BITCOIN EM 10 MINUTOS

Tudo o que você sempre quis saber sobre Bitcoin

Brought to you by Relai

O QUE É BITCOIN?

Bitcoin, a criptomoeda mais bem-sucedida do mundo, está fazendo manchetes em todo o mundo. Muitos querem lucrar com seu sucesso, outros são indiferentes ou até céticos. A moeda digital provocou inúmeras discussões sobre dinheiro, investimento e tecnologia. Alguns veem o Bitcoin como um veículo de pura especulação ou o denunciam como uma bolha, enquanto outros falam de inovação, revolução monetária ou até mesmo redenção do atual sistema monetário.

Vários países, incluindo a China, veem o Bitcoin como uma ameaça e declararam guerra à criptomoeda. Outros governos, como o de El Salvador, introduziram o Bitcoin como meio de pagamento oficial na esperança de crescimento econômico.

Mas o que é Bitcoin? É dinheiro? Ouro digital? Uma moda passageira para cientistas da computação e especuladores? Ou algo totalmente diferente? Nos parágrafos seguintes, chegaremos ao fundo dessas perguntas e examinaremos mais de perto a moeda digital para entender melhor a filosofia e a funcionalidade por trás do Bitcoin. Para conseguir isso, é importante começar pelo começo: com a história das origens do Bitcoin.

A HISTÓRIA DO BITCOIN

Os primórdios do Bitcoin remontam ao início dos anos noventa. Em 1992, um grupo de cientistas da computação na Califórnia iniciou uma lista de e-mail para trocar ideias com pessoas afins sobre criptografia, matemática, política e filosofia. Eles se chamavam de ‚Cypherpunks' - um jogo de palavras de cyberpunk (uma pessoa na literatura de ficção científica que é cético em relação à sociedade - e com razão) e cifra (criptografar).

Os Cypherpunks

Os Cypherpunks logo se transformaram em uma equipe heterogênea. Apesar de suas origens diferentes, eles estavam unidos pela convicção de que a Internet logo se tornaria uma das arenas mais disputadas pela liberdade humana.

Para se proteger contra a ameaça de controle, vigilância e censura da Internet e preservar uma Internet livre e aberta, os Cypherpunks usavam uma arma poderosa: a criptografia, a encriptação de informações.

Em seu manifesto de 1993, eles declararam: “Cypherpunks escrevem código [de computador]. Sabemos que alguém precisa escrever software para defender a privacidade e [...] nós vamos escrevê-lo.”

Mas a criptografia por si só não seria suficiente para uma Internet livre. Porque, e os Cypherpunks estavam convencidos disso, a Internet não pode ser verdadeiramente livre se não tiver seu próprio dinheiro. Din-

heiro que é independente de estados, bancos centrais e empresas; uma criptomoeda tão justa e descentralizada quanto a própria Internet.

Experimentos Monetários

Mas a criação de dinheiro digital independente apresentou aos Cypherpunks desafios técnicos. Já em 1990, o criptologista David Chaum havia criado o eCash, a primeira criptomoeda, que não era descentralizada, mas garantia o anonimato graças à criptografia. No entanto, o eCash não foi capaz de se afirmar contra outros sistemas de pagamento online a longo prazo. A empresa por trás do projeto teve que pedir falência após 8 anos de serviço e o eCash desapareceu.

Outras tentativas se seguiram, das quais o E-Gold se destacou. E-Gold era uma criptomoeda lastreada em ouro que estava aberta a todos. Fundada durante a era pontocom em 1996, a empresa conquistou seus pares, processando mais de dois bilhões de dólares em transações por ano em seu auge.

Mas o E-gold era controlado por uma instituição central e, portanto, vulnerável a ataques. Problemas legais logo se seguiram e o governo dos EUA tomou medidas legais contra o E-Gold. Em 2008, o E-Gold foi considerado culpado por um tribunal dos EUA de lavagem de dinheiro e violações do Patriot Act. Todos os ativos foram congelados e o E-Gold teve que cessar as operações.

Essas tentativas fracassadas demonstraram dois fatos para os Cypherpunks. Primeiro, tanto o eCash quanto o E-gold tinham sido lastreados por garantias. Essas garantias provaram ser um ponto fraco, pois poderiam ser confiscadas por estados. Portanto, uma criptomoeda livre não deve ter pontos centrais de ataque, como uma empresa registrada, uma conta bancária ou um local de servidor centralizado. E segundo, tanto os governos quanto os reguladores não têm interesse em dinheiro digital independente do estado.

Para os Cypherpunks, a questão básica, para a qual ainda não havia sido encontrada uma solução, permaneceu: como um dinheiro digital independente pode funcionar sem um partido central para manter os livros e garantir que o dinheiro não seja gasto duas vezes? Afinal, se fosse possível resolver o problema do gasto duplo sem depender de um partido central, talvez fosse possível criar dinheiro digital livre que seja nativo da Internet.

Um Ato Místico de Criação

Por essas razões, os Cypherpunks começaram a discutir projetos para uma criptomoeda sem um partido central e garantias. Dois dos conceitos mais importantes foram b-money (1998) e BitGold (2005). Essas ideias teóricas, que nunca foram implementadas na prática, já eram muito

semelhantes ao Bitcoin em seu design. Um par de chaves pública/privada foi previsto para encriptação e uma Prova-de-Trabalho deveria ser fornecida para a criação de moedas digitais adicionais, como também é o caso do Bitcoin. Em seu Whitepaper, o inventor do Bitcoin também confirmou que estava ciente do b-money e do BitGold.

No entanto, como o b-money e o BitGold dependiam de um sistema de votação para consenso (o acordo sobre quem possui quais unidades monetárias no momento), eles eram vulneráveis a ataques maliciosos que poderiam manipular tais eleições e, assim, distorcer a propriedade.

Para este último problema, que ainda impedia a criação de um novo dinheiro na Internet, uma solução foi apresentada na sexta-feira, 31 de outubro de 2008. Naquele dia, o Bitcoin Whitepaper, no qual Satoshi Nakamoto explica seu conceito de uma rede de pagamento descentralizada, foi enviado por e-mail para os Cypherpunks. Dois meses depois, em 3 de janeiro de 2009, a rede Bitcoin foi lançada.

As reações iniciais à nova rede foram silenciadas. Alguns entusiastas começaram a testar a rede e relatar erros. No início, porém, foi principalmente o próprio Satoshi Nakamoto que manteve a rede funcionando. Mas, lentamente, a notícia do novo dinheiro da Internet se espalhou para fóruns de informática e tecnologia e o interesse na rede cresceu. Depois de um ano, a rede Bitcoin já tinha alguns usuários. O próprio Bitcoin, no entanto, ainda não tinha valor.

Quem é Satoshi Nakamoto?

O Whitepaper do Bitcoin, bem como a comunicação por e-mail do inventor do Bitcoin, foram ambos assinados com o nome Satoshi Nakamoto. No entanto, a verdadeira identidade do inventor do Bitcoin permanece desconhecida até hoje, pois seu nome parece ser um pseudônimo. Para abordar pessoas que pensam da mesma forma e, mais tarde, a comunidade de desenvolvedores Bitcoin, Nakamoto usou pelo menos três endereços de e-mail diferentes, que ele criptografou completamente para ocultar a verdadeira identidade do remetente.

Várias pessoas já afirmaram ser Satoshi Nakamoto. Mas até hoje, cada um deles não consiguiu provar isso. Porque a prova final, nomeadamente o envio de Bitcoin de um dos endereços de carteira que provavelmente pertencem a Satoshi, ainda não foi fornecida por ninguém.

Além disso, o grupo daqueles que se comunicaram „pessoalmente“ com Satoshi Nakamoto pela Internet é muito pequeno. Satoshi Nakamoto escreveu sua última mensagem para a comunidade Bitcoin em 12 de dezembro de 2010, mas esta não foi de forma alguma uma mensagem de de-

spedida - Satoshi simplesmente parou de se comunicar depois disso.

Sua retirada, no entanto, foi apenas para a comunidade em geral. Nakamoto continuou a reunir um pequeno grupo de programadores principais ao seu redor e os informou sobre o desenvolvimento da rede Bitcoin. Mas em abril de 2011, ele enviou uma mensagem final a esse grupo também. Tão misteriosamente quanto Nakamoto apareceu em 2008, ele desapareceu novamente três anos depois.

