Mineração de Criptomoedas

Para leigos

AMOSTRA

Peter Kent & Tyler Bain

ALTA BOOKS
EDITORA
Rio de Janeiro, 2020

Sumário Resumido

Introdução 1

Parte 1: Descobrindo o Básico sobre as Criptomoedas 5

CAPÍTULO 1: As Criptomoedas Explicadas 7
CAPÍTULO 2: Entendendo a Mineração de Criptomoedas 29
CAPÍTULO 3: Construindo Blocos: A Jornada das Transações ao Blockchain 39
CAPÍTULO 4: Explorando as Diferentes Formas de Mineração 51

Parte 2: A Evolução da Mineração de Criptomoedas 71

CAPÍTULO 5: A Evolução da Mineração 73
CAPÍTULO 6: O Futuro da Mineração de Criptomoedas 83

Parte 3: Tornando--se um Minerador de Criptomoedas . . 95

CAPÍTULO 7: Facilitando a Mineração: Sua Conta na Piscina 97
CAPÍTULO 8: Escolhendo uma Criptomoeda para Minerar 123
CAPÍTULO 9: Montando Seu Equipamento de Mineração 151
CAPÍTULO 10: Configurando Seu Hardware de Mineração 175

Parte 4: A Economia da Mineração 203

CAPÍTULO 11: Fazendo as Contas: Vale a Pena? 205
CAPÍTULO 12: Minimizando as Perdas e Ganhando Vantagem 231
CAPÍTULO 13: Tocando Seu Negócio de Criptomoedas 251

Parte 5: A Parte dos Dez 275

CAPÍTULO 14: (Mais de) Dez Dicas para as Baixas do Mercado 277
CAPÍTULO 15: Dez Formas de Turbinar Seu ROI 297
CAPÍTULO 16: Dez Recursos para Criptomoedas 307
CAPÍTULO 17: Dez Críticas às Criptomoedas e à Mineração 313

Índice 327

AMOSTRA

1 Descobrindo o Básico sobre as Criptomoedas

AMOSTRA

NESTA PARTE...

Revisando o básico sobre criptomoedas.

Compreendendo o blockchain e o hash.

Trabalhando com carteiras.

Usando criptografia de chaves públicas para comprovar propriedade.

Explorando o papel do minerador de criptomoedas.

Criando mensagens de transação em blockchain.

Assinando mensagens de transação.

Compreendendo a rede.

AMOSTRA

NESTE CAPÍTULO

- Descobrindo as moedas virtuais
- Trabalhando com blockchain
- Hash de blocos
- Compreendendo a criptografia de chave pública
- Assinando mensagens com a chave privada

AMOSTRA

Capítulo **1**

As Criptomoedas Explicadas

Você pode estar ansioso para começar suas operações de mineração, mas, antes que possa criar criptomoedas, queremos garantir que entenda o que realmente elas significam.

O assunto é tão recente — pelo menos, a maior parte do interesse pelas criptomoedas ocorreu recentemente, muito embora elas existam de muitas formas diferentes desde a década de 1980 —, que a maioria das pessoas envolvidas tem uma compreensão questionável sobre o que as criptomoedas são e como funcionam. O proprietário comum de criptomoedas, por exemplo, pode nem saber o que possui.

Neste capítulo, faremos uma revisão da história das criptomoedas e falaremos sobre como os diversos componentes funcionam juntos. Você terá uma fundamentação melhor para entender como minerar criptomoedas se compreender o que elas são.

Uma Breve História dos Dólares Digitais

Uma *criptomoeda* é apenas um tipo de moeda virtual... um tipo especial. No fim das contas, as criptomoedas podem ser consideradas isso mesmo: uma forma de moeda virtual.

Mas, então, o que é uma *moeda virtual*? Bem, esse é um termo muito amplo que abrange uma variedade de coisas diferentes. Porém, em termos gerais, é dinheiro que existe de forma digital, em vez de tangível (como moedas e notas). É possível transferir moedas virtuais por meio de algum tipo de rede eletrônica, seja a internet ou a rede de um banco particular.

DICA

Na verdade, até mesmo as transações do cartão de crédito podem ser consideradas como de moedas virtuais. Afinal, quando você usa seu cartão de crédito ou de débito em uma loja (seja digital ou física), o dinheiro é transferido eletronicamente; a rede não empacota as notas e as envia por correio para o vendedor.

