Bitcoin Para leigos

Bitcoin — que enigma! Aparentemente, surgiu do nada e, treze anos depois, vale centenas de bilhões de dólares, mesmo que poucas pessoas entendam como funciona.

As informações contidas nesta Folha de Cola devem ajudar a reduzir parte do mistério e da confusão para que você possa começar sua "jornada Bitcoin" com confiança.

APRENDENDO O JARGÃO DO BITCOIN

Na verdade, não há Bitcoin. Não há nada tangível, é claro, mas também não há sequer algum tipo de representação digital de uma moeda. Ao contrário, o Bitcoin é representado por registros de transações no "ledger" do Bitcoin, que é armazenado em um "blockchain" — outra coisa que poucas pessoas entendem.

Tudo isso pode ser um pouco confuso, por isso, aqui você encontra uma explicação rápida de alguns termos importantes.

- **Blockchain: É uma *cadeia de blocos*, um tipo especial de banco de dados, como um arquivo de computador que armazena dados estruturados. Na verdade, no caso do blockchain, o banco de dados é distribuído; há cópias do blockchain do Bitcoin em milhares de computadores espalhados pelo mundo todo. Como todas as cópias precisam estar associadas, tal combinação de cópias do blockchain é inviolável.**
- **Ledger do Bitcoin: Um *ledger*, ou *livro-razão*, é um registro das transações financeiras. Tais registros eram originalmente escritos à mão em livros. Hoje, o ledger do Bitcoin armazena informações digitais sobre suas transações no blockchain. A propósito, o livro-razão do Bitcoin não é criptografado; é um sistema público e aberto que permite que qualquer pessoa entre no blockchain e veja o que está acontecendo usando um "explorador de blockchain".**
- **Bitcoin: Inicialmente, isso é confuso para as pessoas, mas, ao contrário de dólares, euros, reais e libras, não só não há Bitcoin físico, como também não há Bitcoin digital — nada que você possa apontar e dizer: "Olha ali um Bitcoin." Em vez disso, ele é apenas representado pelo livro-razão *que diz que* o Bitcoin existe. Em janeiro de 2009, informações foram adicionadas ao ledger do Bitcoin — evento conhecido como Bloco Gênesis — dizendo, com efeito, que "50 Bitcoins foram adicionados ao livro-razão". A partir de então, o Bitcoin passou a existir, porque era isso o que o livro-razão dizia!**

- **Rede Bitcoin**: Assim como a internet é o lar de uma rede de e-mail e da rede mundial — uma rede de sites —, existe também uma rede Bitcoin. Ela é formada por milhares de computadores que se comunicam pela internet. Alguns desses computadores são nós, que têm uma cópia completa ou parcial do blockchain. Alguns também estão envolvidos no processo de "mineração", no qual novos Bitcoins são criados. Mas a maioria é composta por programas de software de carteira empregados pelos investidores e usuários do Bitcoin.
- **Endereço:** Dentro do blockchain, todos os Bitcoins estão associados a vários endereços, que são números longos e únicos. Você pode ter um endereço que, no livro-razão do blockchain, esteja associado a, digamos, um décimo de um Bitcoin (ou um milésimo, ou cinco Bitcoins, e assim por diante). Você controla o endereço (e o Bitcoin associado a ele) pelo uso de criptografia.
- **Transação**: Uma *transação* de Bitcoin ocorre quando alguém envia uma mensagem para o blockchain, como: "Pegue *x* Bitcoin do meu endereço, e mova-o para este outro endereço." Digamos que você tenha meio Bitcoin e queira convertê-lo em reais; você encontra alguém disposto a comprar seu Bitcoin — uma exchange, por exemplo — e envia uma transação para o blockchain movendo o Bitcoin de seu endereço para o endereço do comprador. O ledger mostrará uma transação dizendo: "Meio Bitcoin foi movimentado do endereço *x* para o endereço *y*."
- **Carteira:** Não, uma carteira não é onde o Bitcoin fica armazenado. *Não existe Bitcoin em uma carteira!* Ao contrário, a carteira armazena informações que permitem controlar o endereço no blockchain com o qual seu Bitcoin está associado. As carteiras de software permitem que você envie mensagens para a rede Bitcoin e insira transações no ledger do Bitcoin.

VOCÊ ENTENDE O DINHEIRO?

Quando você pensa sobre o dinheiro, provavelmente cédulas e moedas vêm à sua mente. Entretanto, as principais moedas do mundo não têm moedas e cédulas para todo o dinheiro em circulação. Cerca de 90% de uma grande moeda não têm representação física! Não são (citando o historiador Yuval Noah Harari) "nada além de entradas em um servidor de computador".