O "Dia da Pizza" do Bitcoin

Mas como o Bitcoin obteve valor em primeiro lugar? No começo, o Bitcoin podia ser minerado e enviado de um lado para o outro entre os membros da rede, mas as unidades digitais não tinham valor. Além disso, o grupo das pessoas que conheciam o Bitcoin, quanto mais podiam enviá-lo e recebê-lo, ainda era muito pequeno.

Isso mudou em 22 de maio de 2010, quando um pedido incomum apareceu no fórum da Internet bitcointalk.org. Um homem de 28 anos chamado Laszlo Hanyecz, da Flórida, ofereceu 10.000 Bitcoins para a pessoa que iria pedir duas pizzas para sua casa. Um estudante californiano aceitou a oferta e mandou entregar em sua casa duas pizzas grandes no valor de $41. Em troca, Hanyecz enviou a ele os 10.000 Bitcoins.

Desde aquele dia, 22 de maio tem sido comemorado anualmente pelos Bitcoiners como Bitcoin „Pizza Day". O dia tornou-se popular porque ilustra três coisas:

- Bitcoins têm valor
- Bitcoins são adequados como meio de troca e pagamento
- Bitcoin como moeda é desinflacionário.

O número de Bitcoins adicionais colocados em circulação está diminuindo constantemente, o que pode levar a um aumento no valor.

As duas pizzas entraram para os livros de história como as mais caras do mundo. Calculando seu custo com o preço do Bitcoin de dezembro de 2021, foram pagos incríveis 460 milhões de dólares americanos por eles. Isso é muito dinheiro. Mas o destinatário dos 10.000 Bitcoins também já os gastou. Em uma entrevis-

ta, ele afirmou que havia vendido o Bitcoin não muito tempo depois para pagar por uma viagem de carro - ao preço do Bitcoin de hoje, provavelmente a viagem mais cara da história da humanidade também.

O „Dia da Pizza“ do Bitcoin também ilustra de forma impressionante porque o ‚hodling‘ - derivado de ‚manter‘ (em Inglês, ‚to hold‘) - é tão popular entre os Bitcoiners. ‚Hodling‘ significa manter os Bitcoins por longos períodos com a intenção de (possivelmente) nunca vendê-los. Afinal, quem quer gastar seu Bitcoin hoje quando ele pode valer o dobro, o triplo ou até dez vezes mais nos próximos anos?

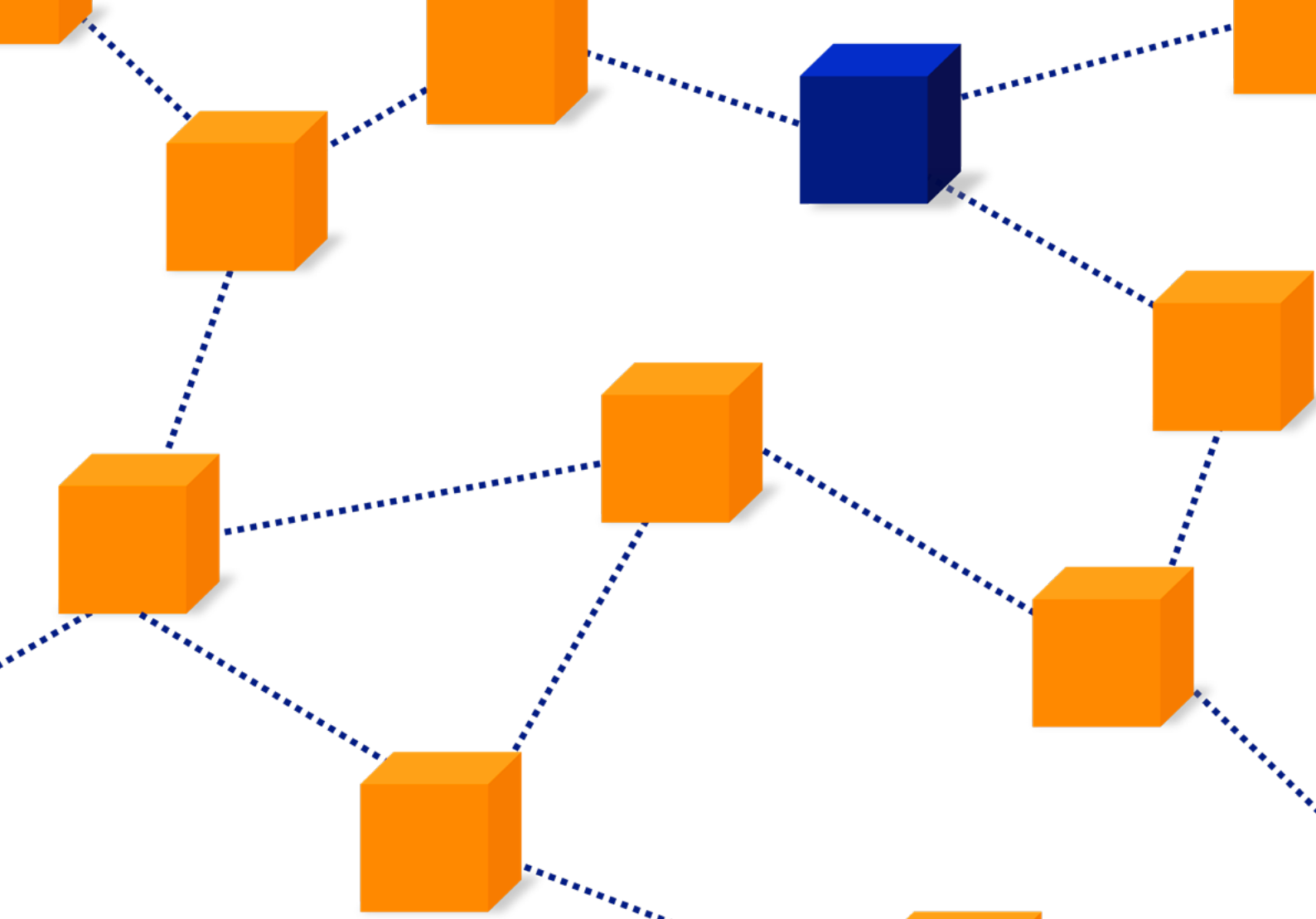
COMO FUNCIONA O BITCOIN?

Depois de aprender sobre a história do Bitcoin, vamos agora mergulhar em sua maneira de operação. O objetivo é entender como funciona a rede Bitcoin, quais problemas ela resolve e quais são seus benefícios práticos.

A intenção por trás do Bitcoin é ser uma rede descentralizada. Nenhum participante da rede deve ser capaz de governar a rede sozinho - o poder de tomada de decisão e supervisão são distribuídos entre todos os participantes. Isso é importante porque nenhum indivíduo, nenhum governo e nenhuma empresa podem mudar a rede de forma independente, mas as mudanças só são possíveis coletivamente.

O Bitcoin funciona de tal forma que cada participante da rede tem uma cópia idêntica do registro de propriedade mais atualizado o tempo todo – como resultado, todo mundo sempre sabe quem atualmente possui quais Bitcoins. Assim, ninguém pode alegar que possui mais Bitcoin do que possui, porque cada participante da rede pode verificar essa reivindicação contra sua cópia do livro-razão e provar que é falsa.

Antes do lançamento do Bitcoin, as redes descentralizadas enfrentavam dois grandes desafios. Primeiro, como garantir que todos os participantes recebam as atualizações mais recentes sobre mudanças de propriedade - ou seja, as informações sobre quais Bitcoins foram transferidos e para quem. E segundo, como



