade, é um negócio tão bom, que Wright declarou que estava *aliviado* pelo fato de que tudo o que precisava pagar eram os US$100 milhões! Mesmo assim, o caso não está encerrado. Não está claro se o patrimônio de Kleiman tem realmente a propriedade da empresa em joint venture, e Wright pode dever US$100 milhões de dólares à sua ex-mulher. Isso não resolve a questão sobre se Wright de fato é ou não Nakamoto. (Wright diz que o júri considerou que ele *é* Nakamoto; o juri nega.) Isso não será resolvido até que Wright — ou o *verdadeiro Satoshi Nakamoto* — movimente parte dos Bitcoins dos endereços no blockchain que pertencem a Nakamoto.

Independentemente disso, a rede Bitcoin continuou a funcionar como projetada muito depois que Satoshi Nakamoto parou misteriosamente de participar dela, pouco depois de afirmar que Julian Assange e o Wikileaks haviam "chutado o ninho dos vespões", uma vez que começaram a aceitar Bitcoin como doações para sua controversa reportagem em 2010.

Entendendo o Que o Bitcoin Realmente É

Então, o que é Bitcoin? Bem, podemos lhe dizer muito rapidamente o que ele não é. Não é tangível — não há nada que você possa tocar ou segurar. Você não pode prová-lo ou cheirá-lo. Você não pode nem mesmo vê-lo. Na verdade — e explicamos isso com mais detalhes no Capítulo 2 —, o Bitcoin realmente *não é*. Quer dizer... *não existe Bitcoin*.

O que existe, porém, é algo conhecido como o *livro-razão* ou *ledger* do Bitcoin (outra palavra, a propósito, que Satoshi Nakamoto não usou em seu famoso whitepaper, mas é assim que os dados armazenados nos blockchains do Bitcoin passaram a ser popularmente conhecidos). Um livro-razão é um registro escrito de transações; o pequeno registro de seu livro de cheques é uma forma de livro-razão, por exemplo (para aqueles com menos de 30 anos, um cheque é um pedaço de papel no qual você pode escrever um número, assinar seu nome e dar a alguém, que pode então entregá-lo ao banco, e o banco dá dinheiro a esse alguém... um sistema incrivelmente eficiente). Ou considere um extrato bancário, mostrando dinheiro entrando e saindo de sua conta (*saindo*, na maioria das vezes). Isso também é uma forma de livro-razão.

Sendo assim, quando Satoshi Nakamoto criou o primeiro Bitcoin, como ele o criou? Bem, quando falamos sobre Bitcoin ser "criado", estamos realmente falando de forma abreviada. Nenhuma *coisa* de Bitcoin foi criada. Quando Nakamoto "criou" o primeiro Bitcoin, o que ele realmente fez foi criar um conjunto de regras para um livro-razão no qual ele *registrou* a criação do Bitcoin. O livro-razão diz, na verdade, "50 novos Bitcoin foram criados hoje". E aí está, o Bitcoin existe.

Quando Nakamoto cunhou aquele primeiro "bloco gênesis", a natureza da rede foi definida. Enterrado no primeiro bloco de dados estava um pequeno texto adicional, palavras da primeira página do *New York Times* daquele dia (3 de janeiro de 2009): "Ministro prestes a fazer segundo resgate financeiro de bancos." Talvez essa tenha sido uma dica do motivo pelo qual Nakamoto tenha criado a rede, como uma alternativa ao que ele achava que eram os sistemas monetários corruptos gerenciados pelo governo.

O livro-razão registra essencialmente duas coisas. A primeira é a *criação* do Bitcoin, que é feita por meio de um processo chamado "mineração". Nakamoto "minerou" os 50 Bitcoins originais (no entanto, esses não podem ser usados, devido à natureza do código). A mineração continua, e, de fato, novos Bitcoins são criados sempre que um novo bloco de transações é adicionado ao blockchain do Bitcoin, a cada 10 minutos ou mais. (O capítulo 7 explica como esse processo de "mineração" funciona.)

No entanto, há um arranjo matemático em tudo isso: os Bitcoins são criados de forma consistente, e a cada quatro anos ou mais (durante um evento chamado *halving*), o número de Bitcoins criados a cada 10 minutos é reduzido pela metade. Neste momento, 6,25 Bitcoins são criados a cada 10 minutos, mas em algum momento em 2024, serão reduzidos para 3,125, depois novamente reduzido pela metade quatro anos depois, e assim por diante (a cada quatro anos) até cerca do ano 2140, quando o número máximo de Bitcoins estará finalmente em circulação.

MOEDA FIDUCIÁRIA?

