

# DOMINANDO BITCOIN — PARA — INICIANTE

TECNOLOGIAS DE BITCOIN E CRIPTOMOEDA,  
MINERAÇÃO, INVESTIMENTO E TRADING  
(Brazilian Portuguese)



ALAN T. NORMAN

Alan T. Norman

# **Dominando Bitcoin Para Iniciantes**

«Tektime S.r.l.s.»

## **Norman A.**

Dominando Bitcoin Para Iniciantes / A. Norman — «Tektime S.r.l.s.»,

Bitcoin não é apenas uma nova palavra na era da Internet, ou um progresso tecnológico e financeiro, é um começo de uma nova era na Terra! Mesmo há dez anos, nem imaginávamos sonhar com dinheiro digital - você não poder tocá-lo fisicamente, mas poder possuí-lo e gastá-lo. Hoje isto é uma realidade! A revolução Bitcoin cobriu o mundo inteiro como uma onda enorme, mais e mais pessoas interessadas neste "Ouro Digital". Bitcoin não é apenas uma nova palavra na era da Internet, ou um progresso tecnológico e financeiro, é um começo de uma nova era na Terra! Mesmo há dez anos, nem imaginávamos sonhar com dinheiro digital - você não poder tocá-lo fisicamente, mas poder possuí-lo e gastá-lo. Hoje isto é uma realidade! A revolução Bitcoin cobriu o mundo inteiro como uma onda enorme, mais e mais pessoas interessadas neste "Ouro Digital". Nos últimos anos, o Bitcoin passou de algo conhecido apenas por alguns nerds de tecnologia a uma moeda revolucionária que mudou, rapidamente, a forma como pensamos sobre o conceito de dinheiro. Você, sem dúvida, vê pagamentos por Bitcoin aceitos em todos os tipos de lugares agora, mas, se você pode acreditar, costumava ser um procedimento bastante complicado encontrar lugares que permitiam pagar em Bitcoin. Enfim, para administrar o mundo, você precisa saber tudo. Não podemos garantir que você saiba TUDO a partir deste livro, mas podemos garantir que você terá a noção de uma nova moeda - Bitcoin. - O que é isso? - De onde veio? - Como utilizar? - É realmente apenas dinheiro falso na Internet, criado por traficantes de drogas? É exatamente isso que responderemos neste livro. Abordaremos tudo o que você precisa saber para começar com Bitcoin: - entender as transações Blockchain e Bitcoin, - onde manter sua Bitcoin (como escolher uma carteira segura), - comprando Bitcoin, - investindo em Bitcoin, - como começar a aceitar e usar Bitcoin como um parte de seus princípios de negócios de mineração de Bitcoin, - a segurança da Bitcoin, etc. Além disso, o autor compartilhará com você fatos interessantes sobre Bitcoin, e fornecerá dicas profissionais sobre o início do seu caminho na família Bitcoin! Já pronto para enfrentar o mundo Bitcoin? Espero

que sim. Eu gostaria de ser o primeiro a recebê-lo oficialmente no mundo Bitcoin!  
(Brazilian Portuguese)

© Norman A.  
© Tektime S.r.l.s.

## Содержание

Capítulo 1. O que é Bitcoin?	7
O Início	8
Então, É Uma Moeda?	11
Sobre O Custo	12
O Que É Uma Criptomoeda?	13
Então, Por Que Bitcoin?	14
Aprendendo Sobre Bitcoin	15
Capítulo 2. Entendendo as transações Blockchain & Bitcoin	16
A Blockchain & Bitcoin	17
Como as Transações de Bitcoin Funcionam?	18
A Blockchain & Transações	20
Capítulo 3. Introdução à Bitcoin	21
Segurança Pessoal na Bitcoin	22
Introdução À Bitcoin	24
Capítulo 4. Onde guardar sua Bitcoin	25
Seu Endereço de Bitcoin	25
Endereços de uso único	26
Criando Um Endereço De Bitcoin	28
Конец ознакомительного фрагмента.	29

# **Alan T. Norman**

## **Dominando Bitcoin Para Iniciantes**

**DOMINANDO BITCOIN PARA INICIANTES**

**Tecnologias De Bitcoin E Criptomoeda, Mineração, Investimento E Trading**

**ALAN T. NORMAN**

**Tradutor: Duda Junqueira Machado**

**Obtenha gratuitamente o livro Bitcoin Whales:  
Guys who fooled the world Livro Bônus**

**(Detalhes no final deste livro.)**

**Copyright © 2020 ALAN T. NORMAN – Todos os direitos reservados**

**Nenhuma parte desta publicação pode ser reproduzida, distribuída ou transmitida por qualquer forma ou por qualquer meio, incluindo fotocópia, gravação ou outros meios eletrônicos ou mecânicos, sem autorização prévia e por escrito do editor, exceto no caso de breves citações disponibilizadas em resenhas críticas e alguns outros usos não comerciais, permitidos pela lei de direitos autorais**

## Capítulo 1. O que é Bitcoin?

Se você escolheu este livro, é provável que tenha ouvido falar sobre Bitcoin.

