

# A BÍBLIA DO INVESTIMENTO EM CRIPTOMOEDA

O GUIA DEFINITIVO SOBRE BLOCKCHAIN, MINERAÇÃO, TRADING, OIM,  
PLATAFORMA ETHEREUM, BOLSAS, TOP CRIPTOMOEDAS PARA INVESTIR  
E ESTRATÉGIAS PERFEITAS PARA GANHAR DINHEIRO



ALAN T. NORMAN

Alan T. Norman

**A Bíblia Do Investimento  
Em Criptomoeda**

«Tektime S.r.l.s.»

**Norman A.**

A Bíblia Do Investimento Em Criptomoeda / A. Norman —  
«Tektime S.r.l.s.»,

ISBN 978-8-83-540204-6

Antes de definir metas nos negócios de criptomoeda, primeiro vamos revisar alguns equívocos comuns sobre criptomoeda. **MITOS SOBRE AS CRIPTOMOEDAS**

Admito francamente que também quase fui infectado pelo ceticismo em relação à criptomoeda no início da minha jornada, pois muitas pessoas me assustaram ao dizer que a criptomoeda é um empreendimento selvagem, uma pirâmide financeira ou algo semelhante. Essas falsas crenças muitas vezes afastam muitas pessoas de um possível sucesso. Apenas um pequeno número de defensores verifica tais declarações sobre criptomoeda em vez de acreditar nelas cegamente. Estou certo de que você também ouviu alegações de que nenhum país jamais reconhecerá as criptomoedas, portanto, elas não têm futuro. Para refutar isso, basta recordar o recente aumento no valor da criptomoeda. Alguns países já as reconheceram como meio de pagamento. Assim, esse chamado “entretenimento para geeks” evoluiu para negócios muito reais para investidores e várias corporações. Portanto Criptomoeda, Bitcoin, ICO, blockchain, mineração ... Ao ouvir essas palavras há apenas alguns anos, as pessoas costumavam dizer: é uma farsa; bolha financeira; não faz sentido investir; o preço é muito baixo; nenhum país nunca reconhecerá a criptomoeda; obviamente é um esquema de pirâmide; é diversão para nerds; não é sério; entrará em colapso em alguns anos... Até recentemente, a criptomoeda era vista como uma espécie de diversão para um punhado de escolhidos que compravam e vendiam algo e acreditavam que a nova moeda seria bem sucedida um dia! Você certamente também estava entre as pessoas que não levaram o Bitcoin e a criptomoeda a sério, mas os eventos atuais atormentam até os maiores céticos. O preço atual do Bitcoin é US\$ 8.640. O preço da criptomoeda mais popular quebra repetidamente todos os recordes inimagináveis. A capitalização é de cerca de US\$ 120 bilhões. Reconhecimento mundial. As maiores economias do mundo - Índia e Japão - reconheceram o Bitcoin como a moeda oficial. As autoridades dos EUA reconheceram a criptomoeda como ativo. Mineração

em escala industrial. Isso é só o começo. O mercado de criptomoedas está mudando extremamente rápido e é quase impossível monitorar a situação e tomar as decisões corretas por conta própria. A maioria das pessoas não tem experiência, tempo ou dinheiro para isso. Meu livro fornece informações básicas, mas bastante abrangentes, não para pessoas que andam perseguindo arco-íris, mas para as que desejam construir um negócio lucrativo a longo prazo em uma das áreas de criptomoeda: da mineração ao investimento. Portanto, este livro não trata de: maneiras ilegais de ganhar dinheiro, elogiando a criptomoeda e incentivando você a investir nela até o último centavo; técnicas de fraude para ganhar dinheiro rapidamente; teoria chata e sem sentido; maneiras de ganhar milhões sem investimentos nem riscos. Aqui o ajudarei a aprender a maneira de ganhar dinheiro no mercado de criptomoedas que melhor combina com você: onde você deve começar se tiver apenas US\$ 500; quais informações sobre criptomoeda os especialistas retêm (tire os óculos de cor rosa!); como elaborar uma estratégia pessoal, configurar seu próprio negócio de criptomoedas e ganhar seus primeiros US\$ 3.000 a 10.000 dentro de um ou dois anos. Também posso garantir que você vai: decifrar a principal tendência atual da moeda, mesmo que não tenha noção de economia, finanças e tecnologia; entender se realmente deseja investir em criptomoeda (talvez esse tipo de negócio não seja o seu preferido e você não vai perder seu tempo); aprender a verificar os riscos e a não investir na primeira moeda disponível; experimentar, proteger-se de possíveis falhas e evitar despejar dinheiro pelo ralo, o que inevitavelmente acontecerá se você ficar cego. Assim, meu objetivo é bastante simples: ajudá-lo a configurar e desenvolver negócios em uma das áreas de criptomoeda. Descubra 7 estratégias de investimento em criptomoeda + 2 estratégias perfeitas hoje!

ISBN 978-8-83-540204-6

© Norman A.  
© Tektime S.r.l.s.

## Содержание

Por que você deve ler este livro	7
Capítulo 1. Mitos Sobre Criptomoeda e As Regras Principais Do Mercado De Criptomoeda	9
Mitos Sobre a Criptomoeda	10
Por que você deve entrar no mundo dos negócios de criptomoeda agora	11
Definir metas e identificar as principais regras do mercado	12
Capítulo 2. Princípios Básicos da Criptomoeda e o Batman dos Nossos Tempos	14
As Vantagens da Criptomoeda	16
O inventor do Bitcoin e por que ele é o Batman dos nossos tempos	17
Capítulo 3. Bitcoin e mineração	18
Como funciona o Processo de Mineração	20
Prova de Trabalho e por que é importante	23
Capítulo 4. Blockchain	25
Como o Blockchain funciona?	26
Конец ознакомительного фрагмента.	28

# Alan T. Norman

## A Bíblia do Investimento em Criptomoeda

A Bíblia do Investimento em Criptomoeda

**O Guia Definitivo Sobre Blockchain, Mineração, Trading,  
OIM, Plataforma Ethereum, Bolsas, Top Criptomoedas  
Para Investir e Estratégias Perfeitas Para Ganhar Dinheiro**

**Alan T. Norman**

**Traduzido por**

**Andrea Luri Abe**

Obtenha seu livro gratuito **Baleias do Bitcoin**

*(Encontre o link no final deste livro)*

**Copyright © 2020 Alan T. Norman.**

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.

## Por que você deve ler este livro

A maioria das pessoas recebe novas ideias com grande medo, ceticismo e até negação. Naturalmente, é muito mais seguro ficar na zona de conforto e continuar andando na mesma trilha batida de sempre. No entanto, em algum momento, talvez valha a pena se perguntar: até onde esse caminho me levará? O mais provável é que não leve você além da volta da esquina.

Movimento é progresso. Portanto, você deve manter a mente aberta e aprender coisas novas para não se deteriorar enquanto o mundo segue em frente. Isso é verdade para muitas áreas de nossas vidas e também para as finanças pessoais.

