BITCOIN EM 10 MINUTOS

Tudo o que sempre quis saber sobre a Bitcoin

Brought to you by **Relai**

O QUE É A BITCOIN?

A Bitcoin, a criptomoeda com maior sucesso no mundo, está a fazer manchetes por todo o globo. Muitos pretendem beneficiar do seu sucesso, enquanto que outros são indiferentes ou mesmo cépticos. Esta moeda digital desencadeou inúmeros debates sobre dinheiro, investimento e tecnologia. Há quem veja a Bitcoin como um veículo de pura especulação e denunciam-a como uma bolha, enquanto que outros falam de inovação, de revolução monetária ou mesmo de resgate do actual sistema monetário.

Vários países, incluindo a China, olham para a Bitcoin como uma ameaça e declararam guerra às criptomoedas. Outros governos, como o de El Salvador, introduziram a Bitcoin como meio de pagamento oficial, na esperança de alcançar maior crescimento económico.

Mas o que é a Bitcoin? Será dinheiro? Será ouro digital? Será uma moda para cientistas informáticos e especuladores? Ou será algo completamente diferente? Nos parágrafos seguintes iremos abordar a fundo estas questões e analisaremos mais de perto esta moeda digital para compreender melhor a sua filosofia e funcionalidade. Para isso, é importante começar com a história sobre as origens da Bitcoin.

A HISTÓRIA DA BITCOIN

A origem da Bitcoin remonta ao início dos anos noventa. Em 1992, um grupo de cientistas informáticos da Califórnia criou uma lista de emails com o intuito de trocar ideias com aqueles que partilham interesses similares sobre criptografia, matemática, política e filosofia. Chamavam-se a si próprios de ‚Cypherpunks' - um jogo de palavras entre ‚cyberpunk' (um personagem da literatura de ficção científica que é céptico em relação à sociedade - e com razão) e ‚cifra' (encriptar).

Os Cypherpunks

Os cypherpunks rapidamente se transformaram num grupo heterogéneo. Apesar das suas diferentes origens estavam unidos na convicção de que a internet se tornaria rapidamente numa das arenas mais disputadas relativamente à liberdade humana.

Para se protegerem contra a ameaça de controlo, vigilância e censura na internet, e no sentido de preservar uma internet livre e aberta, os Cypherpunks utilizaram uma arma poderosa: a criptografia, ou seja, a encriptação da informação.

No seu manifesto de 1993, eles declararam: „Os cypherpunks escrevem código [informático]. Sabemos que alguém tem de escrever software para defender a privacidade, e [...] nós vamos fazê-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 o seu próprio dinheiro. Um dinheiro que seja independente dos estados, dos bancos centrais e das empresas; uma criptomoeda que seja tão justa e descentralizada como a própria Internet.

Experiências Monetárias

Porém, a criação de dinheiro digital e independente apresentou desafios técnicos aos cypherpunks. Já em 1990, o criptologista David Chaum

havia criado o ‚eCash', a primeira moeda criptográfica que não era descentralizada mas assegurava o anonimato graças à criptografia. No entanto, o eCash não foi capaz de se afirmar a longo prazo em relação a outros sistemas de pagamento online. A empresa por detrás do projecto teve que declarar falência após 8 anos de serviço e assim o eCash desapareceu.

Seguiram-se outras tentativas, das quais se destacou o ‚E-Gold'. O E-Gold era uma moeda criptográfica garantida por reservas de ouro e aberta a todos. Fundada durante a era „dot.com" em 1996, a empresa atingiu um ponto alto entre os seus pares quando no seu auge processava mais de dois mil milhões de dólares em transacções por ano.

Mas o E-gold era controlado por uma instituição central e, portanto, vulnerável a ataques. Rapidamente se seguiram problemas legais, e o governo dos EUA tomou medidas legais contra o E-Gold. Em 2008, o E-Gold foi considerado culpado por um tribunal nos EUA em relação a branqueamento de capitais e violações do "Patriot Act." Todos os seus activos foram congelados e o E-Gold teve que cessar as operações.

Estas tentativas que falharam comprovaram dois factos aos Cypherpunks. Em primeiro lugar, tanto o eCash como o E-gold tinham sido sustentados por colaterais. Estas garantias tinham provado ser um ponto fraco, uma vez que poderiam ser apreendidas pelos estados. Portanto, uma moeda criptográfica livre não deveria ter pontos centrais de ataque tais como uma empresa registrada, uma conta bancária ou uma localização centralizada do servidor. E em segundo lugar, foi possível observar que tanto governos quanto reguladores não tinham qualquer interesse em um dinheiro digital independente do Estado.

Para os Cypherpunks, a questão básica, para a qual ainda não tinha sido encontrada uma solução, permaneceu: como pode um dinheiro digital independente funcionar sem um organismo central, gerir as contas e garantir que o dinheiro não seja gasto duas vezes? Afinal, se fosse possível resolver o problema da duplicação de gastos sem depender de um organismo central, talvez fosse possível criar dinheiro digital livre que seja nativo da internet.

Um Acto Místico de Criação

Por estas razões, os Cypherpunks começaram a debater sobre as possíveis configurações de uma criptomoeda sem um organismo central e sem colateral. Dois dos conceitos mais importantes foram o ‚b-money' (1998) e a ‚BitGold' (2005). Estas ideias teóricas, que nunca foram implementadas na prática, já eram muito semelhantes à Bitcoin no seu design. Estava previsto um par de chaves públicas/privadas para a en-

criptação e o protocolo "Prova-de-Trabalho" (em inglês, "Proof-of-Work" ou "PoW") para a criação de moedas digitais adicionais, como é também o caso da Bitcoin. No seu whitepaper, o inventor da Bitcoin confirmou também que estava ciente do b-money e da BitGold.

No entanto, porque o b-money e a BitGold dependiam de um sistema de votação por consenso (o acordo sobre quem possui quais unidades monetárias em um determinado momento), estas eram vulneráveis a ataques maliciosos que poderiam manipular os votos e assim distorcer a propriedade.

Para abordar esse último problema, que impedia a criação de um novo dinheiro para a internet, foi apresentada uma solução na sexta-feira, 31 de Outubro de 2008. Nesse dia, o Whitepaper Bitcoin foi enviado por e-mail para os cypherpunks, no qual Satoshi Nakamoto explica o seu conceito sobre uma rede de pagamentos descentralizada. Dois meses depois, no dia 3 de Janeiro de 2009, a rede Bitcoin entrou em funcionamento.

As reacções iniciais foram moderadas. Alguns entusiastas começaram a testar a rede Bitcoin e a relatar erros. No início, contudo, foi o próprio Satoshi Nakamoto que manteve a rede em funcionamento. Porém, lentamente as notícias sobre o novo dinheiro da internet espalharam-se por fóruns técnicos e informáticos e o interesse pela rede cresceu. Após um ano, a rede Bitcoin já contava com alguns utilizadores. A própria Bitcoin, no entanto, ainda não tinha qualquer valor.

Quem é Satoshi Nakamoto?

O Whitepaper Bitcoin, bem como a comunicação por e-mail do inventor da Bitcoin, foram ambos assinados sob o nome de Satoshi Nakamoto. Contudo, a verdadeira identidade do inventor da Bitcoin permanece desconhecida até hoje, uma vez que o seu nome parece ser um pseudónimo. Para se dirigir a pessoas com os mesmos interesses e, mais tarde, à comunidade de developers da Bitcoin, Nakamoto utilizou pelo menos três endereços de e-mail diferentes, os quais encriptou por completo para ocultar a verdadeira identidade do remetente.

Várias pessoas já alegaram ser Satoshi Nakamoto. Mas até hoje, cada uma delas não o conseguiu comprovar. Porque a prova final, nomeadamente o envio de Bitcoin de um dos endereços da carteira (wallet) que muito provavelmente pertence a Satoshi, ainda não foi apresentada por ninguém.

Além disso, o grupo daqueles que comunicaram „pessoalmente" com Satoshi Nakamoto através da internet é muito pequeno. Satoshi Nakamoto escreveu a sua última mensagem à comunidade Bitcoin no dia 12 de Dezembro de 2010, mas esta não

foi de forma alguma uma mensagem de despedida - Satoshi simplesmente deixou de comunicar depois dessa data.

A sua retirada, porém, foi apenas para a comunidade em geral. Nakamoto continuou a reunir um pequeno grupo de programadores à sua volta e informou-os sobre os avanços no desenvolvimento da rede Bitcoin. Mas em Abril de 2011, ele também enviou uma mensagem final a esse grupo. Tão misteriosamente como Nakamoto apareceu em 2008, ele desapareceu de novo três anos mais tarde.

