Bitcoin: Guia Essencial

Introdução	2
Bitcoin	3
Descentralização	3
Blockchain	5
Mineração	6
Halving	7
Oferta Limitada	8
Satoshi	9
Exchanges	10
Colapso FTX	11
Chaves Privadas	12
Chaves Públicas	13
Altcoins	14

Introdução

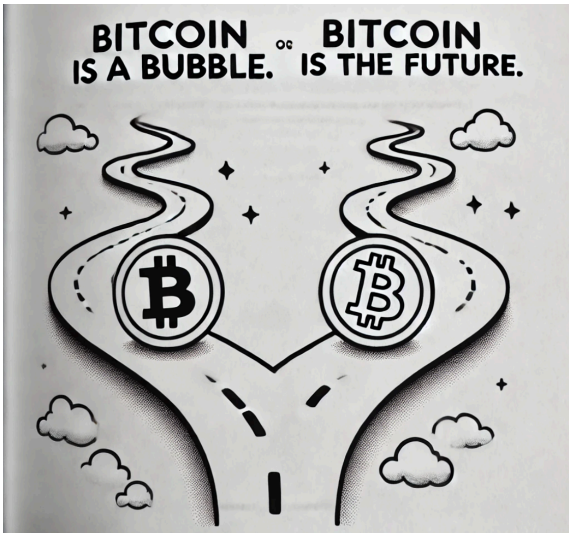
A primeira vez que eu ouvi falar sobre Bitcoin foi no verão de 2018, ano em que o preço da moeda digital atingiu valores exorbitantes pela primeira vez. Eu estava na Praia de Ipanema com pessoas que eu tinha acabado de conhecer, e eles contavam uma história sobre um amigo que tinha ganhado muito dinheiro por causa dessa variação do preço. Eu achei a história suspeita e soltei:

"Bitcoin é uma bolha."

Hoje, 6 anos depois, 100% da minha poupança está alocada em Bitcoin; trabalhei por anos em uma casa de câmbio de moedas digitais em Amsterdam e estou abrindo a minha própria empresa especializada em Bitcoin no Brasil. Sou apaixonado por criptomoedas e trabalho para impulsionar a alfabetização digital, principalmente das pessoas marginalizadas e de baixa renda. Nos dias de hoje quando alguém me pergunta o que é Bitcoin eu respondo:

"Bitcoin é o futuro."

A *informação* foi a principal responsável pela mudança drástica de opinião e pensamento. Com este guia a minha intenção é explicar, de forma prática, como funciona o Bitcoin e de que forma ele revoluciona o sistema financeiro mundial. Bitcoin não é uma bolha, Bitcoin é a nova fase do sistema financeiro. Entender como ele funciona é essencial para se adaptar.



Bitcoin

O Bitcoin é uma moeda como qualquer outra, ele serve como unidade de conta, reserva de valor e como meio de troca. Você pode comprar uma pizza, financiar projetos, e fazer doações utilizando Bitcoin. Ele funciona da mesma forma.

Mas então o que difere Bitcoin das outras moedas tradicionais? E porque ele vale tanto? Espero que com este guia você mesmo seja capaz de responder a essas perguntas.

Descentralização

A principal diferença entre o Bitcoin e as moedas tradicionais é o seu caráter descentralizado. As moedas tradicionais são criadas pelo governo de cada país. Por exemplo: no Brasil a nossa moeda é emitida pelo *Banco Central do Brasil.* Nos Estados Unidos o dólar é produzido pelo *Federal Reserve*. O euro da União Europeia, pelo Banco Central Europeu.

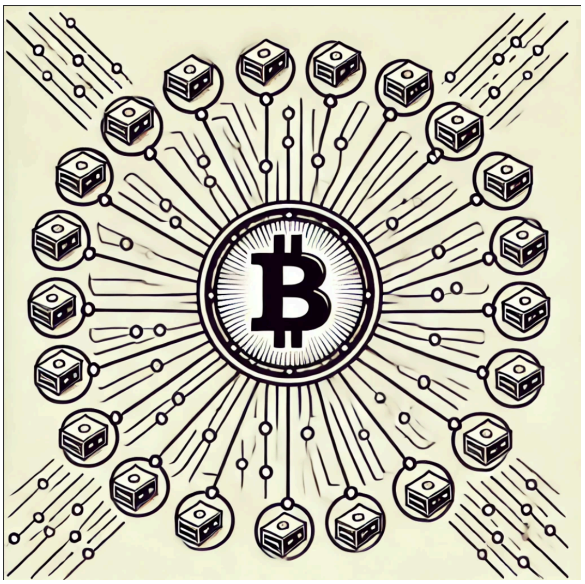
O Bitcoin por sua vez não é criado por um banco central ou uma entidade governamental. Em vez disso, ele é gerado por um processo descentralizado chamado *mineração*, que é uma parte fundamental do sistema de *Blockchain*.

