NEEL MEHTA | ADI AGASHE | PARTH DETROJA

BITCOIN, BLOCKCHAIN E CRIPTOMOEDAS

Tradução
Luís Valente

alma dos livros

NOTA DOS AUTORES

O universo das *blockchains* e das criptomoedas é muito profundo, e nesta obra explorámos pouco mais do que a superfície. No entanto, fornecemos hiperligações para cada uma das fontes que utilizámos durante a nossa pesquisa, e encorajamos os leitores a mergulhar mais profundamente no assunto!

Ao longo do livro irá encontrar chamadas de notas numeradas, e caso algum facto ou opinião despertar o seu interesse, entre em

bubbleorrevolution.com/notes/2.0.0

e leia todas as informações adicionais que aí disponibilizámos.

Aos meus amigos e família, por me apoiarem, por mais loucos que sejam os meus sonhos – Neel

À minha família e amigos, obrigado por apoiarem a minha paixão pelos negócios e me ajudarem a ultrapassar os meus receios em abraçar o empreendedorismo – Adi

Aos meus amigos e família pelo seu apoio infindável aos meus projetos aparentemente ridículos – Parth

INTRODUÇÃO

A Bitcoin é uma ferramenta para libertar a humanidade dos oligarcas e tiranos, disfarçada de esquema «fique-rico-depressa».
– Naval Ravikant, fundador da AngelList[1]

A Bitcoin é provavelmente um veneno de rato ao quadrado.
– Warren Buffett, diretor-executivo da Berkshire Hathaway[2]

Corria o ano de 2017, e as Nações Unidas enfrentavam um problema. A sangrenta guerra civil da Síria levou dez mil sírios a fugir para um campo de refugiados na vizinha Jordânia.[3] O Programa Alimentar Mundial (PAM) da ONU tinha criado supermercados no campo, onde os refugiados podiam comprar artigos como azeite e lentilhas, e precisavam de lhes dar algum dinheiro para que os pudessem adquirir.[4]

O problema era que dar, simplesmente, cartões de crédito pré-pagos aos refugiados não funcionaria. Esta abordagem tinha custado milhões ao PAM no passado, devido às taxas de transação e à necessidade de estabelecer parcerias com bancos locais – dinheiro que poderia ter sido canalizado para milhões de refeições.[5] Dar cartões de identificação aos refugiados que lhes conferissem o direito a bens também não funcionaria; quando o PAM o tentou no passado, os líderes tribais locais roubaram os cartões dos refugiados e começaram a negociá-los como moeda.[6]

Por isso, o PAM recorreu a uma tecnologia recente chamada *blockchain*[*], mais conhecida por ser a tecnologia por trás da moeda digital

[*] Embora também tenha outras designações em português, como «protocolo de confiança», não se prevê que se tornem dominantes. *(NT)*

Bitcoin. Era creditado algum dinheiro na «conta» de cada refugiado e, quando este ia a uma loja, a sua identidade era verificada com um leitor de íris e os seus créditos, depois, trocados por comida e mantimentos, tudo sem abrir a carteira.[7] Os cupões recolhidos podiam depois ser vendidos de novo à ONU.[8]

Este projeto, designado Building Blocks, foi um tremendo sucesso. Reduziu em 98 % as taxas de transferência de dinheiro,[9] reduziu a fraude e simplificou radicalmente o processo de ajuda, tanto para o PAM como para os refugiados.[10] A ONU ampliou rapidamente o programa para servir 100 000 refugiados,[11] com um plano para eventualmente servir todos os refugiados na Jordânia.[12]

Os benefícios para a ONU ultrapassam este tipo de assistência: a ONU anunciou que poderá um dia ser capaz de rastrear as identidades e a história de vida dos refugiados recorrendo à tecnologia *blockchain*, ajudando-os assim a encontrar emprego e empréstimos em novos países, se os seus passaportes ou registos académicos forem destruídos.[13]

Por todo o mundo, as pessoas têm estado bastante entusiasmadas com a *blockchain* e a sua tecnologia irmã, as *criptomoedas* (como a já mencionada Bitcoin). A *Harvard Business Review* perguntou se a *blockchain* conseguiria destronar a tradicional indústria bancária,[14] o famoso capitalista de risco Marc Andreessen disse que esta tecnologia é «a invenção mais importante desde a Internet»,[15] e os analistas de todo o mundo acreditam que as criptomoedas irão revolucionar o dinheiro e a tecnologia tal como os conhecemos.[16]

Por outro lado, estas misteriosas novas tecnologias também adquiriram uma reputação sinistra. Os barões da droga usam a Bitcoin para vender drogas *online* de forma anónima,[17] as criptomoedas têm sido acusadas de contribuir para o aquecimento global,[18] e os piratas informáticos exigem o pagamento em Bitcoin para que as autoridades não os consigam identificar.[19] E até a divulgação positiva destas tecnologias parece muitas vezes ir longe demais: uma empresa de chá gelado, a Long Island Iced Tea, acrescentou a palavra «*blockchain*» ao seu nome[20] e viu o preço das suas ações quase quadruplicar.[21]

Então, qual é a verdade? A tecnologia *blockchain* e as criptomoedas constituem uma bolha alimentada pela propaganda desmesurada, sem qualquer utilidade legítima? Ou são invenções revolucionárias

que remodelarão governos, empresas, economias e sociedades à sua imagem? Por outras palavras: bolha ou revolução?

O objetivo

Como demonstram as histórias anteriores, a *blockchain* e as criptomoedas – coletivamente conhecidas como *cripto* (*crypto*) – estão entre as novas tecnologias mais consequentes e, no entanto, menos compreendidas do nosso tempo. A maioria das conversas públicas sobre cripto são dominadas por entusiastas que dizem que a cripto vai derrubar bancos e governos, e por especialistas que dizem que não é mais do que um esquema. Poucas pessoas fazem uma pausa para desconstruir exatamente o funcionamento destas tecnologias e perceber o seu real potencial.