O dinheiro é meramente um conceito, uma forma de o ser humano armazenar valor e trocá-lo no futuro por bens e serviços reais. Ele pode ser representado por conchas polidas, cédulas, ouro, sal, cevada, moedas, grandes discos de pedra — muitas coisas diferentes. Se você *acredita* na representação, então o que quer que esteja sendo usado para representá-la pode funcionar como dinheiro.

Bem, há outra exigência. Não pode ser muito fácil fazer mais da representação. "Conchas?", pergunta você. "Posso pegá-las na praia." Só um momento! Culturas passadas que usavam conchas para representar o dinheiro escolhiam um tipo muito particular de concha, exigindo que fosse trabalhada extensivamente e até mesmo que fosse de uma área distante. Não havia uma maneira simples de inundar o mercado com dinheiro novo.

Portanto, sim, o Bitcoin pode agir como uma forma de dinheiro, ou pelo menos como uma "reserva de valor". Seu suprimento é muito limitado; um suprimento fixo, mas sempre decrescente, é "minerado" a cada dia. E milhões de pessoas acreditam nisso.

O INCRÍVEL BLOCKCHAIN

Como funciona esse tal de *blockchain*, ou *cadeia de blocos*? Bem, ele é uma forma de banco de dados (como os dados armazenados em uma planilha ou em um programa financeiro pessoal). E é copiado em milhares de computadores em toda a rede Bitcoin.

Mas há mais. Primeiro, há o termo *bloco* (*block*). Isso se refere a blocos de dados. As cadeias de blocos podem ser usadas para muitos propósitos diferentes, mas, no caso do blockchain do Bitcoin, cada bloco contém registros de transações. Um novo bloco de dados é adicionado à cadeia de blocos — e replicado em todas as cópias — a cada dez minutos, mais ou menos.

Em seguida, há o termo *cadeia* (*chain*). Uma cadeia de blocos é, talvez não surpreendentemente, uma forma de banco de dados em que blocos de dados são juntos. Como? Bem, é um pouco complicado, mas isso se dá por meio de *hashes*.

Um *hash* é um número longo e age como uma impressão digital. Ele identifica de forma única um bloco de dados. Portanto, você faz um hash no bloco de dados para criar essa impressão digital. Então tal impressão digital — o hash — é armazenada com o bloco de dados. Quando o próximo bloco de transações estiver pronto, o software Bitcoin pega o hash do bloco *anterior* e faz o hash em todos os dados — as transações junto com o hash anterior — para criar o hash do bloco atual... que será, então, adicionado ao bloco seguinte, e assim por diante.

Isso encadeia os blocos de uma forma que impossibilita mudar até mesmo um único caractere de texto ou um único número. Se fizesse isso, o hash do bloco editado mudaria, o que mudaria o hash do próximo bloco, o que mudaria o bloco depois dele, e assim por diante.

O resultado final? A cadeia de blocos do Bitcoin é praticamente inviolável.

Bitcoin Para leigos

CRIPTOGRAFIA: O "CRIPTO" EM CRIPTOMOEDAS

As criptomoedas, como o Bitcoin, utilizam criptografia — em particular, a *criptografia de chave pública* — para fornecer uma maneira de os proprietários provarem que são os verdadeiros donos. Veja a seguir um resumo rápido de como funciona a criptografia com chave pública:

- **Criptografia:** Ao "criptografar" dados, você os codifica. Você pega, por exemplo, uma mensagem que quer manter privada, legível apenas pelo destinatário, e a codifica para que seja totalmente ilegível. Ela só pode ser lida se estiver ***descriptografada*** (descodificada).
- **Chave ou senha:** Para criptografar a mensagem, você usa uma chave ou uma senha. Por exemplo, talvez você utilize um programa financeiro pessoal, como o Quicken. Para entrar no programa, é necessário inserir uma senha, que é usada para desbloqueá-lo. Com efeito, você pega os dados que deseja desbloquear, adiciona a chave ou senha e passa ela para o programa, que a utiliza para desbloquear o arquivo de dados. Somente essa chave específica desbloqueará os dados codificados.
- **Criptografia de chave pública**: No exemplo anterior, ao abrir um arquivo de dados, como um arquivo Quicken, você usaria uma única chave para criptografar e descriptografar os dados. Os sistemas de criptografia de chave pública são diferentes. Eles têm duas chaves matemática e exclusivamente associadas: uma chave pública e uma chave privada. É impossível decifrar os dados com a chave que você usou para codificá-los. Se você criptografar os dados com a chave pública, só poderá descodificá-los com a chave privada; e se criptografar os dados com a chave privada, só poderá descriptografá-los com a chave pública. Como isso funciona? Quem sabe? Pouquíssimas pessoas entendem a *matemágica* terrivelmente complexa que entra na criptografia da chave pública. Tudo bem, você provavelmente também não sabe como seu smartphone funciona. Mas ele funciona assim mesmo.
- **Chave pública:** Uma chave pública é justamente isso, uma chave que é tornada pública de alguma forma. Você não precisa mantê-la em segredo.