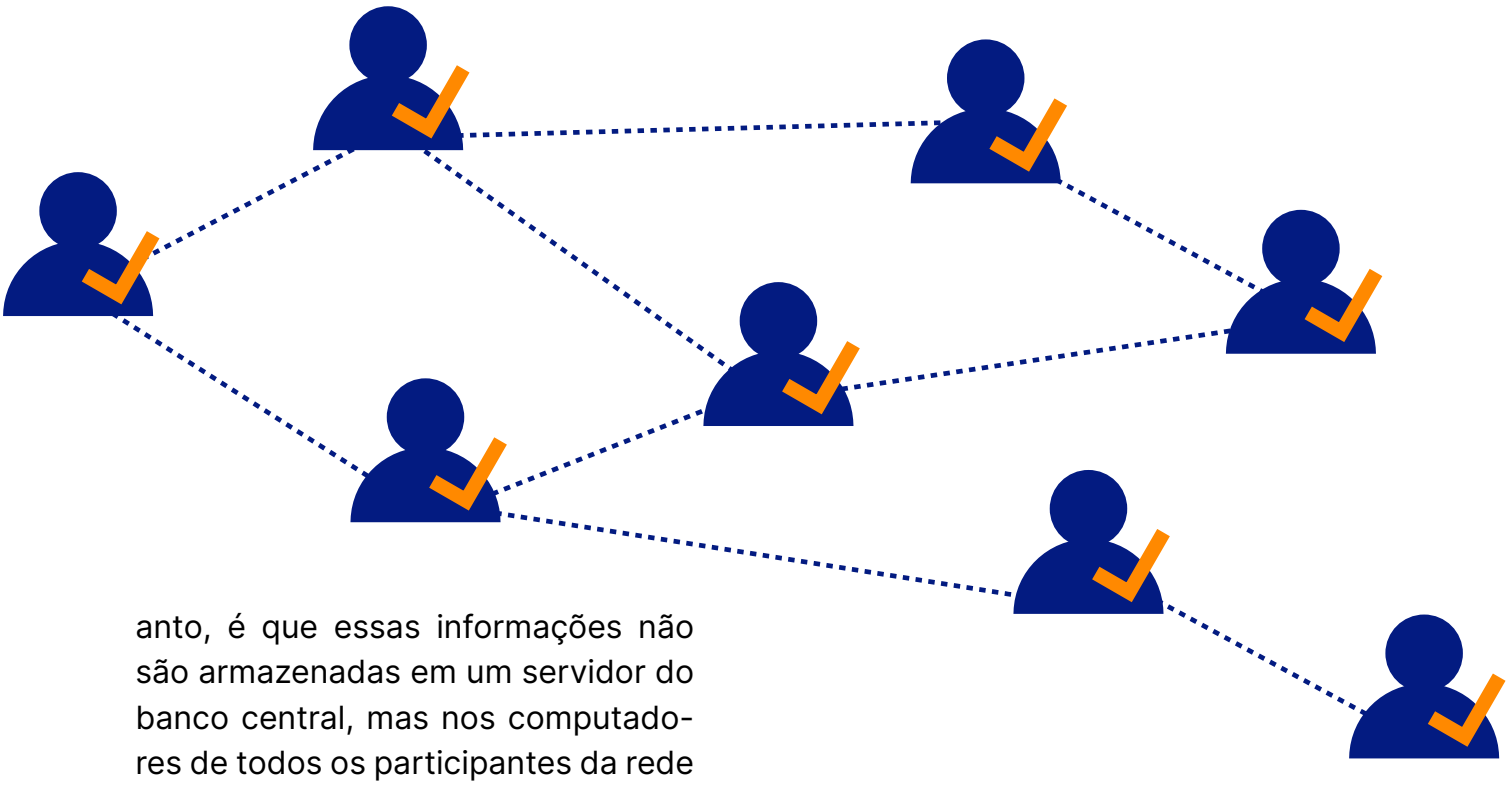
os participantes podem verificar com absoluta certeza que as informações que recebem estão corretas.

O Blockchain

Essas dificuldades foram superadas graças à invenção do blockchain. Um blockchain armazena informações e dados em ordem cronológica. No caso do Bitcoin, todas as transações desde a criação do Bitcoin são armazenadas em ordem cronológica em dezenas de milhares de blocos, que juntos formam o blockchain do Bitcoin. Qualquer participante da rede que queira saber quem possui qual Bitcoin pode rastrear o histórico de transações no blockchain do Bitcoin e determinar exatamente quem possui quantos Bitcoins no momento.

Assim, se alguém quiser enviar um Bitcoin, qualquer um pode verificar se esse Bitcoin realmente pertence à pessoa em questão.

Até este ponto, esse mecanismo não é novidade, pois os bancos usam um processo semelhante. Se um cliente quiser gastar um franco suíço, o banco consulta o histórico de transações para ver se o franco ainda pertence ao cliente ou se já foi gasto (enviado para outra pessoa). A característica única de um blockchain, no ent-



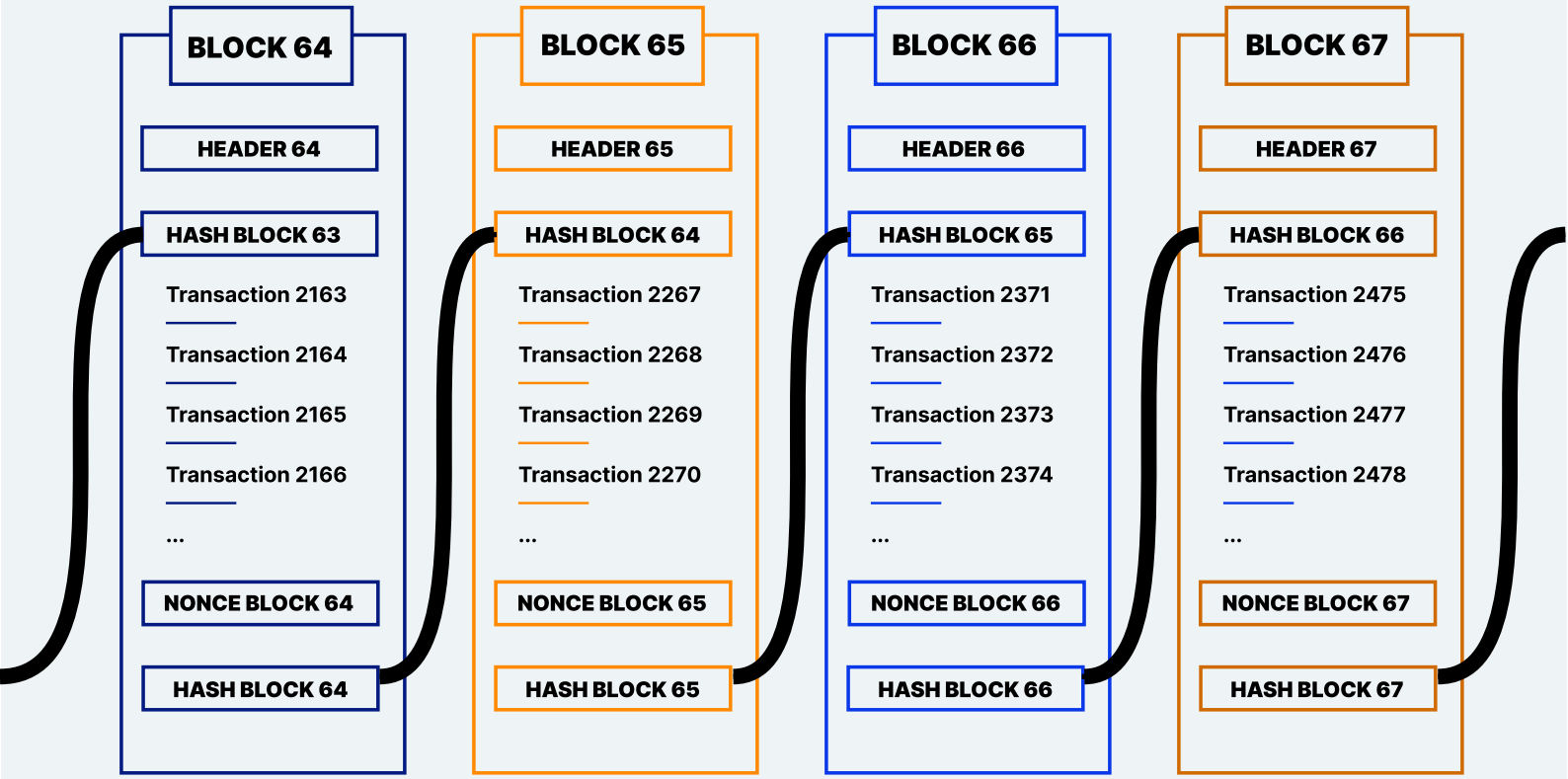
anto, é que essas informações não são armazenadas em um servidor do banco central, mas nos computadores de todos os participantes da rede (os chamados nós completos) e, portanto, existem em dezenas de milhares de cópias em todo o mundo. Esta é também a razão pela qual o Bitcoin não pode ser simplesmente excluído - para isso, seria necessário excluir a cópia do blockchain de todos os computadores participantes em todo o mundo ao mesmo tempo.