Com o livro *Bitcoin, Blockchain e Criptomoedas* pretendemos mudar isso. Através de exemplos reais, explicações numa linguagem simples e análises imparciais, queremos ensinar-lhe como funciona a cripto, onde é útil, e onde não é. Dir-lhe-emos o que pensamos do debate bolha-ou-revolução, mas também lhe daremos as ferramentas necessárias para decidir por si.

O que contém

Com *Bitcoin, Blockchain e Criptomoedas*, aprenderá sobre a *blockchain* e as criptomoedas; explorará os seus pontos fortes e fracos usando estudos de caso; mergulhará profundamente nas suas implicações sociais, políticas, económicas e técnicas; e obterá uma visão do seu futuro a partir das nossas entrevistas exclusivas com dezenas de líderes da indústria tecnológica.

Eis algumas das coisas que vamos cobrir:

- A ciência económica subjacente à mineração de Bitcoin
- Famosas manhas e falhas das criptomoedas
- A *blockchain* da Xbox para videojogos
- A regulação da Comissão de Valores Mobiliários dos Estados Unidos quanto às *start-ups* de cripto.
- A tokenização da moeda e o futuro do dinheiro

O nosso primeiro livro

Quando escrevemos o sucesso de vendas *Swipe to Unlock: The Primer on Technology and Business Strategy*, o nosso objetivo era ensinar aos leitores tudo o que precisariam de saber sobre o mundo da tecnologia, das entranhas do algoritmo de pesquisa do Google às estratégias de negócios de alto nível do Facebook.

Cada secção de *Swipe to Unlock* é um caso de estudo do mundo real, colocando questões possivelmente já levantadas pelo leitor: como é que o Spotify recomenda músicas, como é que os carros autónomos funcionam e porque tem a Amazon entregas gratuitas mesmo que percam dinheiro com isso. Cobrimos uma vasta gama de tecnologias, desde a segurança e a computação em nuvem até à aprendizagem automática.

Mas desde que escrevemos *Swipe to Unlock*, as criptomoedas e as *blockchains* explodiram na consciência pública como poucas tecnologias o fizeram. É essencial que os tecnólogos, empresários, empreendedores, líderes de negócios e até observadores casuais compreendam estas tecnologias, por isso decidimos escrever um livro sobre elas.

Este livro será um mergulho profundo num pilar-chave da tecnologia; se quiser alcançar uma compreensão mais ampla do panorama tecnológico, erigir estruturas para compreender estratégias de negócios tecnológicos e obter um conjunto de ferramentas mentais para avaliar novas tecnologias, talvez queira também dar uma leitura a *Swipe to Unlock*. Confira em swipetounlock.com ou encontre-o na Amazon.

Quem somos

Antes de começarmos, eis um pouco mais sobre nós.

Neel Mehta é gestor de produto na Google tendo trabalhado anteriormente na Microsoft e no governo dos Estados Unidos, onde criou o primeiro programa de estágio tecnológico do governo federal.

Adi Agashe é gestor de produto na Microsoft e foi fundador e diretor executivo da Belle Applications.

Parth Detroja é gestor de produto no Facebook e anteriormente trabalhou em funções ligadas a produtos e *marketing* na Microsoft, Amazon e IBM.

Obrigado

Mais uma vez, obrigado por ler *Bitcoin, Blockchain e Criptomoedas*! Esperamos que ache este livro informativo, interessante e, talvez, até, divertido.

De todos nós, desfrute!

Neel Mehta
namehta.com
linkedin.com/in/neelmehta18

Adi Agashe
adityaagashe.com
linkedin.com/in/adityaagashe
quora.com/profile/Adi-Agashe

Parth Detroja
parthdetroja.com
linkedin.com/in/parthdetroja

Capítulo Um

BITCOIN E *BLOCKCHAIN*

A Bitcoin permite, pela primeira vez, que um utilizador da Internet transfira um objeto único de propriedade digital para outro utilizador, de tal forma que a transferência é garantida como segura e protegida, todos sabem que a transferência ocorreu e ninguém pode contestar a legitimidade da transferência. As consequências deste avanço são difíceis de estimar.

– Marc Andreessen, cofundador de Andreessen Horowitz[1]

O sistema de confiança tripla (trusted third parties ou TTP) *representa um buraco na segurança. Gostaria de meter isso na cabeça de todas as pessoas no espaço da* blockchain*. Essa é basicamente a chave de todo o conceito.*

– Nick Szabo, criador da Bit Gold (uma precursora da Bitcoin)[2]

No Dia das Bruxas de 2008,[3] um cientista computacional que se apresentava como Satoshi Nakamoto, publicou um livro branco (*whitepaper*) em que apresentava a Bitcoin, uma moeda digital que permitia às pessoas trocarem dinheiro sem a intervenção de um banco, um processador de cartão de crédito ou outra instituição financeira.[4] Ninguém sabia quem era realmente Satoshi, mas todos aqueles a quem o *e-mail* tinha sido endereçado prestaram atenção.

Com um único *e-mail*, Satoshi apresentou ao mundo as *blockchains* e criptomoedas, um par de tecnologias que se tornaram familiares para todos. Mas para compreender essas tecnologias, temos de começar por desvendar a invenção do misterioso cientista.

O problema com o dinheiro

Ao longo da maior parte da história humana, existiram duas formas de guardar dinheiro: possuir bens físicos (numerário, peças de ouro, gado, sal, etc.) ou ter uma instituição de confiança, como um banco ou um chefe de família que controle quanto dinheiro tem.

