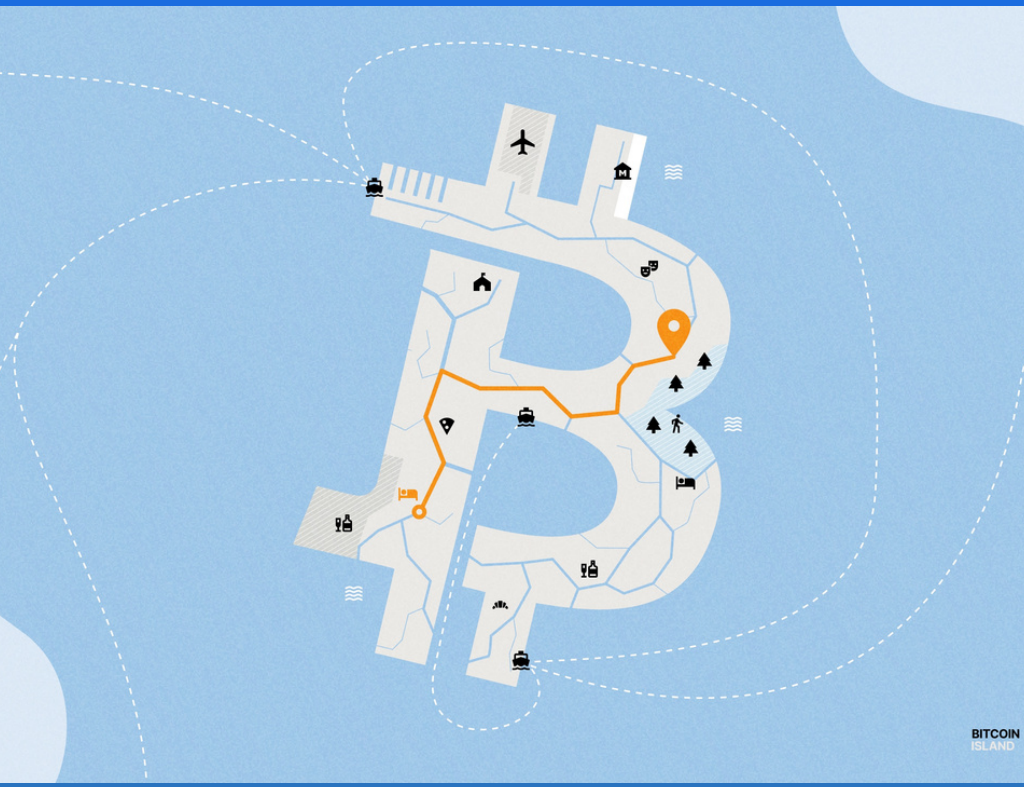
BITCOIN

CONCEITOS BASICOS PARA COMEÇARES

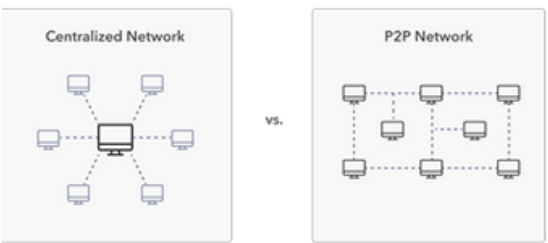


NEY CARVALHO

O QUE É A BITCOIN

bitcoin é dinheiro digital. Ao contrário das moedas fiduciárias, como o euro, a bitcoin não é controlada por nenhuma autoridade central. Em vez disso, a bitcoin é regulada por um conjunto de regras que o torna descentralizado e acessível a todos.

As transações da bitcoin são estritamente peer-to-peer, ou seja, diretamente de quem envia para quem recebe, não precisa de intermediários como acontece no nosso sistema atual

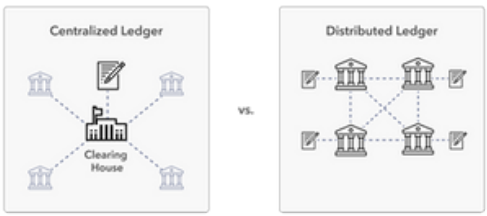


Rede centralizada vs rede peer-to-peer

bitcoin foi criada com um conjunto de regras que regem o seu uso e a sua oferta. A oferta de bitcoin, como regularmente chamada “bitcoin supply”, nunca devera exceder 21 milhões de unidades, o que torna bitcoin extremamente escassa.

