# Inventando o Bitcoin

**Explicando a tecnologia por trás do primeiro dinheiro verdadeiramente escasso e descentralizado**

Yan Pritzker

Obtenha a versão atualizada online em inventingbitcoin.com



Tradução feita por KoreaComK / @KoreacomK

“Este livro é dedicado a meus pais Yury e Lana, que tiraram nossa família da ex-URSS, um regime socialista autocrático com rígidos controles de capital”.

“Também é dedicado à minha esposa Jessica, que teve que suportar minha incapacidade de parar de falar sobre o Bitcoin, e por ficar acordada comigo até tarde para terminar este livro”.

# Sumário

# Introdução

Bem-vindo ao *Inventando o Bitcoin!*

Meu objetivo é simplesmente agradar seu cérebro e dar a você um gostinho da ciência da computação e da teoria dos jogos econômicos que fazem do Bitcoin uma das invenções mais interessantes e profundas de nosso tempo.

A maioria das pessoas, ao ouvir pela primeira vez sobre o Bitcoin, realmente não o entendem. É dinheiro mágico da internet? De onde isso vem? Quem o controla? Por que é tão importante?

Para mim, entender todas as coisas que se juntam para fazer o Bitcoin funcionar - física, matemática, criptografia, teoria dos jogos, economia e ciência da computação - foi um momento profundo. Neste livro, espero compartilhar esse conhecimento com você de uma forma muito simples e fácil de entender.

A forma como o faremos isso é um passo de cada vez. Com nada além de uma base de matemática de nível médio, iremos percorrer a *invenção do bitcoin*, passo a passo. Espero que este livro seja o suficiente para dar um gostinho do que é essa tecnologia e mandá-lo para o buraco do coelho do Bitcoin. Então, vamos começar!

# 1 O que é o Bitcoin?

O Bitcoin é um *dinheiro eletrônico ponto a ponto*. Um dinheiro digital que pode ser transferido entre pessoas ou computadores sem nenhum intermediário confiável (como um banco) e cuja emissão não está sob o controle de nenhuma parte.

Pense em uma nota de dois reais ou em uma moeda de metal. Quando você dá esse dinheiro para outra pessoa, ela não precisa saber quem você é. Eles só precisam confiar que o dinheiro que recebem de você não é uma falsificação. Tipicamente, as pessoas fazem isso com dinheiro físico, usando apenas os olhos e os dedos, ou ate em casos de quantias maiores usando equipamentos próprios para testar cédulas.

Conforme mudamos para uma sociedade digital, pagamentos começaram a ser feitos digitalmente pela internet por meio de um serviço de intermediário, do que fisicamente: uma empresa de cartão de crédito como Visa, um provedor de pagamento digital como PayPal ou Apple Pay ou um serviço online de uma plataforma, como o WeChat na China.

A mudança para pagamentos digitais traz consigo a dependência em uma entidade central que tem que aprovar e verificar cada pagamento. Isso ocorre porque a natureza do dinheiro mudou de uma coisa física que você pode carregar trocar e verificar por si mesmo, para bits digitais que precisam ser verificados pela parte que controla sua transferência.

Ao trocarmos nosso dinheiro físico por pagamentos di-

gitais, nos também criamos um sistemas onde damos poderes extraordinários a aqueles que buscam nos oprimir. Plataformas de pagamentos digitais se tornaram a base de um futuro sistema autoritário distópico, tal qual aqueles utilizados pelo governo chines para monitorar seus dissentes e prevenir cidadãos, cujo seu comportamento não estão ao seu agrado, de comprar bens e serviços.

O Bitcoin oferece uma alternativa ao dinheiro digital controlado centralmente com um sistema de três componentes básicos. Veremos as motivações por trás desse

design na próxima seção.