Primeiro, pegue a internet

A história das criptomoedas começa, na verdade, com a internet. Elas existiam antes de a internet ser amplamente utilizada, mas, para que sejam úteis, é necessário, bem, algum tipo de método de transporte digital para elas. Se quase ninguém está usando uma rede digital de comunicações — e, até 1994, poucas pessoas o faziam —, então qual é a utilidade de uma moeda virtual?

Porém, após 1994, milhões de pessoas estavam usando uma rede digital e global de comunicações — a internet — e surgiu um problema: como é possível gastar dinheiro online? Tudo bem, hoje em dia a resposta é muito simples: por meio dos cartões de crédito, débito ou conta no Paypal. Mas, lá em meados da década de 1990, o buraco era mais embaixo.

Adicionando confusão ao cartão de crédito

Talvez alguns de vocês se lembrem (e reconheço que muitos de vocês também eram jovens demais naquela época para conseguirem se lembrar) de que, lá em meados da década de 1990, as pessoas tinham receio de usar cartões de crédito na internet. Quando criei minha própria editora e vendia livros no meu site em 1997, eu (Peter — o Tyler é novo demais para se lembrar de 1997) frequentemente recebia, pelo correio, prints das páginas de produtos de meu site, junto com um cheque para pagar pelo livro que estava sendo adquirido. Eu aceitava apenas cartões de crédito, mas muitas pessoas simplesmente não queriam usá-los; elas não confiavam que a web protegeria seu cofre de plástico.

AMOSTRA

Além disso, era difícil e caro, para o comerciante, estabelecer um portal de pagamento para cartões de crédito. Hoje em dia, adicionar o processamento de cartões de crédito em um site é um procedimento bem simples — e está incorporado virtualmente a todos os softwares de comércio digital, e, com serviços como Stripe e Square, que diminuem as barreiras de entrada, obter uma *conta comercial* não é mais uma enorme dor de cabeça e algo caro como costumava ser.

Obviamente, estamos nos referindo a transações comerciais aqui. Mas e quanto às transações pessoais? Como alguém pode enviar dinheiro que deve a um amigo? Ou como os pais podem enviar dinheiro para o filho que está na faculdade poder comprar cerveja? (Refiro-me ao PPP... pré-PayPal e transferências online entre contas bancárias.) Se vamos viver em um mundo digital, certamente precisamos de dinheiro digital.

LEMBRE-SE

Uma característica importante do dinheiro vivo é que suas transações são essencialmente anônimas — não há rastros físicos ou registros eletrônicos da transação. Muitas pessoas achavam que uma forma equivalente de moeda virtual anônima ou pseudônima seria uma grande melhoria dos métodos tradicionais de transação.

Assim, muita gente achava que deveria haver uma opção melhor. Precisávamos de uma moeda virtual para um mundo digital. Hoje em dia, talvez esse ponto de vista pareça ingênuo; voltando no tempo, era óbvio que as empresas de crédito não aceitariam ver trilhões de dólares em transações passando a ocorrer online e simplesmente dizer "tchauzinho"! Elas queriam sua parcela na ação, relutantes em abrir mão de seu monopólio, então, hoje em dia, os métodos primários de transações nos EUA e na maior parte da Europa é por meio de cartões de vários tipos.

Adicione uma pitada de David Chaum

Em meados da década de 1990, as pessoas acessavam a internet aos bandos, mas, por vários motivos, muitas não queriam ou não podiam usar cartões de crédito (veja a seção anterior). Os cheques eram ainda mais difíceis (a menos que quisessem enviá-los por correio), e dinheiro estava fora de questão. (Embora — e aqui vai uma piada para vocês que são geeks mais velhos — eu me lembre de um amigo dizendo para eu fazer a codificação UUENCODE dos $10 que devia para ele e enviar por e-mail. Novamente, é o Peter falando aqui; aposto que Tyler é novo demais para saber o que é UUENCODE.)

Mas, lá em 1983, uma cara chamado David Chaum havia escrito um artigo intitulado "Blind Signatures for Untraceable Transactions" [Assinaturas Cegas para Transações Não Rastreáveis, em tradução livre]. Chaum era criptógrafo (alguém que trabalha com criptografia) e professor de ciência da computação. Seu artigo descrevia uma forma de usar criptografia para criar um sistema de dinheiro digital que poderia possibilitar transações anônimas, como com dinheiro vivo (a criptografia moderna é a ciência de proteger comunicações online; falaremos sobre isso posteriormente). Na verdade, Chaum é geralmente mencionado como o Pai do Dinheiro Digital, assim como o Pai da Anonimidade Online.