- Talvez você tenha ouvido falar sobre isso nos círculos financeiros, já que o valor da Bitcoin aumentou rapidamente.
- Talvez você tenha ouvido falar disso em um contexto tecnológico, já que a Bitcoin é construída em cima de uma nova tecnologia chamada Blockchain.
- Ou, como muitos, você deve ter ouvido falar sobre a Bitcoin na imprensa popular, devido à quantidade de novos usuários, celebridades famosas e empresários de sucesso que começaram a usar Bitcoin no ano passado.

Nos últimos anos, a Bitcoin passou de algo conhecido apenas por alguns nerds de tecnologia a uma moeda revolucionária que mudou, rapidamente, a forma como pensamos sobre o conceito de dinheiro.

Aqui está a sinopse (muito) básica: Bitcoin é uma moeda digital. De muitas maneiras, funciona como dólares, euros ou ienes, permitindo-nos a transferência de valor. No entanto, a força da Bitcoin é a sua rede. A tecnologia Blockchain permite que o Bitcoin seja descentralizado, o que significa que qualquer pessoa pode acessar e negociar no livro contábil público do Bitcoin. Usando o Bitcoin, você pode enviar fundos para qualquer pessoa no mundo, sem a necessidade de grandes instituições como bancos, conversores de moeda e processadores de pagamento.

Tudo acontece na rede pública da Bitcoin.

Além dos pagamentos pessoa a pessoa, os pagamentos Bitcoin são, agora, aceitos em vários tipos de empresas. Alguns anos atrás, apenas, encontrar lugares que permitissem pagar em Bitcoin era um desafio. Para ser sincero, nos primeiros dias da Bitcoin, poderíamos ter preenchido apenas esta página com todos os lugares que aceitavam Bitcoin. Agora, a aceitação da Bitcoin explodiu.

Outro uso da Bitcoin surgiu nos últimos anos: investimento. À medida que mais pessoas começaram a usar Bitcoin, seu preço aumentou dramaticamente. Como veremos mais adiante neste livro, muitas pessoas estão comprando Bitcoin como um ativo, esperando que se valorize com o tempo.

Claro, a Bitcoin ainda tem seus problemas e desafios para o seu futuro. Vamos dar uma olhada em alguns desses desafios nas próximas páginas.

Neste livro, abordaremos tudo o que você precisa saber para começar a usar Bitcoin, então, vamos começar por de onde ele veio.

Pronto para mergulhar? Vamos lá!

## O Início

Pense em alguns anos atrás. Em 2008, a crise financeira estava em pleno andamento, e pessoas de todo o mundo estavam sentindo os efeitos do desastre econômico dos Estados Unidos. Isto foi um daqueles momentos da história em que os problemas das moedas nacionais mostraram sua relevância. A crise financeira americana desvalorizou o dólar, e os problemas econômicos nos Estados afetaram o mundo inteiro.

Às vezes, a ocorrência de um colapso econômico completo parecia provável. Onde estavam todas aquelas pessoas que deveriam garantir que nada disso jamais acontecesse? Eles estragaram tudo, bastante. E Isso sendo moderado, para dizer o mínimo.

### Respostas Centralizadas

As pessoas “conhecedoras” mais importantes decidiram que tinham uma resposta, que somente um banco centralizado poderia oferecer. Para combater o rápido colapso dos mercados financeiros, governos de todo o mundo decidiram o que é chamado de "alívio quantitativo", durante o qual imprimiam e injetavam mais dinheiro em suas economias, de modo que seus cidadãos tivessem os fundos necessários para evitar outra Grande Depressão.

Estes tipos de mudanças rápidas leva a "guerras cambiais", e, logo, os governos estavam competindo para ser o único com os preços mais baixos, que os manteria competitivos. Quando, então, os bancos enfrentaram problemas, devido ao baixo valor da moeda e às taxas de juros reduzidas, os governos foram forçados a resgatá-los com dinheiro dos contribuintes. Como você pode imaginar, isto apenas desvalorizou ainda mais a oferta de moeda existente.

Embora esta seja uma visão muito simplificada de um momento complexo da história econômica, a lição permanece. Os bancos centrais, que manipulam a oferta monetária, desvalorizaram moedas em todo o mundo.

No final, com as taxas de juros baixas e os resgates dos contribuintes, os próprios bancos, inicialmente responsáveis pelo problema financeiro, foram os que mais se beneficiaram com a economia em colapso. Foi durante este período que um homem, conhecido como Satoshi Nakamoto, se inspirou.

### Quem é Satoshi?

Antes de explicar exatamente como a Bitcoin surgiu, vale a pena explorar quem é Satoshi Nakamoto. Sua história é a história da Bitcoin, e ele era misterioso.