Fique na comunidade Bitcoin o tempo suficiente e, mais cedo ou mais tarde, ouvirá as pessoas falando sobre moeda *fiduciária*, ou *fiat money*, geralmente, de forma depreciativa. Uma moeda fiduciária é aquela estabelecida por decreto, por ordem oficial. Ela é emitida por um governo, sem ter lastro com uma mercadoria como o ouro. (Para citar o economista ganhador do Prêmio Nobel Paul Krugman, "as moedas fiduciárias têm valor subjacente porque os homens com armas dizem que têm".) A maioria das moedas hoje em dia é fiduciária; o "padrão ouro" caiu em desuso geral na década de 1930, durante a Grande Depressão. (A Grã-Bretanha abandonou o padrão ouro em 1931.) O dólar norte-americano costumava ter lastro em prata, mas em 1900, foi aprovada uma lei ligando-o ao ouro. Ele permaneceu assim durante a maior parte do século, até ser completamente desvinculado do ouro em 1971 e se tornar uma moeda fiduciária. (Entretanto, em 1934, os EUA desvalorizaram o dólar em relação ao ouro; ou seja, reduziram o peso do ouro por dólar.)

A vantagem da moeda fiduciária é que ela dá aos governos mais controle sobre a oferta de dinheiro. Muitos economistas, provavelmente a maioria, acreditam que a adesão ao padrão ouro prolongou a Grande Depressão, já que os governos não foram capazes de estimular suas economias aumentando a oferta de dinheiro. A desvantagem, de acordo com muitos verdadeiros crentes em Bitcoin, é que ela proporciona aos governos muito controle sobre a oferta de dinheiro!

A segunda coisa que o livro-razão registra é o que acontece com o Bitcoin após ter sido criado. Como discutimos no Capítulo 2, cada Bitcoin está associado a "endereços" no blockchain, e à medida que as pessoas compram e vendem Bitcoins, ou os usam para comprar algo (basicamente o mesmo que vender Bitcoin), as moedas são enviadas de um endereço para outro no blockchain. O livro-razão do Bitcoin mantém um registro do fluxo do Bitcoin, de endereço para endereço. Cada endereço está sob o controle de alguém, e, portanto, o blockchain, na verdade, está mantendo o controle de quem é dono do quê. Se o livro-razão do blockchain do Bitcoin diz que o endereço que você controla tem 2 Bitcoins associados a ele, então você controla esses 2 Bitcoins. (Nos Capítulos 3 e 4, explicamos como exercer esse controle — ou seja, como você pode transferir seus Bitcoins para outros endereços para obter moeda fiduciária do governo ou bens e serviços.)

Agora, se tudo isso soa um pouco confuso, como se fosse um pequeno jogo de trapaça — e certamente há muitas pessoas que lhe dirão que o Bitcoin é uma "pirâmide" —, explicaremos dentro de alguns instantes o que é *dinheiro*. Você pode pensar que sabe o que é, mas provavelmente não sabe, e sem entender o que é dinheiro, é difícil entender como Bitcoin *pode ser* dinheiro. Mas primeiro, um pouco mais sobre o Bitcoin.

Entendendo as Unidades de Bitcoin

Para começar, você precisa entender que o Bitcoin pode ser decomposto e comprado e vendido em pedacinhos. Um Bitcoin não é como uma moeda de ouro; se, por exemplo, você comprar uma moeda de ouro, estará comprando a coisa toda. Você não pode comprar a metade ou uma fração.

Mas com o Bitcoin, que pode ser vendido a US$50 mil ou US$60 mil, ou seja qual for o valor *por moeda*, a maioria das pessoas não pode se dar ao luxo de comprar se tiver que adquirir a coisa toda. E em qualquer caso, não há *moeda*. É apenas uma entrada no livro-razão.

Dessa forma, a entrada no livro-razão pode dizer o que quisermos que diga. Pode dizer que você comprou meio Bitcoin, ou um décimo ou centésimo, ou um décimo milésimo, ou até um centésimo milionésimo. Ou seja, você pode comprar moedas parciais — fragmentos de um Bitcoin. A Tabela 1-1 traz um panorama sobre as unidades de Bitcoin.

TABELA 1-1 **Unidades de Bitcoin**

Unidade	Nome da unidade
1; um	Bitcoin, BTC, B
1/10; um décimo	deciBitcoin, dBTC
1/1.000; um milésimo	milliBitcoin, millibit
1/1.000.000; um milionésimo	microBitcoin, µBTC, bit
1/100.000.000; um centésimo milionésimo	Satoshi, sat

A tabela não mostra todas as unidades, mas essas são as que você provavelmente verá e sobre as quais mais ouvirá. Como os Bitcoins são divididos em Satoshis — 100 milhões de Satoshis em cada Bitcoin —, você pode dividir um Bitcoin em décimos: deciBitcoin, centiBitcoin, milliBitcoin, microBitcoin, e assim por diante. (Na verdade, existe até uma forma teórica de dividir um Bitcoin abaixo do nível Satoshi em *milliSatoshi*, utilizando uma rede auxiliar especial chamada Lightning Network, da qual falamos no Capítulo 4.)

Será que existe o suficiente da menor unidade de Bitcoin para todos? Bem, vamos dar uma olhada. Haverá apenas 21 milhões de Bitcoins; isso significa que haverá, no máximo, 2.100.000.000.000.000 de Satoshis em circulação.

Hoje, porém, cerca de 19 milhões de Bitcoins estão em circulação, e há algo em torno de 1.900.000.000.000.000 Satoshis.

