DOMINAR A BITCOIN — PARA — PRINCIPIANTES

A BITCOIN, AS TECNOLOGIAS DE CRIPTOMOEDAS,
A MINERAÇÃO, O INVESTIMENTO E A NEGOCIAÇÃO

ALAN T. NORMAN

Alan T. Norman

Dominar A Bitcoin Para Principiantes

«Tektime S.r.l.s.»

Norman A.

Dominar A Bitcoin Para Principiantes / A. Norman — «Tektime S.r.l.s.»,

A bitcoin não é apenas uma nova palavra da Era da Internet ou do progresso tecnológico e financeiro. É o começo de uma nova Era na Terra. Mesmo há dez anos atrás, nem imaginávamos sonhar com dinheiro digital. Não se pode tocar fisicamente, no entanto podemos deter ou gastar. Hoje isto é uma realidade.
A revolução da bitcoin cobriu o mundo inteiro com uma enorme onda. Cada vez mais existem pessoas interessadas neste ”Ouro Digital”. A bitcoin não é apenas uma nova palavra da Era da Internet ou do progresso tecnológico e financeiro. É o começo de uma nova Era na Terra. Mesmo há dez anos atrás, nem imaginávamos sonhar com dinheiro digital. Não se pode tocar fisicamente, no entanto podemos deter ou gastar. Hoje isto é uma realidade. A revolução da bitcoin cobriu o mundo inteiro com uma enorme onda. Cada vez mais existem pessoas interessadas neste ”Ouro Digital”. Nos últimos anos, a bitcoin passou de algo conhecido apenas por alguns ”nerds” de tecnologia a uma moeda revolucionária que mudou rapidamente a maneira como pensamos o conceito de dinheiro. É certo que agora vemos pagamentos em bitcoin aceites em todo o tipo de sítios, mas, pode acreditar, costumava ser um procedimento bastante complicado encontrar lugares que permitissem pagar em bitcoin. Enfim, para administrar o mundo, precisa de saber tudo. Não podemos garantir que saiba TUDO com este livro, mas podemos assegurar que terá a noção de uma nova moeda - a bitcoin. - O que é isto? - De onde veio? - Como se usa? - Será realmente dinheiro falso da Internet criado por traficantes de droga? É exatamente a isto que responderemos neste livro. Abordaremos tudo o que precisa de saber para começar a utilizar a bitcoin: - entender as transações de cadeia de blocos e bitcoin; - onde guardar a sua bitcoin (como escolher uma carteira segura); - como comprar bitcoin e como investir; - como começar a aceitar e usar esta moeda como uma parte dos seus ativos de negócio, de mineração, de segurança, entre outros. Além disso, o autor compartilhará factos interessantes sobre esta moeda e disponibilizará dicas profissionais sobre o início do seu caminho na família bitcoin! Sente-se pronto para

enfrentar este novo mundo? Acredito que sim. Gostaria de ser o primeiro a recebê-lo oficialmente no mundo da bitcoin!

Содержание

Capítulo 1. O que é a Bitcoin? 8
O Início 9
Trata-se então de uma moeda? 11
Sobre o custo 12
O que é uma criptomoeda? 13
Então, porquê a bitcoin? 14
Aprender sobre a bitcoin 15
Capítulo 2. Compreender a Cadeia de Blocos e as Transações de Bitcoin 16
A Cadeia de Blocos e a Bitcoin 17
Como funciona a transação de bitcoin? 18
A Cadeia de Blocos e as Transações 20
Capítulo 3. Começar a Usar Bitcoins 21
Segurança Pessoal na Bitcoin 22
Começar a Usar a Bitcoin 24
Capítulo 4. Onde Guardar as Bitcoins 25
O nosso endereço bitcoin 25
Endereços de Uso Único 26
Конец ознакомительного фрагмента. 27

Alan T. Norman
Dominar a Bitcoin Para Principiantes

dominar a bitcoin para PRINCIPIANTES

A Bitcoin, as Tecnologias de Criptomoedas,

a Mineração, o Investimento e a Negociação

Alan T. Norman

Tradutora: Luis Eduardo Junqueira Machado

Obtenha as suas baleias bitcoin: Livro grátis

“As Pessoas Que Enganaram o Mundo”

(Detalhes no final do livro)

Capítulo 1. O que é a Bitcoin?

Se abriu este livro, é provável que já tenha ouvido falar na bitcoin.

- É possível que tenha ouvido falar nos círculos financeiros uma vez que o valor desta moeda aumentou rapidamente.
- Possivelmente, deparou-se com este assunto num contexto tecnológico, pois a bitcoin é construída sobre uma nova tecnologia designada por cadeia de blocos.
- Ou então, leu algo sobre a bitcoin na comunicação social, devido à quantidade de novos utilizadores, famosas celebridades e empresários de sucesso que começaram a utilizar esta moeda há alguns anos.