Por um lado, o papel-moeda não é mais prevalente. Você provavelmente concordará que é mais conveniente pagar nossos custos e confortos com aquele cartãozinho de plástico emitido pelo seu banco. Este tipo de liquidação sem dinheiro é muito melhor por razões de segurança também.

Não faz muito tempo, a humanidade descobriu outro tipo de dinheiro completamente novo – dinheiro digital ou criptomoeda. Esta é uma nova geração de moeda que é criada através do uso de software de criptografia. Essas unidades de criptomoeda são formadas e mantidas através de criptografia algorítmica.

Eu gostaria de me concentrar um pouco nos tipos de problemas que a criptomoeda pode resolver. Essa é uma questão que vou abordar ao longo deste livro, mas, por enquanto, quero chamar sua atenção para um conceito chamado *confiança*. É esse importante problema que a criptomoeda resolve. Deixe-me explicar usando um exemplo da minha vida.

Decidi que queria criar um negócio e ganhar algum dinheiro quando estava na faculdade. Três colegas e eu começamos a vender flores. Cada um de nós escrevia as informações sobre seus ganhos em um caderno velho, que íamos passando um para o outro. Quando o caderno chegou às minhas mãos, e eu realmente queria sorvete, me perguntei se poderia mudar os números registrados para meu próprio benefício. Mas eu me repreendi e pensei: e se meu amigo fizesse o mesmo? Assim, é óbvio que a desconfiança pode surgir mesmo entre os amigos mais próximos. A criptomoeda resolve este problema, pois não nos permite adicionar ou alterar algo, uma vez que está no sistema.

No entanto, o surgimento da criptomoeda, que resolve o enorme problema da confiança, não deve ser associado à explosão de um cometa, de um presente do céu ou de qualquer outro tipo de começo de conto de fadas. De fato, a criação da criptomoeda é muito mais simples.

Primeiro, as tecnologias correspondentes, como a EXEMPLE, apareceram e, em seguida, a criptomoeda surgiu em sua base, seguida pela mineração (a produção de criptomoeda). Somente depois disso, tokens, OIMs e vários modelos de negócios de criptomoeda surgiram com base em todo esse ecossistema. O registro, que as protege contra manipulação (por exemplo, repositório de banco de dados), tornou-se a primeira tecnologia na economia de criptomoedas. Há uma pequena (ou grande) peculiaridade de tais registros: você pode inserir qualquer dado nesse banco de dados, mas não pode forjar nada ou inserir informações retroativas. Esses contratos auto-obrigatórios são a segunda tecnologia importante no mundo da criptomoeda. Eles são *estritamente ligados* ao banco de dados.

Não vou me aprofundar nos detalhes por trás de toda essa tecnologia neste livro já que expliquei o básico do meu livro anterior, *Dominar a Bitcoin para Principiantes* (<https://geni.us/bitcoin-pt>). No presente manual, vou dizer-lhe como funciona a criptomoeda, as dez principais criptomoedas e quais são os câmbios de criptomoedas e os câmbios de moeda digital. Também explicarei a implementação técnica do Blockchain, da plataforma Ethereum e de muitas outras questões do mundo da criptomoeda. O ponto mais interessante é que vou descrever muitas estratégias inteligentes de investimento.

Desde o início, quero avisá-lo que o mercado de criptomoedas está vivo e mudando. Funciona 24 horas por dia, sete dias por semana. Portanto, as informações atualizadas no dia em que escrevi o

livro podem não estar tão atualizadas no dia em que você o ler. Eu recomendarei recursos neste livro os quais você possa consultar para acompanhar as mudanças.

A última coisa a mencionar aqui: suponho que haja céticos entre os leitores deste livro. Concordo que devemos conhecer todas as novas ideias, mantendo um certo grau de ceticismo, mas também devemos ser razoáveis. Portanto, antes de tirar conclusões precipitadas sobre a criptomoeda, sugiro que leia atentamente o livro e depois analise as informações que compartilho aqui. Dito isso, coloque seu veredicto sobre criptomoeda no congelador por enquanto.

Se você está pronto para mergulhar no mundo da criptomoeda, venha!

## **Capítulo 1. Mitos Sobre Criptomoeda e As Regras Principais Do Mercado De Criptomoeda**

Antes de estabelecer metas no negócio de criptomoeda, vamos passar por alguns equívocos comuns sobre ela.

## Mitos Sobre a Criptomoeda

Eu francamente admito que também quase me infectei com ceticismo em relação à criptomoeda no começo da minha jornada, já que muitas pessoas me assustaram dizendo que a criptomoeda é um empreendimento selvagem, uma pirâmide financeira ou algo parecido. Tais falsas crenças frequentemente afastam muitas pessoas do possível sucesso. Apenas um pequeno número de defensores verifica tais afirmações sobre criptomoeda, em vez de apenas acreditar cegamente nelas.

Tenho certeza de que você também ouviu alegações de que nenhum país jamais reconhecerá a criptomoeda, portanto a criptomoeda não tem futuro. Para refutar isso, basta lembrar o recente aumento no valor da criptomoeda. Alguns países já reconheceram a criptomoeda como meio de pagamento. Assim, este chamado "entretenimento para geeks" evoluiu para negócios muito reais de bancos de investimento e várias corporações.

Portanto, se você, pessoalmente, ainda não ganha dinheiro em criptomoedas, é mais provável que seja devido ao grande número de declarações mencionadas anteriormente, que você pode ter ouvido de pseudoespecialistas.

Vamos enumerar as declarações que fazem muitas pessoas desistirem no meio do caminho:

1. É muito arriscado. E se eu investir dinheiro e a criptomoeda for banida em todo o mundo no dia seguinte?
2. Eu não tenho nenhuma educação financeira, então eu não saberia o que estou fazendo;
3. Meu amigo / irmão / vizinho investiu dinheiro em criptomoedas e perdeu tudo;
4. O tema da criptomoeda é muito novo e difícil de entender, pois é melhor esperar alguns anos quando tudo ficar claro.

Todas essas declarações são apenas desculpas para a sua inércia. Enquanto você vem com mais desculpas, pessoas de todo o mundo já construíram um negócio no mercado de criptomoedas e estão lucrando. Pergunte a si mesmo: o que me faz pior do que essas pessoas? Se você perceber que não é pior do que seu amigo / irmão / vizinho, que já ganha dinheiro no mercado de criptomoedas, então faça a seguinte pergunta: por que eu deveria entrar no mundo dos negócios de criptomoedas agora mesmo?

## Por que você deve entrar no mundo dos negócios de criptomoeda agora

Então eu vou responder a esta questão ponto por ponto. Cada um dos argumentos começará com as palavras **agora mesmo**, para que você entenda melhor por que deveria fazer isso **agora mesmo**.

Primeiro, **agora mesmo** há muito pouca concorrência no mercado. Alguém se surpreendeu? É verdade. Sim, o interesse neste tópico cresce constantemente, mas em geral a concorrência ainda é muito baixa. Este mercado ainda é bastante "selvagem" e não dominado. A razão para isso é que a maioria das pessoas costuma não confiar em novas tendências e empreendimentos, como já mencionamos acima.