Estas duas formas monetárias têm os seus problemas.

As desvantagens das formas físicas, ou tangíveis – seja numerário ou vacas –, são bastante claras: são fáceis de roubar, não podem ser usadas para transações *online* ou de longa distância (tente comprar algo em numerário a alguém num país estrangeiro), muitas vezes podem ser falsificadas e constituem uma dor de cabeça no que diz respeito ao armazenamento e ao transporte.

Dinheiro mediado por intermediários

Para resolver estes problemas, a humanidade inventou o dinheiro mediado por uma instituição de confiança como um banco ou um chefe local. Muitas formas de dinheiro e de pagamento enquadram-se neste conceito: contas bancárias, empréstimos bancários, cartões de crédito, cheques, e muitas das outras ferramentas financeiras que usamos atualmente. Ao confiar numa instituição central, ou *intermediário*, pode resolver a maioria dos problemas do dinheiro tangível:

- Pode confiar num banco para manter o seu dinheiro mais seguro do que se o guardasse em casa (compare uma conta bancária com o dinheiro debaixo do colchão).
- Pode efetuar rapidamente pagamentos *online* e digitais, uma vez que pagar a alguém é tão fácil como deixar o seu banco e o banco dessa pessoa atualizar os saldos da conta (que são apenas números numa base de dados algures).
- É mais difícil produzir dinheiro falso quando uma autoridade de confiança rastreia exatamente quanto dinheiro todos têm. (Uma vez que não há um registo central de quanto dinheiro todos têm, a única maneira de conseguir detetar um falsificador é distinguindo o dinheiro falso do dinheiro real).

- Se confiar o seu dinheiro a um intermediário, não precisa de o levar consigo.

Este tipo de dinheiro mediado por intermediários é realmente notável. Mas há uma razão para as pessoas ainda usarem numerário, e algumas lojas aceitarem apenas essa forma de pagamento: o dinheiro mediado por um intermediário (que abreviaremos por *DMI*) tem a sua quota-parte de desvantagens, sendo que a maior parte delas advém do próprio facto de haver um intermediário.

O primeiro problema: quando o seu dinheiro flui através de intermediários, tem de jogar de acordo com as regras deles, o que muitas vezes significa ter de pagar taxas. Quando paga por algo com um cartão de crédito, o comerciante não fica com o valor total; tem de pagar taxas ao processador do cartão de crédito (cerca de 1,5-2,5 % no caso da Visa, Mastercard e Discover, e 2,5-3,5 % para a American Express).[5*]

Enviar dinheiro para o estrangeiro com a PayPal custar-lhe-á cerca de 3 % em taxas e, se for um comerciante, aceitar o pagamento através de PayPal também lhe custará cerca de 3 %.[6] E as taxas de envio de dinheiro para o estrangeiro com a Western Union, MoneyGram, Xoom, entre outras, podem ser também de vários por cento.[7]

Compreende agora porque muitas lojas aceitam apenas numerário ou estipulam um limite mínimo de compras para que possa usar cartões de crédito.

Outro problema com o DMI é que só pode usá-lo se os intermediários lhe concederem acesso. Na prática, isto significa que os dois mil milhões de pessoas que não têm conta bancária[8] não podem usar dinheiro que envolva uma conta bancária (ou seja, a maior parte do DMI), e as pessoas com más avaliações ou sem crédito não podem usar cartões de crédito.

O último grande problema do DMI é estar a confiar-lhes o seu dinheiro – e, hoje em dia, os seus dados. Os bancos são muito bons a não perder o seu dinheiro, mas o historial das instituições financeiras em matéria de proteção de dados está longe de ser tão bom.

---

* É devido às taxas mais elevadas da American Express que muitas lojas não a aceitam como forma de pagamento.

Piratas informáticos roubaram dados de 100 milhões de clientes do JPMorgan em 2014,[9] e foi roubada informação sensível (datas de nascimento, moradas, etc.) de 100 milhões de clientes da Capital One, em 2019.[10] Isso para não falar daquele que talvez tenha sido o mais infame golpe de pirataria de todos: quando os dados pessoais (incluindo números de Segurança Social) de quase 150 milhões de americanos foram roubados à Equifax.[11]

Em suma, o dinheiro tangível é inseguro, inconveniente, fácil de falsificar e pouco prático para pagamentos digitais. O dinheiro mediado por intermediários, ou DMI, resolve estes problemas, mas introduz taxas, falta de acessibilidade e uma forma diferente de insegurança. Neste momento, temos de escolher o nosso veneno.

Intangibilidade

Contudo, se pensarmos bem, o que realmente precisamos no dinheiro é intangibilidade. O DMI oferece-lhe intangibilidade ao introduzir intermediários: se confiar em instituições para gerir e movimentar o seu dinheiro por si, já não precisa de possuir dinheiro tangível. Mas, é claro, os intermediários trazem o seu próprio cabaz de inconvenientes. Existirá alguma maneira de eliminar o intermediário mantendo a intangibilidade? Por outras palavras, pode ter uma forma de dinheiro que seja ao mesmo tempo intangível *e* livre de intermediários?

Provavelmente vê onde queremos chegar. Mas acontece que as pessoas inventaram uma forma de dinheiro intangível e sem intermediários séculos antes de Satoshi ter apresentado a Bitcoin ao mundo. Para conhecermos estas pessoas, temos de visitar a minúscula ilha de Yap, na Micronésia, no meio do Oceano Pacífico.