Moeda	**Emissão**	**Forma de Controle**
Real	Banco Central do Brasil	Centralizado
Dólar	Federal Reserve	Centralizado
Euro	Banco Central Europeu	Centralizado
Bitcoin	*Mineração*	*Descentralizado*

Diferenças na Emissão e Controle de Moedas

Não existe uma pessoa, ou uma organização, capaz de interferir diretamente no processo de criação e distribuição do Bitcoin. Tudo é programado e criptografado. A descentralização da moeda garante independência de políticas monetárias.

Em situações de colapso econômico, hiperinflação ou instabilidade cambial, o Bitcoin aparece como uma alternativa viável para as pessoas que perdem confiança em suas moedas nacionais. Isso já acontece em países como Venezuela e Argentina, onde a população começou a utilizar o Bitcoin como uma forma de preservar valor diante da desvalorização de suas moedas.

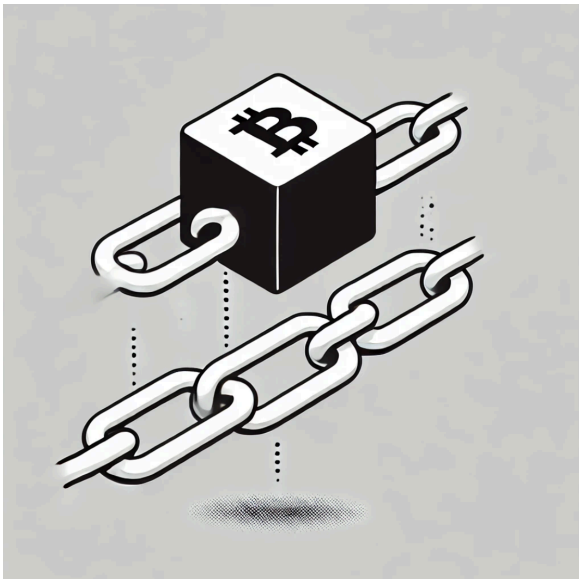


A descentralização do Bitcoin dá poder aos seus usuários, removendo o controle governamental e garantindo liberdade financeira. Para entender como isso é possível precisamos nos familiarizar com as tecnologias e processos que compõem o ecossistema do Bitcoin.

Blockchain

Imagine um lugar onde todas as transações de uma moeda são armazenadas. Sempre que uma quantia é transferida, um novo registro é criado. Um conjunto determinado dessas transações compõe um bloco, e quando um bloco atinge o seu tamanho máximo ele é validado e armazenado. É assim que funciona a tecnologia *blockchain*. Os blocos compostos por um conjunto de transações são validados, armazenados e conectados entre si, eles formam uma cadeia de blocos, por isso o nome *blockchain*.

Ou seja, a blockchain é a tecnologia de criação dos registros de todas as transações realizadas em Bitcoin. Ela funciona como um livro-razão *distribuído e imutável.* É distribuído porque não é armazenado em um único local ou servidor centralizado, e é imutável porque sempre que uma transação é registrada em um bloco e esse bloco é adicionado à Blockchain, os dados não podem ser alterados.



Qualquer pessoa pode ter acesso ao livro-razão da Blockchain do Bitcoin, uma vez que ela é pública. Por ser pública, além de ferramentas online disponíveis que permitem a qualquer pessoa navegar por ela e visualizar informações detalhadas sobre os blocos e transações, também é possível rodar um programa de computador que mantém uma cópia completa do Blockchain, o que permite participar ativamente da validação e propagação de transações e blocos.

Você percebe como o caráter descentralizado já começa a fazer sentido? A tecnologia é publicamente disponível, sustentado por uma rede descentralizada de computadores que valida e armazena transações. E não pode ser modificada ou comprometida, o que garante a transparência das transações.

Mineração

A mineração é o processo pelo qual novas transações de Bitcoin são validadas e adicionadas à Blockchain, ela também funciona como o mecanismo de emissão de novos Bitcoins.

A diferença entre um minerador e uma pessoa comum com acesso ao Blockchain é que o minerador utiliza um hardware especializado e um software de mineração para participar deste processo.