Em segundo lugar, **agora mesmo** você pode obter altos retornos nesse mercado. Os preços da criptomoeda estão no estágio de crescimento e desenvolvimento, mas mesmo assim, você pode ganhar uma quantia razoável de dinheiro. Contanto que gerencie seus riscos com sabedoria, você pode obter lucros com o tempo.

Terceiro, **agora mesmo** existem muitos espertinhos no mercado. Eles chegam ao mercado de criptomoedas para fazer um dinheirinho rápido sem se aprofundar no assunto. Normalmente, essas pessoas vêm dos esquemas de pirâmide liderados pelos chamados "especialistas" que ensinam as pessoas sem ter nenhuma experiência real no assunto. Devo admitir que o mercado encorajou essas pessoas no começo, quando tiveram a chance de ganhar muito dinheiro na época. No entanto, hoje em dia, se você quiser alcançar algo como isso no mercado de criptomoedas, você terá que fazer esforços reais.

Em quarto lugar, **agora mesmo** existem baixos riscos no mercado. Cinco anos atrás, a maioria das pessoas esperava pelo dia em que a criptomoeda seria banida oficialmente. Atualmente, muitos países ao redor do mundo já reconheceram a relevância da criptomoeda. A criptomoeda ganhou tal impulso que ninguém pode simplesmente pressionar o botão de parada agora. Você realmente acha que esse fato não prova que você pode investir seu dinheiro sem medo de várias proibições e restrições?

Finalmente, antes de passar para as regras do jogo no mercado de criptomoedas, sugiro considerar o futuro da criptomoeda através do exemplo da empresa Tesla. Atualmente, o custo de um Tesla é estimado no valor que, de acordo com as previsões dos especialistas, ele não poderá recuperar suas despesas em 300 anos. Por que os especialistas inteligentes classificam Teslas tão altamente? Vamos resolver isso.

Hoje em dia, um carro elétrico é bonito e elegante, mas caro e não é um veículo muito prático. No entanto, os especialistas não estão preocupados com hoje. Eles visualizam um futuro que pode se tornar realidade em 20 ou 30 anos. É difícil imaginar nos próximos anos os carros comuns que vemos diariamente nas ruas agora. Você pode imaginar seu antigo carro amado no futuro, mas, pessoalmente, imagino algum tipo de veículo semivoador com painéis solares ou algo ainda mais sofisticado. Portanto, é o veículo elétrico que terá um futuro brilhante e bem-sucedido, e a Tesla provavelmente ocupará uma posição de liderança no mercado.

Acontece que, em geral, ninguém sabe ao certo se a Tesla manterá sua posição no mercado pelos próximos 20 a 30 anos. No entanto, muitas pessoas acreditam firmemente que isso acontecerá, e essa crença faz com que elas invistam na empresa. Portanto, pessoalmente, posso facilmente acreditar que a Tesla manterá o monopólio em todo o setor de fabricação automotiva em 20 anos.

Como este exemplo está ligado ao futuro da criptomoeda? Hoje em dia, algumas pessoas veem a criptomoeda (como um veículo elétrico) como algo sem sentido – uma tendência moderna, interessante e tecnicamente curiosa. Mas uma tendência, no entanto. No entanto, essa pequena gota agora deve crescer em um grande mar dominante no futuro.

## **Definir metas e identificar as principais regras do mercado**

Antes de abrir novos caminhos, verdadeiros profissionais aprendem as regras do jogo e estabelecem metas, determinando o tipo de resultado que desejam alcançar. Como somos profissionais, primeiro vamos lidar com essa tarefa.

Os seguintes pontos devem certamente estar entre os objetivos comerciais de criptomoeda que você definirá para si mesmo:

- defina a soma específica de dinheiro ou porcentagem de sua renda que você investirá mensalmente na área de criptomoeda;
- defina o grau de sua disponibilidade para riscos;
- defina seus objetivos específicos a curto e longo prazo.

Tendo definido as metas, é importante entender o que é necessário para uma inicialização bem-sucedida e rápida no mercado de criptomoedas. Você ficará surpreso, mas a teoria é a coisa menos importante neste campo. Muitas pessoas dizem que lhes falta informação e conhecimento para fazer este tipo de negócio. No entanto, a maioria das estratégias sobre as quais falarei não exige um profundo conhecimento do mundo dos negócios de criptomoedas. Será o suficiente para você ter controle sobre os princípios básicos da economia da criptomoeda.

Então qual é o problema? Você precisa praticar. Só praticar, não um livro (nem o meu), ajudará você a entender onde comprar, onde vender, como armazenar e como transferir criptomoedas.

Também precisa de:

- Diversas estratégias prontas com baixo risco para entrar no mercado;
- Capacidade de filtrar conteúdo e informações ao seu redor;
- Comunicação com operadores mais experientes do mercado de criptomoedas e "espionagem" em suas ações;
- Gestão de Riscos;
- Uma auditoria de um curador experiente.

E agora vamos para a afirmação que você deve lembrar de uma vez por todas: fazer qualquer investimento no mercado de criptomoedas É UM RISCO. Se você não está pronto para aceitar isso, nem se incomode em tentar. Qualquer opinião ou previsão para o desenvolvimento de uma moeda em particular, a confiabilidade do OIM (isso será discutido mais adiante) é apenas uma posição tendenciosa. Não há uma única pessoa em todo o mundo que possa lhe dar uma garantia de ferro para futuros desenvolvimentos. Não há nenhuma decisão absoluta e garantias de 100%. Eu ou outra pessoa só podemos dar-lhe um conselho, não garantias.

Você é a única pessoa a assumir a responsabilidade por cada decisão. Você não deve, conseqüentemente, culpar um recurso on-line – onde lê sobre as perspectivas de alguma moeda – ou um amigo que recomendou a você uma confiável, ou mesmo a mim, para suas possíveis perdas financeiras! Eu, como autor deste livro, compartilharei meus pensamentos sobre criptomoedas confiáveis com você. No entanto, esta será apenas a minha opinião subjetiva, novamente, apenas neste exato momento. Portanto, se você tende a culpar os outros por seus possíveis fracassos, não a si mesmo, é melhor fechar esse livro imediatamente e não perder tempo.

O mercado de criptomoedas está vivo e em constante mudança. Portanto, ao lidar com o comércio de criptomoedas, é preciso aprender a assumir a responsabilidade pessoal por suas decisões e sempre lembrar que nenhum ganho pode ser obtido sem correr riscos. Sim, existem estratégias menos arriscadas, mas existem riscos em qualquer caso. Invista apenas a soma que você está disposto a perder sem muito arrependimento.