Bitcoin Para leigos

- **Chave privada**: É essencial que você mantenha uma chave privada... em segredo.
- **Endereço:** Seu Bitcoin está associado a um endereço no blockchain. Especificamente, a chave privada, a chave pública e o endereço estão todos matemática e exclusivamente associados. O endereço está associado à sua chave pública, e somente a ela. E sua chave pública está associada com a chave privada, e somente a ela.
- **Criptografando uma mensagem**: Ao criptografar mensagens secretas usando um sistema de criptografia de chave pública, você criptografa a mensagem usando a chave pública do destinatário. A única pessoa que pode decifrar a mensagem é o destinatário, porque somente ele tem a chave privada.
- **Assinando uma mensagem**: Ao usar a criptografia de chave pública, você pode *assinar* uma mensagem. Lembre-se, a chave pública é apenas isso, de conhecimento público. Se você criptografar uma mensagem usando a chave privada, ela não será muito privada — qualquer um com a chave pública pode decodificá-la, e a chave pública é pública! Mas se você pode decodificá-la com a chave pública, isso significa que a mensagem deve ter vindo da pessoa que tem a chave privada associada à chave pública. Na verdade, a mensagem foi atribuída pela pessoa que possui a chave pública.
- **Assinando mensagens no blockchain do Bitcoin**: A criptografia de chave pública é utilizada pelo Bitcoin, mas *não* para criar mensagens secretas que são enviadas para o blockchain. Em vez disso, é usada para *assinar* mensagens. Quando você envia uma mensagem para o blockchain transferindo Bitcoin de seu endereço para outro, seu software de carteira usa a chave privada para criptografar as informações da transação, adiciona a chave pública e envia a mensagem. Claro, a mensagem foi criptografada, mas não é segura, pois pode ser descriptografada por qualquer pessoa. O nó Bitcoin que processa a mensagem pega a chave pública e descriptografa a mensagem. Ele também verifica se a chave pública está associada com o endereço especificado na mensagem. Caso esteja — lembre-se, chave pública, chave privada e endereço estão matemática e unicamente associados uns aos outros —, o nó sabe que a pessoa que possui a chave privada usada para criptografar a mensagem deve "possuir" o endereço associado com a chave pública usada para descriptografar a mensagem.

PROTEGENDO SEU BITCOIN

Se o blockchain é inviolável, como as pessoas perdem seus Bitcoins? Bem, há duas maneiras:

- **Você perde sua chave privada**: Se perder sua chave privada, não poderá provar que é proprietário do endereço no blockchain com o qual seu Bitcoin está associado. Portanto, você não pode enviar mensagens de transações para o blockchain... seu Bitcoin está travado. Para sempre, se não conseguir encontrar a chave privada!
- **Alguém encontra sua chave privada**: Se alguém mais encontrar sua chave privada, terá acesso ao seu Bitcoin. Será possível enviar mensagens para o blockchain "provando" que é proprietário do endereço e do Bitcoin associado. Quem tiver as chaves é dono do Bitcoin! Portanto, proteger sua chave privada é essencial. Você *realmente* precisa ter certeza de que nunca poderá perder sua chave privada — mesmo em inundações, incêndio, mau funcionamento de hardware etc. — e, ao mesmo tempo, garantir que ninguém mais possa chegar até ela, a menos que você queira.

FORMAS DE COMPRAR BITCOIN

Quando o assunto é comprar Bitcoin, você tem diversas opções. Cada uma tem seus prós e contras:

- **Caixa eletrônico de Bitcoin**: Caro, mas rápido e fácil. Você pode se transformar em um proprietário de Bitcoin da próxima vez que for ao supermercado.
- **Exchanges**: Há inúmeras opções, sendo que algumas vendem centenas de criptomoedas diferentes. Mas escolha sabiamente. Os preços variam, e algumas exchanges são mais respeitáveis do que outras.
- **Lojas de varejo**: Nos EUA, CVS, Rite Aid e MoneyGram são alguns exemplos. Mas provavelmente também são caras.
- **Empresas de serviços financeiros e de transações de pagamentos**: Compre no Nubank, no PayPal, no Mercado Pago e em outras.
- **Negociação entre duas pessoas**: Muito arriscado! É melhor saber o que está fazendo.