COMO FUNCIONA A BITCOIN

A bitcoin usa uma blockchain para armazenar todas as transações que ocorrem na rede. A blockchain da bitcoin é um livro público compartilhado que todos os participantes têm acesso. Lotes de transações são adicionadas a blockchain em blocos. Cada bloco é anexado cronologicamente ao bloco anterior, garantindo que nenhuma bitcoin é gasta duas vezes. Esse design torna a bitcoin transparente e resistente à corrupção ou fraude, e funciona há mais de uma década.



Livro de razão centralizado vs Livro de razão descentralizado

Cada bloco contém transações da bitcoin. Há um limite para o número de transações que podem ser incluídas em um único bloco.

A mineração da bitcoin, o processo utilizado para adicionar novos blocos a blockchain, garante que as transações anteriores não possam ser alteradas. Essa imutabilidade garante que os pagamentos nunca sejam revertidos ou redirecionados.

COMO UTILIZAR A BITCOIN?

A bitcoin pode ser usada igualmente como outras moedas, para pagar bens e serviços. Para pagar com bitcoin, o remetente só precisa saber o "endereço bitcoin" do destinatário.

Todas as transações são públicas e podem ser vistas por todos, e o saldo de um determinado "endereço" pode ser facilmente verificado, no entanto os endereços não identificam as pessoas que os controlam.

Isso torna a rede pseudoanónima, as transações e os endereços são públicos, mas não podemos associar um endereço a necessariamente, uma pessoa.

QUALIDADE DA BITCOIN

Muitos optam por utilizar a bitcoin em detrimento de outras moedas porque elas satisfazem bem as características e qualidades de uma moeda. Entre outros fatores, a divisibilidade, portabilidade, durabilidade e escassez da bitcoin a tornam uma forma de dinheiro muito eficaz.

Em média, as transações usando bitcoin são confirmadas a cada dez minutos. Uma transação geralmente é confiável após uma única confirmação, mas a maioria das pessoas preferem esperar de 2 a 6 confirmações adicionais antes de aceitar o pagamento, uma medida de segurança adicional, as transações são irreversíveis, mas quanto mais confirmações, maior a sua irreversibilidade.

Sistema finacneiro atual vs bitcoin

ESCASSEZ

Nunca haverá mais de 21 milhões de bitcoins. Isso significa que, não importa quão alta a procura por bitcoin, a oferta será sempre a mesma, portanto, o valor da bitcoin pode subir indefinidamente. A escassez é uma característica valiosa para uma moeda porque permite que a moeda seja uma medida de valor verdadeiramente justa e imutável.

DIVISIBILIDADE

Embora existam apenas 21 milhões de bitcoins, cada bitcoin é divisível em 100 milhões de unidades, chamados satoshis. Isso permite que a bitcoin seja gasta em pequenas quantidades, mesmo que o preço de uma única bitcoin continue a aumentar.

Unidade	Símbolo	Valor bitcoin
bitcoin	BTC	1
satoshi	sat	0.000 000 01

DESCENTRALIZAÇÃO

A bitcoin é completamente descentralizada. Isso significa que, ao contrário de outras moedas, principalmente moedas fiduciárias, nenhuma entidade pode de forma arbitraria alterar as regras, produzir ou redistribuir a bitcoin. Além disso, ninguém pode ser banido da rede Bitcoin. Qualquer pessoa pode minerar, participar ou enviar e receber transações. Não é necessária nenhuma qualificação ou permissão. Ninguém pode entrar na lista “negra” ou devedora da bitcoin.

BITCOIN MINING

A mineração de bitcoin é o processo pelo qual novas bitcoins são colocadas em circulação. É também a forma como a rede confirma novas transações e é um componente crítico da manutenção e desenvolvimento da blockchain.

A "mineração" é realizada usando hardware sofisticado que resolve um problema de matemática computacional extremamente complexo. O primeiro computador a encontrar a solução do problema recebe o próximo bloco de bitcoins e o processo recomeça. A pessoas que possuem esses computadores são chamados de mineradores.

PROOF OF WORK

Prova de trabalho

A prova de trabalho (abreviada para PoW) é um dos mecanismos de consenso para alcançar um acordo na rede blockchain da bitcoin para confirmar transações e produzir novos blocos para a cadeia.

Com o Proof of work, os mineradores competem entre si para validar transações e serem recompensados.
A probabilidade de ser selecionado para construir o próximo bloco está ligada ao poder computacional.