No entanto, o desafio que os blockchains enfrentam é que cada participante da rede deve ser capaz de determinar com absoluta certeza que sua cópia do blockchain está correta e que nenhuma transação errônea ou fraudulenta entra em sua cópia do livro-razão. Como novos blocos com novas transações são adicionados ao blockchain a cada 10 minutos, o blockchain está em constante crescimento e deve ser atualizado continuamente em todos os computadores participantes em todo o mundo.

Esses blocos recém-anexados devem ser verificáveis por todos. A verificação é feita usando regras imutáveis que são definidas no código de computador da rede Bitcoin. Essas regras definem exatamente quais transações são permitidas e quais não são. Cada usuário que baixa a cópia do blockchain pode, portanto, verificar se todas as transações estão de acordo com as regras dadas. Se uma transação violar as regras, ou seja, se estiver incorreta ou fraudulenta, ela será rejeitada pelos participantes da rede (nós completos) e não incluída na blockchain.

Mineração de Prova de Trabalho (em Inglês, "Proof-of-Work" (PoW))

Além disso, a rede Bitcoin tem um mecanismo para limitar o acréscimo de novos blocos. Se novas transações e blocos pudessem ser adicionados ao blockchain por qualquer pessoa, a rede acabaria em caos, pois o blockchain não seria capaz de se atualizar em todo o mundo para o mesmo estado com rapidez suficiente.



O cabeçalho, o resultado da função hash do bloco anterior, todas as transações do bloco atual e um Nonce (número aleatório) são colocados em uma função matemática. O Nonce é alterado até que o resultado da função hash tenha zeros anteriores suficientes. Esse processo é chamado de mineração."

Para evitar isso, o Bitcoin funciona com um mecanismo de Prova de Trabalho. Para alguém ganhar o direito de adicionar um novo bloco ao blockchain, eles devem fornecer prova de trabalho. Uma ilustração simples desse processo é um grupo de pessoas procurando agulhas em um palheiro. Quem encontrar uma agulha primeiro tem permissão para adicionar um novo bloco ao blockchain. Além disso, o localizador é recompensado com novas unidades de Bitcoin, bem como as taxas de transação contidas neste bloco. Assim que o bloco for anexado, esse processo será iniciado novamente.

Na realidade, os mineradores estão executando uma função de hash matemática (algoritmo de hash SHA-256) na busca por números específicos. O número de hash do bloco anterior, as transações do bloco atual e um número aleatório (chamado 'nonce', uma abreviatura de "number only used once", ou em Português „número usado apenas uma vez") são misturados juntos. O número aleatório é alterado até que a função hash gere um resultado com um número mínimo de zeros à esquerda. Por exemplo, o bloco #700000, criado em 11 de setembro de 2021, tinha o número de hash válido: 0000000000000000590fc0f3eba193a278534220b2b37e 9849e1a770ca959.

A busca por esse número, também

chamada de mineração, tem duas funções principais: primeiro, ela liga os blocos de maneira matemática-criptográfica para que todos possam verificar facilmente a ordem correta. Ao mesmo tempo, o mecanismo de Prova de Trabalho torna quase impossível alterar essa ordem. Em segundo lugar, esse mecanismo atrasa a adição de novos blocos para que, em média, um novo bloco seja adicionado ao blockchain apenas a cada 10 minutos. Assim, todos os participantes da rede em todo o mundo têm tempo suficiente para atualizar para o mesmo estado mais recente do blockchain.

Em resumo, os mineradores mantêm a rede Bitcoin funcionando. Graças a eles, novas transações estão sendo processadas e adicionadas ao blockchain. Os nós completos guardam cópias do livro-razão, garantem que as regras sejam cumpridas e garantem que nenhuma transação fraudulenta entre no blockchain.

21 milhões de Bitcoins

Embora mais blocos estejam constantemente sendo adicionados ao blockchain do Bitcoin e os mineradores sejam recompensados por esse trabalho com novos Bitcoins, o número total de Bitcoins é limitado a 21 milhões de Bitcoins. Nunca haverá mais de 21 milhões de Bitcoins. Mas essas 21 milhões de moedas não estavam em circulação desde o início. Em vez disso, eles são liberados pelo código Bitcoin de acordo com um cronograma de emissão estrito.

Quando o Bitcoin foi lançado, o código liberou 50 novos Bitcoins para os mineradores aproximadamente a cada 10 minutos. Quatro anos após o lançamento, o número de Bitcoins liberados a cada dez minutos caiu pela metade. Esse processo é chamado de “halving” (“reduzindo pela metade”) e descreve o fato de que a recompensa do bloco para os mineradores diminui pela metade a cada 4 anos. Atualmente, já existem 19 milhões de Bitcoin em circulação. O Bitcoin restante será extraído até o ano de 2140. Depois disso, os mineradores serão compensados apenas por meio de taxas de transação.

A quantidade estritamente limitada de unidades Bitcoin é uma das propriedades fundamentais da criptomoeda e torna o Bitcoin uma mercadoria extremamente escassa. Essa escassez digital absoluta também é um pré-requisito importante para a função do Bitcoin como uma reserva de valor durante longos períodos e é a razão pela qual o Bitcoin é frequentemente chamado de ouro digital ou ouro 2.0.

O Resultado: Propriedade Digital

Examinando todas as características da rede Bitcoin em combinação, pode-se ver a importância dessa invenção. Pela primeira vez na história, existe um bem digital que só está

disponível em um número estritamente limitado. Bitcoins não podem ser copiados ou duplicados.

Graças a essa conquista, o Bitcoin é frequentemente referido como propriedade digital. Porque assim como cada pedaço de terra neste globo é único e existe apenas uma vez, cada unidade Bitcoin também é única e existe apenas uma vez no espaço digital.

E essas unidades de Bitcoin podem ser verdadeiramente possuídas. Somente a pessoa na posse da chave privada correspondente, que é uma combinação de números e letras consistindo de 64 caracteres, pode mover o Bitcoin associado. Em outras palavras, sem essa chave privada, o Bitcoin não pode ser roubado, confiscado ou bloqueado. Isso permite que o proprietário tenha controle absoluto sobre seus recursos financeiros, independentemente de ser milionário, refugiado político ou um credor perseguido. Pela primeira vez desde a invenção do computador, é possível realmente possuir ativos digitais.

POR QUE BITCOIN?

Mas por que toda essa propaganda exagerada em torno do Bitcoin? A possibilidade de realmente possuir um ativo digital pode ser revolucionária. Mas por que alguém iria querer possuir Bitcoin em primeiro lugar?

O Melhor de Dois Mundos

Nos séculos passados, metais preciosos e, mais tarde, dinheiro em forma de moedas e notas foram usados como meio de pagamento. Estes tinham a vantagem de poderem ser armazenados e gastos independentemente de terceiros. O ditado "dinheiro é liberdade impressa" resume isso muito bem. No entanto, a desvantagem de metais preciosos e dinheiro é que eles são difíceis de usar no espaço digital da Internet. O mais tardar desde o advento das compras online, os cartões de débito e crédito tornaram-se, portanto, estabelecidos entre a população em geral.

Mas agora que a maioria das pessoas está usando dinheiro digital em contas bancárias em vez de numerário, os riscos de contraparte que enfrentam estão aumentando. Se, por exemplo, uma instituição financeira declarar insolvência, as poupanças dos clientes podem ser perdidas. Ou, como aconteceu em Chipre em 2013, se as retiradas de dinheiro forem severamente limitadas, controles de capital forem implementados e a expropriação forçada de contas de poupança estiver acontecendo, então as pessoas não estão mais no controle de seu dinheiro. Ou, como atualmente é o caso em muitos países ocidentais, se os clientes bancários não estão autorizados a enviar dinheiro para parentes porque vivem em Cuba ou no Irã, eles dependem de um terceiro para aprovar todas as suas transações.