A verdadeira identidade de Satoshi ainda permanece desconhecida, até hoje. Segundo suas próprias declarações em 2012, ele tinha 37 anos e morava em algum lugar do Japão. No entanto, muitas dúvidas sobre isso persistem. Ele escreve em inglês fluente, e o software Bitcoin não está documentado em japonês, levando muitos a pensar que ele não é de fato japonês, embora pudesse estar morando lá na época.

Com um pouco de trabalho de detetive, um codificador suíço determinou que Satoshi poderia morar na América do Norte, dada a hora do dia que ele postou nos fóruns de Bitcoin. O codificador fez isso analisando os horários de postagem mais comuns, e constatando que eles estavam alinhados com o horário médio de sono de alguém que vive no continente.

Será que algum dia saberemos quem é o criador da Bitcoin? Será ele, na verdade, uma equipe de pessoas? Podemos não descobrir nunca, mas uma coisa é certa: Esta pessoa controla

aproximadamente um milhão de Bitcoin. Em junho de 2017, isso equivalia a quase US \$ 3 bilhões! Com uma fortuna assim, eles podem comprar o direito à privacidade.

## **A Criação**

Portanto, este codificador anônimo analisou o estado do mundo financeiro e viu muitos problemas. As formas tradicionais de resolver esta crise haviam sido tentadas e, embora funcionassem, por enquanto, ele viu que pouco foi feito para evitar futuros desastres. O que poderia ser feito sobre isso? Qualquer tipo de solução centralizada conseguiria resolver problemas deste tipo de uma vez por todas?

Ele decidiu que era necessária uma força disruptiva. Algo que pudesse mudar potencialmente a maneira como pensamos sobre moeda. A resposta foi uma forma de moeda completamente descentralizada e aberta a todos. Nenhum banco central controlando, nenhuma cadeia de transferências com um único superintendente. Nenhum grupo de elite de pessoas tomando decisões que afetariam cada pessoa usando suas moedas.

## **Descentralização**

### **B**

Descentralização: a movimentação de departamentos de uma grande organização para longe, de um único centro administrativo para outros locais.

Essa descentralização foi a principal força motriz por trás do trabalho de Satoshi. Essencialmente, a descentralização significa que todos fazem parte da economia Bitcoin, e todos estamos contribuindo de alguma forma. NÓS somos a força motriz, e não um banco central que controla quanto vale nossa moeda e quanto dela temos disponível em nossa economia. Melhor ainda, ao mesmo tempo, nenhum de nós tem controle sobre isso.

Não há governo, banco ou intermediário que possa nos dizer como usar a Bitcoin, pois ela, literalmente, pertence a todos que a usam. Com isso dito, quanto mais pessoas a utilizam, melhor ela funciona e mais viável se torna. É assim que a tecnologia pessoa-a-pessoa funciona. É diretamente entre usuários.

No sentido mais verdadeiro da palavra, é um mercado livre. Ouvimos muito falar sobre livre mercado ao longo dos anos, mas nenhum mercado pode ser verdadeiramente livre quando há uma força motriz tomando decisões por ele.

## **Como Satoshi Conseguiu**

Satoshi está longe de ser a primeira pessoa a trabalhar no problema da moeda digital descentralizada. Criptógrafos e codificadores estavam trabalhando no problema muitos anos antes de 2008.

O desafio da descentralização é manter um livro contábil de transações. Normalmente, quando você paga alguém, o banco subtrai o dinheiro da sua conta e o adiciona à conta do destinatário. Manter o registro contábil da transação é a função principal de um banco.

Em um sistema descentralizado, no entanto, não há banco. Qualquer pessoa pode enviar uma solicitação de transação para a rede descentralizada. Isso torna o livro contábil descentralizado muito vulnerável a ataques. Maus participantes poderiam alterar o livro, ou gastar uma moeda digital várias vezes antes que a rede percebesse.

A inovação de Satoshi foi a tecnologia que, agora, chamamos de blockchain. Ele encontrou uma maneira de manter um livro-razão seguro, usando registros de data e hora, muito poder de

processamento descentralizado e criptografia. Bitcoin – o primeiro blockchain – ainda hoje usa a arquitetura de Satoshi para garantir pagamentos.

## **Então, É Uma Moeda?**

Uma das maiores perguntas que as pessoas têm sobre a Bitcoin é "É uma moeda"?

A resposta se encontra em uma área cinzenta. Bitcoin é um método de pagamento e uma maneira de transferir fundos. Você pode usar Bitcoin para fazer compras ou enviar pagamentos. É possível converter Bitcoin em dólares, euros, libras, ienes ou qualquer outra moeda. No entanto, não é apoiada por nenhuma instituição. Não há governo central para o qual você possa apontar, e não há garantias quando se trata de possuir Bitcoin. Só é valiosa na medida do número e tipos de lugares e pessoas que a aceitam.