O „Dia da Pizza“ da Bitcoin

Mas como é que a Bitcoin se valorizou no início? No começo, a Bitcoin podia ser minerada e enviada de um lado para o outro entre os membros da rede, mas as unidades digitais não tinham valor. Além disso, o grupo daqueles que conheciam a Bitcoin, e menos ainda os que a podiam enviar e receber, era ainda muito pequeno.
Esta situação alterou-se no dia 22 de Maio de 2010, quando um pedido invulgar apareceu no fórum da internet bitcointalk.org. Um homem de 28 anos chamado Laszlo Hanyecz, da Flórida, ofereceu 10.000 Bitcoin à pessoa que encomendasse duas pizzas para a sua casa. Um estudante californiano aceitou a oferta e mandou entregar na sua casa duas pizzas grandes no valor de 41 dólares. Em troca, Hanyecz enviou-lhe as 10.000 Bitcoin.

Desde esse dia, o 22 de Maio tem sido celebrado anualmente pelos Bitcoiners como o „Dia da Pizza“ da Bitcoin. O dia tornou-se popular porque representa três coisas:

- As Bitcoin têm valor.
- As Bitcoin são convenientes como meio de troca e pagamento.
- A Bitcoin como moeda é desinflacionária. O número de Bitcoin adicionais colocadas em circulação está a diminuir constantemente, o que pode levar a um aumento do seu valor.

As duas pizzas foram consideradas nos livros de história como as mais caras do mundo. Calculando o seu custo comparado com o preço da Bitcoin em Dezembro de 2021, foram pagos uns inacreditáveis 460 milhões de dólares americanos pelas pizzas. Isto é muito dinheiro. Mas o destinatário das 10.000 Bitcoin tam-

bém já as gastou. Numa entrevista, declarou que as tinha vendido pouco tempo depois para pagar uma viagem de carro - ao preço actual da Bitcoin, provavelmente também a viagem de carro mais cara da história da humanidade.

O „Dia da Pizza“ da Bitcoin também ilustra de forma impressionante porque é que o „hodling“ - proveniente do inglês „hold“ (em português „manter“) - é tão popular entre os Bitcoiners. „Hodling“ significa manter as suas Bitcoin durante longos períodos de tempo com a intenção de (possivelmente) nunca as vender. Afinal, quem quer gastar as suas Bitcoin quando hoje em dia podem valer o dobro, o triplo, ou mesmo dez vezes mais no futuro?

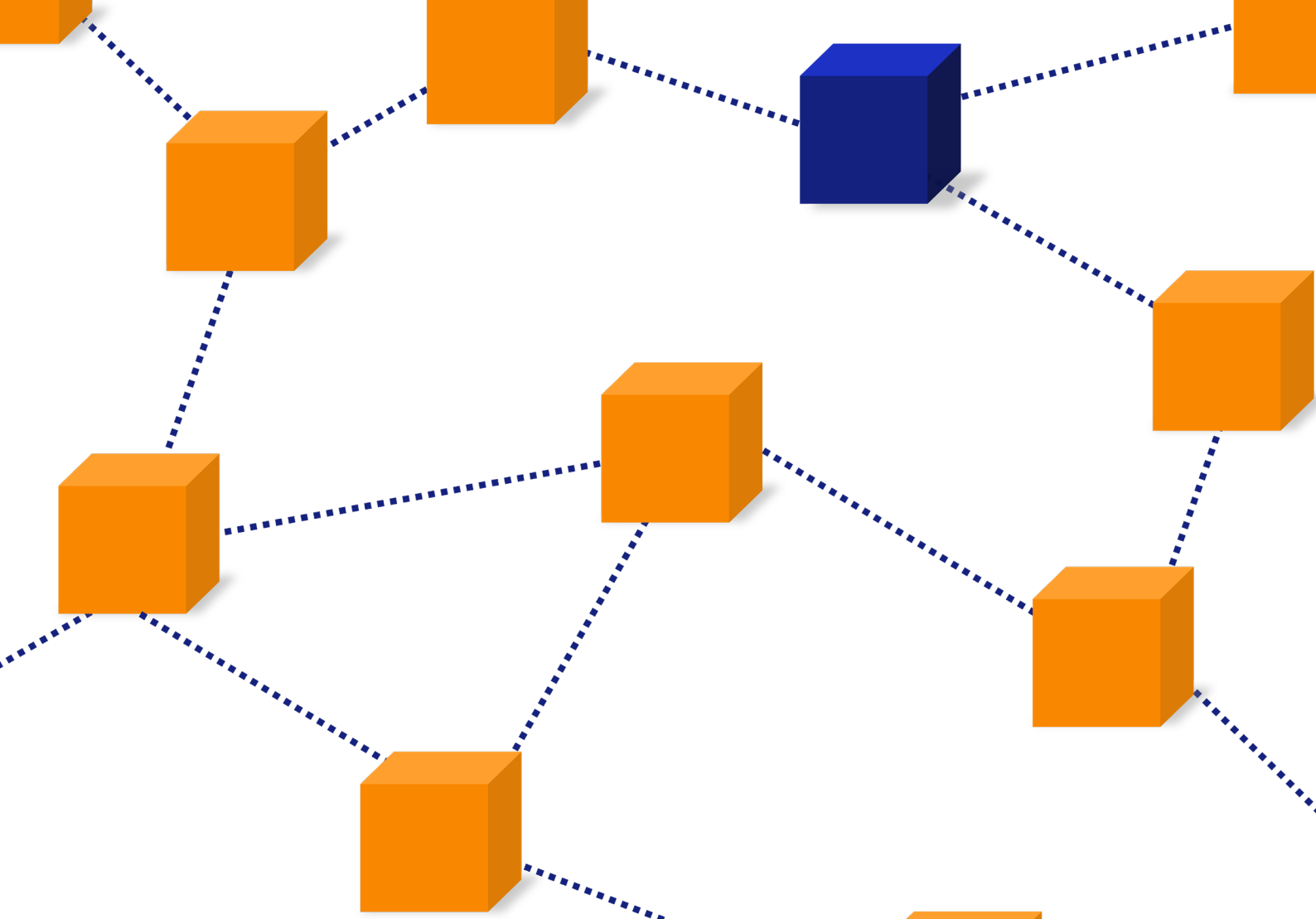
COMO FUNCIONA A BITCOIN?

Depois de termos aprendido sobre a história da Bitcoin, vamos agora mergulhar no seu modo de funcionamento. O objectivo é compreender como funciona a rede Bitcoin, quais os problemas que ela resolve e quais são os seus benefícios práticos.

A intenção por detrás da Bitcoin é tornar-se numa rede descentralizada. Nenhum participante da rede deve ser capaz de a governar sozinho - o poder de decisão e supervisão são distribuídos entre todos os participantes. Isto é importante porque nenhuma pessoa, nenhum governo e nenhuma empresa pode mudar a rede de forma unilateral, já que as mudanças só são possíveis colectivamente.

A Bitcoin funciona de tal forma que cada participante da rede tem sempre uma cópia idêntica do registo de propriedade (a “ledger”) mais actualizado - como resultado, todos sabemos sempre quem é actualmente o proprietário de qual Bitcoin. Assim, ninguém pode alegar que possui mais Bitcoin do que realmente tem, porque cada participante da rede pode verificar esta alegação através da sua cópia do registo (“ledger”) e provar que é falsa.