Com a mudança do dinheiro baseado em papel para o dinheiro digital arm-

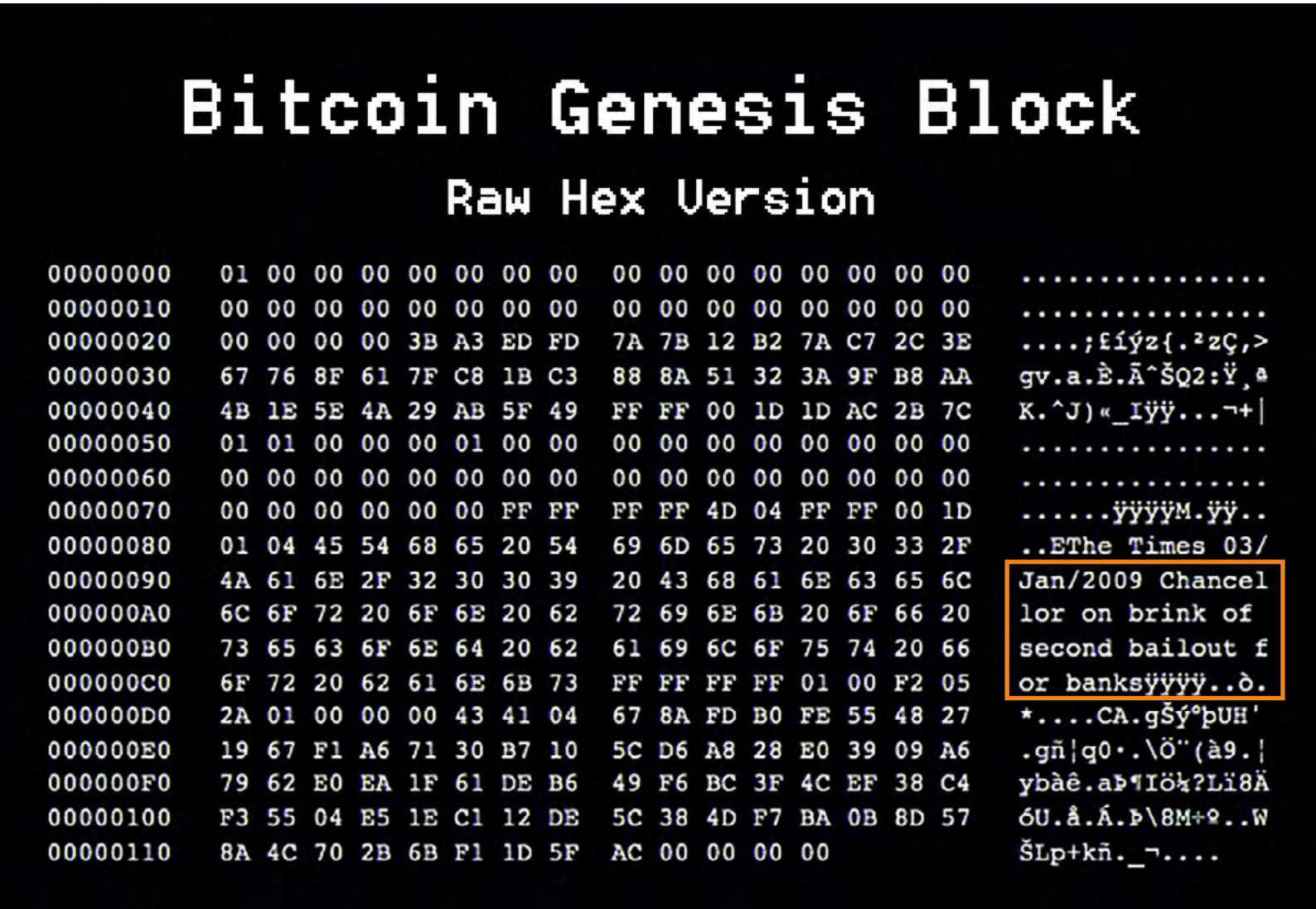
azenado em contas bancárias, em última análise não estamos mais no controle de nosso próprio dinheiro. Até agora, no entanto, essa desvantagem tem sido o preço que tivemos que pagar para participar de uma vida digitalizada.

O Bitcoin oferece uma solução para esse dilema. Como dinheiro digital, é ideal para uso no espaço digital. Ao mesmo tempo, o Bitcoin pode ser armazenado como propriedade digital sem ter que depender de terceiros (bancos) para sua guarda. Assim, os proprietários de Bitcoin podem armazenar suas moedas - na forma de chaves privadas - sob o colchão ou onde acharem é mais seguro.

Momento Perfeito

O Bitcoin foi criado em meio à crise financeira global de 2008/09. No primeiro bloco do blockchain do Bitcoin - também chamado de bloco Genesis - Satoshi Nakamoto deixou uma mensagem forte. Ele citou uma manchete publicada no jornal The Times dizendo: “Chanceler à beira de um segundo resgate para os bancos”.

Com este ato, Satoshi expressou a filosofia crítica do estado dos Cypherpunks. Na crise financeira de 2008, os bancos centrais colocaram grandes quantidades de dinheiro novo em circulação para salvar os bancos. No final, no entanto, os poupadores pagaram por isso, pois suas econo-



mias perderam valor através da diluição pelo excesso de dinheiro. Esse fato mais uma vez confirmou a desconfiança dos Cypherpunks no estado e nos bancos centrais e reforçou sua convicção de que o dinheiro independente do estado era urgentemente necessário.

O mesmo procedimento, apenas em maior escala, tem se repetido desde o surto da pandemia de Covid-19. Somente em 2020, a oferta monetária dos EUA foi expandida em 50% e em outros países - incluindo a Suíça - a impressora digital está funcionando constantemente. Uma consequência direta disso são as baixas taxas de juros recordes - até mesmo taxas de juros negativas na Suíça - e a forte inflação de ativos.

Cobertura contra a Desvalorização da Moeda

O Bitcoin foi, portanto, lançado no melhor momento possível. Raramente a questão do dinheiro foi tão relevante e os pontos de interrogação maiores do que hoje. Com sua oferta limitada de 21 milhões, o Bitcoin oferece um contraste agradável com os balanços cada vez maiores dos bancos centrais. Sua oferta limitada oferece proteção contra a diluição do capital, como foi observado com todas as moedas em todo o mundo nas últimas décadas.

Devido à sua configuração específica, o Bitcoin é projetado para garantir a preservação do poder de compra por longos períodos. Como o Bitcoin é escasso, deve ser ainda melhor nessa tarefa do que o ouro, que tem um fluxo líquido de 1-2% a cada ano. Além disso, os custos de armazenamento e transporte do Bitcoin também são significativamente menores em comparação com o ouro, o que também permite uma melhor preservação do valor ao longo do tempo.

Proteção de Propriedade

Outra questão que o Bitcoin atenua é a proteção da propriedade. Enquanto o ouro ou o dinheiro geralmente devem ser armazenados com segurança a um grande custo para protegê-los contra roubo, o Bitcoin pode ser armazenado e transportado a um custo praticamente zero. Mesmo quantidades substanciais podem ser tomadas em qualquer lugar do mundo com um código que consiste em doze ou vinte e quatro palavras. Uma vez memorizado e fisicamente destruído, esse código não pode ser roubado por ninguém, tornando o Bitcoin por trás do código seguro e permitindo que seu dono os leve com ele para o túmulo, se desejar.

COMPRE BITCOIN

Existem duas maneiras de se apossar do Bitcoin. Ou você ganha Bitcoin como minerador ou você compra Bitcoin de outra pessoa. Como a mineração com dispositivos domésticos se tornou praticamente impossível hoje em dia, a única maneira que resta para os recém-chegados é comprar Bitcoin.

Trocas e Corretoras de Criptomoedas

A maneira mais fácil de comprar Bitcoin é por meio de uma troca de criptografia ou uma corretora. Estes funcionam de forma semelhante às plataformas de negociação de ações. Depois de abrir uma conta pessoal, francos suíços, euros ou dólares americanos podem ser transferidos por transferência bancária ou cartão de crédito. Uma vez que o dinheiro tenha chegado à conta pessoal na bolsa de negociação, o Bitcoin pode ser comprado 24 horas por dia, 7 dias por semana, com apenas alguns cliques, ao preço de mercado atual. Na Europa, é possível comprar Bitcoin sem registro, verificação ou depósito de dinheiro primeiro com o popular aplicativo de investimento exclusivo para Bitcoin, Relai.

Entre Pares

Como alternativa às trocas de criptomoedas, o Bitcoin também pode ser comprado diretamente de outros participantes do mercado por meio de plataformas peer-to-peer sem envolver uma troca. Isso permite um maior anonimato, pois nenhum dado pessoal deve ser revelado no processo.

Caixas Eletrônicos Bitcoin

Também existe a possibilidade de sacar Bitcoin através de caixas eletrônicos. Estes já estão disponíveis em muitos países, incluindo Suíça,

Alemanha e Áustria. Nos caixas eletrônicos Bitcoin, o Bitcoin pode ser sacado anonimamente com dinheiro ou cartão de crédito. Nem uma conta nem uma carteira criptográfica existente são necessárias.