Agora, coloque o livro de lado e anote as duas regras que você nunca deve quebrar:

1. Não invista até o último centavo.
2. Tenha uma reserva de dinheiro para aproveitar oportunidades.

E finalmente, os iniciantes devem aprender vários pontos de segurança:

- Ao negociar na bolsa, proteja sua conta com autenticação de dois fatores e mantenha seu nome de código privado.
- Sua senha deve ter pelo menos 26 caracteres; um gerador de senha especial pode ajudá-lo a criar um.
- Nunca guarde todo o seu dinheiro em um mercado ou em uma carteira.
- Negocie apenas em bolsas testadas e comprovadas.
- Não use pontos de acesso público para negociar no mercado de criptomoedas.

## Capítulo 2. Princípios Básicos da Criptomoeda e o Batman dos Nossos Tempos

Vamos dar uma abordagem completa a esse tópico, começando pelo setor bancário.

Todo o sistema bancário dos nossos dias, independentemente do país, está organizado de tal forma que não possuímos o nosso dinheiro. Os bancos centrais em qualquer estado detêm o monopólio das emissões, que é fornecido através de legislação, criando um obstáculo seguro à legalização das criptomoedas.

A *moeda fiduciária* é um termo usado pela comunidade de criptomoeda para designar uma moeda sem valor intrínseco como dinheiro por regulamentação governamental ou lei (dólar, euro, etc.).

Em teoria, essa moeda deve ser garantida pelo menos pelos bens, produtos ou serviços que são produzidos no território de um determinado país (PIB), de modo que cada cidadão deste país possa trocar seu dinheiro por produtos. Todos os bancos do país também usam a mesma moeda, e o banco central promete manter sua estabilidade e confiabilidade. É assim que funciona na teoria, mas ninguém pode garantir a estabilidade da moeda.

O governo de um país é o principal cliente de todos os bens e serviços para a população, ou seja, um dos maiores empregadores. É também o maior cliente para a construção de estradas, casas, hospitais, escolas, etc. Isso compõe a parte do leão do PIB de cada país em particular. Assim, o governo garante a vida da população – paga pensões e benefícios sociais. Todos esses fundos são retirados do banco central, que pode emitir moeda e financiar o governo.

Uma política *apelidada de flexibilização quantitativa* já foi implementada nos EUA e depois se espalhou para a Europa e o Japão. Devido a esse fenômeno, a quantidade de dinheiro no mundo aumentou muito, enquanto o poder de compra do dólar diminuiu nos últimos 100 anos em 95%. Essa tendência continua. Quanto mais dinheiro existe, mais barato ele se torna.

É importante ter em mente que cada tipo de moeda sofre inflação, o que indica a depreciação da moeda ao longo do tempo. Em outras palavras, a inflação é a velocidade da circulação monetária. As economias dos países têm ciclos próprios à medida que as pessoas pegam empréstimos e depois os pagam.

Não posso deixar de mencionar esses empréstimos. Nos EUA, as taxas de juros dos empréstimos são em média de 1%. Eles permaneceram no nível zero por um longo tempo no passado. Os bancos centrais emitiram dinheiro e compraram ativos financeiros e, portanto, os pobres continuaram pobres e as pessoas que tinham ativos financeiros, ações ou imóveis tiveram lucro constante. É por isso que cada crise torna os pobres ainda mais pobres e os ricos ainda mais ricos. Esses processos resultam em uma estratificação muito poderosa da população. No entanto, infelizmente, a economia funciona dessa maneira, e nos aproximamos de uma espécie de beco sem saída, como muitos analistas financeiros afirmam. Tudo isso para demonstrar que os bancos centrais não cumprem muito bem sua função.

Então, as pessoas começaram a procurar uma maneira alternativa de preservar o valor do dinheiro. Se não multiplicá-lo, pelo menos não perdê-lo. É por isso que muitas pessoas investem em ouro, instrumentos de renda fixa, ações, etc. Ao mesmo tempo, a economia começou a se desenvolver rapidamente depois que a Internet apareceu, então as pessoas perceberam que não precisam mais guardar dinheiro em forma física. Assim, o conceito de dinheiro eletrônico surgiu.



A ideia de criar uma moeda digital como o Bitcoin não é inteiramente nova. Ainda assim, há uma diferença entre o Bitcoin e outros tipos de dinheiro digital. Se você usa sistemas de dinheiro eletrônico como PayPal, Western Union ou Skrill, suas finanças são armazenadas nas mesmas empresas. Neste caso, lidamos com a gestão centralizada de dinheiro, ou seja, o destino do seu dinheiro depende de decisões de pessoas específicas dessas empresas. Você não tem poder para influenciar essas decisões.

## As Vantagens da Criptomoeda

As criptomoedas são bem diferentes. Essas moedas não dependem de um único centro de processamento de transações. É muito difícil rastrear transações de criptomoedas e é impossível cancelá-las. Usando esse tipo de moeda, duas pessoas podem realizar uma transação de compra e venda diretamente na Internet, sem recorrer ao centro de transações financeiras.

Mas vamos discutir mais detalhadamente as vantagens da criptomoeda sobre o dinheiro fiduciário ou tradicional. Tais vantagens são óbvias!

- **Padrões de emissão e circulação:** a criptomoeda é estabelecida uma vez e é inviolável, enquanto os padrões de moeda fiduciária são alterados arbitrariamente pelos bancos centrais.

- **Como a emissão é feita:** as criptomoedas fluem da rede para o participante, enquanto o dinheiro tradicional flui do banco central para os bancos, dos bancos para empresas e apenas das empresas para os participantes.

- **O fluxo de fundos:** direto para criptomoeda; através de bancos, sistemas de pagamento e dinheiro para moedas tradicionais.

- **O número de participantes:** 5 milhões para criptomoeda; 7 bilhões para dinheiro tradicional.

- **Velocidade de transação:** alta para criptomoeda; baixa para dinheiro tradicional.

- **Anonimato:** sempre possível para criptomoedas; às vezes é possível quando se trata de dinheiro vivo em moeda tradicional.

- **Inflação:** impossível apenas para criptomoedas; uma realidade constante para o dinheiro tradicional.

- **Taxa de volatilidade:** definitivamente alta para criptomoeda; baixo para dinheiro tradicional.

## **O inventor do Bitcoin e por que ele é o Batman dos nossos tempos**

No meio da crise financeira global de 2008, alguém sob o nome de Satoshi Nakamoto projetou o Bitcoin e criou sua implementação de referência original. Ele lançou o primeiro software Bitcoin que lançou a rede e as primeiras unidades da criptomoeda Bitcoin. O Bitcoin tornou-se um novo tipo de moeda digital, muito diferente de todas as outras. Sua principal diferença reside no fato de ser descentralizada. Portanto, cada participante não pode influenciar seu destino.

A seguinte pergunta surge: existem muitas pessoas na rede, elas não se conhecem e é lógico que elas não confiem umas nas outras. Então, como eles podem ter certeza de que os pagamentos são realizados e seu dinheiro não será roubado? No entanto, tudo foi pensado com antecedência por Satoshi Nakamoto e cuidadosamente descrito por mim no livro *Mastering Bitcoin for Starters*. Basta dizer que a visão de Nakamoto para uma moeda descentralizada se manteve fiel, resolvendo muitos problemas.