Nos últimos anos, a bitcoin passou de algo conhecido apenas por alguns *nerds* das tecnologias a uma moeda revolucionária que mudou rapidamente a forma como pensamos o conceito de dinheiro.

Aqui está uma sinopse muito básica: A bitcoin é uma moeda digital. De muitas formas, funciona como o dólar, o euro ou o iene, permitindo a transferência de valor. No entanto, a força da bitcoin está na sua rede. A tecnologia de cadeia de blocos permite que esta moeda seja descentralizada, o que significa que qualquer pessoa pode aceder e negociar no registo público da bitcoin. A sua utilização permite enviar fundos para qualquer pessoa no mundo, sem a necessidade de recorrer a grandes instituições, como bancos, conversores de moedas ou processadores de pagamentos.

Tudo ocorre na rede pública da bitcoin.

Além dos pagamentos pessoa a pessoa, os pagamentos nesta moeda são agora aceites em todo o tipo de negócios. Há uns anos, encontrar sítios que permitissem efetuar pagamentos em bitcoin era um desafio. Para sermos sinceros, nos seus primeiros dias, poderíamos ter preenchido esta página com todos os sítios onde era aceite. Agora a sua aceitação disparou.

A bitcoin tem de momento outra utilidade: o investimento. À medida que as pessoas começaram a usar cada vez mais a bitcoin, o seu preço aumentou drasticamente. Como veremos mais adiante neste livro, muitas pessoas estão a comprar esta moeda como um ativo, à espera que valorize com o tempo.

Claro, a bitcoin ainda tem os seus problemas e desafios para o seu futuro. Iremos dar uma vista de olhos em alguns destes desafios nas próximas páginas.

Neste livro, abordaremos tudo o que precisa de saber para começar a utilizar a bitcoin. Começaremos pela sua origem.

Passemos ao que interessa!

O Início

Relembremos o que se passou há uns anos. Em 2008, a crise financeira estava em pleno andamento, e pessoas de todo o mundo sentiam os efeitos do desastre económico dos Estados Unidos.

Este foi um daqueles momentos da história em que os problemas das moedas nacionais revelaram a sua força. A crise financeira americana desvalorizou o dólar e os desafios económicos do país afetaram o mundo inteiro.

Em certos momentos, parecia provável dar-se um colapso económico completo. Onde estavam aqueles que deveriam ter garantido que nada disto pudesse ter acontecido? Dizer que foram incompetentes é uma forma ligeira de caracterizar o que aconteceu.

Respostas Centralizadas

Os grandes "conhecedores" da área decidiram que a resposta poderia apenas ser dada pelo banco central. Com o intuito de combater o colapso rápido dos mercados financeiros, os governos de todo o mundo decidiram adotar uma medida designada por "flexibilização quantitativa", em que imprimiam mais dinheiro para ser injetado nas suas economias, de forma a que os seus cidadãos tivessem fundos, evitando assim outra Grande Depressão.

Este género de mudanças rápidas gerou "guerras monetárias" e os governos, de imediato, começaram a competir para serem os que praticavam os preços mais baixos, de forma a permanecerem competitivos. Quando os bancos enfrentaram problemas face ao baixo valor da moeda e cortes nas taxas de juro, os governos foram forçados a resgatá-los com dinheiro dos contribuintes. Obviamente, isto apenas desvalorizou, ainda mais, a oferta de moeda existente.

Apesar de esta ser uma visão bastante simplificada de um momento histórico complexo, a lição permanece. A manipulação da oferta de moeda pelos bancos centrais desvalorizou moedas em todo o mundo.

No final, com as taxas de juro baixas e com os regates dos contribuintes, os próprios bancos inicialmente responsáveis pelo problema financeiro, foram aqueles que beneficiaram com a economia quase em colapso. Foi nesta época que se inspirou um senhor conhecido por Satoshi Nakamoto.

Quem é Satoshi?

Antes de explicar precisamente como surgiu a bitcoin, vale a pena entender quem é Satoshi Nakamoto. A sua história e a história da sua moeda são misteriosas.

A verdadeira identidade de Satoshi permanece desconhecida até hoje. De acordo com declarações suas de 2012, tinha 37 anos e morava algures no Japão. No entanto existem muitas dúvidas sobre estes dados. Escreve em inglês fluente e o *software* bitcoin não está documentado em japonês, levando muitos a pensar que não seja, de facto, nipónico, embora possa lá ter morado naquela época.