Bitcoin é o que chamamos de moeda digital em sua forma mais pura, ou o que é conhecido como criptomoeda. Bitcoin foi a primeira criptomoeda, mas, agora, existem muitas delas. As criptomoedas operam de maneira diferente das moedas tradicionais, pois são baseadas em código, não nas decisões de um banco central. Esta diferença as torna atraentes, mas também mais voláteis.

## Sobre O Custo

Uma das maiores características de uma moeda verdadeira é o valor estável. Muitas pessoas argumentam que a Bitcoin não é uma moeda, devido ao seu valor volátil. O preço da Bitcoin tem flutuado bastante e, ocasionalmente, dobra de valor em um curto período de tempo.

Por exemplo, em julho de 2010, o preço era de US \$ 0,08 por Bitcoin. Em dezembro de 2017, a Bitcoin atingiu US \$ 20.000. Em média, varia em torno de 2% ao dia. Isso é algo que você não vê nas moedas tradicionais, levando muitos a dizer que é inútil tratá-la como uma. Um preço estável é o que convencerá o investimento tradicional e levará a um crescimento sustentado.

Isso importa para a Bitcoin? Depende de como você olha. No curto prazo, a volatilidade do preço pode ter um enorme impacto na confiança das pessoas. Ao tentar atrair novas pessoas para o mundo das criptomoedas, o preço em rápida mudança pode, definitivamente, ser um problema.

A chave é olhar para a situação geral. Se você é alguém que está interessado em fazer parte de uma mudança econômica verdadeiramente revolucionária, o plano a longo prazo é o mais importante.

Com isso em mente, muita pesquisa mostrou que a Bitcoin deverá se estabilizar em algum momento no futuro, e flutuar muito menos. Os altos e baixos típicos podem ser amplamente atribuídos à quantidade de publicidade que a Bitcoin está recebendo em um determinado momento.

Há também uma alta probabilidade de os governos começarem a regular as criptomoedas nos próximos anos. Embora a própria regulamentação não seja capaz de acabar com as moedas descentralizadas, ela terá um forte efeito moderador sobre quanto e com que rapidez as avaliações mudam.

## O Que É Uma Criptomoeda?

**B**

“Criptomoeda: uma moeda digital na qual são usadas técnicas de criptografia para regular a geração de unidades de moeda e verificar a transferência de fundos, operando independentemente de um banco central.”

A definição de criptomoedas requer muitas informações técnicas que abordaremos mais detalhadamente mais adiante neste livro, mas vale a pena uma introdução aqui para que você possa entender do que estamos falando.

Em termos simples, uma criptomoeda é composta por linhas de código que têm valor monetário. Usando criptografia, a rede descentralizada cria novas moedas e protege as transações. Alguns membros da rede descentralizada configuram computadores que processam o código. Em troca, esses nós processadores – conhecidos como mineradores – recebem uma recompensa por proteger as transações na Blockchain.

## Então, Por Que Bitcoin?

Bitcoin está longe de ser a única criptomoeda. No entanto, ela consistentemente manteve seu domínio como a criptomoeda número um do mundo nos últimos dez anos.

Há um forte argumento a ser feito de que a Bitcoin não é a melhor criptomoeda do mundo. Novos projetos surgiram com escalabilidade, velocidade e privacidade de transação superiores. No entanto, estas novas moedas não foram capazes de derrubar a Bitcoin do seu trono.

Parte da razão pela qual a Bitcoin manteve sua liderança é o seu começo. A Bitcoin foi a primeira Blockchain de todos os tempos. Todo o interesse inicial na Blockchain, de 2008 a 2013, focou-se na Bitcoin. Isso significa que a Bitcoin tinha a maior base de usuários e a sua escolha de ótimos desenvolvedores para construir o sistema.

Este processo é um ciclo virtuoso para a Bitcoin. Por ter a maior rede, também tem a maior aceitação. Efeitos de rede significa que quanto mais pessoas usam uma tecnologia, mais útil ela se torna.

Veja o email, por exemplo. Não seria útil se você fosse a única pessoa no mundo com um endereço de email. Seria útil se você e algumas outras pessoas tivessem e-mail. Mas é extremamente útil quando quase todo mundo tem um endereço de email. A adoção da Bitcoin é igual. /se torna mais útil quanto mais pessoas a aceitam.

A Bitcoin ainda recebe o máximo presença na imprensa do que qualquer criptomoeda hoje, principalmente porque ainda é a maior. Sua longa história também lhe confere alguma legitimidade.

Ao longo de uma década, a Bitcoin enfrentou e superou muitos obstáculos e desafios técnicos, sempre crescendo novamente. Seu comprovado registro de segurança também a torna a compra de criptomoeda mais segura para iniciantes.

Enquanto outras criptomoedas podem focar em funções específicas, a Bitcoin é uma moeda digital versátil, disponível em quase todas as trocas de altcoin. No estágio atual, é a moeda que possui os investimentos, a base de usuários, a segurança e o histórico.