1. Um ativo digital (normalmente *bitcoin* com *b* minúsculo) com um suprimento que é limitado, conhecido com antecedência e imutável. Isso contrasta fortemente com o dinheiro com o qual a maioria de nós está acostumado atualmente, que são notas emitidas por governos ou bancos centrais cuja oferta se expande a uma taxa imprevisível, com o passar do tempo.

2. Um monte de computadores interconectados (a *rede Bitcoin*, com *B* maiúsculo), aos quais qualquer pessoa pode entrar. Essa rede serve para rastrear a propriedade de bitcoins e transferi-los entre os participantes, evitando qualquer intermediário, como bancos, empresas de pagamento e entidades governamentais.

3. O software Bitcoin Client, que é um pedaço de código que qualquer pessoa pode executar em seu computador para se tornar um participante da rede. Este software é de código aberto, o que significa que qualquer pessoa pode ver como funciona, bem como contribuir com novos recursos e correções de bugs.

## De onde veio o Bitcoin?

O Bitcoin foi inventado por uma pessoa ou grupo de pessoas, conhecido pelo pseudônimo de Satoshi Nakamoto, por volta de 2008. Ninguém sabe a identidade dessa(s) pessoa(s) e, pelo que sabemos, sumiram, não se houve falar dele(s) há anos.


*bitcoin e Bitcoin*

Em 11 de fevereiro de 2009, Satoshi revelou o primeiro protótipo do Bitcoin em um fórum online para os cypherpunks, pessoas que trabalham com tecnologia de criptografia e se preocupam com a privacidade individual. Embora essa não é o primeiro anuncio do Bitcoin, contem uma bom sumario das motivações de Satoshi, a usaremos para fundamentar nossa discussão

Extraí as partes relevantes abaixo. Na próxima seção, explicaremos algumas dessas declarações e as motivações de Satoshi para a invenção do Bitcoin e quais problemas ele buscava solucionar.

> “ *Desenvolvi um novo sistema de e-cash P2P de código aberto chamado Bitcoin. É totalmente descentralizado, sem servidor central ou partes confiáveis, porque tudo é baseado em criptografia ao invés da confiança. [. . . ]*

*A raiz do problema com a moeda convencional é toda a confiança necessária para fazê-la funcionar. O banco central deve ser confiável para não depreciar a moeda, mas a história das moedas fiduciárias está cheia de violações dessa confiança. Os bancos devem ser confiáveis para manter nosso dinheiro e transferi-lo eletronicamente, mas eles o emprestam em ondas de bolhas de crédito ficando apenas com uma fração na reserva. Temos que confiar neles à nossa privacidade, confiar que não irão permitir que ladrões de identidade drenem nossas contas. Seus enormes custos indiretos tornam os micro pagamentos impossíveis.*

*Na geração passada, os sistemas de compartilhamento de tempo multiusuário tinham um problema semelhante. Antes da criptografia forte, os usuários tinham que confiar na proteção por senha para proteger seus arquivos[...]*

*Então, a criptografia forte tornou-se disponível para as massas e a confiança não era mais necessária. Os dados podiam ser protegidos de uma forma fisicamente impossível para outras pessoas acessarem, não importa por que razão, não importa quão boa seja a desculpa, não importa o quê seja criptografado.*

> *É hora de termos o mesmo no nosso dinheiro. Com a moeda eletrônica baseada em prova criptográfica, sem a necessidade de confiar em um intermediário, o dinheiro pode ser seguro e as transações com o mínimo de esforço.[. . . ]*
>
> *A solução do Bitcoin é usar uma rede ponto a ponto para verificar se há gastos duplos. Em suma, a rede funciona como um servidor de carimbo de data/hora distribuído, carimbando a primeira transação a gastar uma moeda. Ele tira proveito da natureza da informação ser fácil de ser espalhada, mas difícil de ser reprimida. Para obter detalhes sobre seu funcionamento, consulte o design desta solução no artigo disponibilizado em http://www.bitcoin.org/bitcoin.pdf*"
>
> – Satoshi Nakamoto

Quando o Bitcoin foi lançado, apenas algumas pessoas o utilizavam e executavam seu sistema em seus computadores (chamados de *nodes*) para alimentar a rede Bitcoin. A maioria das pessoas na época achou que era uma piada ou que o sistema revelaria sérias falhas no projeto, que o tornaria impraticável.