Com um pouco de trabalho de detetive, um codificador suíço descobriu que Satoshi poderia estar a residir na América do Norte, tendo em consideração as alturas do dia em que fazia publicações nos fóruns da bitcoin. O codificador analisou os momentos das publicações mais comuns e constatou que estavam alinhadas com o horário médio de sono de alguém que residia no continente.

Saberemos algum dia quem é o criador desta moeda? Será um grupo de pessoas? Talvez nunca se descubra, mas uma coisa é garantida, esta pessoa, ou equipa, controla aproximadamente um milhão de bitcoins. Em junho de 2017 este valor equivalia a quase 3 biliões de dólares americanos. Com uma fortuna destas, poderiam comprar o direito à privacidade.

A Criação

Este codificador anónimo analisou o estado do mundo financeiro e detetou bastantes problemas. As formas tradicionais para a resolução da crise tinham sido tentadas e, embora tivessem funcionado, reparou que, até àquele momento, pouco tinha sido feito para prevenir futuros desastres. O que poderia ser feito? Algum tipo de solução centralizada resolveria de vez problemas como este?

Decidiu que era necessária uma força disruptiva. Algo que pudesse modificar a forma de como a moeda é pensada. A resposta foi criar um tipo de moeda completamente descentralizada e aberta a todos, sem ter bancos centrais a controlar, nem uma cadeia de transferências com um supervisor. Nenhuma elite tomaria decisões que pudessem afetar os utilizadores da sua moeda.

Descentralização

B

> Descentralização: movimentação de departamentos de uma grande organização com um único centro administrativo, para outros locais.

Esta descentralização foi a força motriz que impulsionou o trabalho de Satoshi. Basicamente, a descentralização significa que todos fazem parte da economia bitcoin e que todos estamos a contribuir de algum modo. NÓS somos a força motriz, e não um banco central que controla o valor da nossa moeda e quanto desta temos disponível na nossa economia. Ainda melhor, ao mesmo tempo, ninguém tem o seu controlo.

Nenhum governo, banco ou intermediário pode dizer como deve ser usada a bitcoin, uma vez que esta pertence, literalmente, a todos aqueles que a utilizam. Neste sentido, quanto mais for utilizada, melhor funciona e mais viável se torna. É desta forma que funciona a tecnologia ponto-a-ponto, sendo direcionada pelos seus utilizadores.

No verdadeiro sentido da palavra, é um mercado livre. Ouvimos falar bastante sobre mercados livres ao longo dos anos, mas nenhum mercado pode ser verdadeiramente livre quando há uma força motriz que toma decisões a seu respeito.

Como fez Satoshi

Satoshi está longe de ser a primeira pessoa a trabalhar no problema da moeda digital descentralizada. Antes de 2008, criptógrafos e codificadores já tinham trabalhado sobre esse problema, durante anos.

O desafio da descentralização é manter um registo de transações. Normalmente, quando pagamos a alguém, o banco subtrai o dinheiro da nossa conta e adiciona-o à conta do destinatário. Manter as transações registadas é a função principal de um banco.

No entanto, num sistema descentralizado, não existe um banco. Qualquer pessoa pode enviar uma solicitação de transação para a rede descentralizada. Isto torna o registo descentralizado bastante vulnerável a ataques. O registo pode ser alterado por malfeitores ou poderão gastar a moeda digital, múltiplas vezes, antes que seja constatado pela rede.

A inovação de Satoshi foi a tecnologia a que designamos por cadeia de blocos. Encontrou uma forma de manter o registo em segurança utilizando selos temporais, bastante poder de processamento descentralizado e criptografia. A bitcoin – a primeira cadeia de blocos – utiliza atualmente a arquitetura de Satoshi para garantir pagamentos.

Trata-se então de uma moeda?

Uma das dúvidas mais frequentes que as pessoas têm sobre a bitcoin é se esta realmente se trata de uma moeda.

Não há uma resposta concreta. A bitcoin é um método de pagamento e uma forma de transferência de fundos. Pode usar a bitcoin para fazer compras ou enviar pagamentos. É possível converter bitcoins em dólares, euros, libras, ienes ou em qualquer outra moeda. No entanto, não é apoiada por nenhuma instituição. Não existe um governo central que possa servir de referência e não há garantias quando se trata de possuir bitcoins. É apenas valioso devido à quantidade e ao tipo de sítios e pessoas que o aceitam.

A bitcoin é o que chamamos de moeda digital na sua forma mais pura, ou aquilo que é conhecido como criptomoeda. Esta foi a primeira criptomoeda, no entanto, atualmente, existem muitas outras. As criptomoedas operam de modo diferente das moedas tradicionais, pois são baseadas em código e não nas decisões de um banco central. Esta diferença torna-as atraentes, mas também mais voláteis.