Antes do lançamento da Bitcoin, as redes descentralizadas enfrentavam dois grandes desafios. Em primeiro lugar, como assegurar que todos os participantes recebessem as atualizações mais recentes sobre mudanças de propriedade - ou seja, a

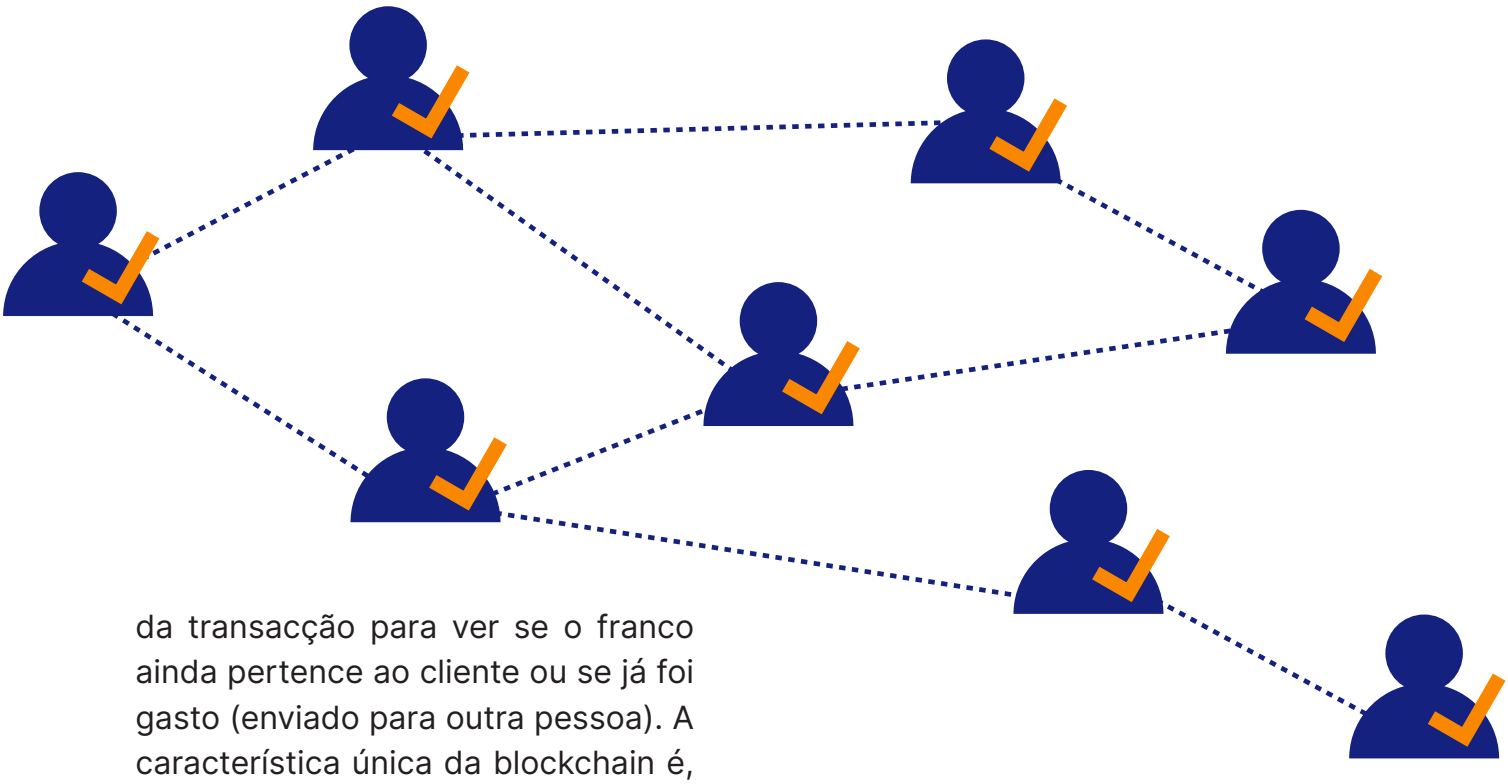


informação sobre quais Bitcoin foram transferidas e para quem. E em segundo lugar, como podem os participantes verificar com absoluta certeza que a informação que recebem está correcta.

A Blockchain

Estas dificuldades foram ultrapassadas graças à invenção da blockchain. Uma blockchain armazena informações e dados por ordem cronológica. No caso da Bitcoin, todas as transacções desde a criação da Bitcoin são armazenadas por ordem cronológica em dezenas de milhares de blocos, que juntos formam a blockchain da Bitcoin. Qualquer participante da rede que queira saber quem é o proprietário de cada Bitcoin pode rastrear o histórico de transacções na blockchain da Bitcoin e determinar exactamente quem é o proprietário actual de determinadas Bitcoin. Assim, se alguém quiser enviar Bitcoin, qualquer pessoa pode verificar se essa Bitcoin pertence realmente à pessoa em questão.

Até este ponto, este mecanismo não é novidade, uma vez que os bancos utilizam um processo semelhante. Se um cliente quiser gastar um franco suíço, o banco consulta o histórico



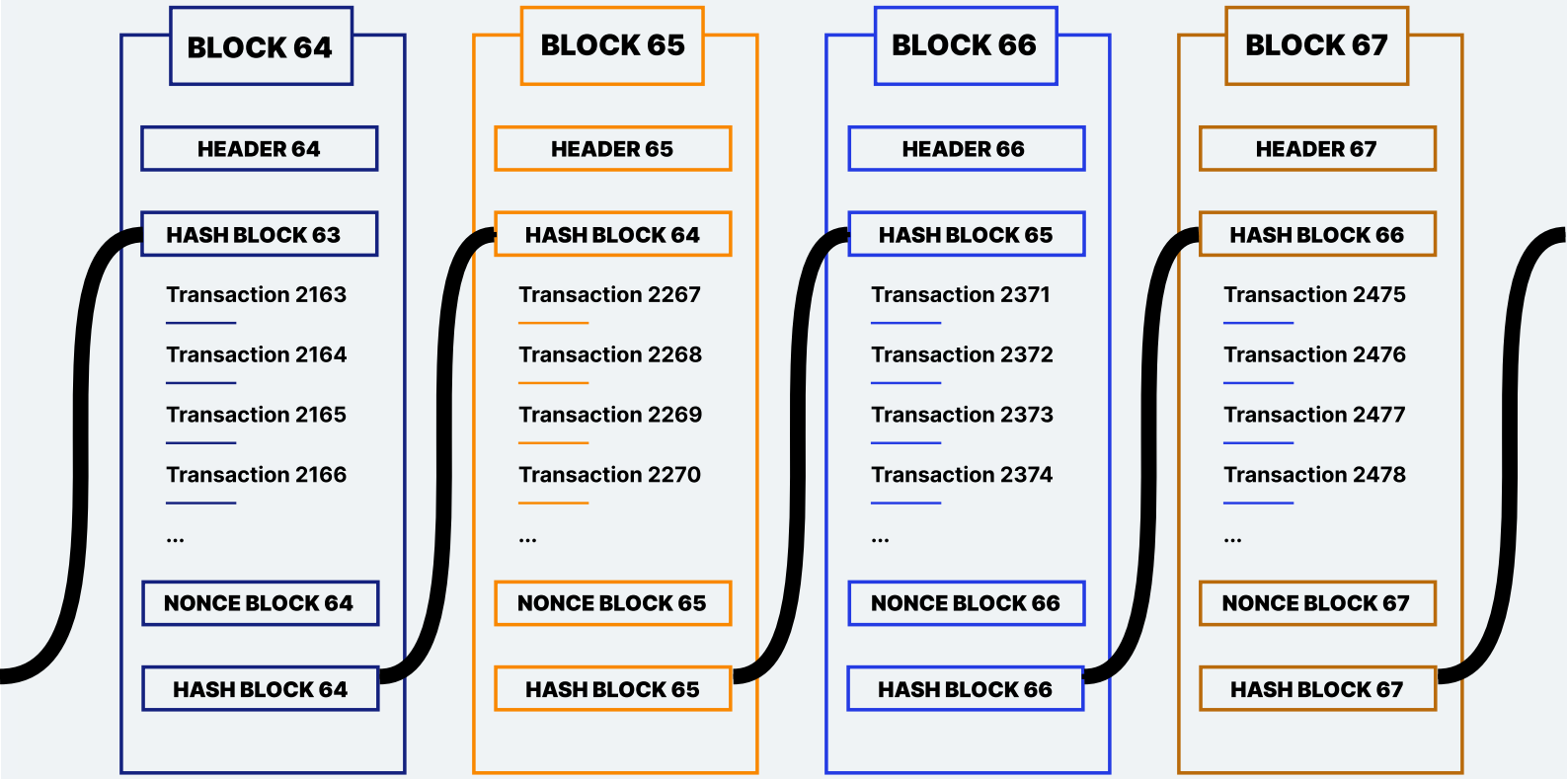
da transacção para ver se o franco ainda pertence ao cliente ou se já foi gasto (enviado para outra pessoa). A característica única da blockchain é, no entanto, que esta informação não é armazenada num servidor de um banco central, mas nos computadores de todos os participantes da rede (os chamados „full nodes“, em português, os “nós completos”) e, portanto, existe em dezenas de milhares de cópias em todo o mundo. Esta é também a razão pela qual a Bitcoin não pode simplesmente ser eliminada - para o fazer, seria necessário eliminar a cópia da blockchain de todos os computadores participantes a nível mundial e ao mesmo tempo.