Pedras rai

A moeda tradicional em Yap são anéis de pedra gigantescos conhecidos como pedras rai. Estas pedras são enormes: algumas atingem 3 metros de diâmetro e pesam tanto como uma carrinha.[13] Cada aldeia de Yap tem dezenas de pedras rai espalhadas por todo o lado.[14]

Uma pedra rai, uma forma tradicional de moeda
na ilha de Yap, no Pacífico. Fonte: Wikimedia[15]

Como pode imaginar, as pessoas não conseguem carregar estas pedras pela ilha para fazer pagamentos. Em vez disso, os yapeses lembram-se coletivamente de quem é dono de cada pedra e mantêm um registo mental das transações passadas. Por exemplo, se a filha do chefe local quiser comprar um barco ao carpinteiro, poderá anunciar aos outros habitantes que uma pedra rai que ela possui (digamos, a que está na praia) pertence agora ao carpinteiro. Os aldeões espalhariam, então, a notícia de que a filha do chefe deu uma pedra ao carpinteiro.

Depois, se o carpinteiro quiser dar aquela pedra a outra pessoa, os aldeões deixá-lo-ão, uma vez que os registos mentais coletivos dizem que aquela pedra agora lhe pertence.[16] (Grosso modo, alguém pode gastar uma pedra se a maioria dos aldeões concordar que é sua).

Intangível

A parte impressionante do sistema de pedras rai é que permite a ocorrência de todo o tipo de atividades económicas sem que as pedras se movam fisicamente; de facto, pode possuir uma pedra mesmo que ela esteja no ponto mais afastado da sua casa. Pode até usar pedras rai que nunca mais possam ser vistas. Há centenas de anos, um navio que

transportava uma pedra rai afundou-se ao largo. Os aldeões locais concluíram que a pedra ainda devia existir algures no fundo do oceano, por isso continuaram a fazer pagamentos com aquela pedra como se nada tivesse acontecido![17]

Por outras palavras, no sistema de pedras rai, a localização física e o movimento das pedras são irrelevantes. Isto contrasta com os sistemas tradicionais tangíveis, nos quais a localização física e o movimento do dinheiro *importam*: o único dinheiro que possui é o que está em sua casa ou o que traz consigo, e a única maneira de poder pagar a alguém é entregando-lhe objetos físicos.

Isto significa que o sistema de pedras rai é uma forma monetária intangível. É como o dinheiro num banco, que sabemos ser intangível: não importa onde estão as notas – ou se de facto existem! – e quando envia dinheiro a alguém, não é movido qualquer objeto físico.

Livre de intermediários

Além disso, o sistema de pedras rai é democrático: é proprietário de uma pedra se a maioria dos seus conterrâneos estiver de acordo. Em vez de confiar numa única pessoa ou instituição para controlar quanto dinheiro possui, como no caso do DMI, difunde a sua confiança por toda a aldeia.

Este sistema democrático de decidir quem possui pedras – por outras palavras, este *consenso* – apresenta muitas vantagens face a um sistema moderado por intermediários. Imagine um universo alternativo em que o chefe da aldeia mantém o registo oficial dos pagamentos e da titularidade das pedras, no lugar de os aldeões conservarem coletivamente, por meio de consenso, um registo mental. (Neste universo, o sistema monetário yapês funcionaria como o DMI; o chefe de aldeia assumiria o papel de um banco). O chefe poderia facilmente obrigar todos a pagar-lhe uma taxa aquando de um pagamento, apropriar-se de pedras ao apagar estrategicamente os pagamentos do seu livro de registo, perder o livro de registo (e, assim, fazer parar a economia local), e por aí em diante.

O sistema de pedras rai é, portanto, intangível *e* livre de intermediários. Tem a conveniência do DMI – não precisa de carregar pedras – sem os problemas inerentes à dependência de um intermediário.

Este sistema é um exemplo do «melhor dos dois mundos» de que falámos na secção anterior.

A lição a retirar é a de que os sistemas de dinheiro intangível requerem sempre confiança: só abdicará do controlo físico sobre o seu dinheiro se puder confiar que algo ou alguém irá manter um registo exato sobre ele. A inovação de Yap baseou-se na perceção de que se pode confiar nos *sistemas*, não nos intermediários; neste caso, o sistema de confiança foi o registo mental das transações que os aldeões yapeses partilhavam. Ao depositarmos confiança num sistema partilhado, baseado no consenso – um grupo de pessoas que seguem regras comuns – em vez de numa única pessoa ou entidade, o resultado é o dinheiro intangível sem o intermediário.

A *blockchain* da Bitcoin

Não sabemos se Satoshi estudou a ilha de Yap enquanto desenvolvia a Bitcoin, mas a sua visão era muito semelhante.

A Bitcoin é uma moeda digital sendo, por isso, intangível e (em teoria) livre de intermediários porque não depende de um banco ou outra instituição para controlar os saldos financeiros das pessoas. Em vez disso, a Bitcoin depende de uma rede de computadores em todo o mundo para manter um registo partilhado, ou *livro-razão* (*ledger*), de cada pagamento efetuado. É a este «livro-razão público partilhado», como é conhecido, que chamamos *blockchain*, e este é, basicamente, uma versão de alta tecnologia da memória partilhada dos aldeões de Yap.

Em suma, a Bitcoin é uma versão moderna e adaptada à Internet das pedras rai. É intangível e (em teoria) livre de intermediários, o que a torna uma atraente alternativa aos nossos sistemas monetários tradicionais, que obrigam à tangibilidade ou à intermediação.

A folha de cálculo da Google partilhada

Outra forma, mais técnica, de pensar a *blockchain* é vê-la como uma gigantesca folha de cálculo do Google partilhada com todas as pessoas do mundo, com uma linha por transação:

	A	B	C	D
1	**Transaction ID**	**From**	**To**	**Amount**
2	1	(origin)	A	50
3	2	(origin)	B	50
4	3	A	C	20
5	4	B	D	25
6	5	D	C	15
7	6	B	A	5

Uma forma simplificada de pensar a *blockchain* da Bitcoin:
uma folha de cálculo do Google partilhada com o mundo inteiro.