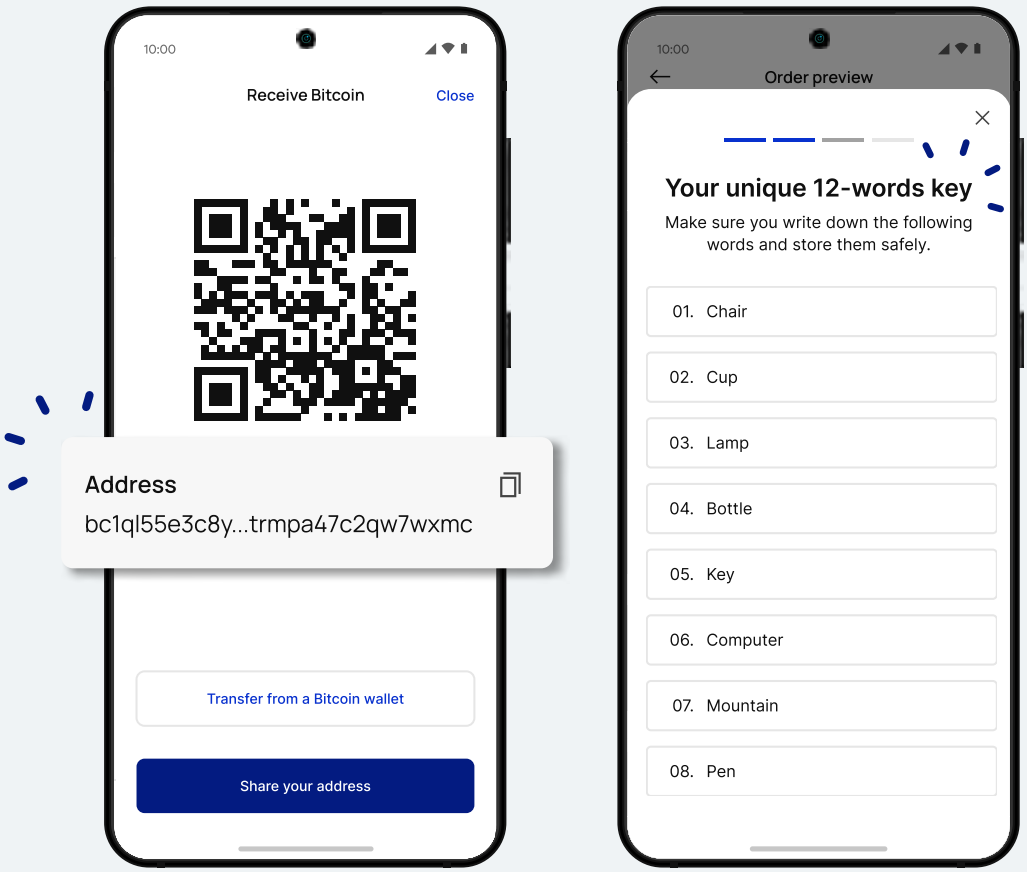
Armazene o Bitcoin com segurança

Uma vez que os Bitcoins foram adquiridos, surge a questão de seu manuseio e armazenamento seguros. Bitcoin e criptomoedas são regidos pelo princípio: „não suas chaves, não suas moedas“. Para realmente possuir seu Bitcoin, você deve estar em posse das chaves privadas correspondentes. Essa expressão um tanto técnica significa que você só tem realmente controle sobre seus Bitcoins se você armazená-los em uma carteira digital pessoal da qual você tem as chaves privadas.

Enquanto os Bitcoins são mantidos em uma troca de criptomoedas, eles estão sob o controle da troca. Se a troca for hackeada, falir ou for fraudulenta, o Bitcoin pode ser perdido para sempre.

Autocustódia

Ao contrário de uma conta bancária, o Bitcoin oferece a opção de armazenar suas unidades monetárias em uma carteira pessoal. Isso permite que você seja seu próprio banco e tem a vantagem de que você tem controle absoluto sobre seu Bitcoin. Em troca, isso também vem com responsabilidades. A chave privada, que muitas vezes vem na forma de doze ou vinte e quatro palavras, deve ser armazenada e mantida segura



pelo próprio proprietário do respectivo Bitcoin. O manuseio incorreto ou negligente pode levar à perda irrevogável de Bitcoins.

Carteiras: Carteiras Digitais

As carteiras digitais ajudam a armazenar Bitcoin com segurança ou, mais precisamente, as chaves privadas. Os próprios Bitcoins são sempre armazenados no blockchain e não podem ser transferidos para uma carteira. Apenas as chaves de acesso ao Bitcoin podem ser armazenadas em uma carteira.

Assim, as carteiras foram criadas para armazenar as chaves privadas com segurança e de forma simples. Além disso, elas permitem enviar e receber Bitcoin com apenas alguns cliques. Assim, as carteiras são uma ferramenta útil para lidar com o Bitcoin.

Carteira de Software

As carteiras mais comuns são carteiras de software. As carteiras de software podem ser configuradas como aplicativos de desktop ou como aplicativos de smartphone. Durante a configuração, as chaves privadas da carteira são listadas na forma de doze ou vinte e quatro palavras (frase de semente). Essas palavras são sinônimos do Bitcoin naquela carteira. Quem conhece essas palavras tem controle sobre as moedas. Portanto, as palavras devem ser anotadas de forma análoga, preferencialmente em papel, em sigilo e guardadas. Caso o computador ou smartphone seja perdido ou roubado, a carteira pode ser restaurada a qualquer momento com estas palavras.

As carteiras de software têm a vantagem de poderem ser configuradas rapidamente e serem fáceis de usar. No entanto, como as carteiras de software são programas de computador instalados em um dispositivo e conectados diretamente à Internet, sempre existe o risco de ataques de hackers.

Carteira de Hardware

Se você valoriza a segurança, você deve usar uma carteira de hardware em vez disso. Esses pequenos dispositivos armazenam os códigos de acesso para o Bitcoin em um dispositivo USB semelhante a um pendrive que só é conectado ao computador quando necessário. O dispositivo é projetado de tal forma que mesmo um computador infectado com software malicioso não pode acessar os códigos.

Ao configurar uma carteira de hardware, doze ou vinte e quatro palavras (frase de semente) são geradas que devem ser anotadas de forma análoga e mantidas seguras. Se a carteira de hardware for perdida, ela pode ser restaurada com a ajuda das palavras. Exemplos de carteiras de hardware são o BitBox e o Trezor.