Contudo, o desafio que as blockchains enfrentam é que cada participante da rede deve ser capaz de determinar com absoluta certeza de que a sua cópia da blockchain está correcta e que nenhuma transacção errónea ou fraudulenta entra na cópia do seu registo (“ledger”). Uma vez que novos blocos com novas transacções estão a ser adicionados à blockchain a cada 10 minutos, a blockchain está em constante crescimento e deve ser continuamente actualizada em todos os computadores envolvidos em todo o mundo.

Estes blocos recém-anexados devem ser verificáveis por todos. A verificação é feita utilizando regras inalteráveis que são definidas no código informático da rede Bitcoin. Estas regras definem exactamente as transacções que são permitidas e as que não são. Cada utilizador que fizer o download da cópia da blockchain pode, portanto, verificar se todas as transacções cumprem as regras em questão. Se uma transacção violar as regras, ou seja, se for incorrecta ou fraudulenta, ela é rejeitada pelos participantes da rede (os nós completos) e não é incluída na blockchain.

A Mineração Prova-de-Trabalho (PdT)

Além do mais, a rede Bitcoin tem um mecanismo para limitar a anexação



O ‚Header', o resultado da função hash do bloco anterior, todas as transacções do bloco actual, e um ‚Nonce' (número aleatório) são introduzidos numa função matemática. O Nonce é alterado até que o resultado da função de hash tenha um número de zeros precedentes suficiente. Este processo é chamado de mineração.

de novos blocos. Se novas transacções e blocos pudessem ser adicionados à blockchain por qualquer pessoa, a rede acabaria em caos, uma vez que a blockchain não seria capaz de se actualizar a si própria a nível global e com rapidez suficiente.

Para prevenir esta situação, a Bitcoin funciona com um mecanismo de Prova-de-Trabalho. Para que alguém ganhe o direito de adicionar um novo bloco à blockchain, deverá apresentar a „prova de trabalho." Uma ilustração simples deste processo é um grupo de pessoas à procura de agulhas num palheiro. Quem encontrar primeiro uma agulha pode adicionar um novo bloco à blockchain. Além disso, quem a encontra é recompensado com novas unidades de Bitcoin, assim como com as taxas de transacção contidas naquele bloco. Assim que o bloco tenha sido anexado, este processo começa novamente.

Na realidade, os mineiros estão a executar uma função matemática de hash (algoritmo de hash SHA-256) em busca de números específicos. O número de hash do bloco anterior, as transacções do bloco actual, e um número aleatório ("nonce") são agrupados. O número aleatório é modificado até a função hash emitir um resultado com um número mínimo de zeros à cabeça. Por exemplo, o bloco #700000, criado no dia 11 de Setembro de 2021, tinha o número de hash válido: 0000000000000000590fc0f3e-

ba193a278534220b2b37e9849e1a-770ca959.

A procura por este número, também chamada de mineração, tem duas funções principais: Primeiro, liga os blocos de uma forma matemática e criptográfica para que todos possam facilmente verificar a ordem correcta. Ao mesmo tempo, o mecanismo de Prova-de-Trabalho torna quase impossível a alteração desta ordem. Em segundo lugar, este mecanismo atrasa a adição de novos blocos para que, em média, um novo bloco seja adicionado à blockchain apenas a cada 10 minutos. Assim, todos os participantes da rede a nível global têm tempo suficiente para se actualizarem para o mesmo e mais recente estado da blockchain.

Em resumo, os mineiros mantêm a rede Bitcoin a funcionar. Graças a eles, novas transacções estão a ser processadas e acrescentadas à blockchain. Os nós completos (em inglês, „full nodes“) mantêm cópias do registo (“ledger”), certificam-se de que as regras são cumpridas, e asseguram que nenhuma transacção fraudulenta entre na blockchain.

21 milhões de Bitcoin

Embora sejam constantemente adicionados mais blocos à blockchain da Bitcoin e os mineiros sejam recompensados por este trabalho com novas Bitcoin, o número total de Bitcoin está limitado a 21 milhões. Nunca teremos mais de 21 milhões de Bitcoin. Mas estes 21 milhões de moedas não estiveram em circulação desde o início. Pelo contrário, estas são disponibilizadas através do código da Bitcoin, de acordo com um calendário de emissão rigoroso.

Quando a Bitcoin foi colocada em circulação, o código emitiu 50 novas Bitcoin aos mineiros, aproximadamente a cada 10 minutos. Quatro anos após o seu lançamento, o número das Bitcoin lançadas a cada dez minutos diminuiu para metade. Este processo chama-se „redução para metade“ (em inglês, „halving“) e descreve o facto de que a recompensa do bloco para os mineiros diminui para metade a cada 4 anos. Actualmente, já há 19 milhões de Bitcoin em circulação. A Bitcoin restante será minerada até ao ano de 2140. Depois disso, os mineiros só serão compensados através de taxas de transacção.

A quantidade estritamente limitada de unidades de Bitcoin é uma das propriedades fundamentais da criptomoeda e torna a Bitcoin um bem extremamente escasso. Esta escassez digital absoluta é também um pré-requisito importante para a função da Bitcoin como reserva de valor durante longos períodos de tempo e é a razão pela qual a Bitcoin é frequentemente chamada de ouro digital ou ouro 2.0.

O Resultado: Propriedade Digital

Examinando todas as características da rede Bitcoin em conjunto, é possível constatar a importância desta invenção. Pela primeira vez na história existe um activo digital que está disponível apenas num número estritamente limitado. As moedas Bitcoin não podem ser copiadas ou duplicadas.

Graças a esta proeza, a Bitcoin é frequentemente referida como propriedade digital. Porque assim como cada pedaço de terra neste planeta é único e existe apenas uma vez, cada unidade de Bitcoin também é única e existe apenas uma vez no espaço digital.

E estas unidades de Bitcoin podem tornar-se realmente propriedade. Somente a pessoa que possui a chave privada correspondente, uma combinação de números e letras composta por 64 caracteres, pode mover a Bitcoin associada. Por outras palavras, sem esta chave privada, a Bitcoin não pode ser roubada, confiscada, ou bloqueada. Isto permite que o proprietário tenha controlo absoluto sobre os seus recursos financeiros, independentemente de ser um milionário, um refugiado político ou um credor perseguido. Pela primeira vez desde a invenção do computador, é possível possuir verdadeiramente bens digitais.

PORQUÊ A BITCOIN?

Qual a razão de toda esta moda em torno da Bitcoin? A possibilidade de ter realmente um activo digital pode ser revolucionária. Mas porque iria alguém querer ter a Bitcoin em primeiro lugar?

O Melhor de Dois Mundos

Nos séculos passados foram utilizados metais preciosos e mais tarde dinheiro na forma de moedas e notas bancárias como meio de pagamento. Estes tinham a vantagem de poderem ser depositados e gastos independentemente de terceiros. O ditado „o dinheiro é a liberdade impressa" resume isso muito bem. Contudo, a desvantagem dos metais preciosos e do dinheiro é que eles são difíceis de utilizar no espaço digital da Internet. O mais tardar desde o início do comércio online, os cartões de débito e de crédito foram adoptados entre a população geral.

Mas agora que a maioria das pessoas está a utilizar dinheiro digital em contas bancárias em vez de dinheiro em numerário, os riscos de contraparte que enfrentam estão a aumentar. Se, por exemplo, uma instituição financeira declarar insolvência, as poupanças dos clientes podem desaparecer. Ou, como aconteceu no Chipre em 2013, se os levantamentos de numerário forem severamente limitados, se o controlo de capital for implementado, e se a expropriação forçada das contas de poupança acontecer, então as pessoas perdem o controlo do seu próprio dinheiro. Ou, como acontece actualmente em muitos países ocidentais, se os clientes bancários não estão autorizados a enviar dinheiro a familiares porque moram em Cuba ou no Irão, estes ficam dependentes de terceiros para aprovar todas as suas transacções.

Com a mudança do papel-moeda para o dinheiro digital acumulado em contas bancárias, acabamos por não ter controlo sobre o nosso próprio dinheiro. Até agora, porém, esta desvantagem tem sido o preço que tivemos de pagar para participar numa vida digitalizada.