(Naturalmente, esta folha de cálculo só devia permitir adições: para que utilizadores desonestos não alterassem transações passadas.)

Seja como for, imagine que cada utilizador da Bitcoin no mundo tem uma cópia desta folha de cálculo guardada nos seus computadores. Sempre que alguém faz uma nova transação, a transação é transmitida a todos e, em seguida, todos os computadores descarregam novas versões da folha de cálculo.

Mineração

A única falha óbvia na criação de uma tal folha de cálculo do Google para acompanhar os pagamentos reside no facto de alguém poder tentar gastar dinheiro que não tem. Claramente, precisaria de alguém para verificar as transações antes de estas serem submetidas, para que as transações problemáticas não se concretizassem.

Em vez disso, a Bitcoin adjudica este trabalho de fiscalização aos membros da comunidade. Qualquer utilizador da Bitcoin pode usar o seu computador para verificar transações pendentes e adicionar apenas as transações válidas à *blockchain*. Por uma questão de eficiência, as transações são agrupadas em *blocos* (*blocks*), cada um composto por alguns milhares de transações.[18]

Incentivos

Mas, claro, as pessoas não vão fazer o trabalho informático de verificar as transações gratuitamente. Por isso, o *software* da Bitcoin tem de contribuir com algum dinheiro para as incentivar. Se verificar um bloco de transações, ganhará comissões (ou taxas) por cada transação no bloco, para além de o *software* da Bitcoin também lhe pagar um valor fixo de bitcoins,* conhecido como *recompensa por bloco* (*block reward*). As bitcoins da recompensa por bloco não existem antes da verificação, o *software* da Bitcoin cria-as a partir do nada.[19]

Como a Bitcoin se vê a si mesma como uma versão digital do ouro[20] e os verificadores trabalham para extrair dinheiro novinho em folha, este processo de verificação chama-se *mineração* (*mining*), e os verificadores são conhecidos como *mineiros*. (Está a minerar com um computador em vez de com picareta e pá, mas o modelo de negócio é basicamente o mesmo.)

Assim, se quiséssemos voltar à nossa folha de cálculo do Google e fazer com que ela se parecesse mais com uma verdadeira *blockchain*, adicionaríamos colunas relativas a blocos, taxas e recompensas, deste modo:

	A	B	C	D	E	F	G	H
1	**Block ID**	**Transaction ID**	**From**	**To**	**Amount**	**Miner**	**Mining Fee**	**Block Reward**
2	B1	T1	A	B	10	C	1	25
3		T2	A	D	15		1	
4		T3	A	E	5		1	
5	B2	T4	B	C	2	E	1	25
6		T5	D	E	5		1	
7		T6	C	A	10		1	

Um modelo mais avançado da *blockchain* da Bitcoin, incorporando mineração, taxas e recompensas.

Assim, C minou o bloco B1, que continha três transações, e ganhou 28 bitcoins pelo seu incómodo: 25 da recompensa por bloco e 1 por cada transação.

* A moeda é designada «Bitcoin» com um «B» maiúsculo, enquanto as unidades de moeda são designadas «bitcoins», com um «b» minúsculo. É como a diferença entre «o dólar americano» (o nome da moeda) e «dólares» (as unidades da moeda).

Questionário: assumindo que cada pessoa (A, B, C, D e E) começou com 100 bitcoins, quantas têm depois de efetuarem estas transações?

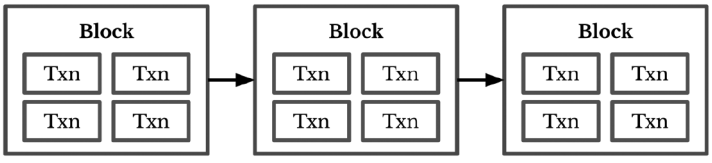
As respostas:

- A enviou 10 bitcoins para B e pagou uma taxa de 1 bitcoin, depois enviou 15 bitcoins para D e pagou uma taxa de 1 bitcoin, depois enviou 5 bitcoins para E e pagou uma taxa de 1 bitcoin, depois recebeu 10 bitcoins. Isto significa que A acaba com 100 – 10 – 1 – 1 – 15 – 1 – 5 – 1 + 10 = 77 bitcoins.
- B ganhou 10 bitcoins de A e enviou 2 bitcoins (mais uma taxa de 1 bitcoin) para C. Então, B agora tem 100 + 10 – 2 – 1 = 107 bitcoins.
- C ganhou 25 + 1 + 1 + 1 = 28 bitcoins do bloco de mineração B1, portanto tem 100 + 28 + 2 – 10 – 1 = 119 bitcoins.
- D agora tem 100 + 15 – 5 – 1 = 109 bitcoins.
- E também ganhou 28 bitcoins do bloco de mineração B2, por isso possui 100 + 5 + 28 + 5 = 138 bitcoins.*

Blocos e cadeias

Acontece que o nosso modelo de folha de cálculo é exatamente isso: um modelo. É uma simplificação. A verdadeira *blockchain* da Bitcoin não armazena blocos em formato do tipo folha de cálculo.

Em vez disso, a *blockchain* da Bitcoin armazena blocos numa «cadeia» linear, em que cada bloco aponta matematicamente para o anterior:[21]



A *blockchain* armazena blocos numa cadeia linear; «txn» é a abreviatura da Bitcoin para «transação». Cada bloco refere-se ao anterior, mas os cientistas informáticos normalmente desenham cadeias desta forma, com as setas a apontar de um bloco para o seguinte, para que seja mais intuitivo.

* Um dia bastante lucrativo. Todos nós gostaríamos de ser o E.