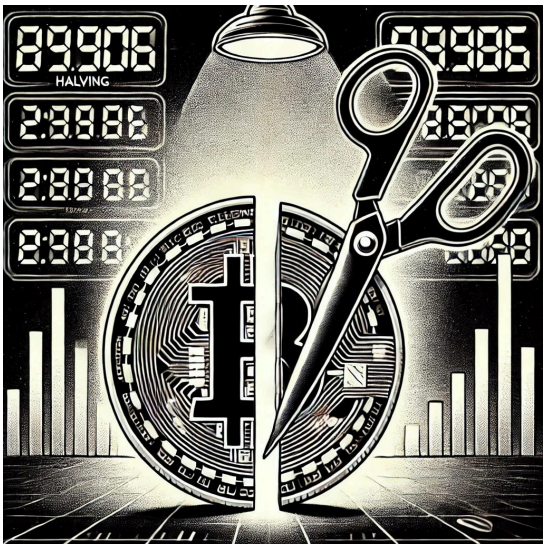
Os mineradores competem entre si para resolver problemas matemáticos complexos, e o primeiro a encontrar a solução pode adicionar o próximo bloco de transações à Blockchain e por consequência recebe uma recompensa em Bitcoins. Este processo é chamado de *proof-or-work* e envolve muito poder computacional.

Essa recompensa em Bitcoin obtida pelos mineradores é como funciona a emissão de novas moedas de Bitcoin, é assim que novas moedas entram no mercado. Ao invés de um Banco Central responsável por definir a quantidade de novas moedas emitidas, Bitcoins são criados sempre que um bloco de transações é validado.

Halving

Halving é o processo pelo qual, a cada 210.000 blocos minerados - aproximadamente a cada quatro anos - a recompensa por bloco para os mineradores é reduzida pela metade. Isso significa que, ao longo do tempo, a quantidade de novos Bitcoins que entram em circulação vai diminuindo, até que, eventualmente, não haverá mais novos Bitcoins a serem minerados. O limite máximo de Bitcoins a serem emitidos é de 21 milhões, e o Halving é uma das formas de garantir que essa oferta se mantenha controlada e previsível.

O Halving é um evento importante na economia do Bitcoin, pois influencia diretamente a oferta e, indiretamente, a demanda. Como a quantidade de novos Bitcoins disponíveis para os mineradores é cortada pela metade, a pressão de venda potencial vinda dos mineradores diminui, o que pode impactar o preço da moeda. Historicamente, muitos enxergam o Halving como um gatilho para a valorização do Bitcoin, pois a oferta reduzida tende a gerar escassez, enquanto a demanda continua a crescer ou se mantém estável.



Além disso, o Halving tem um impacto significativo na mineração. Com a redução da recompensa por bloco, apenas os mineradores mais eficientes e com acesso a energia barata conseguem continuar lucrativos. Isso leva a uma maior competição e evolução tecnológica no setor de mineração, forçando os mineradores a buscarem constantemente maneiras de otimizar seus custos e equipamentos.

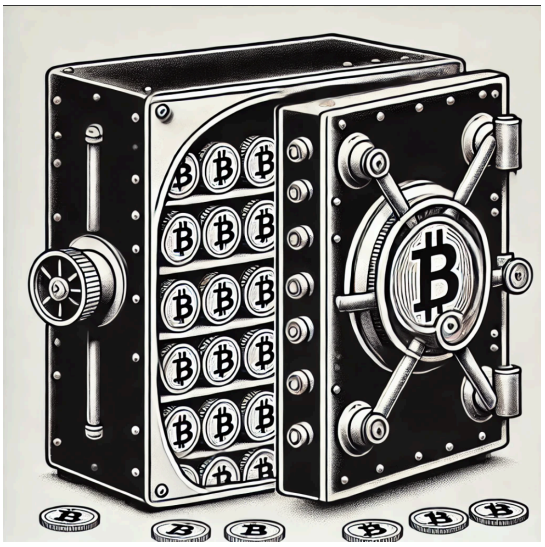
Este mecanismo é essencial para a sustentabilidade da rede Bitcoin, pois promove uma descentralização contínua e incentiva o comportamento de longo prazo dos participantes. Como resultado, o Halving tem sido um dos fatores mais discutidos e aguardados no ecossistema Bitcoin, tanto por investidores quanto pela comunidade técnica.

Oferta Limitada

O Bitcoin tem uma oferta limitada de 21 milhões de unidades por design, para criar escassez e valor. A produção de Bitcoin está programada para terminar por volta do ano 2140.