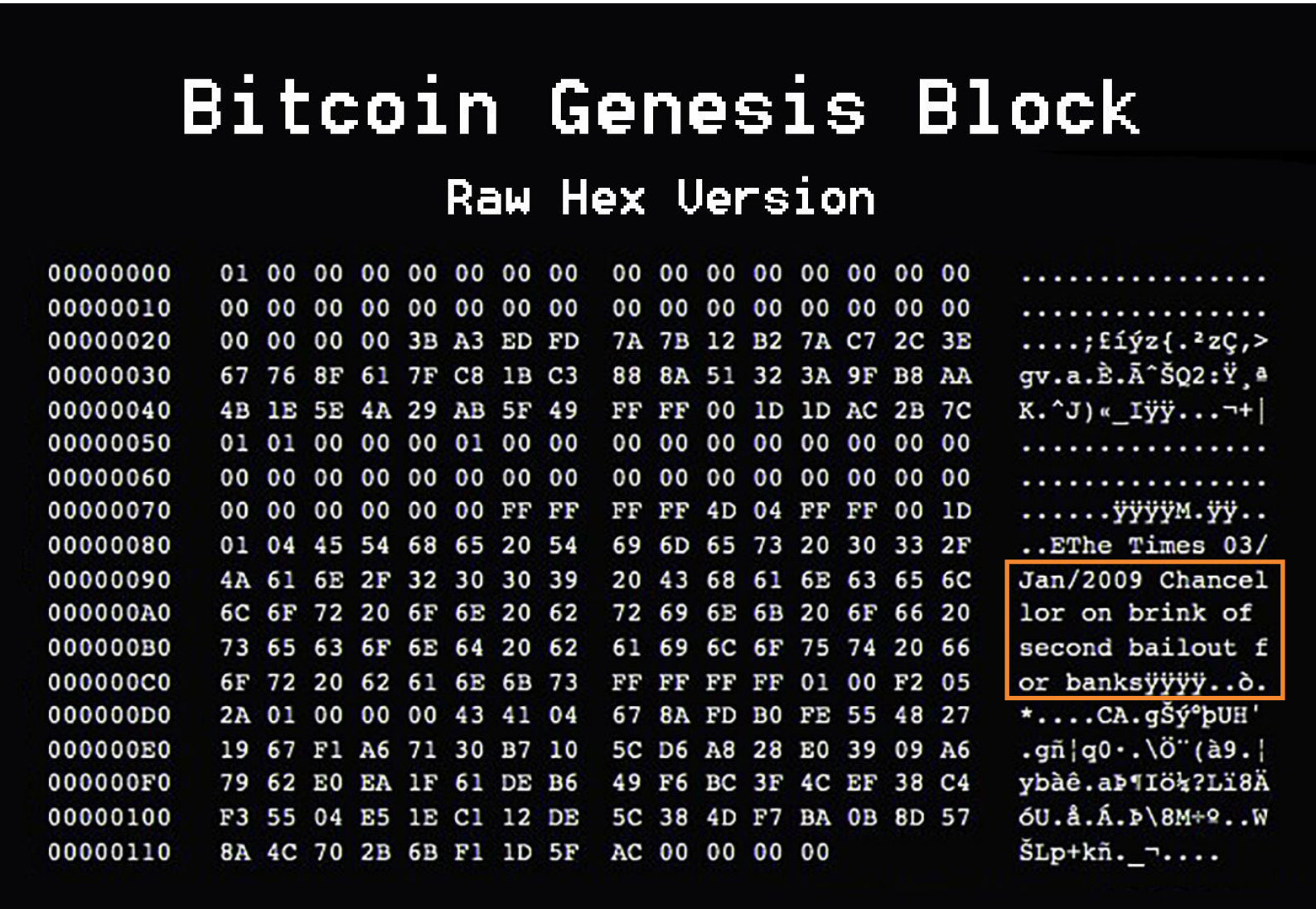
A Bitcoin oferece uma solução para

este dilema. Como dinheiro digital, é ideal para ser utilizado no espaço digital. Ao mesmo tempo, a Bitcoin pode ser armazenada como propriedade digital sem ter de depender de terceiros (os bancos) para a sua custódia. Assim, os proprietários da Bitcoin podem guardar as suas moedas - na forma de chaves privadas - debaixo do colchão ou onde acharem que é mais seguro.

O Timing Perfeito

A bitcoin foi criada no meio da crise financeira mundial de 2008/09. No primeiro bloco da blockchain da Bitcoin - também chamado de bloco Génesis - Satoshi Nakamoto transmitiu uma mensagem forte. Ele citou uma manchete publicada no jornal The Times que dizia: „Chanceler à beira do segundo resgate aos bancos“.

Com este acto, Satoshi manifestou a filosofia dos Cypherpunks que critica o Estado. Na crise financeira de 2008, os bancos centrais colocaram em circulação vastas quantidades de “dinheiro novo” para salvar os bancos. No entanto, no final, aqueles com poupanças acabaram por pagar com essa decisão, uma vez que as suas poupanças perderam valor através da diluição do valor do dinheiro. Este facto deu razão aos Cypherpunks na sua desconfiança em relação ao Estados e aos bancos centrais, e reforçou a sua convicção de que dinheiro independente do Estado era urgentemente necessário.



O mesmo procedimento tem sido repetido, só que em maior escala, desde o início da pandemia do Covid-19. Só em 2020, a massa monetária dos EUA expandiu-se em 50%, e em outros países - incluindo a Suíça - a impressora digital está constantemente a ser utilizada. Uma consequência directa disso são as baixas taxas de juro recorde - até mesmo as taxas de juro negativas na Suíça - e uma forte inflação de activos.

Protecção contra a Desvalorização da Moeda

A Bitcoin foi, portanto, lançada no melhor momento possível. Raramente a questão do dinheiro foi mais relevante e as dúvidas maiores do que hoje. Com a sua reserva limitada a 21 milhões, a Bitcoin proporciona um contraste agradável em relação aos balanços infinitamente crescentes dos bancos centrais. A sua escassa quantidade oferece protecção contra a diluição do próprio capital, como tem sido observado com todas as moedas em todo o mundo nas últimas décadas.

Devido à sua configuração específica, a Bitcoin foi concebida para assegurar a preservação do poder de compra durante longos períodos de tempo. Uma vez que a Bitcoin é escassa, deverá ser ainda melhor nesta função do que o ouro, que tem um influxo líquido de 1-2% todos os anos. Além disso, os custos de armazenamento e transporte da Bitcoin também são significativamente menores em comparação com o ouro, o que também permite uma melhor preservação do seu valor ao longo do tempo.

Protecção de Propriedade

Outra questão que a Bitcoin atenua é a protecção de propriedade. Enquanto que o ouro ou o dinheiro em numerário devem ser armazenados de forma segura e com alto custo para os proteger contra o roubo, a Bitcoin pode ser armazenada e transportada a um custo praticamente nulo. Até mesmo montantes substanciais podem ser levados para qualquer parte do mundo com um código composto por doze ou vinte e quatro palavras. Uma vez memorizado e fisicamente destruído, este código não pode ser roubado por ninguém, tornando as Bitcoin por detrás do código seguras e permitindo ao seu proprietário levá-las com ele para a sua sepultura, se assim o desejar.

COMPRAR BITCOIN

Há duas formas de obter Bitcoin. Ou se ganha Bitcoin através de mineração ou podemos comprar a Bitcoin de outra pessoa. Uma vez que a mineração com dispositivos domésticos se tornou praticamente impossível hoje em dia, a única maneira que resta para os recém-chegados é comprar Bitcoin.

Exchanges e Corretoras de Cripto

A forma mais fácil de comprar Bitcoin é através de uma exchange ou corretora de cripto. Estas funcionam de forma semelhante às plataformas de negociação de acções. Após abrir uma conta pessoal podem ser transferidos francos suíços, euros, ou dólares americanos através de transferência bancária ou de cartão de crédito. Assim que o dinheiro chegar à sua conta pessoal na exchange, a Bitcoin pode ser comprada 24 horas por dia, 7 dias por semana, com apenas alguns cliques, ao preço actual do mercado. Na Europa, é possível comprar a Bitcoin sem registo, sem verificação, ou sem a necessidade de em primeiro lugar depositar dinheiro, através da conhecida aplicação de investimento Relai, focada apenas em Bitcoin.

Peer-to-peer (Entre Pares)

Como alternativa às exchanges de cripto, a Bitcoin também pode ser comprada directamente de outros participantes no mercado, através de plataformas peer-to-peer (entre pares) e sem envolver uma exchange. Isto permite um maior anonimato, uma vez que nenhum dado pessoal necessita de ser revelado no processo.

Bitcoin ATMs

Existe também a possibilidade de levantar Bitcoin em caixas automáticas (ATMs). Estas já estão disponíveis em muitos países, incluindo a Suíça, a Alemanha e a Áustria. Nas ATMs de Bitcoin, esta pode ser levantada anonimamente com dinheiro ou com o cartão de crédito. Não é necessária

nem uma conta nem uma carteira de criptomoedas.