AMOSTRA

Resultado? DigiCash, E-Gold, Millicent, Cybercash e mais

Misture a internet, transações online complicadas, medo de usar cartões de crédito online, desejo pela anonimidade do dinheiro vivo nas transações online e o trabalho de David Chaum nos anos 1980 (veja a seção anterior). Que resultado você obterá?

Para começar, você terá DigiCash, o sistema de dinheiro digital criado em 1990 por David Chaum. Infelizmente, parece que o Sr. Chaum chegou cedo demais à festa, e o DigiCash saiu de cena em 1998. Também houve o E-Gold, um sistema de dinheiro digital supostamente ancorado pelo outro, o Millicent de DEC (sim, sim, a maioria de vocês é jovem demais para se lembrar do DEC também... estou começando a me sentir velho enquanto escrevo esta seção "histórica"), o First Virtual, o Cybercash, o b-money, o Hashcash, o eCash, o BitGold, o Cybercoin e muitos outros. Também tivemos o Beenz, com capital de investimento na casa dos US$100 milhões; o Flooz, promovido por Whoopi Goldberg (é sério!); o Liberty Reserve (encerrado após acusações de lavagem de dinheiro); e os QQ Coins, da China.

Com a exceção dos QQ Coins, que ainda são utilizados nos serviços de Mensagens QQ da Tencent, todas essas moedas virtuais já eram. Notavelmente, muitas dessas primeiras unidades monetárias eram, de uma forma ou de outra, centralizadas.

No entanto, as moedas virtuais não acabaram. Elas tiveram um começo difícil, com muitas tentativa e erros, mas muitas pessoas ainda achavam que o mundo precisava de transações online como se fosse dinheiro vivo (ou seja, anônimas). Uma nova era estava prestes a começar: a era das criptomoedas.

As primeiras moedas virtuais também dependiam da criptografia, é verdade, mas elas não eram conhecidas como criptomoedas. Foi apenas após as criptomoedas serem combinadas com um blockchain em 2008 que o termo "criptomoeda" começou a ser usado, e ele realmente só começou a aparecer amplamente apenas por volta de 2012. (Blockchain? É uma forma especial de banco de dados, mas o descreveremos em mais detalhes posteriormente, neste capítulo.)

O whitepaper do Bitcoin

Em 2008, Satoshi Nakamoto publicou em um fórum de criptografia conhecido como "Cypherpunk Mailing List" um documento intitulado "Bitcoin: A Peer-to-Peer* Electronic Cash System" [Bitcoin: Um Sistema de Dinheiro Eletrônico

* N. do T.: Peer-to-peer: Entre pares, ou diretamente entre os usuários. Algumas fontes usam: ponto-a-ponto.

AMOSTRA

Peer-to-Peer], dizendo: "Estou trabalhando em um novo sistema de dinheiro eletrônico que tem as operações completamente peer-to-peer, sem a necessidade de confiar em uma terceira parte."

A lista de atributos a seguir, postulou Nakamoto, era essencial para o Bitcoin:

- Gastos duplos não ocorrem com uma rede peer-to-peer.
- Sem Casa da Moeda ou necessidade de confiar em terceiros.
- Os participantes podem ser anônimos.
- Novas moedas são criadas a partir do Proof of Work (PoW) ao estilo Hashcash.
- O Proof of Work para criação de novas moedas também impede o gasto duplo na rede.

A leitura do documento não é muito prazerosa, mas vale a pena gastar alguns minutos para dar uma conferida nele. É fácil encontrá-lo. Acesse `https://bitcoin.org/bitcoin.pdf` [conteúdo em inglês; há várias versões em português, como a disponível em: `https://bitcoin.org/files/bitcoin-paper/bitcoin_pt_br.pdf`]. O resumo do *whitepaper do bitcoin* começa com a seguinte afirmação: "Uma versão de dinheiro eletrônico puramente peer-to-peer permitiria que pagamentos online fossem enviados diretamente de uma pessoa para outra sem a necessidade de passar por uma instituição financeira", escreveu Nakamoto. Ele explica que seu método resolveu o problema do "gasto duplo", uma questão que atormentou as primeiras moedas virtuais: o desafio era garantir que uma moeda virtual não pudesse ser gasta duas vezes.