Sobre o custo

Uma das maiores características de uma verdadeira moeda é a estabilidade do valor. Muitas pessoas argumentam que a bitcoin não é uma moeda, devido à volatilidade do seu valor. O preço da bitcoin tem flutuado bastante e, em algumas ocasiões, duplicou o seu valor, num curto espaço de tempo.

Por exemplo, em julho de 2010, o preço era de 0,08 dólares por bitcoin. Em dezembro de 2017 a bitcoin atingiu os 20.000 dólares. Em média, varia à volta de 2% ao dia. Trata-se de algo que não acontece com as moedas tradicionais, levando muitos a afirmar que, como moeda, é inútil. Um preço estável é o que convencerá o investimento tradicional e levará a um crescimento sustentado.

Isto importa para a bitcoin? Depende do ponto de vista. A volatilidade do preço pode ter, a curto prazo, um enorme impacto na confiança das pessoas. Pode, definitivamente, ser um problema tentar atrair alguém para o mundo das criptomoedas, quando o preço se encontra numa rápida mudança.

O segredo é olhar para o panorama de um modo global. Se estivermos interessados em fazer parte de uma mudança económica verdadeiramente revolucionária, o plano a longo prazo é o mais importante.

Neste sentido, várias pesquisas já demonstraram que a bitcoin deverá estabilizar futuramente e flutuará muito menos. Os típicos altos e baixos podem ser largamente atribuídos à quantidade de publicidade que a bitcoin recebe num determinado momento.

Existe uma grande probabilidade de os governos começarem a regular as criptomoedas nos próximos anos. Enquanto a regulamentação não for capaz de controlar moedas descentralizadas, existirá um forte efeito moderador sobre a sua quantidade e sobre a rápida variação de valorização.

O que é uma criptomoeda?

B

> "Criptomoeda: moeda digital na qual são utilizadas técnicas de encriptação para regular uma geração de unidades de moeda e verificar a transferência de fundos, que operam fora do controlo de um banco central."

A definição de criptomoeda requer muita informação técnica que abordaremos detalhadamente mais adiante neste livro, no entanto vale a pena introduzir neste ponto, para possa ser mais bem entendida.

De forma simplificada, podemos dizer que as criptomoedas são linhas de código que têm valor monetário. Utilizando a criptografia, a rede descentralizada, cria novas moedas e protege transações. Alguns membros da rede descentralizada configuram computadores que processam o código. Em troca, esses nós de processador – conhecidos como mineiros – recebem uma recompensa por protegerem as transações na cadeia de blocos.

Então, porquê a bitcoin?

A bitcoin está longe de ser a única criptomoeda. No entanto, manteve sempre o seu domínio como a criptomoeda número um do mundo, ao longo dos últimos dez anos.

Existe um forte argumento, pouco justificado, que diz que a bitcoin não é a melhor criptomoeda do mundo. Surgiram novos projetos com escalabilidade, velocidade e privacidade de transação superiores. No entanto, estas novas moedas não foram capazes de destronar a bitcoin.

Parte da razão pela qual a bitcoin mantem a liderança é a sua vantagem inicial. A bitcoin foi a primeira cadeia de blocos, de sempre. De 2008 a 2013, todo o interesse que esta cadeia despertou inicialmente focou-se na bitcoin. Isto significa que a teve a maior base de utilizadores e uma seleção de ótimos programadores, para construir o sistema.

Este processo é um círculo virtuoso para a bitcoin. Por ter a maior rede, é também a que tem mais aceitação. O efeito de rede significa que quanto mais pessoas utilizarem uma determinada tecnologia, mais útil esta se torna.

Vejamos o exemplo do email. Não teria qualquer utilidade se um de nós fosse a única pessoa no mundo com um endereço eletrónico. Teria um pouco mais de utilidade se mais pessoas tivessem. Seria extremamente útil, se quase todos tivessem. A adoção da bitcoin baseia-se no mesmo princípio, pois torna-se mais útil à medida que a sua aceitação for maior.

Até ao momento, é a mais famosa das criptomoedas de hoje, em grande parte porque continua a ser a maior. A sua longa história confere-lhe alguma legitimidade.

Ao longo de uma década, enfrentou e superou muitos obstáculos e desafios técnicos, continuando sempre a crescer. O seu registo de segurança comprovado torna a compra de criptomoeda a mais segura para principiantes.

Enquanto que outras criptomoedas poderão focar-se em funcionalidades específicas, a bitcoin é uma moeda digital versátil disponível em quase todos os câmbios de *altcoin*. Neste ponto, é a moeda que tem investimentos por trás, tem a base de utilizadores, tem a segurança e o tem histórico.