LIGHTNING NETWORK

A Bitcoin Lightning Network (Lightning Network) é um protocolo de pagamento construído em cima do Bitcoin. O Lightning não emite um token ou possui uma blockchain. Em vez disso, a Lightning utiliza a moeda da rede Bitcoin (bitcoin) para pagamentos e sua blockchain para liquidação final e segurança.

Como uma analogia simples, você pode pensar na Lightning Network como sendo o MB Way e a rede Bitcoin como semelhante ao envio de uma transferência bancária. As duas redes, embora relacionadas, cada uma tem casos de uso exclusivos. Por exemplo, não usarias o MB Way para dar entrada em uma casa.

Por outro lado, usar uma transferência bancária para enviar a um amigo a tua parte da conta de um jantar seria excessivo, para não dizer caro.

Lightning, então, não é um substituto para a camada base do Bitcoin. Em vez disso, decidir entre o Lightning ou a camada base é simplesmente uma questão de escolher a ferramenta certa para o trabalho. Por exemplo, se a tarefa em questão for uma pequena transação, a ferramenta certa pode ser o pagamento via Lightning. O Lightning se torna uma escolha óbvia se souberes que terás várias transações com a mesma pessoa ou empresa.

CHAVE PRIVADA

Cada endereço da bitcoin tem uma chave pública e uma chave privada correspondente, juntas elas são chamadas de “keypar”. Se tiveres acesso a chave privada, terás acesso efetivo aos fundos que constam na carteira e conseguirás gastá-lo sem problemas.

A chave privada é uma cadeia de caracteres hexadecimal de 64 (ou 256 se descritas em 1s e 0s binários) gerada pelo algoritmo de criptografia. Eles se parecem assim na forma hexadecimal:

5KYZdUEo39z3FPrtuX2QbbwGnNP5zTd7yyr2SC1j299sBCnWjss

Ou assim em forma extensa:

xprv9zrji5mK3nb4RbuR2ZYFtyzK3gn78KnEzkNP4ZxwwPPwcgQQVZqnjTMAGxmmM3jpmfsthQUtfD9iYPvnaqwejCjcyEswLqEhX4LPKNFUXT5

Como a chave privada é o "bilhete" que permite que gastes as tuas bitcoins, é importante que eles sejam mantidos em segredo e seguros. As chaves privadas podem ser mantidas em arquivos de computador, mas também são frequentemente escritas em papel.

Se as tuas bitcoins estiverem numa corretora, não tens acesso a tua chave privada, ou seja, não tens acesso ao teu fundo, o que tens é uma promessa de que a corretora vai te dar as moedas quando precisares, é exatamente igual ao nosso sistema atual, em que tens dinheiro numa conta no banco e dependes da vontade do banco para teres acesso a ele.

Nunca armazenes a bitcoin numa carteira em que não tenhas a chave privada.

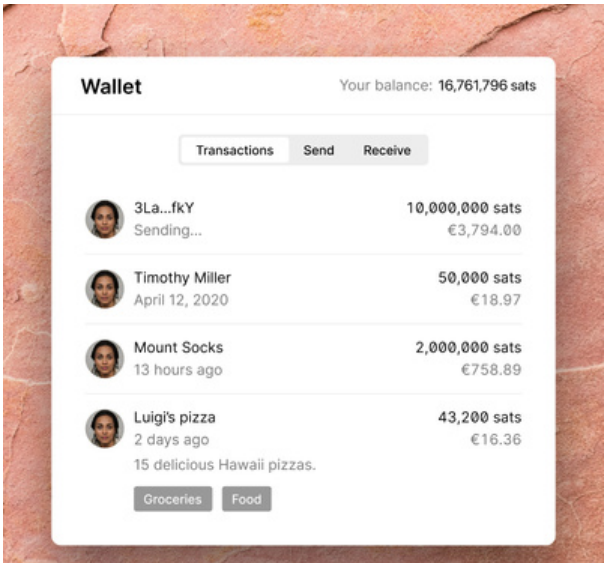
FRASE DE RECUPERAÇÃO

Também conhecido como Seed, Mnemonic e Frase de Backup

A frase de recuperação fornece acesso total a uma carteira bitcoin, pois contém a chave privada e, portanto, é muito valiosa.

É extremamente importante mantê-lo seguro, tanto para que outras pessoas não tenham acesso a ela, quanto para que não a percas.