Nakamoto também descreve a funcionalidade do uso do blockchain, embora o termo "blockchain" não apareça em seu artigo:

> *"Estamos propondo... usar uma rede peer-to-peer. A rede insere data e hora nas transações usando um hash em uma cadeia contínua de Proof of Work à base de hash, formando um registro que não pode ser alterado sem refazer o Proof of Work."*

Bitcoin: O primeiro aplicativo em blockchain

No início de janeiro de 2009, Nakamoto colocou a rede de bitcoins para funcionar usando blockchain (um conceito que existe desde o início da década de 1990, embora esta fosse a primeira vez que tivesse sido corretamente implementado), e criou o primeiro bloco no blockchain, conhecido como o bloco *gênesis*.

Esse bloco continha cinquenta bitcoins, bem como o texto *"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"* [alusão à matéria do

AMOSTRA

jornal *The Times* sobre a iminência de um segundo resgate financeiro dos bancos], como justificativa e explicação sobre a importância de um sistema como o Bitcoin. Nakamoto continuou codificando atualizações no protocolo, rodando um nó e muito provavelmente minerou 1 milhão de bitcoins, número este que o faria uma das pessoas mais ricas do mundo no fim de 2017 (ou, pelo menos, "no papel").

Chegando o fim de 2010, Satoshi Nakamoto publicou seu último post no fórum e oficialmente saiu do projeto, mas, a essa altura, muitos outros entusiastas das criptomoedas já haviam se juntado ao grupo e começaram a minerar, dando suporte ao desenvolvimento de código-fonte aberto, e o resto é história.

Quem (ou o que) é Satoshi Nakamoto?

Então, quem foi esse cara... ou essa moça... ou organização chamada Satoshi Nakamoto? Ninguém sabe. Satoshi Nakamoto não parece ser um nome real; muito provavelmente é um pseudônimo. E se alguém sabe, de fato, quem é Nakamoto, essa pessoa não dirá. É um grande mistério das criptomoedas.

Há um nipo-americano chamado Dorian Prentice Satoshi Nakamoto, aparentemente nascido Satoshi Nakamoto. Ele tinha formação em física e engenharia de sistemas e de computação e trabalhava para empresas financeiras — talvez ele fosse Satoshi Nakamoto. No entanto, ele negou o fato diversas vezes.

Que tal Hal Finney, que morava a apenas alguns quarteirões da casa de Dorian Prentice Satoshi Nakamoto? Ele era criptógrafo antes de existir o bitcoin, uma das primeiras pessoas a usar essa moeda, e alega ter se comunicado por e-mail com o fundador dos bitcoins. Algumas pessoas sugeriram que ele "pegou emprestado" o nome de Satoshi Nakamoto e o usou como pseudônimo.

Temos ainda Nick Szabo, que está envolvido com moedas virtuais há muito tempo e até publicou um whitepaper sobre bit gold, antes do whitepaper de Nakamoto sobre bitcoin. E que tal Craig White, que a certa altura alegou ser Nakamoto, mas foi acusado posteriormente de fraude? Ou o Dr. Vili Lehdonvirta, sociólogo econômico finlandês, ou um aluno irlandês graduando em criptografia; ou os três caras que deram entrada em uma patente que incluía uma frase obscura ("computacionalmente impraticáveis de reverter"), também usada no whitepaper de Nakamoto sobre bitcoin; ou o matemático japonês Shinichi Mochizuki; ou Jed McCaleb; ou algum tipo de agência governamental; ou algum tipo de equipe de pessoas; ou Elon Musk; ou... bem, ninguém sabe, mas não faltam teorias.

O segundo maior mistério de bitcoins? Nakamoto possuía cerca de 1 milhão de bitcoins, que valiam cerca 19 ou 20 bilhões de dólares em dezembro de 2017. A totalidade da fortuna em bitcoins estimada de Nakamoto não foi movimentada ou gasta. Por que ele ou ela (ou eles) não encostou nesse dinheiro?

AMOSTRA

O que É Blockchain?

Para compreender as criptomoedas, é necessário saber um pouco sobre blockchains — uma tecnologia complicada. Mas tudo bem, não precisamos entender tudo, apenas o básico.

Blockchains são tipos de bancos de dados. Um *banco de dados* é apenas uma coleção de dados estruturados. Digamos que você junte um punhado de nomes, endereços de ruas, de e-mail e números de telefone e os digite em um processador de textos. Isso não é um banco de dados, é apenas um amontado de textos.