Aprender sobre a bitcoin

Isto tudo é apenas o início. Ao longo deste livro, serão abordados todos os aspetos da bitcoin e serão dados conselhos reais sobre como iniciar.

Há muito a aprender. É fácil ficar atolado na minúcia da bitcoin e na forma como funciona a sua tecnologia, mas para se iniciar é necessário compreender os fundamentos. É, precisamente, o que será apresentado nas próximas páginas.

Capítulo 2. Compreender a Cadeia de Blocos e as Transações de Bitcoin

Antes de abordarmos as noções básicas da compra e armazenamento da sua primeira bitcoin, vamos examinar os fundamentos da tecnologia que faz a bitcoin funcionar – a cadeia de blocos. Recentemente, a "Cadeia de Blocos" ganhou o status de chavão para as novas *startups*. Muitas pessoas que usam o termo não têm uma ideia clara da forma como esta protege uma rede descentralizada. No final deste capítulo, entenderá o básico da cadeia de blocos, possivelmente melhor do que muitos entusiastas de criptomoedas.

A Cadeia de Blocos e a Bitcoin

Em 2008 Satoshi Nakamoto publicou pela primeira vez um *whitepaper* sobre a tecnologia bitcoin onde descreveu o sistema ponto-a-ponto que executa transações de bitcoin. Esta criptomoeda, por si, é uma ideia revolucionária, contudo, a tecnologia que a sustenta é a verdadeira inovação. A cadeia de blocos de Satoshi possibilita a criação de um registo descentralizado seguro para tudo o que for necessário, não apenas para a criptomoeda.

A cadeia de blocos da bitcoin é o registo público que contem a totalidade das transações efetuadas na história desta moeda. Como não existe um corpo governativo central ou base de dados, o registo assenta na rede composta por todos os computadores que executam o *software* bitcoin. Todos trabalham em conjunto para construir a rede.

Tudo acontece em público e encontra-se acessível a visualização do tráfego, em andamento. Este nível de transparência é quase inédito em qualquer outro sistema financeiro e é o que torna as criptomoedas algo único.

De forma geral, a cadeia de blocos pode afetar qualquer parte das nossas vidas onde seja necessário verificar a identidade, estabelecer uma transação ou garantir um contrato. O registo público na cadeia de blocos pode ser mais rápido, menos dispendioso e mais seguro do que muitas instituições em que, atualmente, confiamos.

Como funciona a transação de bitcoin?

As bitcoins não existem fisicamente e não existe sequer um cofre de bitcoins. Se pensarmos bem, não é muito diferente do dinheiro tradicional. Podemos visualizar dinheiro ao iniciarmos a sessão na nossa conta bancária, mas isso não significa que existe uma caixa onde os nossos fundos estão guardados. Da mesma forma, nunca poderemos afirmar: "Isto é uma bitcoin".

Em vez disso, ao iniciarmos uma transação, estamos a enviar uma solicitação de transação para toda a rede. Na rede, os mineradores adicioná-la-ão ao registo público, juntamente com outras solicitações de transação correntes. Este registo é selado com o tempo, ligado ao último registo produzido e bloqueado com uma chave criptográfica. Um registo selado, ligado e bloqueado é designado por bloco.

Bloco

Os blocos de transações contêm tudo o que necessitam para adicionar novas transações e ligar, também, o bloco a todas as anteriores. Existem quatro pormenores incluídos em cada bloco: uma referência ao bloco anterior da cadeia, as transações que estão a ser adicionadas, um selo temporal e a prova criptográfica que demonstra como o bloco foi criado.

Esta combinação de selagem, interligação e bloqueio de blocos foi a inovação de Satoshi na criação da bitcoin. Resolve o problema de criação de um registo, que qualquer utilizador pode adicionar:

- O selo temporal mostra onde o bloco pertence, ordenadamente, garantindo que não se misturem, sendo que, ao mesmo tempo, múltiplos blocos não são respeitados pela rede.
- A ligação é uma referência ao bloco anterior, incorporado no conteúdo do bloco corrente. Assim, é garantido o lugar deste numa longa cadeia. A cadeia de blocos!
- O bloqueio criptográfico no bloco é conhecido por *hash*. Os mineiros da rede usam o seu poder computacional para calcularem o *hash*. Para a bitcoin, é um quebra-cabeças extremamente difícil que leva aos processadores mais rápidos do mundo uma média de dez minutos para serem resolvidos.

Ao recolher todas estas informações num único bloco, o sistema de cadeia é capaz de se autorregular não requerendo vigilância nem supervisão. É desnecessário alguém verificar manualmente as transações. Após o cálculo do *hash*, é praticamente impossível alterar o conteúdo de um bloco.