Made in Switzerland

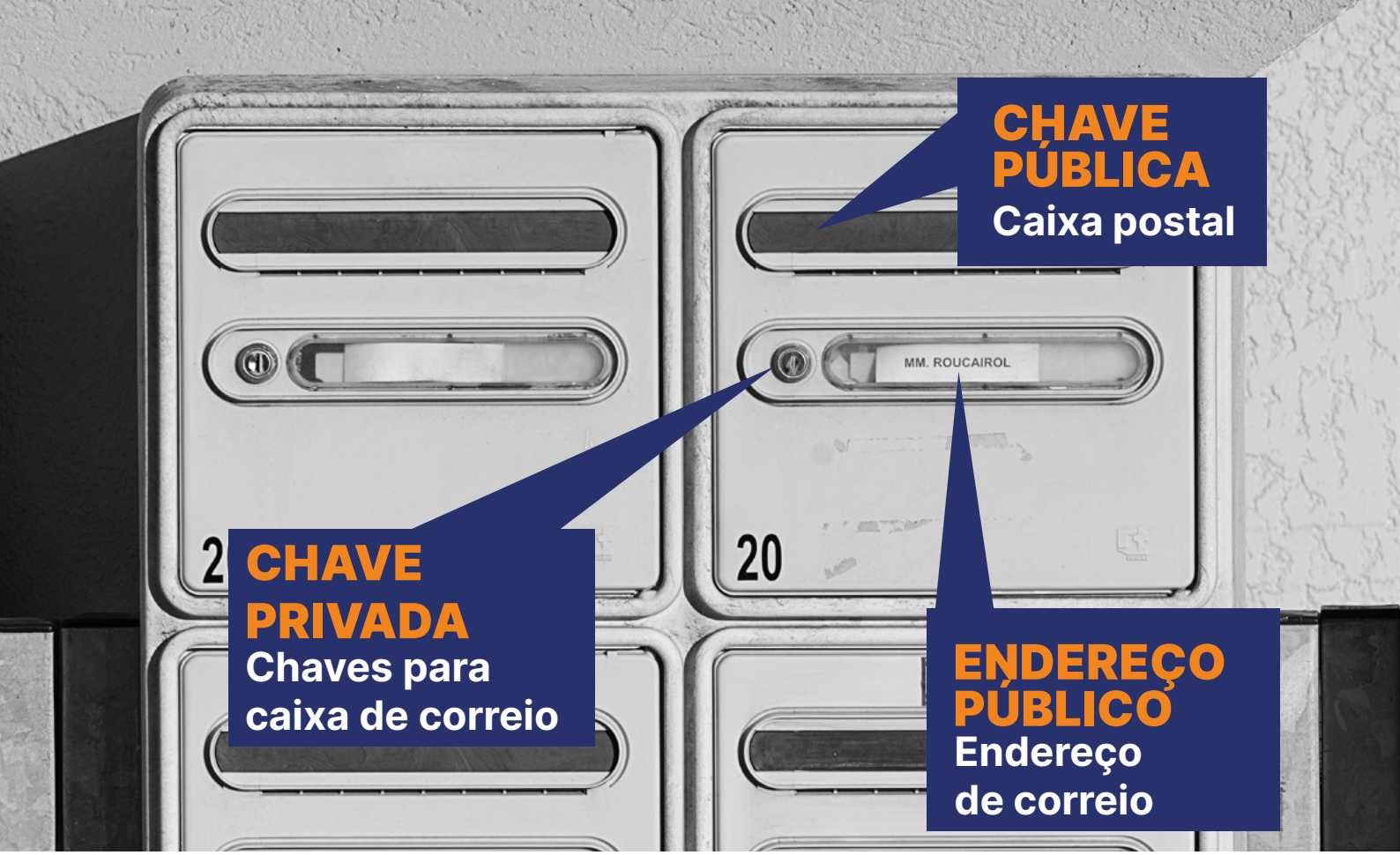
EUROPE'S EASIEST BITCOIN APP

Relai

Download on the App Store

GET IT ON Google Play

Buy bitcoin in 1 minute from as little as 10 EUR/CHF without verification.



Envie e Receba Bitcoin

Enviar e receber Bitcoin é muito fácil. Cada carteira Bitcoin tem seu endereço público gerado a partir da chamada chave pública. Isso serve como o endereço de recebimento, semelhante a um IBAN. Qualquer pessoa que tenha esse endereço pode enviar Bitcoin para a carteira correspondente. O endereço é frequentemente exibido como um código QR, o que simplifica ainda mais o manuseio.

Se você quiser enviar Bitcoin para alguém, você pode inserir o endereço Bitcoin do destinatário em sua carteira em 'enviar' ou escanear o código QR correspondente. As taxas de transação incorridas são automaticamente deduzidas da carteira do remetente. O valor das taxas de transação varia dependendo da carga da rede e pode ser consultado aqui. Demora em média 10 minutos para que a transferência chegue ao destinatário. No entanto, também pode levar mais tempo, dependendo do valor das taxas de transação que você está disposto a pagar.

Pague com Bitcoin

Quando o Bitcoin foi criado, esperava-se que o Bitcoin pudesse um dia ser usado para pagar por bens do dia a dia. E, em teoria, isso é possível hoje. Alguns departamentos fiscais do governo, organizações sem fins lucrativos e um número crescente de empresas aceitam o Bitcoin como meio de pagamento. Mas como as transações através da rede Bitcoin podem custar vários francos e levar pelo menos 10 minutos, isso só faz sentido para quantias maiores. Para

enviar Bitcoin de forma barata e rápida, é necessária uma solução alternativa.

Rede Lightning - mais rápida e mais barata

Portanto, uma camada adicional foi construída em cima da rede Bitcoin. Essa rede, chamada Lightning, permite pagar com Bitcoin em segundos a um custo mínimo. Em países como El Salvador, a rede Lightning já está em uso ativo e bem-sucedido.

O pagamento de bens do dia a dia com Bitcoin, portanto, ocorrerá em grande parte através da rede Lightning no futuro. Os desenvolvimentos nesta área estão a decorrer a toda a velocidade. O Twitter, por exemplo, introduziu recentemente uma função de 'dica' que usa a rede Lightning. Além disso, o aplicativo Strike oferece pagamentos em todo o mundo em várias moedas a custo zero por meio da rede Lightning. É de se esperar, portanto, que no futuro apenas quantias maiores sejam liquidadas diretamente pela rede Bitcoin, enquanto todas as outras transações serão executadas pela rede Lightning.

Como principalmente quantidades menores são enviadas pela rede Lightning, Satoshis, ou Sats para abreviar, são usados como unidade de conta em vez de Bitcoin. 1 Bitcoin é igual a 100.000.000 Satoshis. Para usar a Lightning Network, uma carteira Lightning deve ser configurada.

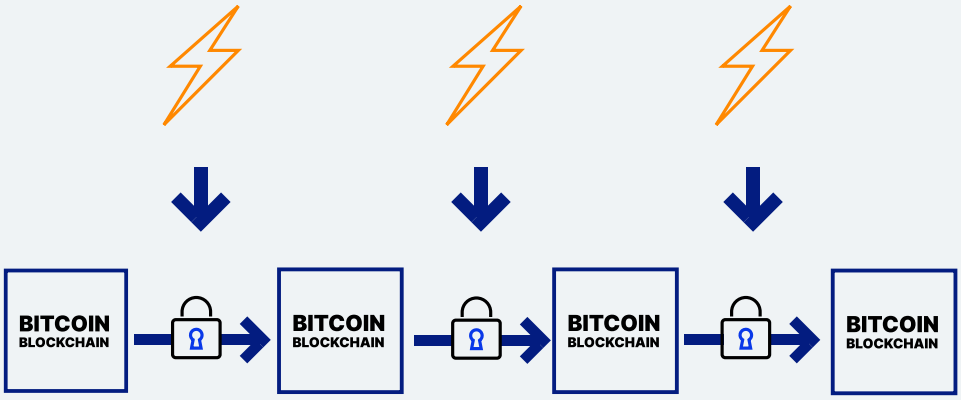
UM OLHAR PARA O FUTURO

Em seus mais de dez anos de existência, o Bitcoin passou por muitos altos e baixos. A criptomoeda foi declarada morta ou caiu no esquecimento entre o público em geral várias vezes após fortes perdas de preço. No entanto, o Bitcoin se espalhou inexoravelmente pelo mundo na última década.

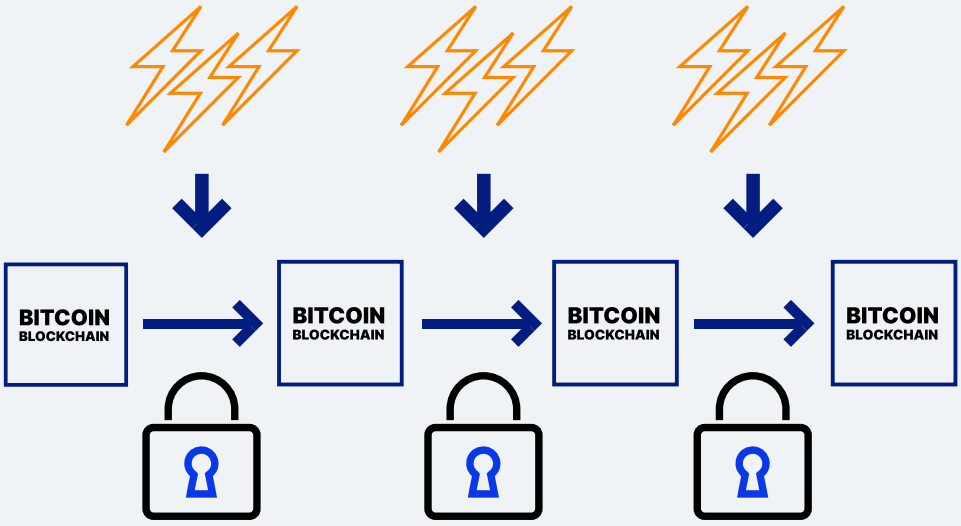
Bitcoin e Energia

Uma das primeiras preocupações que muitas vezes são levantadas em relação ao desenvolvimento do Bitcoin é o consumo de energia da rede Bitcoin. A mineração de Bitcoin já consome uma quantidade significativa de eletricidade em todo o mundo. E esse consumo provavelmente

Quanto menos energia na forma de poder de computação for utilizada para construir o blockchain do Bitcoin, mais fácil será alterá-lo mais tarde.