Mas digamos que você insira esses dados em uma planilha. A primeira coluna é para o primeiro nome, a segunda é para o sobrenome; e depois, as colunas para e-mail, telefone, endereço, CEP, país e assim por diante — agora temos dados estruturados. Isso é um banco de dados.

A maioria das pessoas usa banco de dados o tempo todo. Se você usa algum tipo de programa de gestão financeira, como Quickbooks, Quicken ou Mint, seus dados estão armazenados em um banco de dados. Se você usa um programa de gerenciamento de contatos para armazenar esse tipo de informação, ela fica em um banco de dados. Nos bastidores, os bancos de dados são uma parte integral da vida digital moderna.

Volta ao mundo com blockchain — A rede

O blockchain é um banco de dados; ele armazena informações de forma estruturada. Podemos usar blockchains para muitos propósitos diferentes: por exemplo, para *registro de direitos de propriedade* (quem é o dono deste terreno, e como se tornou o dono?) ou *acompanhamento da cadeia de suprimentos* (qual é a procedência de seu vinho ou peixe e como chegou até você?). Os blockchains podem armazenar qualquer tipo de dados. Porém, no caso das criptomoedas, os blockchains armazenam dados de transações: quem possui qual quantia de criptomoedas, sua procedência e destino (como foi gasta)?

Obviamente, os blockchains têm diversas características especiais. Para começar, funcionam em rede. Há a rede do Bitcoin, do Litecoin, do Ethereum, assim como há uma rede de e-mails ou a rede World Wide Web.

O Bitcoin, por exemplo, é uma rede de milhares de nós, ou servidores, espalhados por todo o planeta.

Cada um desses nós contém uma cópia do blockchain do bitcoin, e eles se comunicam entre si e se mantêm sincronizados. Eles usam um sistema de *consenso* para chegar a um acordo com respeito à aparência do banco de dados válido e atual do blockchain. Ou seja, todos eles têm uma cópia de combinação do blockchain.

AMOSTRA

Hash: Colocando a "impressão digital" nos blocos

Duplicar o blockchain em vários outros computadores é muito importante, torna-o muito mais difícil de hackear ou manipular. Mas há outra coisa que é muito poderosa também: o *hash*. Um *hash* é um número comprido que pode ser considerado uma impressão digital para os dados. O blockchain o utiliza da seguinte maneira:

1. **Um computador roda um nó, coleta e valida as transações de bitcoins (registros de bitcoins enviadas entre endereços dentro do blockchain) que serão adicionadas ao blockchain.**

2. **Uma vez que um computador tenha coletado transações suficientes, ele cria um bloco de dados e faz o *hash* dos dados — isto é, passa os dados para um algoritmo especial de hash, que faz o hash de volta.**

   Veja um exemplo de um hash da vida real, retirado de um bloco no blockchain do bitcoin:

   000000000000000000297f87446dc8b8855ae4ee2b35260dc4af61e-1f5eec579Th

   Um *hash* é uma impressão digital para os dados, e, graças à mágica da matemática complexa, não é possível ser igualado por nenhum outro conjunto de dados. Se os dados com hash forem levemente alterados — um 0 muda para 5, ou um A muda para B —, a impressão digital do hash não estará mais compatível com os dados originais.

3. **O hash é adicionado ao bloco de transações.**

4. **O bloco é adicionado ao blockchain.**

5. **Mais transações são coletadas para o próximo bloco.**

6. **Depois que um bloco cheio de operações está pronto, o hash do bloco anterior é adicionado ao bloco atual.**

7. **O bloco — as transações e o hash do bloco anterior — recebe o hash novamente.**

8. **O processo se repete, criando uma cadeia de blocos carimbados com o dia e a hora da transação.**

Portanto, cada bloco contém dois hashes: o do bloco anterior e o do bloco atual, que é criado ao fazer o hash da combinação de todas as transações de bitcoins e do hash do bloco anterior.

É assim que os blocos vão se encadeando no blockchain (veja a Figura 1-1). Cada bloco contém o hash do bloco anterior — na verdade, uma cópia da impressão

AMOSTRA

digital única do bloco anterior. Cada bloco também está, de fato, identificando sua posição no blockchain; o hash do bloco anterior identifica a ordem na qual o bloco atual está.