## **Aprendendo Sobre Bitcoin**

E isto é apenas o começo. Ao longo deste livro, abordaremos todos os aspectos da Bitcoin e forneceremos conselhos do mundo real sobre como começar.

Há muito o que aprender. É fácil ficar perdido nas minúcias da Bitcoin e como sua tecnologia funciona, mas para começar com a Bitcoin, você só precisa entender os fundamentos. É exatamente isso que você lerá nas próximas páginas.

## **Capítulo 2. Entendendo as transações Blockchain & Bitcoin**

Antes de começarmos a comprar e armazenar sua primeira Bitcoin, vamos falar sobre os fundamentos da tecnologia que faz a Bitcoin funcionar – a Blockchain. Recentemente, a "Blockchain" ganhou status como uma palavra da moda para novas startups. Muitas pessoas que usam o termo não têm uma ideia clara de como a Blockchain protege uma rede descentralizada. Até o final deste capítulo, você entenderá o básico da Blockchain melhor do que muitos entusiastas de criptomoeda.

## **A Blockchain & Bitcoin**

Se você se lembra, foi em 2008 que Satoshi Nakamoto publicou, pela primeira vez, um white paper sobre a tecnologia Bitcoin e detalhou o sistema ponto a ponto que executa as transações de Bitcoin. A moeda Bitcoin em si mesma é uma ideia revolucionária. No entanto, a tecnologia que a alimenta é a verdadeira inovação. A Blockchain de Satoshi torna possível criar registros descentralizados seguros para qualquer coisa, não apenas para criptomoedas.

A Blockchain Bitcoin é o livro público que contém todas as transações de que foram feitas na história da Bitcoin. Como não existe um órgão de administração central ou banco de dados, o razão fica em uma rede composta por todos os computadores que executam o software Bitcoin. Todos trabalham juntos para construir a rede.

Tudo isso acontece em público, e qualquer pessoa pode ver o tráfego enquanto está acontecendo. Este nível de transparência é quase inédito em qualquer outro sistema financeiro. Essa transparência é o que torna as criptomoedas únicas.

De maneira mais geral, a Blockchain pode afetar qualquer parte de nossas vidas em que precisamos verificar a identidade, realizar uma transação ou garantir um contrato. O registro público na Blockchain pode ser mais rápido, mais barato e mais seguro do que muitas instituições em que confiamos hoje.

## Como as Transações de Bitcoin Funcionam?

Bitcoins não existem fisicamente. Não há cofre de bitcoins em algum lugar. Quando você pensa sobre isso, não é tão diferente do nosso dinheiro moderno. O dinheiro que você vê ao fazer login na sua conta bancária não significa que existe uma caixa com seus fundos. Da mesma forma, não há nada que possa ser definido, como "esta é uma Bitcoin".

Em vez disso, quando você inicia uma transação, envia sua solicitação de transação para toda a rede. Os mineradores na rede adicionarão sua transação ao razão público, juntamente com outras solicitações de transação atualmente na rede. Esse livro é carimbado com a hora, vinculado ao último livro produzido e bloqueado com uma chave criptográfica. Um livro razão carimbado, vinculado e bloqueado é chamada de bloco.

### Blocos

Os blocos de transações contêm tudo o que precisam tanto para adicionar novas transações como também conectar o bloco a todas as anteriores. Há quatro itens incluídos em cada bloco: uma referência ao bloco anterior na cadeia, todas as transações sendo adicionadas, um carimbo de data e hora e a prova criptográfica que mostra como o bloco foi criado.

Esta combinação de carimbo, vinculação e bloqueio de blocos foi a inovação da Satoshi na criação da Bitcoin. Ela resolve os problemas de criação de um livro razão ao qual qualquer pessoa pode adicionar:

- O registro de data e hora mostra onde o bloco pertence na ordem, garantindo que os blocos não se misturem ou que vários blocos não sejam respeitados pela rede ao mesmo tempo.
- O link é uma referência ao bloco anterior, incorporado no conteúdo do bloco atual. Isto assegura o lugar do bloco em uma longa cadeia de blocos. A Blockchain!
- O bloqueio criptográfico no bloco é conhecido como hash. Os mineradores da rede usam seu poder computacional para calcular este hash. Para a Bitcoin, é um quebra-cabeça incrivelmente difícil que leva aos processadores mais rápidos do mundo, em média, 10 minutos para resolver.

Ao hospedar todas estas informações em um único bloco, o sistema Blockchain é capaz de se auto-regular, não requerendo vigilância para sua supervisão. Não há necessidade de alguém verificar manualmente as transações. Depois de se fazer o hash, é quase impossível alterar o conteúdo de um bloco.