Com o tempo, mais pessoas se juntaram à rede, usando seus computadores para adicionar segurança à ela e reforçando seu valor, trocando outras moedas pelo Bitcoin ou aceitando-a por bens e serviços. Hoje, dez anos depois, é usado por milhões de pessoas com dezenas a centenas de milhares de nodes executando o software gratuito do Bitcoin, que é desenvolvido por centenas de voluntários e empresas em todo o mundo.

O Bitcoin não foi uma invenção criada do nada. Em seu artigo, Satoshi citou várias tentativas importantes de implementar sistemas semelhantes, incluindo o b-money de Wei Dai e o Hashcash de Adam Back. A invenção do Bitcoin apoiou-se nos ombros de gigantes e, no entanto, foi profunda em sua simplicidade ao criar o primeiro sistema verdadeiramente descentralizado - isto é, que não está sob controle de uma pessoa - para emitir e transferir dinheiro digital.

## O Bitcoin resolve quais problemas?

Vamos detalhar algumas das postagens do Satoshi. Ao longo do livro, abordaremos como esses conceitos são realmente implementados. Não é importante que você entenda imediatamente todos os conceitos difíceis desta seção, mas você vai querer ver quais eram os objetivos do Satoshi, para que possamos almejá-los à medida que avançamos no exercício de *Inventar o Bitcoin*.

*Desenvolvi um novo sistema de e-cash P2P de código aberto*

O P2P significa ponto a ponto (*peer-to-peer*, no inglês) e indica um sistema onde uma pessoa pode interagir com outra sem intermediários, como sendo pares iguais. Você deve se lembrar das tecnologias de compartilhamento de arquivos P2P, como Napster, Kazaa e BitTorrent, que permitiam que as pessoas compartilhassem música sem baixá-las de um site. O Satoshi projetou o Bitcoin para permitir que as pessoas troquem *e-cash*, dinheiro eletrônico, sem passar por um intermediário da mesma maneira.

O software é de *código aberto*, o que significa que qualquer pessoa pode ver como funciona e contribuir para o projeto. Isso é importante porque elimina a exigência de confiança no próprio Satoshi. Não precisamos acreditar em nada que o Satoshi escreveu em sua postagem sobre como o software funciona. Podemos olhar o código e verificar como ele funciona nós mesmos. Melhor ainda, se não gostarmos de algo, podemos mudar.

*É totalmente descentralizado, sem servidor central ou partes confiáveis[. . . ]*

Satoshi menciona que o sistema é *descentralizado* para diferenciá-lo de sistemas que possuem controle central. As tentativas anteriores de criar um dinheiro digital como o DigiCash de David Chaum de 1989, eram apoiadas por um *servidor central*, um computador ou conjunto de computadores que era responsável pela emissão e verificação de pagamento, administrado por uma empresa.

Esses esquemas de emissão de dinheiro privado, controlados por uma entidade central, estavam fadados ao fracasso. As pessoas não podem contar com um dinheiro que pode ir embora quando a empresa fecha as portas, é hackeada, sofre uma falha no servidor ou, é fechada pelo governo.

A natureza descentralizada do Bitcoin traz de volta o conceito de dinheiro para o mundo digital: você pode transferi-lo sem falar com ninguém, sem pedir permissão, 24 horas por dia, 365 dias por ano, sem passar por nenhuma autoridade que exige confiança.