O blockchain é "imutável"

Talvez você tenha ouvido que o blockchain é praticamente *imutável*, o que simplesmente significa que não é fácil de alterá-lo. Se o sistema blockchain de bitcoins diz que você possui x bitcoins, então é o que você possui, não há como discordar. E ninguém conseguirá acessar o blockchain para hackeá-lo, mudá-lo ou alterá-lo de alguma forma.

Imagine o que aconteceria se alguém acessasse um bloco (vamos chamá-lo de Bloco A) e mudasse alguns poucos dados — por exemplo, a pessoa acessa e mostra que, em vez de ter enviado um bitcoin a alguém, você enviou nove bitcoins.

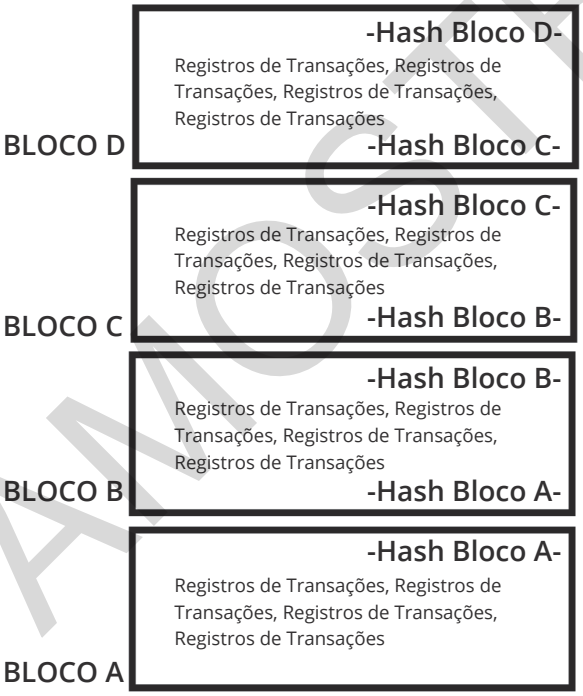

FIGURA 1-1: O hash de cada bloco fica armazenado no próximo bloco de dados. Os hashes encadeiam os blocos de forma ordenada.

Bem, o hash no Bloco A não seria mais compatível com seus dados. Lembre-se: um hash é uma impressão digital que identifica os dados, então, se você mudar os dados, o hash não será mais compatível.

Tudo bem, então o hacker poderia refazer o hash dos dados do Bloco A e salvar o hash "corrigido". Mas espere um momento! Agora o próximo bloco (Bloco B) não seria mais compatível, porque ele está carregando o hash do Bloco A. Digamos, então, que agora o hacker muda o hash do Bloco A armazenado no Bloco B.

AMOSTRA

Mas então o hash do Bloco B não é mais compatível com os dados do Bloco B, porque esse hash foi criado a partir de uma combinação dos dados de transações do Bloco B e do hash do Bloco A!

Portanto, o Bloco B teria de receber um novo hash, e o hash teria que ser atualizado. Mas espere aí! Isso significa que o hash do Bloco B armazenado no Bloco C agora não é mais compatível!

Vê aonde estamos indo? Isso interferiria ao longo de todo o blockchain. Ele estaria completamente quebrado agora, com apenas a modificação de um único caractere em um bloco bem mais embaixo. Para resolver o problema, o blockchain inteiro precisa ser recalculado. Começando nesse bloco hackeado, ele deve ser "reminerado". O que podia parecer um hackeamento simples e uma mera edição de banco de dados agora se transforma em uma dor de cabeça computacional gigantesca que não pode ser facilmente resolvida.

Dessa forma, a função de hash, combinada com o fato de que milhares de outros nós devem estar sincronizados com cópias idênticas do blockchain, torna o blockchain praticamente imutável; ele simplesmente não pode ser facilmente hackeado.

Ninguém consegue mudá-lo ou destruí-lo. Os hackers não conseguem acessar a rede de nós peer-to-peer e criar transações para roubar criptografia, os governos não conseguem fechá-lo (a China, por exemplo, poderia tentar encerrar o bitcoin dentro de seu território, mas o blockchain continuaria a existir em muitos outros países), um grupo terrorista não pode destruí-lo, uma nação não pode atacar outra e destruir seu blockchain e assim por diante. Como há muitas cópias do blockchain, ele é praticamente imutável e indestrutível.

Cadê o Dinheiro?

Talvez você esteja se perguntando "Então, onde está a criptomoeda? Cadê o dinheiro?" Ou talvez tenha ouvido falar sobre carteiras de criptomoedas e acha que é nelas que o dinheiro fica armazenado. Errado. Não há dinheiro na carteira de criptomoedas. Na verdade, não há criptomoedas.