Armazenar a Bitcoin em Segurança

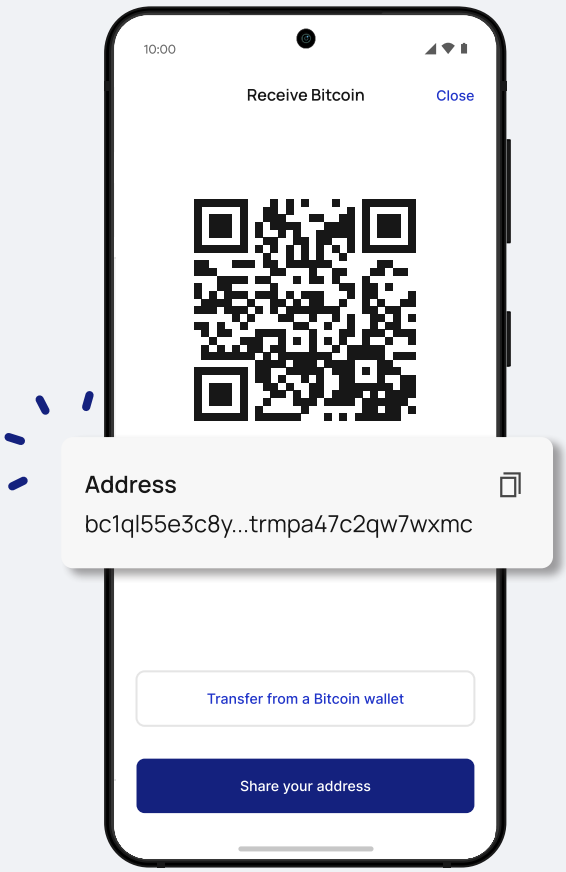
Uma vez adquiridas as Bitcoin, coloca-se a questão do seu manuseamento e armazenamento em segurança. A Bitcoin e as moedas criptográficas são regidas pelo princípio: „sem as suas chaves, não tem as suas moedas“. Para ser verdadeiramente proprietário da sua Bitcoin, deve estar na posse das chaves privadas correspondentes. Esta expressão um tanto técnica significa que só terá realmente o controlo das suas Bitcoin se as guardar numa carteira digital pessoal, para a qual tem as respectivas chaves privadas.

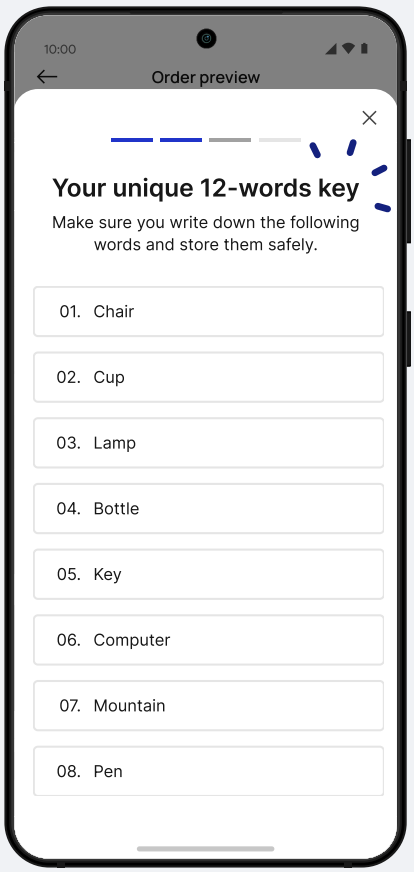
Enquanto as Bitcoin forem depositadas numa cripto exchange, estas estarão sob o controlo da mesma. Se a exchange for pirateada, falir, ou se cometer fraude, a Bitcoin pode perder-se para sempre.

Auto-Custódia

Ao contrário de uma conta bancária, a Bitcoin dá-lhe a opção de guardar as suas unidades monetárias numa carteira pessoal. Isto permite-lhe ser o seu próprio banco com a vantagem de ter o controlo absoluto sobre a sua Bitcoin. Por outro lado, isto também traz responsabilidades. A chave privada, que geralmente corresponde a doze ou vinte e quatro palavras, deve ser armazenada e guardada em segurança pelo proprietário da respectiva Bitcoin.

Carteiras: As Carteiras Digitais





As carteiras digitais ajudam a guardar a Bitcoin, ou mais precisamente, as chaves privadas em segurança. As próprias Bitcoin são sempre armazenadas na blockchain e não podem ser transferidas para uma carteira. Apenas as chaves de acesso à Bitcoin podem ser guardadas numa carteira.

Por isso, foram criadas carteiras para guardar chaves privadas com segurança e de uma forma simples. Aliás, estas permitem enviar e receber Bitcoin com apenas alguns cliques. Deste modo, as carteiras são uma ferramenta útil para manusear Bitcoin.

A Carteira de Software

As carteiras mais comuns são as carteiras de software. As carteiras de software podem ser configuradas como aplicações de desktop ou como aplicações de smartphone. Durante a configuração, as chaves privadas da carteira são listadas na forma de doze ou vinte e quatro palavras (isto é a frase semente, em inglês „seed phrase“). Estas palavras são sinónimos de Bitcoin nessa carteira. Quem quer que conheça estas palavras terá controlo sobre as respectivas moedas. Por isso, as palavras devem ser escritas de forma análoga, de preferência em papel, em segredo e guardadas em segurança. Se perder o computador ou o smartphone, ou se for roubado, a carteira pode ser restaurada em qualquer altura com estas palavras.

As carteiras de software têm a vantagem de poderem ser configuradas rapidamente e de serem fáceis de utilizar. No entanto, uma vez que as carteiras de software são programas de computador instalados num dispositivo e ligados directamente à internet, há sempre o risco de ataques por piratas informáticos.

A Carteira de Hardware

Se valoriza a segurança, deve, em vez disso, utilizar uma carteira de hardware. Estes pequenos dispositivos armazenam os códigos de acesso da Bitcoin num dispositivo do tipo pen drive USB que só está ligado ao computador quando necessário. O dispositivo é concebido de tal forma que mesmo um computador infectado com software malicioso não pode aceder aos códigos.

Ao criar uma carteira de hardware são geradas doze ou vinte e quatro palavras (a frase semente, ou em inglês “seed phrase”) que têm de ser anotadas de forma análoga e mantidas em segurança. Se a carteira de hardware for perdida, pode ser restaurada com a ajuda destas palavras. Exemplos de carteiras de hardware são a BitBox e o Trezor.