*. . . tudo é baseado em criptografia ao invés de confiança*

A internet e a maioria dos sistemas de computadores modernos são construídos em torno de criptografia, um método de obscurecer informação de tal maneira que apenas o receptor da informação possa decodificar ela. Como o Bitcoin se livra da exigência de *confiança*? Vamos nos aprofundar neste assunto nos próximos capítulos do livro, mas a ideia básica é que em vez de confiar em alguém que diz "Eu sou Ana"ou "Eu tenho R$10,00 em minha conta bancária", que significaria acreditar em sua palavra, podemos usar a criptografia matemática para declarar os mesmos fatos de uma forma que seja facilmente verificada pelo destinatário e impossível de ser forjada. Bitcoin usa criptografia matemática ao longo de todo seu projeto para permitir que participantes possam verificar o comportamento dos mesmos sem confiar em terceiros. Isso se tornaria a base do sistema do Bitcoin para provar a propriedade dos saldos, bem como fornecer segurança para a rede.

*Temos que confiar [nos bancos] nossa privacidade, confiar que não irão permitir que ladrões de identidade drenem nossas contas.*

Ao contrário de usar sua conta bancária, sistema de pagamento digital ou cartão de crédito, o Bitcoin permite que duas partes façam transações sem fornecer nenhuma informação de identificação pessoal.

Os repositórios centralizados de dados de consumidores armazenados em bancos, empresas de cartão de crédito, processadores de pagamentos e governos são chamarizes gigantescos para os hackers. Quase que para provar o ponto de Satoshi, a Equifax, foi imensamente comprometida em 2017, quando hackers conseguiram vazar as

identidades e dados financeiros de mais de 140 milhões de pessoas.

O Bitcoin separa as transações financeiras das identidades do mundo real. Afinal, quando damos dinheiro físico a alguém, ela não precisa saber quem somos, nem precisamos nos preocupar se, após essa troca, ela poderá usar algumas informações que demos para roubar o nosso dinheiro. Por que não devemos esperar o mesmo, ou coisa pior, quando usamos o dinheiro digital?

*O banco central deve ser confiável para não depreciar a moeda, mas a história das moedas fiduciárias está cheia de violações dessa confiança.*

*Fiat*, que em latim, significa "que seja feito", refere-se à moeda emitida pelo governo e pelo banco central que é decretada como curso legal pelo governo. Historicamente, o dinheiro era escolhido livremente pelos participantes do mercado entre coisas difíceis de serem produzidas, fáceis de serem verificadas e transportadas, como sal, conchas, pedras, prata e ouro. Toda vez que 'algo' era utilizado como dinheiro havia a tentação de criar mais dele. Se alguém viesse com tecnologia superior para rapidamente criar muitos de 'algo', esse 'algo' perdia valor. Era assim que Colonizadores europeus foram capazes de despir o continente africano de suas riquezas, trocando petecas de vidros, facilmente produzidos, por escravos humanos, dificilmente produzidos. Por isso que ouro foi considerado dinheiro por tanto tempo, era difícil de produzir mais dele rapidamente.

Lentamente, mudamos para uma economia mundial que usava o ouro como dinheiro para uma em que o papel passou a representar uma reivindicação desse metal

precioso. Eventualmente, o papel foi totalmente separado de qualquer respaldo físico com o pronunciamento do presidente Nixon, que acabou com a conversibilidade internacional do dólar americano em ouro em 1971.

O fim deste padrão permitiu que governos e bancos centrais aumentassem a oferta de dinheiro à vontade, diluindo o valor de cada nota em circulação, conhecida como *depreciação*. Embora apoiada pelo governo e impossível de ser resgatável por algo palpável, a moeda puramente fiduciária é o dinheiro que todos conhecemos e usamos no dia a dia, na verdade é um conceito relativamente novo, com menos de um século de vida.

Confiamos que nossos governos não abusarão de suas impressoras, mas não precisamos ir muito longe na história em busca de exemplos de *violação dessa confiança*. Em regimes autocráticos e de planejamento central, em que o governo tem a posse direta da máquina de impressão de dinheiro, como a Venezuela, a moeda perdeu quase todo o seu valor. O bolívar venezuelano passou de 2 bolívar por dólar em 2009 para 250.000 bolívar por dólar em 2019. No momento em que escrevo este livro, a Venezuela está em processo de colapso devido à terrível má gestão de sua economia por seu governo.