Alterar o conteúdo exigiria a edição do registo, a reconstrução do bloco e a resolução do quebra-cabeças criptográfico, novamente. Será desejável possuirmos um computador que seja mais rápido do que todos os outros da rede, uma vez que desejaremos vencer a corrida para concluir o quebra-cabeças, isto se pretendermos que o nosso bloco seja implementado. Isto é altamente improvável, dado o enorme poder de computação na rede bitcoin.

Os blocos são organizados numa cadeia, pelo que se pretendermos alterar uma transação antiga, será necessário editar esse bloco e resolver o novo quebra-cabeças. No entanto, a resposta para o antigo quebra-cabeça original está incorporada no seguinte bloco da cadeia. Este deverá ser atualizado, desta vez com a nova resposta do quebra-cabeças. Sempre que se editar um bloco é necessário resolver novamente o quebra-cabeça de todos os blocos que se seguiram. Quanto mais quebra-cabeças de blocos for necessário resolver, menor a probabilidade de implementar se um

ataque com sucesso. As transações de Bitcoin que existam há mais de uma hora, estatisticamente, são quase impossíveis de modificar.

Depois que uma transação ser adicionada à cadeia, existirá para sempre e é registada em todos os computadores da rede. Neste sentido, a cadeia de blocos é uma das bases de dados mais seguras que se possa imaginar.

Confirmações

As transações bem-sucedidas devem ser confirmadas de forma a garantir que estão corretas. Os mineradores, que criam o bloco adicionando-o à cadeia, a cada dez minutos, confirmam. Estes verificam as transações, gravam no registo público e adicionam ao bloco seguinte. Uma vez resolvido o bloco, a transação é considerada verificada e as alterações tornam-se improváveis.

Conforme descrito acima, torna-se cada vez mais difícil alterar uma transação, quanto mais tempo o bloco estiver na cadeia. Por esse motivo, algumas pessoas preferem esperar por vários blocos, antes de optarem pela transação "confirmada".

Quando utilizarmos a bitcoin numa loja, talvez alguns comerciantes não nos façam esperar. No entanto, isso significa que estão a arriscar deixar passar o pagamento. Geralmente é mais comum em transações de baixo valor, pois existe um risco menor de fraude.

Taxas

Como em todos os sistemas transacionais, a bitcoin tem taxas para cada transferência. No entanto há aqui uma distinção importante, as taxas não são necessárias e podem ser determinadas por quem envia os fundos.

Em troca de confirmações mais rápidas, os mineiros coletam e processam as taxas. Pague o suficiente e o mineiro moverá a sua transação para o topo da pilha, para ser adicionada ao bloco seguinte. Depois de terem criado com sucesso um novo bloco bitcoin, cobrarão as taxas de todas as transações incluídas nesse bloco específico.

As taxas são inteiramente voluntárias e quem inicia a transação pode decidir se deseja ou não incluir uma taxa. No entanto, ao incluir uma taxa, podemos garantir que os mineiros têm um incentivo para processar a transação. Se optarmos por não incluir uma taxa, estes processarão outras transações à frente. Poderemos esperar horas, ou mesmo dias, antes de a transação gratuita ser incluída num bloco.

Algumas carteiras, que gerem e guardam as bitcoins, decidem por nós a taxa de transação. Falaremos mais sobre carteiras, mais adiante.

A Cadeia de Blocos e as Transações

A cadeia de blocos já não parece tão misteriosa? Isto é apenas o início desta incrível invenção. Escrevi um livro sobre a tecnologia da cadeia de blocos (http://mybook.to/BlockchainExplained). Se tiver interesse, este recurso aprofunda o âmago da questão.

Mais à frente será aprofundado o tema de mineração, mas, por enquanto serão facultadas outras informações úteis sobre como obter e gastar bitcoins.

Capítulo 3. Começar a Usar Bitcoins

Com uma criptomoeda como a bitcoin, o mais importante é obter informações corretas e entender o sistema antes de iniciar. Esta moeda não tem uma autoridade central, portanto, as transações não podem ser revertidas. Se cometermos algum erro com a bitcoin, será permanente. Dito isto, devemos agir com cautela, investir apenas um pouco de cada vez e fazer a nossa pesquisa.

Este livro é uma boa introdução, mas, possivelmente, não abrange tudo aquilo que se pode encontrar no mundo da bitcoin. O melhor conselho que se pode dar é ler o máximo possível.

A bitcoin pode parecer assustadora ou complicada. O objetivo deste capítulo é familiarizar-se com conceitos básicos e regras fundamentais para começar a usar a bitcoin. É de salientar que, mais adiante, haverá explicações aprofundadas sobre estes assuntos, sendo que devem ser encarados pacientemente.