Desta forma, a ordenação de blocos é clara, mesmo que os blocos não tenham números explícitos. Imagine que rasga todas as páginas de um romance, removendo também todos os números de página e de capítulo. Depois imagine que espalha todas as páginas no chão.

Ainda assim, poderia voltar a colocar as páginas em ordem, uma vez que cada página faz implicitamente referência ao que aconteceu na última página. (Por exemplo, se a página X terminar com um personagem a conduzir até ao tribunal e a página Y começar com o personagem a entrar no tribunal, pode ter a certeza de que a página Y vem logo a seguir à página X).

Hashing

Claro que a Bitcoin não tem noção de enredo, pelo que os blocos se referem uns aos outros através da matemática. Para sermos mais específicos, usamos uma técnica matemática chamada *hashing*, que pressupõe a introdução de um monte de informação (palavras, números, blocos de Bitcoin, etc.) num algoritmo que devolve uma pequena «impressão digital» daquela informação.[22]

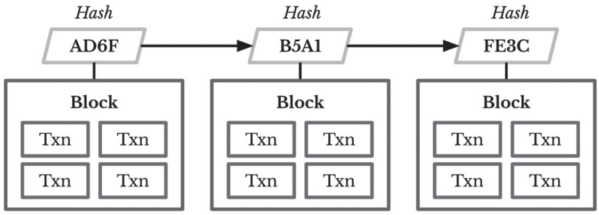
Nós, humanos, usamos constantemente *hashing*, por exemplo com as iniciais. Um nome longo pode facilmente ser condensado em algumas letras: «John Fitzgerald Kennedy» pode ser encurtado para «JFK».

Há uma entrada (o nome completo); a *função hash* (o processo de obter as iniciais de alguém); e uma saída, ou *hash* (as iniciais).

Os computadores utilizam funções *hash* mais sofisticadas – as mais populares são os algoritmos MD5[23] ou SHA-256[24] – mas a ideia central é a mesma: entradas volumosas de dados convertem-se em saídas curtas.

Na Bitcoin, cada bloco tem um *hash* associado. O *hash* de cada bloco é baseado parcialmente no *hash* do bloco precedente.* Desta forma, cada bloco refere-se ao bloco precedente. Assim, se tiver uma lista não ordenada de blocos e respetivos *hashes* associados, pode muito facilmente voltar a colocar os blocos em ordem, tal como a pessoa poderia organizar as páginas, analisando a progressão do enredo.

* Explicaremos exatamente como funciona o *hash* daqui a algumas páginas.



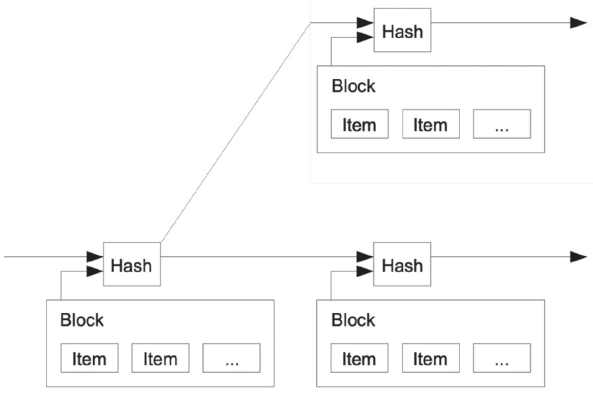
Os blocos são encadeados usando os seus *hashes*;
cada *hash* é calculado (entre outras coisas) a partir do *hash* do bloco anterior.

(Qual a razão dos números e letras nos *hashes*? Os *hashes* são escritos no formato *hexadecimal*, ou *base-16*.* Também são muito mais longos do que 4 caracteres,[25] mas as nossas versões abreviadas bastam por agora.)

Portanto, a Bitcoin realiza transações em blocos, e liga-os uns aos outros numa cadeia.

Ramos e fraude

Olhe para o nosso sistema de encadeamento com base em *hash* e perceberá que, na realidade, não requer que os blocos sejam colocados numa cadeia linear. Nada impede que dois ou mais blocos venham logo a seguir a um determinado bloco:

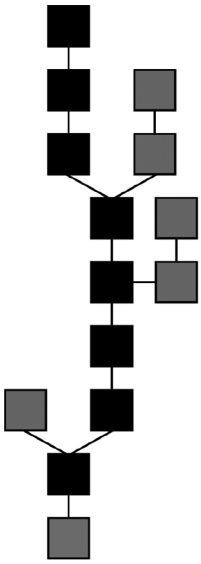


Vários blocos podem citar qualquer bloco específico como sendo seu predecessor, por isso a *blockchain* pode ramificar-se, como efetivamente acontece.
Imagem adaptada de: Satoshi Nakamoto[26]

* Consulte o Apêndice A para ler mais sobre o sistema hexadecimal e outros sistemas numéricos.

Árvore de blocos

Como resultado, a *blockchain* não tem de ser uma cadeia linear. Na verdade, geralmente não é. A *blockchain* tende a parecer-se mais com uma *árvore de blocos* (*blocktree*) com um «tronco» e «ramos»:



A *blockchain* pode ter muitos ramos, tal como uma árvore (imagine que o bloco da base está ao nível do solo o que torna este diagrama muito parecido com uma árvore). O ramo mais longo é considerado o «oficial». Fonte: Wikipedia[27]

A árvore de blocos por vezes desenvolve um novo ramo quando dois mineiros geram (ou «mineram») um bloco ao mesmo tempo. Isto é raro, mas acontece. Quando isso acontece, há duas transações que dividem a transação mais recente, e nasce um novo ramo da árvore de blocos.[28]

Mas, tal como com o sistema de pedras rai, a Bitcoin precisa de ter um histórico único e linear de transações. Não se pode permitir a coexistência de vários ramos. (Imagine dizer a alguém, «numa versão da história, tenho 500 dólares, mas na outra, tenho 600»?)