Os blockchains de criptomoedas são geralmente descritos como livros-razão. Um *livro-razão* é descrito no Google Dicionário como "livro usado pelos comerciantes como índice do livro diário" — uma coleção de registros financeiros de determinado tipo. Os livros-razão existem há centenas de anos e são usados para registrar as transações de pessoas físicas, jurídicas, departamentos governamentais etc. O recibo que você obtém de sua conta no banco ou de seu cartão de crédito é uma forma de livro-razão, demonstrando suas transações individuais e o dinheiro que paga e recebe dos outros.

AMOSTRA

DESCOBRINDO SEU SALDO NO BLOCKCHAIN

PAPO DE ESPECIALISTA

Certo, tudo bem, o blockchain na verdade não armazena o saldo para cada endereço. O blockchain não declara em nenhum lugar quanto de criptomoedas qualquer pessoa em particular tem, ou quantos endereços específicos estão associados a ela. Em vez disso, você pode usar um explorador de blockchain para seguir todas as suas transações, de débito e crédito, e o explorador pode determinar seu saldo com base nessas transações.

No contexto da criptomoeda, o blockchain é um livro-razão digital que registra as criptomoedas que você envia e recebe dos outros.

Pense assim: digamos que você seja um pouco compulsivo e goste de manter um registro do dinheiro que carrega em seu bolso. Você sempre leva um bloco para registrar cada vez que coloca dinheiro no bolso e cada vez que o gasta, calculando o balanço atual. O bloquinho é um tipo de livro-razão de transações, não é mesmo?

A criptomoeda é muito similar a esse livro-razão de transações de dinheiro... excluindo o fato de que não há bolsos. O blockchain é o livro-razão; ele armazena um registro de cada transação (a primeira vez que você comprou ou recebeu criptomoedas, quando as gastou ou vendeu e o saldo que possui).

Mas não há bolsos, e as criptomoedas não estão armazenadas em algum galpão. O blockchain é apenas uma série de transações "míticas" (ou virtuais) armazenadas no livro-razão. Não há transferência de moedas físicas; apenas atualização do registro, para declarar que aquela moeda foi transferida.

O livro-razão diz que você possui criptomoedas, então todos podem validar e aceitar o fato. E lembre-se: o livro-razão não pode ser editado após ter sido solidificado no encadeamento — e não pode ser hackeado. (Veja a seção anterior para obter mais detalhes sobre esse assunto.) Assim, se o livro-razão diz que você possui, digamos, meio bitcoin, então você de fato o possui e pode vendê-lo para outra pessoa ao modificar o livro-razão informando que aquela pessoa o possui!

Mas, e a carteira? Ela deve conter dinheiro, não é? Não, as carteiras de criptomoedas não as armazenam. Elas armazenam chaves particulares e públicas, além de endereços. As chaves particulares são as mais importantes, porque controlam os endereços com os quais as criptomoedas ficam associadas no blockchain.

AMOSTRA

O que É o Cripto em Criptomoedas?

O *cripto* em criptomoedas faz referência à criptografia. Então, o que a criptografia é exatamente?

De acordo com o dicionário Michaelis, criptografia é "a arte ou processo de escrever em caracteres secretos". A explicação da Wikipédia é mais complicada e digital: "O estudo e prática de princípios e técnicas para comunicação segura... a criptografia refere-se à construção e análise de protocolos que impedem terceiros, ou o público, de lerem mensagens privadas."

A história da criptografia remonta a, pelo menos, 4 mil anos. As pessoas sempre precisaram enviar mensagens secretas de vez em quando, e é exatamente sobre isso que trata a criptografia.

A criptografia atual, com a ajuda de computadores, é muito mais complicada do que as cifras antigas do mundo clássico e é usada mais extensivamente. Na verdade, ela é uma parte integral da internet; sem ela, a internet simplesmente não funcionaria da forma que necessitamos que funcione.

Quase todas as vezes que você usa seu navegador, está empregando a criptografia. Lembra-se do iconezinho de cadeado, apresentado na Figura 1-2, na barra de endereços?