Segurança Pessoal na Bitcoin

Antes de se dar algum conselho sobre como comprar, deter, vender e transacionar bitcoins, é necessário falar sobre segurança. A própria rede revela um alto nível de segurança. A bitcoin nunca sofreu um ataque, diretamente, e é muito improvável que alguém possa vir a alterar uma transação no registo público da bitcoin.

O risco de segurança de possuir bitcoins surge da falta de cuidado pessoal ou por lidar com provedores de serviços de terceiros. Apresentam-se algumas dicas:

Nunca partilhe a chave privada

Esta é, obviamente, a primeira regra de segurança da bitcoin. Nenhuma empresa ou pessoa legítima jamais solicitará a chave privada da Bitcoin (a menos que se esteja a autorizar um gasto). Os endereços bitcoin não estão associados à nossa identidade. Não é necessário facultar a nossa identificação ao criar a maioria das carteiras e o único aspeto que distingue o proprietário de uma carteira é conhecer a chave privada.

Como tal, alguém que possua a nossa chave privada pode gastar as nossas bitcoins. É ponto assente! Para além disso, não existe um modo de reverter transações ou denunciar fraudes na bitcoin. É fundamental, nunca partilhar a chave privada.

Não perca a sua chave privada

O efeito secundário de endereços anónimos é que não existe uma forma de recuperar a chave privada se a perdermos. A única solução para aceder ao endereço é através da chave. Perdê-la, implica perder os fundos, para sempre.

A maioria das carteiras, através de uma *password* recuperável, encarrega-se de armazenar as principais informações. De qualquer modo, é importante fazer uma cópia de segurança de toda a informação da chave privada, em vários locais.

Tenha uma Carteira Segura

Como se pode depreender, uma carteira é aquilo que detém a bitcoin que recebemos. Existem várias opções diferentes que discutiremos, nomeadamente: baseadas na Internet, baseadas em *hardware*, dispositivos móveis, entre outras. Muitos mantêm as suas bitcoins do dia-a-dia numa carteira normal da Internet, sendo que o restante, guardam numa carteira mais segura, disponível para fazer uma cópia de segurança. Desta forma, mesmo que o nosso computador seja alvo de um ataque, não poderão tocar nas nossas economias. Falaremos sobre os diferentes tipos de carteiras, mais adiante.

Saiba que o preço irá mudar

O preço da bitcoin muda a cada minuto. É importante perceber isto, pois, por vezes, pode ser um caminho acidentado. Tem subido constantemente, no entanto também teve a sua cota-parte em quedas de valor. Há uns anos, seria quase inimaginável que uma bitcoin valesse 100 dólares. Neste preciso momento, vale mais de 11.000 dólares. Mesmo que seja esperado, a sua subida com o passar do tempo, haverá momentos em que o preço baixa. Devemos ter presente que isto faz parte do percurso.

Não Pode Reverter Pagamentos

Os pagamentos em bitcoins não se efetuam do mesmo modo que os cartões de crédito ou o Paypal. A pessoa a quem for enviado o dinheiro é a única que poderá devolver. Neste sentido, é fundamental confiar na pessoa a quem o fundo está a ser enviado e conferir, mais do que uma vez, o endereço da carteira.

No caso de enviarmos bitcoins para o endereço errado, é provável que não se recupere essa quantia. Devem ser verificados, duas ou três vezes, todos os detalhes da transação antes de se enviar qualquer fundo, pelo que, se algo de errado ocorrer, não existirá uma "sede da empresa" que possa auxiliar. Isto revela bons e maus efeitos no uso da bitcoin, em comparação com outros métodos de pagamento, mas falaremos sobre estes pontos de vista, um pouco mais adiante.

As Bitcoins são Rastreáveis

Uma vez que a bitcoin opera num registo público, qualquer pessoa pode ver o histórico de transações na rede. As transações são apenas uma lista de endereços públicos e valores de transação. Ainda assim, investigadores astutos poderão criar uma rede de transações e identificar tendências. Com o tempo, um investigador dedicado pode descobrir qual é o nosso endereço, bem como todos os endereços para os quais efetuámos pagamentos em bitcoins.

Existem formas de evitar ser rastreado na bitcoin. É possível utilizar vários endereços ou até um novo endereço por cada transação. Podem ainda ser utilizados serviços de mistura de moedas que mascaram a fonte dos fundos, misturando-os com outros fundos. É, deste modo, de salientar que o registo público é, na realidade, público.