Bitcoin Para leigos

UMA LINHA DO TEMPO (CURTA) DO BITCOIN

O histórico do Bitcoin é uma montanha-russa desde 2008. Começou devagar. No início, é claro, o Bitcoin era essencialmente inútil. Na verdade, só em meados de 2010 foi possível que um usuário de Bitcoin fizesse a primeira compra de um produto tangível usando a criptomoeda. (E, como verá, ele provavelmente se arrependeu disso agora!)

Mas, no início de 2011, um Bitcoin valia um dólar, e, embora tenha continuado a aumentar gradualmente de valor, em meados de 2017, o mundo o percebeu, e seu valor disparou.

Aqui estão alguns destaques na louca história do Bitcoin, a primeira criptomoeda no blockchain:

18 de agosto de 2008: O domínio bitcoin.org é registrado.

31 de outubro de 2008: Satoshi Nakamoto publica "Bitcoin: Um Sistema de Dinheiro Eletrônico Peer-to-Peer", um documento que descreve como o Bitcoin poderia funcionar.

3 de janeiro de 2009: Nasce o primeiro Bitcoin, quando Satoshi Nakamoto desenvolve o blockchain do Bitcoin e "cria" (minera) os primeiros 50 Bitcoins.

9 de janeiro de 2009: O software cliente de código aberto do Bitcoin é lançado.

12 de janeiro de 2009: Na primeira transação da história do Bitcoin, Satoshi Nakamoto transfere 10 Bitcoins (na época, não valiam quase nada) ao criptógrafo Hal Finney.

22 de maio de 2010: Laszlo Hanyecz paga 10 mil BTC por duas pizzas. Essa é a primeira transação comercial em Bitcoin e fica conhecida como a pizza mais cara da história. A uma fração de um centavo por Bitcoin, provavelmente, parece um preço razoável. Em abril de 2021, 10 mil Bitcoins valiam US$600 milhões.

Fevereiro de 2011: O Bitcoin atinge US$1 por moeda.

Junho de 2011: O Wikileaks começa a aceitar Bitcoin.

23 de junho de 2013: A Agência de Combate às Drogas dos EUA relata a apreensão de 11,02BTC — a primeira apreensão governamental relatada.

10 de outubro de 2013: O Bitcoin é negociado a US$130, antes de iniciar sua subida meteórica.

Outubro de 2013: O FBI apreende 26.000BTC do *Silk Road*, mercado virtual e ilegal de drogas operado na deep web.

Bitcoin Para leigos

2 de dezembro de, 2013: O Bitcoin atinge US$1.151. (Seu preço cai para cerca de US$800 até o fim daquele ano.)

4 de dezembro de 2013: Alan Greenspan, ex-diretor do Federal Reserve Bank (o banco central dos EUA), chama o Bitcoin de bolha.

Fevereiro de 2014: Mt. Gox, uma das maiores exchanges do mundo, bloqueia os saques após relatar que 744 mil Bitcoins haviam sido roubados.

12 de janeiro de 2015: Após pouco mais de um ano de declínio, o Bitcoin é negociado a US$178.

Janeiro de 2015: A exchange *Coinbase* levanta US$75 milhões em financiamento.

31 de março de 2017: O Bitcoin é negociado a US$1.080, mas o preço começa a subir rapidamente.

Abril de 2017: O Japão aceita o Bitcoin como método legal de pagamento e a Rússia planeja regular a criptomoeda.

Terceiro trimestre de 2017: A imprensa começa a falar muito sobre o Bitcoin.

15 de dezembro de 2017: O Bitcoin atinge US$19.497 — e depois cai.

2 de janeiro de 2018: O investidor bilionário George Soros chama o Bitcoin de bolha.

4 de fevereiro de 2018: O Bitcoin cai para US$6.955.

14 de dezembro de 2018: Um ano ruim... o Bitcoin é negociado a US$3.253.

25 de junho de 2019: As coisas parecem melhorar. Novamente o Bitcoin é negociado acima dos US$13 mil.

13 de março de 2020: Certo, não é bem assim. O Bitcoin cai aos US$5.200. Mas, espere, as coisas mudarão.

Outubro de 2020: O PayPal anuncia que adotará o Bitcoin.

14 de março de 2021: Após um ano de aumento no preço, o Bitcoin atinge US$63.110!

8 de junho de 2021: El Salvador transforma o Bitcoin em "moeda corrente".

19 de junho de 2021: Bem, a alta não durou. O Bitcoin é negociado a US$29.807.

31 de dezembro de 2021: O ano termina com o Bitcoin valendo US$47.687.