Alterar o conteúdo de um bloco exigiria a edição do razão, a reconstrução do bloco e a resolução do quebra-cabeça criptográfico novamente. É melhor que você espere que seu computador seja mais rápido do que todos os outros computadores da rede, porque você precisará vencer a corrida para concluir o quebra-cabeça, se quiser que seu bloco seja implementado. Isto é altamente improvável, dado o enorme poder de computação na rede Bitcoin.

Os blocos são organizados em uma cadeia e, se você quiser alterar uma transação mais antiga, precisará editar este bloco e resolver o novo quebra-cabeça. Mas a resposta para o antigo quebra-cabeça original está embutida no próximo bloco da cadeia. Você também teria que atualizar o próximo bloco, desta vez com a nova resposta do quebra-cabeça! Toda vez que você edita um bloco, você teria que resolver novamente o quebra-cabeça de todos os blocos que vieram depois. Quanto mais quebra-cabeças de blocos você tiver que resolver, menor a probabilidade de implementar seu ataque

com sucesso. As transações de Bitcoin com mais de uma hora de idade são estatisticamente quase impossíveis de mudar.

Depois que uma transação é adicionada à Blockchain, ela existe para sempre e é registrada em todos os computadores da rede. Dessa forma, a Blockchain é um dos bancos de dados mais seguros que se possa imaginar.

## **Confirmações**

As transações bem-sucedidas devem ser confirmadas, para garantir que estejam corretas. Mineiros, que criam um novo bloco e o adicionam ao Blockchain a cada dez minutos, fazem isso. Os mineiros verificam transações, registram-nas no livro público e adicionam-nas ao próximo bloco. Uma vez resolvido o bloco, a transação é considerada verificada e as alterações são improváveis.

Conforme descrito acima, torna-se cada vez mais difícil alterar uma transação quanto mais o tempo o bloco estiver na cadeia. Por este motivo, algumas pessoas preferem esperar vários blocos antes de chamar a transação de "confirmada".

Ao usar Bitcoin em uma loja, alguns comerciantes podem não forçá-lo a esperar. No entanto, isto significa que eles estão se arriscando com você, no recebimento de seu pagamento. Isto é mais comum geralmente em transações de baixo valor, pois existe um menor risco de fraude.

## **Taxas**

Como em todos os sistemas transacionais, a Bitcoin tem taxas a cada transferência. Há uma distinção importante aqui, no entanto: As taxas não são obrigatórias e podem ser determinadas pela pessoa que envia os fundos.

Em troca por confirmações mais rápidas, os mineradores coletam e processam as taxas. Pague o suficiente, e o minerador moverá sua transação para o topo da pilha, para ser adicionada já ao próximo bloco. Depois de criarem com sucesso um novo bloco Bitcoin, eles cobrarão as taxas de todas as transações incluídas neste bloco específico.

As taxas são totalmente voluntárias e a pessoa que inicia a transação pode decidir se deseja ou não incluir uma taxa. Ao incluir uma taxa, no entanto, você pode garantir que os mineradores tenham um incentivo para processar sua transação. Se você optar por não incluir uma taxa, os mineiros processarão outras transações antes da sua. Você pode esperar horas (ou mesmo dias) antes de sua transação gratuita ser incluída em um bloco.

Algumas carteiras (onde você mantém e gerencia sua Bitcoin) decidem a taxa de transação por você. Falaremos mais sobre carteiras em breve.

## **A Blockchain & Transações**

A Blockchain parece um pouco menos misteriosa agora? Este é apenas o começo desta incrível invenção. Eu escrevi um livro inteiro sobre a tecnologia Blockchain (<https://geni.us/blockchain-es>). Se você estiver interessado, este livro mergulha no âmago da questão.

Mais tarde, abordaremos mais a respeito dos mineradores sobre os quais você está lendo, mas, por enquanto, vamos passar para algumas informações úteis sobre como obter e gastar Bitcoins.

## Capítulo 3. Introdução à Bitcoin

Com uma criptomoeda como a Bitcoin, o mais importante é obter boas informações e entender o sistema antes de entrar. A Bitcoin não tem uma autoridade central, portanto, as transações não podem ser revertidas. Se você cometer um erro com sua Bitcoin, será permanente. Dito isto, tenha cuidado, invista apenas um pouco de cada vez e faça suas pesquisas.

Este livro é uma boa introdução, mas é praticamente impossível cobrir tudo o que você encontrará no mundo da Bitcoin. O melhor conselho que posso dar é leia o máximo que puder.

A Bitcoin pode parecer assustadora ou complicada. O objetivo deste capítulo é familiarizar-se com conceitos básicos e regras básicas para começar com a Bitcoin. Lembre-se de que haverá explicações mais profundas sobre estas coisas no livro; portanto, não se prenda muito a nenhum destes aspectos.

## **Segurança Pessoal na Bitcoin**

Antes de dar algum conselho sobre como comprar, manter, vender e negociar em Bitcoin, precisamos falar sobre segurança. A própria rede Bitcoin é altamente segura. A rede Bitcoin nunca foi hackeada diretamente, sendo extremamente improvável que alguém possa mudar uma transação no razão público da Bitcoin.