Poderá Haver "Dores de Crescimento"

A bitcoin está a crescer rapidamente, pelo que poderá haver muitas mudanças no futuro. As novas atualizações podem fazer com que alguns operadores repensem os seus serviços e preços, as confirmações podem abrandar, as taxas podem subir ou quaisquer outras situações podem ocorrer. É impossível afirmar de que forma ocorrerá, mas se entendermos os fundamentos que sustentam, ficaremos precavidos.

Começar a Usar a Bitcoin

Em relação à bitcoin, estamos apenas no início. Há muito a aprender e interessa estarmos orientados de forma a garantirmos que nos sentimos seguros e informados, o suficiente, para entrarmos nesta moeda digital de rápido crescimento, que, simplesmente, irá continuar a crescer.

Capítulo 4. Onde Guardar as Bitcoins

O nosso endereço bitcoin

Já todos enviámos um email a alguém, correto? Esse endereço específico permite que se envie e receba mensagens para alguém ou de alguém na Internet, desde que possua também um endereço eletrónico. Os endereços bitcoin funcionam da mesma forma, embora haja uma diferença fundamental.

O que é um endereço bitcoin?

Um endereço bitcoin é a sequência específica de caracteres que identifica a sua carteira. Ao contrário do exemplo do endereço eletrónico, uma única carteira, pode ter vários endereços, inclusive, um novo para cada nova transação feita.

No caso da bitcoin, o endereço tem, de comprimento, entre 26 e 35 caracteres alfanuméricos. Cada endereço começa pelo algarismo 1 ou 3 e é sensível a maiúsculas e minúsculas. Esta sequência de caracteres deverá ser exata ou os fundos não poderão ser transferidos. Isto não surpreenderá quem, anteriormente, já tenha realizado transferências.

Quando desejarmos receber um determinado fundo, o endereço bitcoin deverá ser partilhado com quem pretende efetuar o pagamento. Pode inclusivamente publicá-lo. Partilhar o nosso endereço não dá acesso à nossa conta. Apenas informa a rede sobre para onde o fundo deverá ser direcionado.

B

> “Aqui está um exemplo de endereço bitcoin:
> 1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2”

Endereços de Uso Único

Enquanto que o endereço eletrónico nunca se altera, neste caso, a maioria dos especialistas recomenda a utilização de um novo endereço bitcoin, para cada transação. Deste modo, uma vez que o endereço não corresponde à carteira, não está a ser criada uma nova, mas está, simplesmente, a ser utilizado um novo identificador para quem está a enviar bitcoins. Existem vários motivos para que se proceda deste modo.

Anonimato

Existe um grande problema com a reutilização de um endereço bitcoin, corre-se o risco de se perder o anonimato, caraterístico desta moeda.

À medida que um determinado endereço vai sendo usado, está a ser publicada informação sobre a origem e destino da bitcoin. Como opera num registo público, assim que surgir, o endereço pode ser visualizado por todos. Com a utilização do mesmo endereço repetidamente, malfeitores poderão rastrear relações, transações, fundos de rendimento. Quanto mais um endereço é usado, mais informações são disponibilizadas.

B

> "Existem poucas probabilidades de acontecer, no entanto, deve tornar-se numa preocupação, se quisermos garantir o anonimato."

Neste sentido, é de salientar que a criação de novos endereços, para cada transação, ajuda a preservar a identidade, bem como manter as transações mais anónimas. Mesmo sendo, as transações, registadas em público, este é um modo eficaz de manter um escudo de anonimato.

Criar um endereço é tão simples quanto clicar no botão do seu cliente de carteira. Falaremos de carteiras mais adiante.

Identificar Pagamentos

No caso de uma empresa que pretende acompanhar as suas transações, é muito mais fácil se forem utilizados endereços de uso único.

Ao vincular as transações a um endereço único, é possível verificar se foi recebido um pagamento com base no endereço disponibilizado. Pode dar-se o caso de atribuir um determinado endereço a cada cliente, no entanto este não é o modo recomendado para o recebimento de fundos.

Assim, cada pagamento recebe o seu próprio tipo de identificador único. É particularmente útil se estivermos a gerir um grande departamento de contas, a receber ou a pagar.

Algum motivo para não o fazer?

Pode parecer um incómodo e totalmente irrelevante criar endereços para cada transação. No caso de efetuarmos transações mínimas e nem sequer estivermos preocupados com rastreamentos, qual será o problema?

Tudo se resume à aquisição de bons hábitos. Aumentar o anonimato dos pagamentos, individualmente, aumenta o anonimato geral da rede. Se a totalidade dos utilizadores criarem endereços, o rastreamento dos pagamentos será difícil, mesmo havendo um registo público. Mais adiante será possível verificarmos que essa privacidade geral da rede é importante para a fungibilidade e usabilidade da bitcoin.

Конец ознакомительного фрагмента.