A regra da cadeia mais longa

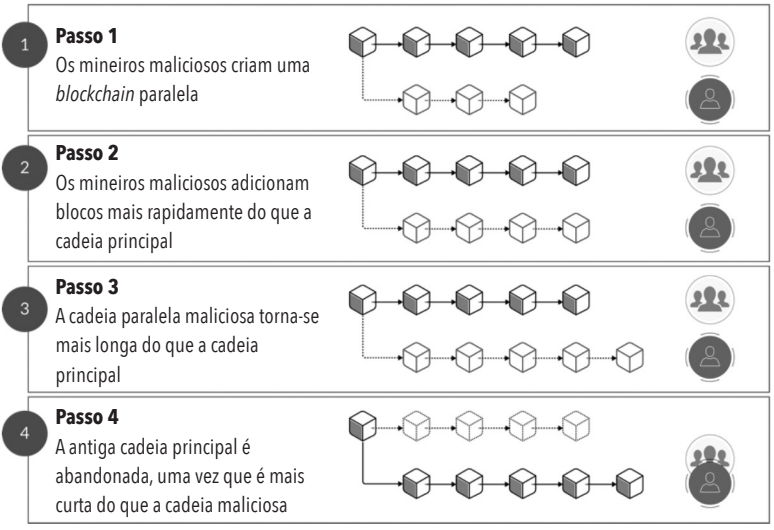
Para ter uma história oficial linear, a Bitcoin usa uma regra de ouro chamada *regra da cadeia mais longa*, segundo a qual o ramo da árvore de blocos com mais blocos é a *blockchain* oficial.[29] A cadeia mais longa

determina quanto dinheiro realmente possui, que transações passadas aconteceram, e assim por diante. Se não estiver na cadeia mais longa, não aconteceu.

O *software* Bitcoin, que é executado nos computadores dos utilizadores de Bitcoin, reforça a regra da cadeia mais longa, ao pagar apenas aos mineiros que adicionaram um bloco à cadeia mais longa.[30] Isto é geralmente suficiente para manter os mineiros na linha. (No entanto, produz um efeito secundário infeliz. Se dois mineiros extraem um bloco ao mesmo tempo, nascem dois ramos, mas apenas um ramo vai ganhar e tornar-se a cadeia mais longa. O outro ramo fica «órfão» e é expulso, e o azarado mineiro que minerou o bloco na base desse ramo não recebe nada. Estas «orfandades» acontecem algumas vezes por dia.[31])

Sequestro de cadeias

Contudo, a regra da corrente mais longa deixa uma brecha na segurança. E se um mineiro corrupto criasse um novo ramo e minasse blocos mais rapidamente do que todos os outros, tornando assim o seu ramo mais longo do que o ramo legítimo? Bem, o ramo do mineiro corrupto tornar-se-ia a cadeia mais longa, portanto, a *blockchain* oficial. Todos os blocos da sua cadeia fraudulenta passariam a ser a história oficial, e alguns dos blocos da cadeia legítima seriam expulsos.



Como um atacante poderia sequestrar a *blockchain* minerando mais rapidamente do que todos os outros.

Claro que deixar um vigarista controlar a *blockchain* provocaria o caos, mas também poderia conduzir à fraude. Imagine que o mineiro corrupto compra milhares de dólares em mercadoria com a Bitcoin e coloca essa transação na *blockchain*. Em seguida, executa o seu ataque, construindo uma nova cadeia mais longa do que a cadeia oficial. A transação com que pagou ao comerciante é expulsa, uma vez que já não está na cadeia mais longa; é como se nunca tivesse sido feito o pagamento. Portanto, o mineiro corrupto recebeu toda a sua mercadoria, mas não teve de pagar por ela!

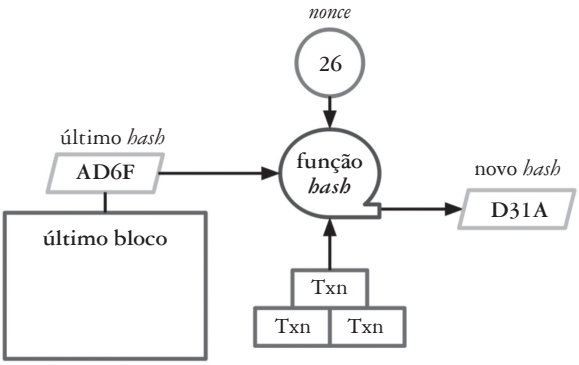
Jogo de *nonces*

Como se impedem ataques como estes? É necessário tornar mais difícil aos atacantes minarem mais rapidamente do que os mineiros honestos. Para isso, Satoshi fez com que a mineração de um bloco demorasse muito tempo.

O processo concebido por Satoshi começa com as transações. As transações à espera de serem examinadas e confirmadas ficam no *acervo de transações* (*transaction pool*), também conhecido por *acervo de memórias* (*memory pool* ou *mempool*)[32]. Quando quer extrair um bloco, escolhe alguns milhares de transações do acervo, verifica-as, e constrói o seu bloco.

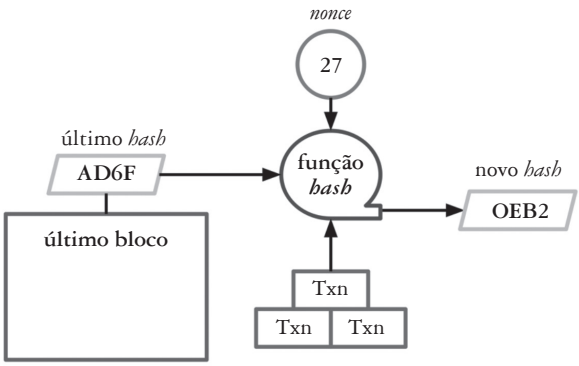
Depois, tudo o que tem de fazer é gerar um *hash* para o seu bloco, e poderá colocá-lo na cadeia e receber as suas recompensas.