O risco de segurança de possuir Bitcoin vem de descuido pessoal ou de lidar com terceiros provedores de serviços. Aqui alguns pequenos conselhos:

### **Nunca Compartilhe Sua Chave Privada**

Esta é a primeira regra de segurança da Bitcoin, e deveria ser óbvia. Nenhuma empresa ou pessoa legítima solicitará sua chave privada Bitcoin (a menos que você esteja autorizando um gasto). Os endereços Bitcoin não estão vinculados à sua identidade. Você não precisa fornecer identificação ao criar a maioria das carteiras, e a única coisa que distingue o proprietário de uma carteira é conhecer a chave privada.

Como tal, qualquer pessoa que possua sua chave privada pode gastar sua Bitcoin. Ponto. E não há como reverter transações ou denunciar fraudes na Bitcoin. Nunca compartilhe sua chave privada.

### **Não Perca Sua Chave Privada**

Um efeito colateral dos endereços anônimos é que não há como recuperar sua chave privada se você a perder. A única maneira de acessar seu endereço é com essa chave. Se você perder sua chave, seus fundos estarão perdidos para sempre.

A maioria das carteiras cuida disso para você, armazenando sua informação de chave com uma senha recuperável. Certifica-se, entretanto, de fazer backup de todas as informações referentes à sua chave confidencial em múltiplos lugares.

### **Tenha Uma Carteira Segura**

Como você suporia, uma carteira é o que contém a Bitcoin que você recebe. Existem muitas opções diferentes que discutiremos, incluindo baseadas na Web, baseadas em hardware, dispositivos móveis e muito mais. Muitas pessoas mantêm sua Bitcoin de uso diário em uma carteira normal da Web, enquanto armazenam o restante em uma carteira mais segura, da qual podem fazer backup e manter em segurança. Dessa forma, mesmo que alguém invada seu computador não poderá afetar suas economias. Falaremos mais sobre carteiras diferentes mais tarde.

### **Saiba Que O Preço Mudará**

O preço da Bitcoin muda a cada minuto. É importante entender isso, porque, às vezes, pode ser uma estrada acidentada. Ela tem subido constantemente, mas teve também sua justa parte de quedas de valor. Alguns anos atrás, era quase inacreditável que uma Bitcoin valesse US \$ 100. No momento da redação deste livro, está acima de US \$ 11.000! Embora seja esperado que aumente com o passar do tempo, haverá dias em que o preço cai, e sabemos que tudo faz parte do caminho.

## **Você Não Pode Estornar Pagamentos**

Os pagamentos em Bitcoin não são como cartões de crédito ou PayPal. Depois de enviar dinheiro para alguém, eles são a única pessoa que pode devolvê-lo. Com isso em mente, é vital que você confie na pessoa para quem está enviando fundos e sempre verifique o endereço da carteira.

Caso você envie Bitcoin para o endereço errado, é provável que não a recupere. Verifique, dupla e triplamente, todos os detalhes da transação antes de enviar fundos.

Se algo acontecer, não há uma empresa central que possa ajudar. Isto tem efeitos bons e ruins no uso de Bitcoin em comparação com outros métodos de pagamento, mas falaremos sobre isso um pouco mais adiante.

## **Bitcoins são Rastreáveis**

Como a Bitcoin opera em um livro público, qualquer pessoa pode ver o histórico de transações na rede. As transações são apenas uma lista de endereços públicos e valores de transação. Ainda assim, investigadores inteligentes podem criar uma rede de transações e identificar tendências. Com o tempo, um investigador dedicado pode descobrir qual endereço é seu e ver todos os endereços para os quais você efetuou pagamentos em Bitcoin.

Existem maneiras de evitar ser rastreado na Bitcoin. Você pode usar vários endereços ou até um novo endereço para cada nova transação. Você também pode usar serviços de mescla de moedas que mascaram a fonte de fundos ao misturá-los com outros fundos. Ainda assim, vale a pena reconhecer, de antemão, que o razão público é exatamente isso: público.

## **Pode Haver Dores No Crescimento**

A Bitcoin está crescendo rapidamente e pode haver muitas mudanças no futuro. Novas atualizações podem fazer com que alguns fornecedores repensem seus serviços e preços, as confirmações podem desacelerar, as taxas podem aumentar ou qualquer outra coisa pode acontecer. Não há como dizer como as coisas vão mudar, mas desde que você entenda o que está por trás de tudo isso, você ficará bem.

## **Introdução À Bitcoin**

Este é apenas o começo da Bitcoin. Há muito a aprender, mas vou orientá-lo para garantir que você se sinta seguro, e bem informado o suficiente, para entrar nesta moeda digital de rápido crescimento e que só vai aumentar!