CARTEIRA BITCOIN



Exemplo carteira bitcoin

Semelhante a uma carteira tradicional que carregas no bolso, uma carteira bitcoin é usada para armazenar a bitcoin. A diferença é que, em vez de armazenar uma coleção de cartões, uma carteira bitcoin armazena uma coleção de chaves privadas. Normalmente, uma carteira é criptografada com uma senha ou protegida contra acesso não autorizado.

Ao contrário da rede Bitcoin, uma carteira bitcoin é controlada apenas pelo seu proprietário (não é distribuída e compartilhada como a blockchain). É importante manter sua carteira bitcoin segura definindo uma senha forte ou mantendo-a fora do alcance de indivíduos mal-intencionados.
Exemplos de Carteira: Muun Wallet, BlueWallet, Ledger etc.

CARTEIRA COM CUSTODIA E SEM CUSTODIA

Depois de comprar bitcoin, deves decidir se desejas usar uma carteira com custodia ou sem custodia para armazenar teus fundos.

Com uma carteira sem custódia, tens controle exclusivo de tuas chaves privadas, que por sua vez controlam tua bitcoin e provam que os fundos são teus. Embora não seja necessário confiar em terceiros ao usar uma carteira sem custódia, isso também significa que és o único responsável por não perder tuas chaves e exige que tomes as próprias precauções para proteger teus fundos.

Com uma carteira com custódia, outra parte controla as tuas chaves privadas. Em outras palavras, estás a confiar em um terceiro para proteger teus fundos e devolvê-los se quiseres negociar ou enviá-los para outro lugar. Embora uma carteira de custódia diminua a responsabilidade pessoal, ela exige confiança no custodiante que detém teus fundos.

Atualmente, a maioria das carteiras com custódia são as corretoras.

CHAVE PÚBLICA

Uma sequência de letras e números que o proprietário de uma carteira envia às pessoas para receber bitcoin.
Diferente das chaves privadas, a chave pública permite que recebas bitcoin na tua carteira.
Assim como enviar a alguém teu endereço de e-mail, uma chave pública pode ser fornecida a outras pessoas que desejam te enviar bitcoin.

CARTEIRA QUENTE OU FRIA

Quente e frio descrevem uma carteira em termos de conexão com a internet. Onde uma carteira quente está conectada à internet, uma carteira fria não está. A ideia é que uma carteira fria seja menos suscetível a roubos de terceiros pela internet.

A maioria das carteiras de software seriam vistos como quentes (embora alguns possam ser usados apenas para assinar em um dispositivo não conectado à Internet), e a maioria das carteiras de hardware seriam vistos como frios (embora às vezes estejam conectados para fins de assinatura) .

TIPOS DE CARTEIRAS

Mobile Wallets

Carteiras móveis são simplesmente carteiras de bitcoin projetadas para um dispositivo móvel. Isso significa que eles podem escancear facilmente códigos QR, são fáceis de navegar com uma tela sensível ao toque e são acessíveis enquanto estão em movimento. A carteira móvel permite enviar, receber bitcoin, e algumas permite também comprar e vender.

Hardware Wallet

Uma carteira de hardware é um tipo especializado de dispositivo projetado especificamente para armazenar bitcoins. A vantagem é que as carteiras de hardware são muito mais difíceis de serem comprometidas por um usuário mal-intencionado quando comparadas a uma carteira móvel, pois usam a quantidade mínima de software necessária para armazenar bitcoins com segurança.

Paper Wallets

As carteiras de papel são uma maneira de incorporar bitcoins em um meio físico, como papel ou metal. Como uma nota de banco impressa, se uma carteira de papel for perdida ou destruída, o bitcoin armazenado nela desaparecerá para sempre. Mas traz uma segurança adicional uma vez que não pode ser hackeada.

COMO COMPRAR BITCOIN

O primeiro passo para comprar bitcoin consiste em escolher um serviço ou local de negociação da moeda. Os serviços e locais de negociação populares para a compra de bitcoin são serviços de pagamento, algumas carteiras e corretoras. Destes, as corretoras são a opção mais conveniente porque oferecem uma variedade de recursos e costumam ser mais baratas.

A inscrição em uma corretora permitirá que compres, vendas e mantenhas a bitcoin. Geralmente, é uma prática recomendada que utilizes corretoras que permita que seus usuários retirem a sua bitcoin para sua própria carteira sem custodia.

Eu particularmente utilizo a corretora Blockchain.com e a seguir envio todos os fundos para a minha carteira sem custodia, Muun Wallet.