Mas gerar o *hash* não é fácil. Requer três entradas: o *hash* do último bloco, as transações, e um número especial que se escolhe designado por *nonce*.



A função *hash* usa três entradas para gerar o *hash* de um bloco.

O inconveniente é que o valor do *hash* é diferente para cada *nonce*, e só lhe é permitido adicionar o seu bloco à cadeia, se o seu *hash* começar com o número certo de zeros. Portanto, se o *nonce* que escolheu não conduzir a um bom *hash*, tem de tentar outra vez e outra vez:



Alterar o *nonce* dá-lhe um *hash* de saída completamente diferente.

Adivinhe e confira

O que torna isto difícil é não haver um padrão discernível nos *hashes*; não se pode prever o *hash* a partir da entrada, e mesmo pequenas alterações na entrada tornam a saída completamente diferente. Se executar a palavra «gato» através da popular função *hash* MD5, obtém esta saída inescrutável:

70b783251225354e883a5bef3c011843

Por outro lado, o *hash* MD5 de «pato» não está nem perto:

259823af837e251e560ca1158a4e77c7

Além disso, as funções *hash* utilizadas pelos computadores tendem a ser aquilo a que chamamos *funções unidirecionais*: é fácil calcular a saída dada a entrada, mas é quase impossível adivinhar a entrada dada a saída.

As iniciais de um nome são mais ou menos assim: ao ler as iniciais GMD, não se torna imediatamente óbvio a que nome original se referem.*

* Se estiver curioso, estávamos a pensar em George Mifflin Dallas, o obscuro 11.º Vice-presidente dos Estados Unidos, que exerceu funções entre 1845 e 1849.

Isto significa que a única maneira de «decifrar» uma função *hash* – determinar a entrada dada a saída – seria adivinhar cada uma das saídas. Mas isto seria extremamente difícil: decifrar a função *hash* SHA-256, que a Bitcoin usa, levaria milhões de anos[33] e custaria, muito provavelmente, milhões ou milhares de milhões de dólares.[34*]

Por outras palavras, não pode fazer a engenharia inversa de um bom *nonce*. Portanto, a única maneira de minerar um bloco é adivinhar os *nonces* vezes sem conta até ganhar – como jogar numa lotaria digital. Chamamos-lhe o jogo dos *nonces*. (A palavra *nonce* vem de «número usado apenas uma vez» – «*number used only once*» –, visto que o experimenta uma vez e o deita fora se não servir.[35])

Teste a sua mão

É instrutivo simular este jogo. Vá a md5online.org, um *website* que (como o nome indica) lhe permite processar texto através da função *hash* MD5.[36] O seu desafio é escolher um *nonce* que, quando colocado após a palavra «hello», produz um *hash* começado com um zero.

Pode começar por escolher um *nonce* de 1, pelo que a sua entrada seria «hello1». O *hash* MD5 deste texto é

203ad5ffa1d7c650ad681fdff3965cd2.

Pouca sorte. Poderá então escolher um *nonce* de 2; o *hash* MD5 de «hello2» é

6e809cbda0732ac4845916a59016f954.

Também não serve.

Se continuar a aumentar o *nonce* de um em um, acabará por descobrir que o primeiro *nonce* que produz um *hash* vencedor é o 33: o *hash* MD5 de «hello33» é

---

* A dificuldade depende exatamente de quão complexo é o seu texto de entrada. Se a sua palavra-passe é «hello», e processá-la com a função SHA-256, torna-se bastante fácil de decifrar, uma vez que é provável que alguém na Internet tenha lá colocado o *hash* SHA-256 relativo a «hello». Uma simples pesquisa do *hash* no Google revelaria a entrada.

005529451481309d2b8f708bbb81ea41.

Sucesso!

Não foi assim tão difícil e, matematicamente falando, não deveria ser. Os *hashes* MD5 são escritos no sistema numérico hexadecimal, ou base-16, o que significa que cada dígito é um dos 16 caracteres possíveis (0-9 e A-F).* Os *hashes* são aleatórios, por isso o primeiro dígito de qualquer *hash* tem uma probabilidade de 1/16 de ser um zero. Isto significa que obterá um *hash* de sucesso em média uma vez em cada 16 tentativas. A contagem ascendente de um em um revelou-se de pouca sorte, visto que nos custou 33 tentativas.

Nonce	**Entrada**	**Hash MD5**
29	hello29	fc12c051dd3eb4d7beb430f362522fda
30	hello30	868594340dd4f911fcbdbebf80dbdcaa
31	hello31	5cebee1d96882e6325b758a1fbd80b02
32	hello32	ce62f2f1d58fe37381a2ac08fc544467
33	hello33	005529451481309d2b8f708bbb81ea41
34	hello34	45c66648b3d94b4e46a6ba796fbee7af
35	hello35	44ee8f3e8ef0f8e7085193d123b20a9e
36	hello36	092962df00b7139faca15313ff345c4e
37	hello37	c1b4349f3222aec9916dd1fbe65c02fe
38	hello38	ebcd88fab0212bad35bde21c11185754
39	hello39	2206e08b5186fc0c5d4239259f09037f
40	hello40	5886c943b32a6dd596b19b5897c0306d
41	hello41	20ce5b4e49c7847661a9bf6edfd35760

A saída de *hash* é aleatória, por isso tem de continuar a adivinhar *nonces* até obter um *hash* afortunado. O primeiro *nonce* vencedor neste caso é 33.

* Veja o Apêndice A para obter mais informações sobre sistemas numéricos como o de base-16.