Made in Switzerland

EUROPE'S EASIEST BITCOIN APP

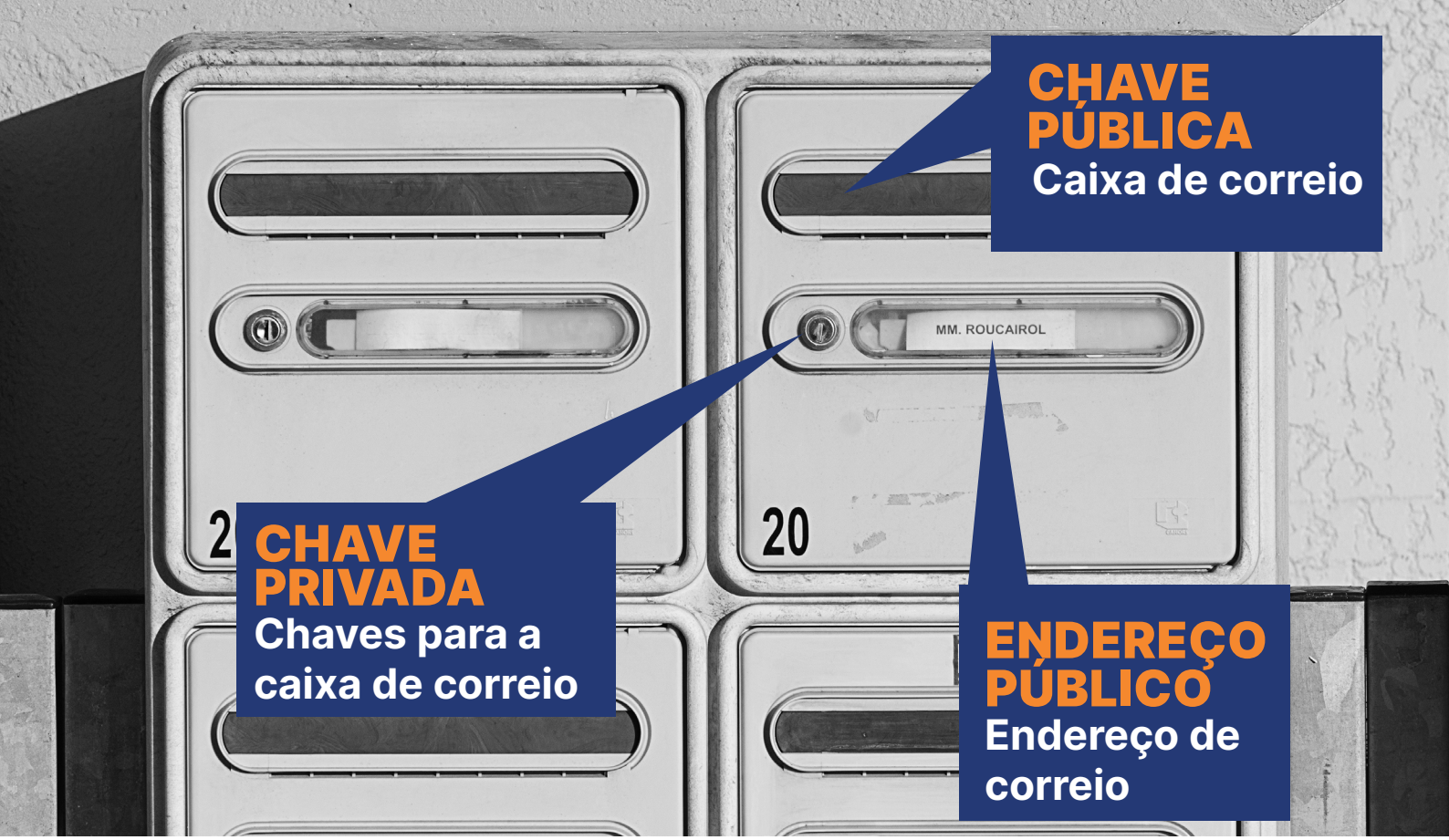
Received Bitcoin	BTC 0.00254340
24.09.2021	CHF 50.65

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.



Enviar e Receber Bitcoin

Enviar e receber Bitcoin é muito fácil. Cada carteira Bitcoin tem o seu endereço público gerado a partir da chamada chave pública. Este serve como um endereço de recepção semelhante a um IBAN. Qualquer pessoa que tenha este endereço pode enviar as Bitcoin para a carteira correspondente. O endereço é frequentemente apresentado através de um código QR, o que simplifica ainda mais o seu manuseamento.

Se quiser enviar Bitcoin a alguém, poderá introduzir o endereço Bitcoin do destinatário na sua carteira onde diz ‚enviar', ou em alternativa fazer o scan do código QR correspondente. As taxas de transacção relacionadas são automaticamente deduzidas da carteira do remetente. O montante das taxas de transacção varia em função da sobrecarga da rede e pode ser consultado aqui. A transferência das Bitcoin demora em média 10 minutos a chegar ao destinatário. No entanto pode também demorar mais tempo dependendo das taxas de transacção que está disposto a pagar.

Pagar com a Bitcoin

Quando a Bitcoin foi criada, esperava-se que pudesse ser utilizada para pagar os bens do dia-a-dia. E em teoria, isso é possível actualmente. Alguns departamentos tributários estatais, organizações sem fins lucrativos, e um número crescente de empresas aceitam a Bitcoin como meio de pagamento. Mas uma vez que as transacções através da rede Bitcoin podem custar vários euros e demorar pelo menos 10 minutos, isto só faz sentido para quantias maiores.

Para enviar a Bitcoin de forma rápida e barata, era necessária uma solução alternativa.

A Rede Lightning - Mais Rápida e Mais Barata

Por isso, foi desenvolvida uma rede adicional sobre a rede Bitcoin. Esta rede, chamada de Lightning (em português, relâmpago), permite pagar com Bitcoin em segundos a um custo mínimo. Em países como El Salvador, a rede Lightning já está em plena actividade e está a ser utilizada com sucesso.

O pagamento de bens de consumo diário com Bitcoin vai realizar-se em grande parte, no futuro, através da rede Lightning. Os desenvolvimentos nesta área estão a decorrer a toda a velocidade. O Twitter, por exemplo, introduziu recentemente a função ‚dar uma gorjeta' (em inglês, „tip") que utiliza a rede Lightning. Além disso, a aplicação Strike oferece pagamentos mundiais em várias moedas a custo zero, através da rede Lightning. É, portanto, de esperar que, no futuro, apenas montantes maiores sejam liquidados directamente através da rede Bitcoin, enquanto que todas as outras transacções serão efectuadas através da rede Lightning.

Uma vez que são enviadas principalmente pequenas quantidades através da rede Lightning, os „Satoshis," ou abreviando os „Sats," são utilizados como unidade de conta em vez de Bitcoin. Uma Bitcoin é igual a 100.000.000 de Satoshis. Para utilizar a rede Lightning, deve ser criada uma carteira Lightning.

UM OLHAR SOBRE O FUTURO

Nos seus mais de dez anos de existência, a Bitcoin tem passado por muitos altos e baixos. A moeda criptográfica foi declarada morta ou caiu no esquecimento do público em geral várias vezes, após grandes descidas de preços. Contudo, a Bitcoin espalhou-se inexoravelmente por todo o globo durante a última década.

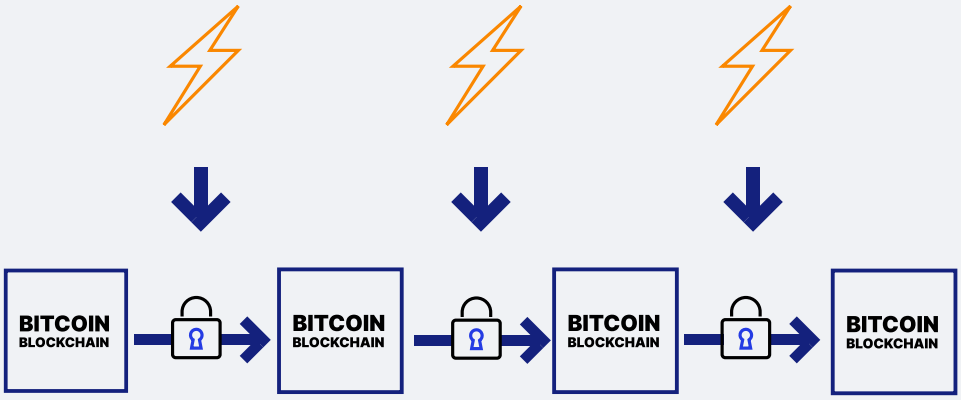
Bitcoin e Energia

Uma das primeiras questões que são frequentemente levantadas em relação ao desenvolvimento da Bitcoin é o consumo de energia da sua rede. A mineração de Bitcoin já consome uma quantidade significativa de electricidade em todo o mundo. E este consumo irá provavelmente aumentar no futuro à medida que mais pessoas participarem na mineração de Bitcoin.

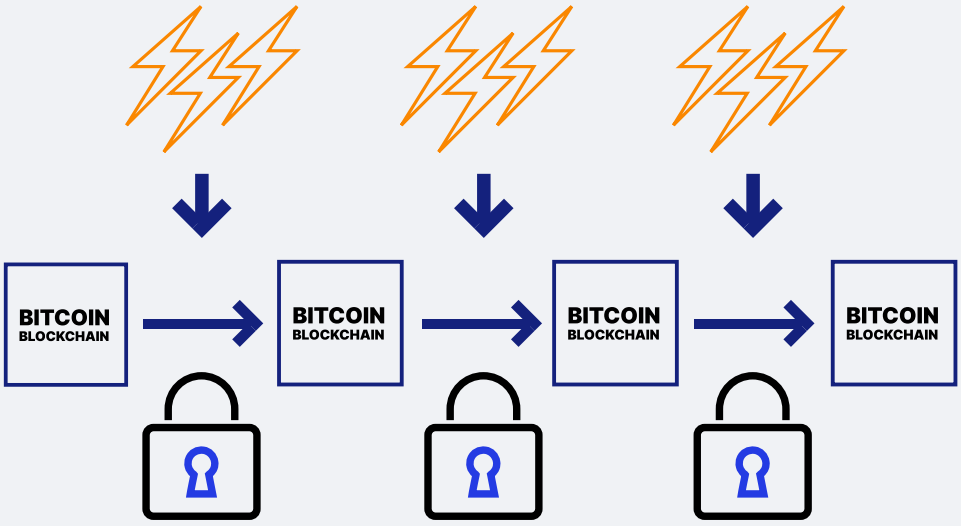
Quando se fala de Bitcoin e energia, é importante compreender que a quantidade de energia que flui para a rede Bitcoin é fundamental para a sua segurança. Quanto mais energia flui para a rede, mais segura ela é. Isto porque, para que a blockchain da Bitcoin seja alterada, a mesma quantidade de poder de computação - e portanto de energia - que foi investida para criar a blockchain em primeiro lugar, deve ser novamente despendida. No entanto, com milhões de computadores em todo o mundo a fornecer poder computacional à rede Bitcoin, é quase impossível para um indivíduo, uma organização ou um estado, alguma vez reunirem poder computacional suficiente para fazerem até as mais pequenas alterações na blockchain. Portanto, o poder de hash e o consumo de energia associado é uma importante característica de segurança da rede Bitcoin.