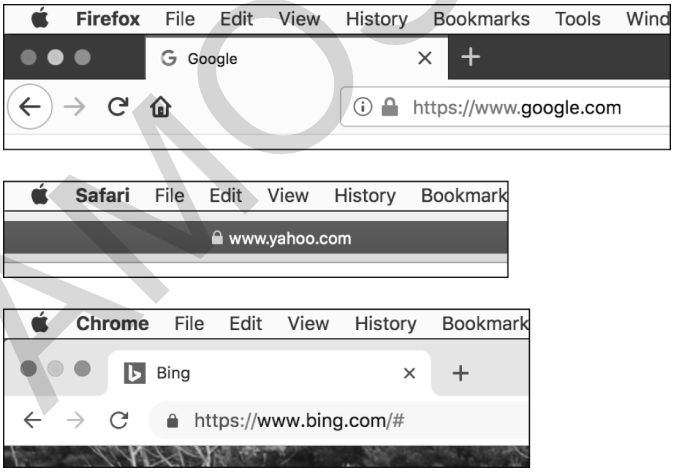

FIGURA 1-2: O ícone de cadeado de seu navegador significa que os dados submetidos de volta à rede serão criptografados.

O ícone de cadeado significa que a página é segura. Ao enviar e receber informações do navegador para o servidor da internet, essa informação será *criptografada* — embaralhada —, para que, caso seja interceptada nas centenas ou milhares de quilômetros de transmissão da internet entre os dois, ela não possa ser lida. Quando o número de seu cartão de crédito é transmitido para um site de comércio eletrônico, por exemplo, ele é embaralhado por seu navegador, enviado para o servidor da internet e, depois, desembaralhado pelo servidor recipiente.

AMOSTRA

PAPO DE ESPECIALISTA

BLOCKCHAINS CRIPTOGRAFADOS

Você pode criar blockchains criptografados e criptografar dados dentro de um blockchain. Por exemplo, embora o bitcoin não seja criptografado, possa ser aberto e inspecionado por qualquer um (veja o explorador de blockchain na Figura 1-3), ainda é possível criar blockchains criptografados que obscurecem os dados de transações, como o ZCash, mas, em geral, blockchains de criptomoedas não são criptografados, então qualquer um pode ler as transações armazenadas neles.

Ah, então o blockchain é criptografado, certo? Bem, não. A criptomoeda usa criptografia, mas não para embaralhar os dados no blockchain. Ele é aberto, público e auditável. A Figura 1-3 mostra um exemplo de um explorador de blockchain projetado para o bitcoin. Por meio do uso de um desses exploradores, qualquer um pode investigar o blockchain e ver todas as transações que ocorreram desde o bloco gênesis (o primeiro bloco de bitcoin criado).

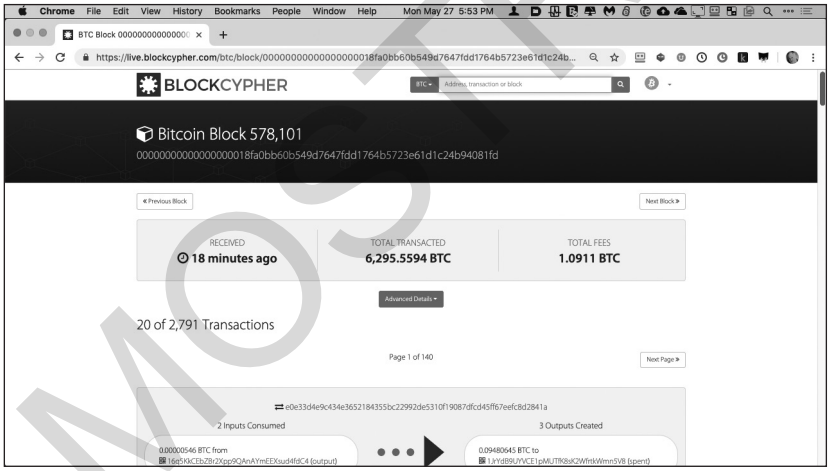

FIGURA 1-3: Exemplo de um explorador de blockchain, disponível em `https://live.blockcypher.com/btc/`.

Não, as criptomoedas não costumam criptografar os dados no blockchain. Elas costumam assinar mensagens que você envia para o blockchain. Essas mensagens são as que acionam as transações e atualizam o livro-razão do blockchain.

A Mágica da Criptografia de Chave Pública

A criptografia de chave pública é um truquezinho esperto criado com o uso da criptografia digital. E, a propósito, esse tipo de criptografia é totalmente realizado com cálculos matemáticos extremamente complicados — o tipo de cálculo que até as pessoas com graduação em matemática não entendem e que

AMOSTRA