Quanto mais energia na forma de poder de computação for utilizada para criar o blockchain do Bitcoin, mais difícil será alterá-lo mais tarde.



aumentará no futuro, à medida que mais pessoas entrarem na mineração de Bitcoin.

Ao falar sobre Bitcoin e Energia, é importante entender que a quantidade de energia que flui para a rede Bitcoin é fundamental para a segurança da rede. Quanto mais energia flui para a rede, mais segura ela é. Isso ocorre porque, para que o blockchain do Bitcoin seja alterado, a mesma quantidade de poder de computação - e, portanto, energia - que foi investida para criar o blockchain em primeiro lugar deve ser gasta novamente. No entanto, com milhões de computadores em todo o mundo fornecendo poder de computação para a rede Bitcoin, é quase impossível para um indivíduo, organização ou estado reunir poder de computação suficiente para fazer até mesmo as menores mudanças no blockchain. Portanto, o poder de hash e o consumo de energia associado são um importante recurso de segurança da rede Bitcoin.

Além disso, os computadores de mineração Bitcoin têm a vantagem de poderem estar localizados em qualquer lugar do mundo. Como os mineradores precisam da eletricidade

mais barata possível para serem lucrativos, eles geralmente se localizam em lugares onde há muitos excedentes e, portanto, energia barata. A longo prazo, é provável que isso ocorra em lugares onde há muita energia renovável, pois isso produz a eletricidade mais barata.

De acordo com o Conselho de Mineração Bitcoin, os mineradores de Bitcoin usam atualmente cerca de 56% de energia renovável e a tendência está aumentando. Muitos especialistas em Bitcoin acreditam que a mineração de Bitcoin será alimentada por até 100% de energia renovável no futuro.

Até que seja esse o caso, no entanto, o consumo de energia do Bitcoin se resume à questão de saber se o dinheiro seguro e infalsificável e a reserva de valor valem esse gasto de energia - ou não.

El Salvador - Bitcoin como Moeda Nacional

Alguns anos atrás, os visionários já achavam possível que o Bitcoin um dia fosse reconhecido como moeda legal pelos estados-nação. No verão de 2021, chegou a hora: El Salvador foi o primeiro país do mundo a introduzir o Bitcoin como moeda legal. Em lojas, restaurantes e prestadores de serviços de todos os tipos, o pagamento não só pode ser feito com dólares americanos, mas também com Bitcoin. Para isso, os cidadãos receberam uma carteira Bitcoin personalizada, que permite pagamentos através da rede Lightning em questão de segundos e com um custo mínimo.

Outros países, como Ucrânia, Brasil e Panamá, estão atualmente discutindo projetos de lei semelhantes. Se outros países seguirem o exemplo de El Salvador, isso, por um lado, aumentaria ainda mais a demanda por Bitcoin e, ainda mais importante, sustentaria a credibilidade do Bitcoin como 'dinheiro'. A aceitação do Bitcoin como moeda legal em mais e mais países, portanto, representa uma fase decisiva no processo de adaptação global do Bitcoin.

Leis e Regulamentos

Esses desenvolvimentos levaram os estados-nação, bancos centrais e empresas a ter que lidar intensamente com criptomoedas. Vários estados, incluindo a Suíça, emitiram regulamentos e diretrizes sobre criptomoedas. Esta etapa é bem-vinda por muitos participantes do mercado, pois cria segurança jurídica tanto para os projetos criptográficos quanto para os investidores envolvidos.

Regulamentos também estão no horizonte nos EUA, que até agora adotaram uma abordagem laissez-faire. A forma exata que essas novas leis de regulamentação nos EUA terão está sendo monitorada de perto pela comunidade cripto global, pois elas terão um grande impacto em todo o setor cripto.

Outras Criptomoedas

Bitcoin não é de longe a única criptomoeda hoje em dia. Existem agora mais de 16.000 criptomoedas e ativos diferentes. Estas moedas e fichas têm características e funcionalidades diferentes e nem todas foram concebidas como 'moedas' ou dinheiro. Alguns são mais como ações, na medida em que seu valor reflete o sucesso de um projeto de criptografia. Outros são obrigados a fazer uso de um determinado serviço. E ainda outros - os chamados fichas de meme - são principalmente moedas divertidas.

Para evitar perdas, é, portanto, aconselhável dar uma olhada mais de perto na respectiva moeda e no projeto por trás dela antes de fazer qualquer investimento.

Moedas Digitais do Banco Central (em Inglês, 'Central Bank Digital Currencies' (CBDCs))

As criptomoedas estão em transição de uma fase não regulamentada do Oeste Selvagem para um mundo financeiro de cripto regulamentado. Esse desenvolvimento não deixou os bancos centrais ilesos, e surgiram ideias de que os bancos centrais deveriam emitir suas próprias criptomoedas. Essas "Moedas Digitais do Banco Central", ou CBDCs (do inglês 'Central Bank Digital Currencies'), combinariam, dizem os proponentes, a estabilidade de uma moeda estatal com os benefícios de uma moeda baseada em blockchain. Em suma, eles criariam dinheiro digital, por assim dizer.

No entanto, dependendo de seu design, uma CBDC pode assumir formas fundamentalmente diferentes. Vários países lançaram testes-piloto com diferentes tipos de CBDCs, e CBDCs já foram lançados em alguns países. No entanto, aguarda-se ansiosamente se, e de que forma, áreas monetárias economicamente fortes, como EUA, UE ou a China, lançarão suas CBDCs.

Competição de Dinheiro

Nossa sociedade se acostumou tanto com as moedas estatais nas últimas décadas que outros tipos de dinheiro eram dificilmente imagináveis para muitos até recentemente. Mas não muito tempo atrás, fazia parte da vida cotidiana ter diferentes tipos de dinheiro circulando em paralelo. Havia cédulas de vários bancos, moedas feitas de diversos metais e outros valores monetários que pudessem ser usados como meio de pagamento.

Com o Bitcoin, as moedas não estatais estão agora disponíveis novamente como uma alternativa às moedas estatais. Até agora, a maioria dos governos tolerou o Bitcoin. Até certo ponto, isso pode ser graças à sua natureza descentralizada, o que torna o Bitcoin difícil de atacar.

Para os cidadãos, isso significa que uma alternativa digital ao dinheiro do estado está agora disponível ao lado do ouro e da prata. Os efeitos dessa competição monetária adicional serão emocionantes de observar no futuro.

BITCOIN, E AGORÁ?

Se você está se perguntando o que deve fazer com todas essas informações, deixe-me fazer uma sugestão. Entrar no mundo do Bitcoin não custa nada, nem tempo nem dinheiro. Mas você conhecerá uma tecnologia que está prestes a mudar nosso mundo e o futuro.

Portanto: crie uma conta numa troca de cripto ou baixe uma carteira em seu smartphone e compre Bitcoin por 50 CHF. Ou peça a um colega que lhe envie um pouco de Bitcoin para sua carteira. Mas coloque as mãos no Bitcoin pelo menos uma vez.

Porque se o Bitcoin fizer o avanço e se tornar tão onipresente quanto a Internet, você não apenas saberá sobre ele teoricamente, mas também terá usado o Bitcoin você mesmo. Às vezes, isso faz toda a diferença, pois dá a você uma visão geral da tecnologia, o que o coloca à frente da maioria das pessoas.

SOBRE O AUTOR

Daniel Jungen é economista e jornalista financeiro com experiência em criptoativos. Daniel é co-fundador da InsightDeFi, uma boutique de pesquisa especializada em todas as coisas cripto. Juntamente com seus parceiros na InsightDeFi, eles publicam um boletim quinzenal (em alemão) sobre Bitcoin, DeFi e Cripto.

O RELAI

Fundado na Suíça por Julian Liniger e Adem Bilican depois que eles lutaram para encontrar um espaço seguro e sem complicações para comprar bitcoin, o Relai está tornando a poupança e o investimento em Bitcoin acessíveis para todos. O aplicativo somente para o Bitcoin é projetado para ser simples e intuitivo, permitindo que qualquer pessoa na Europa possa comprar e vender Bitcoin em poucos minutos, sem necessidade de registro, verificação ou depósitos. Com auditoria independente e com mais de 35 milhões de CHF em Bitcoin investidos por meio de sua plataforma, o Relai está dando aos consumidores a chance de desbloquear novos meios de economizar e investir.

Saiba mais em Relai.app.

Obrigado ao @SelmioC, que traduziu este e-book do inglês para o português.