A propósito, a identidade de Satoshi Nakamoto ainda está envolta em mistério. Várias tentativas foram feitas para revelá-la porque algumas pessoas acreditam que Satoshi Nakamoto é um grupo de pessoas e não uma pessoa. No entanto, nenhuma dessas tentativas se mostrou bem sucedida.

## Capítulo 3. Bitcoin e mineração

Para decifrar a essência do Bitcoin, precisamos mergulhar um pouco no assunto da mineração. Vou falar sobre mineração como uma estratégia de investimento mais tarde, mas por enquanto vamos considerar a mineração apenas em termos do surgimento do Bitcoin.

Há alguns anos, muitas pessoas viam a mineração, a produção de criptomoeda ou Bitcoins, como uma espécie de hobby. Muitos jogaram esse *jogo* até que aconteceu a famosa situação com pizza. Esse dia é conhecido como o Dia da Pizza na comunidade de criptomoedas. Em 22 de maio de 2010, um programador pagou a um usuário do fórum Bitcoin 10.000 BTC por duas pizzas. Naquela época, o Bitcoin era quase inútil. Essas duas pizzas custam ao usuário aproximadamente US\$ 25. Atualmente (outubro de 2017), um Bitcoin custa mais de US\$ 5.000. Você pode facilmente calcular que essas duas pizzas custaram a esse cara milhões de dólares.



Essa foi a primeira vez que o Bitcoin penetrou no mundo real.

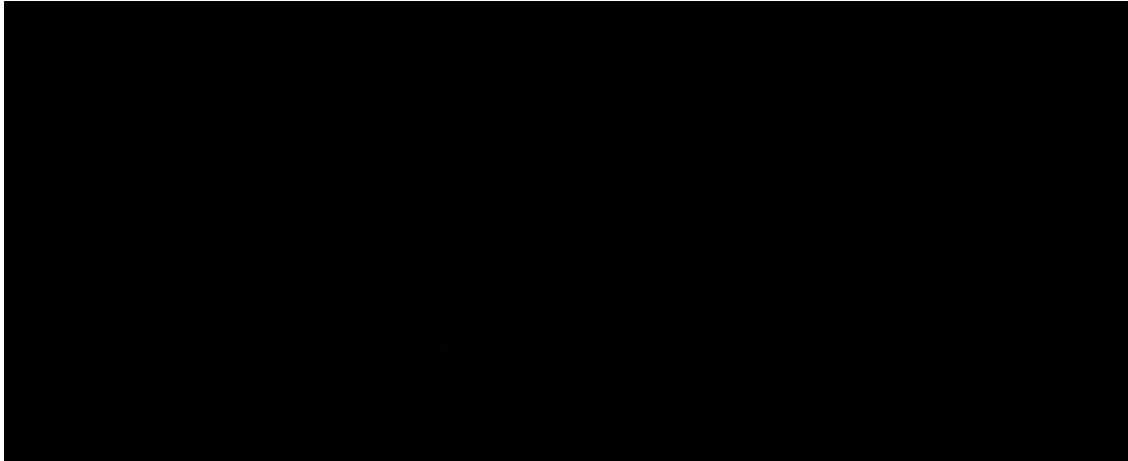


Este gráfico mostra que o Bitcoin teve seus altos e baixos. No entanto, seu valor se multiplicou várias vezes desde 2016.

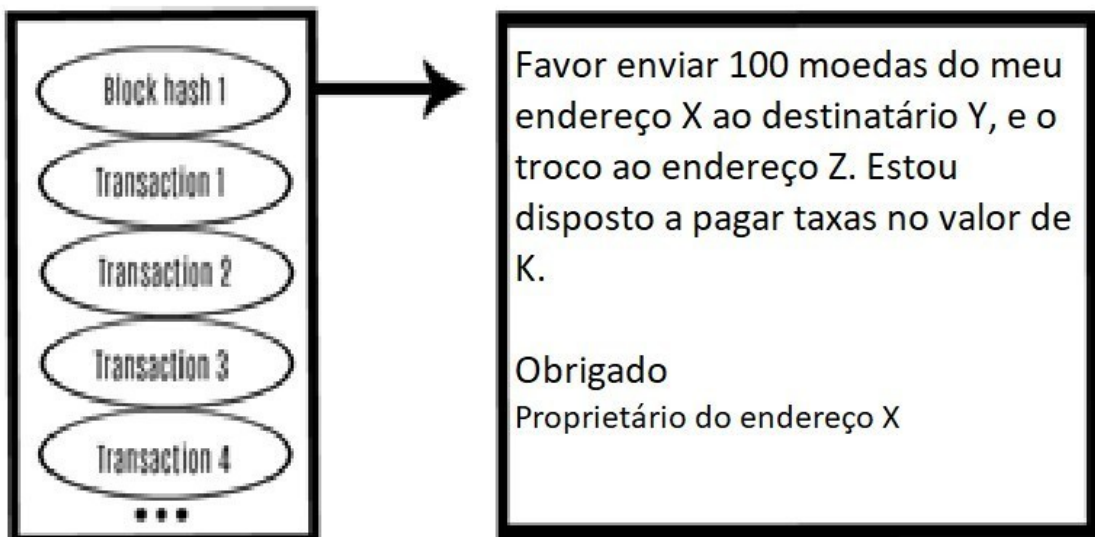
O Bitcoin foi minerado pela primeira vez em escala industrial quando seu valor começou a aumentar. Primeiro, o poder da computação foi usado para minerar o Bitcoin. Mais tarde, os mineiros começaram a usar placas gráficas para formar os blocos. Agora, eles usam equipamentos especializados chamados ASIC. As maiores fazendas desse tipo agora estão localizadas na China.

## Como funciona o Processo de Mineração

Mineração é o processo de produzir novas criptomoedas ou bitcoins. Vamos ver como funciona a mineração. Quando, por exemplo, você envia dinheiro de sua carteira para a carteira de outra pessoa, suas transações caem no chamado "mempool". O mempool Bitcoin é uma coleção de todas as transações aguardando para receber uma confirmação de rede. Mineiros, guiados por seus próprios princípios, coletam transações em blocos específicos e tentam inseri-los no Blockchain. Cada bloco no Blockchain gera a cada dez minutos.



É assim que vemos a transação do Bitcoin.



É assim que um computador a vê.