## Capítulo 4. Onde guardar sua Bitcoin

### Seu Endereço de Bitcoin

Você já enviou um e-mail para alguém antes, certo? Esse endereço específico permite que essa pessoa envie e receba mensagens para qualquer pessoa na Web com um endereço de email. Endereços de Bitcoin funcionam da mesma forma, embora haja uma diferença fundamental.

### O Que É Um Endereço De Bitcoin?

Um endereço Bitcoin é a sequência específica de caracteres que identifica sua carteira. Ao contrário do exemplo de endereço de email, no entanto, uma única carteira pode ter vários endereços e até um novo para cada nova transação que você fizer.

No caso da Bitcoin, o endereço tem entre 26 e 35 caracteres alfanuméricos. Cada endereço também começa com 1 ou 3 e diferencia maiúsculas de minúsculas. Esta sequência de caracteres deve ser exata ou os fundos não podem ser transferidos, mas isso não deve surpreender ninguém que tenha transferido fundos tradicionais antes.

Quando você deseja receber fundos, compartilha seu endereço de Bitcoin com a pessoa que paga. Você também pode listar seu endereço publicamente. Compartilhar seu endereço não fornece acesso à sua conta de forma nenhuma. Apenas informa à rede para onde direcionar os fundos.

**B**

“Aqui está um exemplo de endereço de Bitcoin:

1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2”

## **Endereços de uso único**

Enquanto os endereços de email, para usar nosso exemplo anterior, não mudam, a maioria dos especialistas recomenda o uso de um novo endereço de Bitcoin para cada transação. Como o endereço não é o mesmo da sua carteira, isto significa que você não está criando uma nova carteira, mas simplesmente usando um novo identificador para as pessoas que lhe enviam Bitcoin. Há várias razões para isso.

### **Anonimato**

Há um grande problema com a reutilização de um endereço Bitcoin: Você corre o risco de perder o anonimato que acompanha a Bitcoin.

Cada vez que você usa um endereço Bitcoin, coloca mais informações à disposição do público sobre de onde a Bitcoin veio ou para onde foi. Como a Bitcoin opera em um livro público, as pessoas podem ver seu endereço quando ele aparece no livro. Com o tempo, usar o mesmo endereço repetidamente significa que maus elementos poderiam mapear seus relacionamentos, transações e fundos recebidos. Quanto mais você usa e aborda, mais informações alguém pode aprender sobre você.

#### **B**

“Isso nem sempre é provável. Isso só deve ser uma preocupação se você quiser ter absoluta certeza de que é anônimo.

Com isso em mente, a criação de novos endereços para cada transação ajuda a preservar sua identidade e manter suas transações mais anônimas. Mesmo quando as transações são registradas em público, esta é uma maneira eficaz de manter um escudo de anonimato.

Criar um novo endereço geralmente é tão simples quanto clicar em um botão no seu cliente de carteira. Discutiremos as carteiras em breve.

### **Identificar Pagamentos**

Se você é uma empresa ou é alguém que gostaria de acompanhar as transações, é muito mais fácil fazer isso com endereços de uso único.

Ao vincular as transações a um endereço exclusivo, você sempre pode verificar se recebeu um pagamento com base no endereço que você forneceu. Isto também é verdade se cada cliente usar o mesmo endereço atribuído a eles, mas não é a maneira recomendada de receber fundos.

Desta forma, cada pagamento recebe seu próprio tipo de identificador exclusivo. Isto é especialmente útil se você estiver gerenciando um grande departamento de contas a receber ou a pagar.

### **Alguma Razão Para Não Fazer Isso?**

Pode parecer um aborrecimento, ou irrelevante, criar novos endereços para cada transação. Se você está fazendo apenas transações mínimas ou não está preocupado em ser rastreado, qual é o problema?

No final, é apenas um bom hábito de se criar e manter. Aumentar o anonimato dos seus pagamentos aumenta o anonimato geral da rede. Se todos criassem novos endereços, seria difícil

rastrear os pagamentos, mesmo em um livro público. Como veremos mais adiante, esta privacidade da rede como um todo é importante para a fungibilidade e usabilidade da Bitcoin.

O consenso esmagador é que praticamente não há motivos para não usar um endereço novo para cada transação, exceto a etapa adicional de clicar para criar um.

## **Criando Um Endereço De Bitcoin**

Então, agora que você sabe que deve criar um novo endereço para cada transação, como você, em realidade, faz isso? A resposta não poderia ser mais simples.

Sua carteira fará isso por você. Carteiras são softwares que ajudam a gerenciar seus fundos e vários endereços.

Varia um pouco de carteira para carteira, mas, na maioria dos casos, basta abrir a carteira e clicar em "Criar novo endereço" ou algo semelhante.

## **Конец ознакомительного фрагмента.**

Текст предоставлен ООО «ЛитРес».

Прочитайте эту книгу целиком, [купив полную легальную версию](#) на ЛитРес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.