Além disso, os computadores de mineração da Bitcoin têm a vantagem de poderem ser instalados em qual-

Quanto menos energia sob a forma de poder de computação for utilizada para construir a blockchain da Bitcoin, mais fácil será alterá-la mais tarde.



Quanto mais energia sob a forma de poder de computação for utilizada para criar a blockchain da Bitcoin, mais difícil será alterá-la mais tarde



quer parte do mundo. Uma vez que os mineiros precisam da electricidade o mais barata possível para serem rentáveis, estes encontram-se frequentemente em locais onde há muitos excedentes, e portanto onde há energia barata. A longo prazo, é provável que isto aconteça em locais onde há muita energia renovável, uma vez que esta produz a electricidade mais barata.

De acordo com o Conselho de Mineração Bitcoin (Bitcoin Mining Council), os mineiros da Bitcoin actualmente utilizam cerca de 56% de energia renovável e esta tendência está a crescer. Muitos dos peritos em Bitcoin acreditam que a mineração de Bitcoin será movida por 100% de energias renováveis no futuro.

Até que seja esse o caso, porém, o consumo de energia da Bitcoin resume-se à questão de saber se um dinheiro seguro e impossível de falsificar, bem como a reserva de valor que representa, vale ou não este gasto de energia.

El Salvador - Bitcoin como Moeda Nacional

Há alguns anos atrás, alguns visionários já pensavam ser possível que a Bitcoin um dia fosse reconhecida como moeda legal pelos Estados-

nação. No Verão de 2021, esse momento chegou: El Salvador foi o primeiro país do mundo a introduzir a Bitcoin como moeda de curso legal. Em lojas, restaurantes e em prestadores de serviços de todos os tipos, o pagamento pode ser feito não só com dólares americanos, mas também com Bitcoin. Para este fim, foi disponibilizada aos cidadãos uma carteira de Bitcoin personalizada, que permite fazer pagamentos através da rede Lightning numa questão de segundos e com um custo mínimo.

Outros países como a Ucrânia, o Brasil, e o Panamá estão actualmente a discutir projectos de lei semelhantes. Caso outros países sigam o exemplo de El Salvador, isto, por um lado, aumentaria ainda mais a procura da Bitcoin e, ainda mais importante, reforçaria a credibilidade da Bitcoin como „dinheiro". A aceitação da Bitcoin como moeda legal em cada vez mais países representa, portanto, uma fase decisiva no processo de adopção global da Bitcoin.

Leis e Regulamentos

Estes desenvolvimentos levaram a que os estados-nação, bancos centrais e empresas tivessem de lidar intensivamente com criptomoedas. Vários Estados, incluindo a Suíça, adoptaram regulamentos e orientações para as criptomoedas. Este passo foi bem recebido por muitos participantes do mercado, uma vez que cria segurança jurídica tanto para os projectos cripto como para os investidores envolvidos.

Os regulamentos também estão no horizonte dos EUA, que até agora tem adoptado uma abordagem de laissez-faire. A forma exacta que estas novas leis de regulamentação nos EUA irão assumir está a ser acompanhada de perto pela comunidade cripto a nível global, uma vez que terão um grande impacto em todo o sector.

Outras Criptomoedas

Hoje em dia, a Bitcoin não é de longe a única criptomoeda. Existem actualmente mais de 16.000 criptomoedas e activos diferentes. Estas moedas e tokens têm características e funcionalidades diferentes e não foram todas concebidas como ‚moedas' ou dinheiro. Algumas são mais parecidas com acções, na medida em que o seu valor reflecte o sucesso de um projecto cripto. Outras são necessárias para a utilização de um determinado serviço. E outras ainda - as chamadas "meme tokens" - são principalmente moedas de diversão.

Para evitar prejuízos, é, portanto, aconselhável analisar mais de perto a respectiva moeda e o projecto por detrás da mesma, antes de fazer qualquer investimento.

Moedas Digitais do Banco Central (CBDCs)

As criptomoedas estão em transição de uma fase „Wild-West“ não regulamentada para um mundo de cripto finanças regulamentadas. Este desenvolvimento não deixou os bancos centrais incólumes e foi avançada a ideia de que os bancos centrais deveriam emitir as suas próprias criptomoedas. Estas „Moedas Digitais do Banco Central“, ou as CBDC (do inglês, „Central Bank Digital Currencies“), combinariam, dizem os proponentes, a estabilidade de uma moeda estatal com os benefícios de uma moeda assente numa blockchain. Em resumo, digamos que poderiam criar dinheiro digital.

No entanto, dependendo do seu design, uma CBDC pode assumir formatos fundamentalmente diferentes. Vários estados lançaram testes-piloto com diferentes tipos de CBDCs, e algumas CBDCs já foram introduzidas em alguns países. No entanto, espera-se ansiosamente saber de que forma e como é que áreas monetárias economicamente fortes como os EUA, a UE, ou a China lançarão os seus CBDCs.

Competição Monetária

A nossa sociedade habituou-se tanto às moedas estatais nas últimas décadas que outros tipos de dinheiro tornaram–se, até recentemente, difíceis de imaginar para muitos. Mas não há muito tempo, fazia parte da vida quotidiana ter diferentes tipos de dinheiro a circular em paralelo. Existiam notas de vários bancos, moedas feitas de diferentes metais, e outros valores monetários que podiam ser utilizados como meio de pagamento.

Com a Bitcoin, as moedas não-estatais estão agora novamente disponíveis como uma alternativa às moedas estatais. Até o momento, a maioria dos governos têm tolerado a Bitcoin. Em certa medida, isto pode ser graças à sua natureza descentralizada, o que torna a Bitcoin difícil de atacar. Para os cidadãos, isto significa que uma alternativa digital ao dinheiro do Estado está agora disponível a par do ouro e da prata. Os efeitos desta competição monetária adicional vão ser fascinantes de observar no futuro.

BITCOIN E AGORA?

Caso se pergunte o que deve fazer com toda esta informação, deixe-me fazer uma sugestão. Entrar no mundo da Bitcoin não custa nada, nem tempo, nem dinheiro. Mas irá conhecer uma tecnologia que está prestes a mudar o nosso mundo e o futuro.

Portanto, crie uma conta numa cripto exchange ou descarregue uma carteira no seu smartphone e compre Bitcoin por 50 Euros. Ou peça a um colega que lhe envie um pouco de Bitcoin para a sua carteira. Mas coloque as suas mãos na Bitcoin pelo menos uma vez.

Porque se a Bitcoin fizer a diferença e se tornar tão omnipresente como a internet, não só saberá mais sobre ela ao nível teórico, como também terá utilizado a Bitcoin por si próprio. Por vezes isto faz toda a diferença, pois dá-lhe um olhar e uma impressão clara sobre esta tecnologia, o que o coloca na vanguarda em relação à maioria das pessoas.

SOBRE O AUTOR

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

RELAI

Fundada na Suíça por Julian Liniger e Adem Bilican, depois de terem tido dificuldades para encontrar um espaço seguro e sem complicações para comprar bitcoin, a Relai está a tornar a poupança de Bitcoin e o seu investimento acessível a todos. A aplicação que foca apenas na Bitcoin foi concebida para ser simples e intuitiva, permitindo a qualquer pessoa na Europa comprar e vender Bitcoin em minutos, sem necessidade de registo, verificação, ou depósitos. Auditado de forma independente e com mais de 35 milhões de francos suíços em Bitcoin investidos através da sua plataforma, a Relai está a oferecer aos consumidores a oportunidade de descobrirem novos meios de poupança e de investimento.

Aprende mais em Relai.app.

Obrigado ao Salva que traduziu este e-book do inglês para português europeu. Agradeçemos também o feedback prestado pelo @SelmioC.