**Input Scripts**

```
OP_FALSE
304402201280bf056-
ca0554b4f5a95a2cda31a20f133115c708aab54855ac386fd23b10c02207c5bb3365be40b9de1ebe8759202964d931dab939b23553e3aa7882fd63f6ab201
30450221008c4df3615360c2b26f7655de5bdc995eb2cc24e7759a60c0ee6dbbcab0b1899a022065102895b6868f945517aef647183e4e06e7d03d725f06b
d3c9d71374d33cfff501
522103a623c04847602e74a38ec99977741d6b475c6fe2abfe13fc55dbdcde3aead46312103aa7e108ae96ab9f13478fa152a1c48ff734e14f5064169755b465
09a9519fc52ae
```

```
OP_FALSE
304502210083475cd31a99906966bf069e9100408ba2d2912932be48e36379329726892763302206edccad7406618c1748917dcf02a78b4ff50413721c867
dcb22de7450f1c1c5701
3044022065e58aedb77768193757c72a10ed89ccd6ff35346513e9406c39d02a89a38a6002207805b1fa66887e8cae51a4b14ff00bdc2021686d8980a38292
eef6960be66601
522103a623c04847602e74a38ec99977741d6b475c6fe2abfe13fc55dbdcde3aead46312103aa7e108ae96ab9f13478fa152a1c48ff734e14f5064169755b6d46
509a9519fc52ae
```

**Output Scripts**

```
OP_DUP OP_HASH160 d420a78d07141a3a8d0a53c58dc9da5822e21877 OP_EQUALVERIFY OP_CHECKSIG
OP_HASH160 f0071b1141b8728a45d5d4ff9d147a3f091e50be OP_EQUAL
```

Um mineiro recebe uma recompensa pela mineração de um bloco. Atualmente, a recompensa é de 12 bitcoins. Isto é, se você introduzir um bloco bem formado no sistema, obterá tal recompensa. A propósito, o primeiro bloco (Gênesis) foi criado por Satoshi Nakamoto. Qualquer pessoa poderia encontrá-lo e obter 50 bitcoins por ele. Hoje, a recompensa por um bloco formado adequadamente começa a cair. Dizem que ele vai cair a um valor infinitesimal até 2140.

Um dia, os mineiros perceberam que não era rentável minerar sozinhos. A probabilidade de você encontrar o tal bloco depende da “taxa de hash” ou quão poderosa é a sua máquina de mineração de Bitcoin. Sob certos valores aceitáveis, se dissermos que sua taxa de hash representa 10% do total da taxa de hash, você poderá encontrar esses blocos com uma probabilidade de 10% e receber sua recompensa. Então, se você apenas usa meu laptop em casa, nunca encontrará um novo bloco. Portanto, a fim de obter uma recompensa mais estável, os mineiros se unem nos chamados pools de mineração. Eles usam suas taxas de hash unidas para obter lucros mais regulares.

Agora muitos mineiros começaram a pensar: por que eu deveria minerar se eu posso comprar Bitcoin? Também é uma boa ideia, já que o valor do Bitcoin é determinado apenas pela crença das pessoas que o utilizam, enquanto seu custo é determinado pela demanda. Se ninguém comprar o seu Bitcoin, não vai custar nada. Portanto, desde que as pessoas vejam essa tecnologia como uma oportunidade para usá-la anonimamente, fazer grandes pagamentos, e assim por diante, o valor do Bitcoin ganhará força.

Eu não vou me concentrar no Bitcoin em detalhes, porque dediquei meu livro anterior, *Dominar a Bitcoin para Principiantes* (<https://geni.us/bitcoin-pt>), a este tópico. Por enquanto, vou considerar as vantagens do Bitcoin, que ainda levantam algumas questões.

A primeira vantagem é o **baixo custo de transação**. No entanto, devemos ter em mente que o Bitcoin não é bom o suficiente para micropagamentos. Se você transferir a alguém \$ 1 milhão, custará um centavo. No entanto, se você decidir pagar por uma xícara de café, as taxas serão grandes em comparação com o custo do seu café.

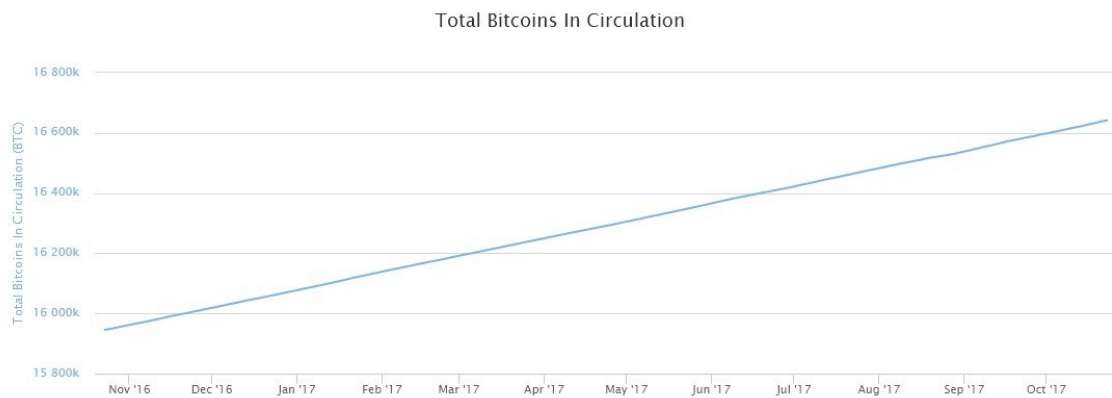
A segunda vantagem é **alta velocidade do processamento das transações**. Aqui também estão alguns problemas. Na verdade, cada bloco no Blockchain gera a cada dez minutos, ou seja, a transação mais rápida possível leva dez minutos. Parece bastante rápido se comparado à transferência SWIFT em um banco, o que pode levar de 2 a 4 dias. No entanto, Visa e MasterCard são muito mais rápidos. Eles podem processar dezenas de milhares de vezes mais transações por unidade de tempo do que o Bitcoin. Vale a pena notar que agora existem outros tipos de criptomoeda que foram desenvolvidas para serem mais rápidas que o Bitcoin.

A terceira vantagem é o **pseudoanonimato dos participantes**. Nós já estudamos que qualquer um pode rastrear todas as transações na rede. Se você conhece o proprietário exato de uma carteira, pode rastrear absolutamente todas as transações realizadas a partir dela. Assim, não se pode dizer

que o Bitcoin é absolutamente anônimo. Assim que alguém consegue relacionar seu endereço com sua pessoa, o anonimato desaparece. Mas se você observar a chamada "higiene cibernética", o que significa que você não mostre sua carteira a ninguém, basicamente suas transações não podem ser rastreadas. Devo mencionar, no entanto, que existem outras criptomoedas que são mais anônimas do que o Bitcoin.