Por causa do Halving (processo no qual a recompensa dada aos mineradores é reduzida pela metade), o Bitcoin não é infinito como as moedas tradicionais. Em um dado momento, os mineradores não terão mais o incentivo da recompensa em novos Bitcoins.

No entanto, mesmo após o fim da emissão de novos Bitcoins, os mineradores continuarão sendo incentivados a manter a rede segura e a processar transações por meio das taxas de transação pagas pelos usuários. À medida que a recompensa por bloco diminui, a expectativa é que essas taxas ganhem maior importância no ecossistema, sendo elas a principal fonte de renda dos mineradores.



Essa oferta limitada e controlada por um algoritmo matemático é uma das principais características que diferenciam o Bitcoin das moedas fiduciárias, que podem ser emitidas de forma ilimitada pelos bancos centrais. Enquanto a oferta de moedas tradicionais é ajustada por políticas monetárias, muitas vezes levando à inflação, a escassez programada do Bitcoin busca preservar seu valor ao longo do tempo.

A limitação de 21 milhões de unidades também cria uma narrativa de "reserva de valor", similar ao ouro, onde a escassez desempenha um papel fundamental na percepção de valor pelos detentores. Dessa forma, a oferta finita do Bitcoin é um dos pilares que sustentam sua atratividade no longo prazo, particularmente em tempos de incerteza econômica e desvalorização de moedas fiduciárias.

Satoshi

Um satoshi representa a menor unidade de medida do Bitcoin. Assim como o centavo é a menor unidade de medida do Real e do Dólar, o satoshi é a fração mínima do Bitcoin, equivalente a 0,00000001 BTC (um centésimo de milionésimo de um Bitcoin). Essa divisão foi projetada para garantir que, mesmo com o aumento potencial no valor do Bitcoin, ele ainda possa ser utilizado em transações cotidianas, permitindo a transferência de frações pequenas da moeda.

A escolha do nome "satoshi" é uma homenagem ao criador ou grupo de criadores anônimos do Bitcoin, conhecido pelo pseudônimo Satoshi Nakamoto. Essa denominação não só destaca a influência de Nakamoto no desenvolvimento da moeda digital, como também reflete a visão de que o Bitcoin deve ser acessível a todos, independentemente do valor que a moeda atinja no mercado.

Com a popularização do Bitcoin e sua adoção em mercados globais, o uso de satoshis em transações diárias pode se tornar mais comum, especialmente em casos onde o valor de um único Bitcoin é considerado alto demais para transações pequenas. Assim, o conceito de satoshi reforça a divisibilidade e a usabilidade do Bitcoin como moeda digital no dia a dia.

Exchanges

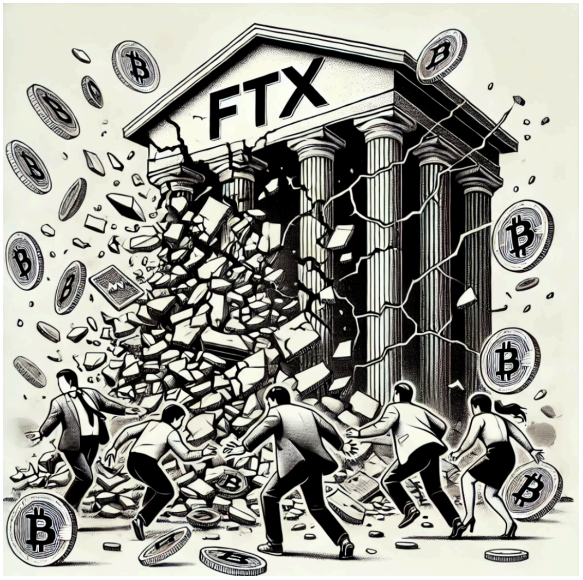
Apesar de serem uma boa forma de adquirir Bitcoin, as casas de câmbio, conhecidas como exchanges, por si só não são descentralizadas. Elas funcionam como intermediárias centralizadas que facilitam a compra e venda de criptomoedas. Ao adquirir Bitcoin por meio de uma exchange, os usuários não recebem o controle total sobre suas moedas, pois as chaves privadas – que garantem a propriedade e o controle dos Bitcoins – permanecem sob custódia da própria exchange.

Isso significa que, enquanto o Bitcoin permanece na exchange, o usuário não tem total soberania sobre seus fundos. A frase comum "not your keys, not your coins" resume bem essa situação: se você não possui as chaves privadas, tecnicamente, você não tem o controle real sobre os seus Bitcoins. Portanto, manter grandes quantias em exchanges pode representar um risco, pois essas plataformas podem ser alvo de ataques, enfrentar problemas de liquidez ou até mesmo encerrar suas atividades, como já ocorreu em casos notórios no passado.