Com cerca de 8 bilhões de pessoas vivendo no planeta, há hoje cerca de 237.500 Satoshis em circulação por pessoa (o número varia; consulte o relógio Satoshi em `https://satoshisperperson.com/` — em inglês). Neste momento, equivale a US$54.

Para colocar isso em perspectiva, cerca de US$2,5 mil estão em circulação (oferta de dinheiro "M1") por pessoa no planeta hoje (de acordo com o site do Federal Reserve dos EUA, disponível em `https://fred.stlouisfed.org/series/M1SL` — em inglês). Isso representa 250 mil centavos por pessoa, semelhante ao número de Satoshis.

LEMBRE-SE

Tudo isso significa que você não precisa de uma grande soma de dinheiro para começar com Bitcoin. Você pode comprar pedacinhos de um Bitcoin, mas tenha cuidado com as taxas. Comprar pequenas quantidades em uma exchange tradicional (veja o Capítulo 3) pode ser caro; em alguns

casos, você provavelmente pagará mais em taxas do que pelo próprio Bitcoin. Há atualmente algumas exchanges que oferecem transações gratuitas*. Consulte, por exemplo, a Strike (`https://strike.me/en` — conteúdo em inglês).

Criptomoeda ou Criptoativo?

O Bitcoin é comumente descrito como uma criptomoeda. É realmente uma moeda? Nós argumentaríamos que não. Fornecemos mais detalhes sobre isso no Capítulo 3, mas, pelo menos no momento, você pode considerar o Bitcoin mais como um ativo do que uma moeda. É mais parecido com o ouro do que com notas de real ou dólar. É difícil gastar o Bitcoin, assim como é difícil gastar o ouro. Claro, você pode fazer isso, mas nem sempre é simples, e a maioria dos lugares onde você gostaria de gastar seus Bitcoins não o aceitam.

E além disso, por que você quer gastar seus Bitcoins quando ele pode dobrar ou triplicar de valor durante os próximos meses? Não, o Bitcoin não é uma moeda verdadeira, embora tenha sido originalmente destinado a ser uma (e talvez no futuro se torne uma).

O Google e o dicionário Oxford Languages descrevem *moeda* como "um sistema de dinheiro em uso geral em determinado país". Bitcoin certamente não é uma moeda na Europa ou na América do Norte ou do Sul. Talvez o único país em que ele se aproxima de ser uma moeda é El

---

***Nota da Editora:** Desconfie de sites ou apps que ofereçam transações gratuitas, pois eles estão ganhando dinheiro de alguma forma, seja cobrando um spread (vendendo bitcoins a você por um preço maior do que o mercado) ou vendendo seus dados. Assim, recomendamos o uso de uma exchange que deixe claro estar cobrando por seus serviços. A seguinte lista pode facilitar sua pesquisa: https://cointradermonitor.com/taxas-exchanges.

Salvador, cujo governo lançou o Bitcoin como moeda secundária. Mas, para a maioria de nós, o Bitcoin é uma *reserva de valor*, não algo que vamos usar no supermercado.

Ainda assim, no Capítulo 3 falaremos sobre como você pode comprar e vender Bitcoin — e vender Bitcoin é essencialmente o mesmo que trocá-lo (você o troca por bens ou serviços).

Se o Bitcoin Não Existe, Como Pode Ser Valioso?

No momento de redação deste capítulo, qualquer pessoa que tenha um Bitcoin pode vendê-lo por cerca de US$24 mil. Mas acabamos de lhe dizer que o *Bitcoin não existe*... que tudo o que existe é um livro-razão declarando que o Bitcoin existe e quem (qual endereço no blockchain) o possui. Como isso pode ter valor!?

Para entender isso, precisamos entender um pouco sobre o dinheiro e como ele funciona. Como ocorre com *qualquer* forma de dinheiro, o Bitcoin tem tudo a ver com *crença*. Se um número suficiente de pessoas acredita que uma forma de dinheiro tem valor, então ela tem valor. O dinheiro pode ser trocado por bens e serviços com outras pessoas que acreditam que ele tem valor. Mas quando as pessoas deixam de acreditar, o dinheiro não tem mais valor. E isso acontece às vezes. Houve cerca de sessenta eventos de *hiperinflação* na história da humanidade, nos quais as pessoas perderam a fé na moeda, e ela caiu precipitadamente de valor até que não valia mais nada. Mais recentemente, isso aconteceu no Zimbábue; em 2008, o país realmente abandonou sua moeda em favor do uso de moedas estrangeiras. (Ironicamente, as notas de dólares zimbabuenses então subiram de valor à medida que os colecionadores do mundo inteiro começaram a pegá-las.)

Portanto, mais uma vez, desde que as pessoas *acreditem* em uma determinada forma de dinheiro, ela tem valor. Digamos que você possua metade de um Bitcoin; em outras palavras, o blockchain do Bitcoin diz que você tem meio Bitcoin. (Lembre-se, não há Bitcoin físico real, apenas um registro de suas transações.) Você quer sacar, para convertê-lo em sua moeda local. O blockchain do Bitcoin diz que você tem o endereço no blockchain em que essa moeda está associada (explicamos como isso funciona no Capítulo 2), e, assim, você pode transferi-la para o endereço de *outra pessoa*.