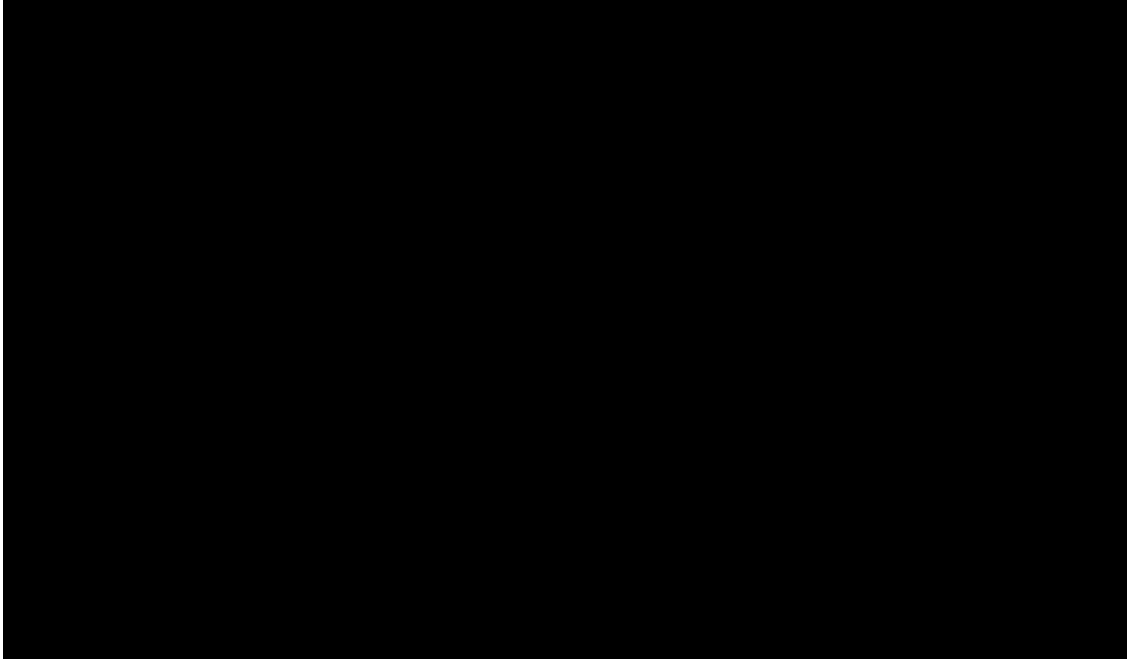
A propósito, se você quiser ficar anônimo ao fazer transações na rede Bitcoin, isso já é possível. Existem muitos serviços que lavam seus bitcoins. Eles são chamados de "serviços de mixagem" e são usados para misturar os fundos com bitcoins de uma pessoa com os de outras, com a intenção de confundir a trilha de volta à fonte original dos fundos. Como você vê, novas tecnologias surgiram para intensificar o anonimato das criptomoedas.

E, finalmente, agora mais de 16 milhões de bitcoins circulam no mundo, enquanto um total de 21 milhões serão minerados. Tais figuras são programadas pelo algoritmo da própria rede. A quantidade limitada de Bitcoin torna a inflação desta moeda impossível. Esta moeda não se deprecia ao longo do tempo porque apenas uma certa quantia será emitida. O Bitcoin ainda tem um modelo deflacionário: muitas pessoas perdem suas moedas esquecendo a senha da carteira ou enviando dinheiro para o endereço errado. Portanto, o número de bitcoins diminuirá gradualmente.



## Prova de Trabalho e por que é importante

Os maiores problemas da rede Bitcoin foram os seguintes: como ter certeza de que as transações são realmente verdadeiras; como ter certeza de que um mineiro não engana ninguém; o que deve ser feito para escolher o bloco correto e realmente construir o Blockchain. Todas estas questões são resolvidas através do *algoritmo de consenso*.



O **Protocolo Prova de Trabalho** confirma que um mineiro faz uma enorme quantidade de trabalho para encontrar um nonce correto e obter um hash bem-sucedido. Você deve gastar muito tempo para encontrar o necessário. Explicarei em mais detalhes.

A dificuldade do bloco é ajustada a cada 2016 blocos e depende de quantos zeros estão no início de um determinado hash. Não é difícil encontrar o hash em si, mas é difícil encontrar um hash bem-sucedido com um certo número de zeros. Se você tiver o hash de um bloco anterior, bem como o timestamp e a hora da transação, parece que é muito fácil criar um novo hash a partir disso e processar esse bloco. No entanto, você precisa encontrar um nonce, cujo valor é definido para que o hash do bloco contenha uma série de zeros à esquerda. Muito tempo é necessário para isso. Uma vez que os mineiros encontram esse hash bem-sucedido, eles enviam um bloco para o Blockchain. Ou seja, eles já confirmaram todas as transações, tendo feito algum trabalho. Portanto, não há sentido em enganar alguém, pois esse trabalho é muito difícil de ser feito.

Depois disso, todas as informações são distribuídas nos nós. Primeiro, um minerador envia um nó. Ele pode verificar se, por exemplo, as pessoas que enviaram dinheiro do ponto A para o ponto B realmente tinham esse dinheiro, ou seja, se todas as transações são válidas. Em seguida, os nós começam a trocar essas informações entre si e, assim, o bloco é formado.

Em teoria, pode acontecer que dois mineiros criem um e o mesmo bloco. Como o Blockchain vai escolher qual bloco é melhor? O primeiro princípio é a velocidade. O segundo princípio é "sucesso" de um hash. Portanto, "sucesso" de um hash é exatamente o esforço que os mineiros devem fazer dentro do protocolo de Prova de Trabalho.

Outra razão pela qual você precisa escolher um hash "bem-sucedido" é um ajuste na dificuldade da rede. Quanto mais mineiros aparecem, mais as dificuldades de rede aumentam, o que significa que

as transações podem ser processadas mais rapidamente. Se os mineiros desaceleram em encontrar os blocos, a dificuldade diminui.

Deixe-me adicionar mais algumas palavras sobre como resolver a situação quando vários mineiros criam blocos idênticos na rede. A essência do consenso Blockchain é que a maior cadeia de blocos é considerada justa. Se os blocos começarem a ser construídos em uma direção diferente da sua, o seu primeiro bloco cairá novamente no conjunto de transações não confirmadas. Isso geralmente acontece quando a rede está sobrecarregada. Então, para ter certeza de que os próximos blocos serão construídos exatamente sob o seu bloco e você receberá a recompensa, espere até que vários outros blocos sejam formados após o seu. Se mais de cinco blocos forem formados, o dinheiro é definitivamente seu.



No final da subseção anterior, discutimos os prós do Bitcoin, então agora é hora de falar sobre os contras do Blockchain, ou seja, o ataque de 51% ou o gasto duplo. Explicarei.

Qualquer pool de mineração pode unir seus esforços a tal ponto que a probabilidade de gerar o próximo bloco nesse pool pode ser de 51%. A comunidade de criptomoedas uma vez testemunhou a situação quando os membros de um pool de mineração chinês restringiram artificialmente os novos membros de seu sistema e conseguiram gerar cerca de seis blocos seguidos. Foi depois desse incidente que ficou claro que se deve aguardar a confirmação da transação por uma hora, não por dez minutos. Isto é, se você criar cinco blocos, e cada um deles for formado por dez minutos, multiplicamos por cinco e obtemos 50 minutos.

## Capítulo 4. Blockchain

Antes de entrar em qualquer um dos detalhes técnicos por trás da tecnologia Blockchain, é importante entender os problemas que o Blockchain resolve. Por que precisamos do Blockchain e o que ele faz que nossa tecnologia atual não pode fazer?