A solução mais segura, após adquirir Bitcoin em uma exchange, é transferir as moedas para uma carteira privada, onde o usuário controla as chaves privadas e, por consequência, tem total controle sobre os seus fundos. As exchanges desempenham um papel importante no ecossistema ao facilitar o acesso ao Bitcoin, mas devem ser usadas com cautela e consciência dos riscos envolvidos.

Colapso FTX

O colapso da FTX, uma das principais casas de câmbio de criptomoedas, prejudicou a reputação do sistema cripto de forma significativa. Escândalos envolvendo má gestão de fundos e falta de transparência mostraram que, apesar de estarem ligadas ao mundo das criptomoedas, as exchanges centralizadas podem carregar os mesmos riscos que instituições financeiras tradicionais. No entanto, é importante lembrar que, mesmo com esses eventos, a filosofia central do Bitcoin permanece intacta: a descentralização.



Enquanto você controlar suas chaves privadas, ninguém, nem mesmo uma exchange, pode acessar sua carteira ou seus fundos. O colapso da FTX serviu como um lembrete de que a verdadeira segurança no universo das criptomoedas depende da autossoberania. Portanto, sempre que possível, após comprar Bitcoin em uma exchange, transfira-o para uma carteira em que você controle as chaves privadas, garantindo a proteção de seus ativos.

Chaves Privadas

As chaves privadas são sequências longas de caracteres geradas criptograficamente e, por isso, são impossíveis de memorizar ou adivinhar. Elas funcionam como a senha definitiva para acessar seus Bitcoins. Quem possui sua chave privada tem controle total sobre seus fundos, o que torna essencial mantê-la segura e nunca compartilhá-la com ninguém. Se alguém tiver acesso à sua chave privada, essa pessoa poderá movimentar seus Bitcoins livremente.

Guardar suas chaves privadas de maneira segura é crucial para evitar perdas. Algumas das formas mais seguras incluem o uso de carteiras físicas (hardware wallets) ou soluções de backup offline. Lembre-se: sem a chave privada, você não tem acesso aos seus Bitcoins, e, se ela for perdida, os fundos podem se tornar inacessíveis para sempre.

Chaves Públicas

As chaves públicas funcionam como uma versão simplificada da chave privada. Elas são derivadas da chave privada por meio de processos criptográficos e podem ser compartilhadas livremente. A chave pública é o endereço que você fornece para receber criptomoedas. Assim como um número de conta bancária, ela serve apenas para receber fundos, mas não concede nenhum controle sobre os Bitcoins armazenados.

Por serem seguras para compartilhamento, as chaves públicas podem ser usadas em transações com qualquer pessoa, sem comprometer a segurança da sua chave privada. No entanto, para manter a privacidade, é recomendável o uso de diferentes chaves públicas em diferentes transações, minimizando a possibilidade de rastreamento das suas atividades na Blockchain.

Altcoins

Altcoins são todas as criptomoedas que surgiram após o Bitcoin. O termo é uma abreviação de "alternative coins" e se refere a qualquer criptomoeda que não seja o Bitcoin. Embora o Bitcoin tenha sido a primeira e permaneça a mais dominante criptomoeda, milhares de altcoins foram criadas com o objetivo de oferecer diferentes funcionalidades, algoritmos de consenso ou melhorias tecnológicas.

Algumas altcoins buscam solucionar limitações percebidas no Bitcoin, como velocidade de transações, escalabilidade ou custos de mineração. Exemplos populares incluem o Ethereum, que introduziu contratos inteligentes, permitindo a criação de aplicações descentralizadas, e o Litecoin, que oferece transações mais rápidas e taxas menores.

No entanto, é importante lembrar que nem todas as altcoins têm um propósito sólido ou garantem longevidade. Muitas delas surgem como experimentos ou especulações, e algumas podem não sobreviver a longo prazo. Enquanto o Bitcoin é frequentemente visto como uma reserva de valor, muitas altcoins são mais focadas em casos de uso específicos ou na exploração de novas tecnologias.

Ao considerar investir em altcoins, é essencial entender a proposta por trás da criptomoeda, seu nível de descentralização e a solidez de sua comunidade e desenvolvimento. Embora algumas altcoins tenham trazido inovações importantes, o mercado é altamente volátil, e muitas moedas acabam desaparecendo com o tempo.