Os primeiros adeptos da tecnologia Bitcoin e Blockchain identificaram o que eles perceberam como uma falha fundamental na maneira como pensamos sobre transações, confiança e instituições sociais. As primeiras versões do Blockchain ocorreram na mesma época da crise financeira de 2007 nos Estados Unidos, quando muitas pessoas perderam a fé em instituições sociais que deveriam proteger os interesses do homem comum. É claro que as pessoas ficaram desiludidas com o sistema bancário na esteira da crise, mas também perderam a confiança no governo para regular os mercados financeiros e na imprensa para investigar possíveis crises.

A maioria das pessoas concorda que nossas instituições têm falhas e não são soluções perfeitas. Mas elas resolvem problemas de confiança e fazem isso há centenas de anos. Na verdade, estamos provavelmente vivendo na era mais pacífica e confortável da história da humanidade. Qualquer alternativa às nossas instituições atuais precisa ter vantagens e pontos fortes claros.

A ideia por trás do Blockchain é substituir instituições dirigidas por seres humanos imperfeitos por tecnologia que possa melhorar o trabalho e também capacitar os indivíduos. Se pudéssemos criar uma maneira de os estranhos confiarem uns nos outros sem precisar de um banco ou de um governo como intermediários, resolveríamos um dos maiores entraves da sociedade. Mas, para isso, precisaríamos de um sistema poderoso para criar consenso entre estranhos, e os criadores do Blockchain acreditam que o poder está na descentralização.

Basicamente, todas as aplicações do Blockchain (e outras tecnologias criptográficas) são baseadas no conceito de descentralização. Em vez de uma autoridade central rígida e lenta que toma decisões e rege as relações, o Blockchain procura devolver o poder regulatório aos indivíduos. Em vez de confiar em uma instituição principal, o Blockchain gera confiança por meio de consenso.

## Como o Blockchain funciona?

Em termos mais simples, o Blockchain usa uma combinação de criptografia e um livro público para criar confiança entre as partes, mantendo a privacidade. Entender a mecânica de como isso funciona é um pouco mais difícil, mas para apreciar plenamente o gênio por trás da tecnologia Blockchain, precisamos nos aprofundar nos detalhes técnicos.

Embora o Blockchain possa incluir muitos outros recursos, os fundamentos de um Blockchain estão no nome da tecnologia:

**O bloco:** um bloco é uma lista de transações de um determinado período de tempo. Ele contém todas as informações processadas na rede nos últimos minutos. A rede cria apenas um bloco por vez.

**A corrente:** cada bloco está ligado ao bloco anterior através de algoritmos criptográficos. Esses algoritmos são difíceis de ser calculados por computadores e geralmente os computadores mais rápidos do mundo levam vários minutos para resolvê-los. Uma vez resolvida, a corrente criptográfica bloqueia o bloco, dificultando a mudança. Vamos ver isso mais profundamente em apenas um minuto.

A corrente cresce mais ao longo do tempo. Depois que um novo bloco é criado, os computadores na rede trabalham juntos para verificar as transações no bloco e proteger o lugar desse bloco na corrente.

A parte mais fundamental do Blockchain é o livro-caixa (ledger). É onde as informações sobre as contas na rede são armazenadas. O livro-caixa dentro do Blockchain é o que substitui o livro de registro em um banco ou outra instituição. Para uma criptomoeda, esse ledger normalmente consiste em números de contas, transações e saldos. Quando você envia uma transação para o Blockchain, você está adicionando informações ao ledger de onde a moeda está vindo e indo.

Um ledger de blockchain é distribuído pela rede. Cada nó da rede mantém sua própria cópia do ledger e atualiza quando alguém envia uma nova transação. Este “registro compartilhado” é como o Blockchain pretende substituir bancos e outras instituições. Em vez de manter o banco com uma cópia oficial do livro, todos manterão sua própria cópia e, em seguida, verificaremos as transações por consenso.

Cada tecnologia Blockchain tem seu próprio ledger, e os vários ledgers funcionam de forma muito diferente, como veremos. No entanto, o ledger do Bitcoin, o primeiro livro de registro do Blockchain, requer três informações para listar uma transação:

1. Uma entrada: se John quiser mandar um Bitcoin para David, ele precisa dizer à rede onde ele obteve o Bitcoin em primeiro lugar. Talvez John tenha recebido o Bitcoin ontem de Sarah, então a primeira parte da entrada do livro diz isso.
2. Uma quantia: quanto John quer enviar para David.
3. Uma saída: o endereço Bitcoin de David e onde o Bitcoin deve ser depositado

Agora vem o conceito que é difícil de entender: O Bitcoin não existe. Claro, não há Bitcoins físicos. Você provavelmente já sabia disso. No entanto, também não há Bitcoins em um disco rígido em algum lugar. Você não pode apontar para um objeto físico, arquivo digital ou pedaço de código e dizer: "este é um Bitcoin". Em vez disso, toda a rede Bitcoin é apenas uma série de registros de transações. Cada transação na história do Bitcoin mora no ledger distribuído do Blockchain do Bitcoin. Se você quiser provar que tem 20 Bitcoins, a única maneira de fazer isso é apontando para as transações em que você recebeu esses 20 Bitcoins.

Quase todas as blockchain têm essa característica em comum. O histórico de transações é a moeda. Não há diferença entre os dois. Algumas novas criptomoedas estão alterando a forma como o ledger é escrito para fornecer maior anonimato e privacidade nas transações. Eles usam certas técnicas

de mascaramento de identidade para ocultar o remetente e o destinatário da transação, mantendo um ledger distribuído funcional.

### **Criando um bloco**

O ledger é o núcleo do bloco, mas não é a única coisa que entra em um bloco recém-criado. Existe um cabeçalho e um rodapé necessários para cada bloco. Além disso, as transações incluídas no bloco são submetidas a um processo que as compacta, codifica e padroniza. Quando um verificador cria um novo bloco, ele parece completamente diferente do ledger no qual foi baseado. No entanto, o ledger subjacente ainda está lá e pode ser acessado no futuro quando novas transações exigirem informações sobre os blocos anteriores.

### **adicionar transações**

O primeiro passo na construção de um bloco é reunir e adicionar todas as transações atuais ao ledger do bloco. Quando um usuário cria uma nova transação, ele transmite essa transação para toda a rede. Em seguida, o computador de um verificador analisará a transação para garantir sua validade.

Como as moedas Blockchain nada mais são do que uma série de transações, o primeiro passo para verificar uma transação é ver de onde o remetente diz que originalmente recebeu o dinheiro. O verificador reverá o histórico do Blockchain para encontrar o bloco e a transação em que o remetente recebeu o dinheiro. Se essa transação de entrada for confirmada no Blockchain, a transação será válida e eles precisarão confirmar o endereço da parte receptora. Se a transação de entrada não foi confirmada, a transação atual é inválida e não será incluída no ledger.

Depois que todas as transações nesse bloco forem verificadas, é hora de criar o ledger. Aqui está um exemplo simples, onde as transações são listadas uma após a outra:

## **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.