Em contraste com a moeda *fiduciária* emitida centralmente, cuja oferta não pode ser prevista, a fim de evitar a *depreciação*, Satoshi projetou um sistema de dinheiro em que a oferta era fixa e emitida a uma taxa previsível e imutável. Haverá apenas 21 milhões de bitcoins, embora cada um possa ser dividido em 100 milhões de unidades, chamadas de satoshis, produzindo um total de 2.1 quadrilhões de satoshis em circulação ate o ano de 2140.

Antes do Bitcoin, os ativos digitais não eram escassos.

É fácil copiar um livro digital, arquivo de áudio ou vídeo e enviá-lo a um amigo. As únicas exceções são os ativos digitais controlados por intermediários. Por exemplo, ao alugar um filme no iTunes, você pode assisti-lo em seu dispositivo apenas porque o iTunes controla a entrega do filme e pode interrompê-lo após o término do período de locação. Da mesma forma, seu dinheiro digital é controlado pelo seu banco. É função do banco manter um registro de quanto dinheiro você possui e, se você transferi-lo para outra pessoa, ele pode autorizar ou negar essa transferência.

O Bitcoin é a primeira rede digital que impõe escassez sem intermediários e é o primeiro ativo conhecido pela humanidade cujo fornecimento inalterável e cronograma de emissão são conhecidos com antecedência. Nem mesmo metais preciosos como o ouro têm essa propriedade, uma vez que sempre podemos minerar mais e mais depósitos de ouro a uma taxa imprevisível, se for lucrativo fazê-lo. Imagina encontrar um asteroide contendo dez vezes mais ouro que nossas reservas no planeta, o que aconteceria com o preço do ouro dado uma oferta tão abundante. Bitcoin é imune a tais descobertas e manipulações de demanda. É simplesmente impossível de produzir mais dele. Veremos como isso é aplicado nos próximos capítulos.

A natureza da dinheiro e o funcionamento do sistema monetário atual são intrínsecos, e neste livro não serão detalhados em profundidade adequada. Caso queiras aprender mais sobre tais fundamentos do dinheiro e como eles se aplicam ao Bitcoin recomendo a leitura do livro *O Padrão Bitcoin* por Saifedean Ammous, como ponto de partida

*Os dados podiam ser protegidos de uma forma fisicamente impossível para outras pessoas acessarem, não importando o motivo, quão boa a desculpa, não importando nada[...] É hora de termos o mesmo no nosso dinheiro.*

Nossos sistemas atuais de proteção de dinheiro, como quando fazemos um depósito em um banco, dependem de confiar em outra pessoa para fazer o trabalho. Confiar em tal intermediário não requer apenas confiança de que eles não farão algo malicioso ou tolo, e que os hackers não irão roubá-lo, mas também que o governo não confiscará ou congelará os fundos. No entanto, foi demonstrado em todo o mundo, repetidamente, que os governos podem e suprimem o acesso ao dinheiro quando se sentem ameaçados.

Pode parecer bobagem para alguém que mora nos Estados Unidos, ou em outra economia altamente regulamentada, pensar em acordar e ter seu dinheiro confiscado. Ocorreu algo parecido comigo, quando tive meus fundos congelados pelo PayPal simplesmente porque não usava minha conta há meses. Levei mais de uma semana para recuperar o acesso ao "meu" dinheiro. Tenho sorte de morar nos Estados Unidos, um dos poucos países onde pelo menos poderia esperar obter algum alívio legal se o PayPal congelasse meus fundos, e onde tenho a confiança básica de que meu governo e meu banco não roubarão meu dinheiro.

Coisas muito piores aconteceram e estão acontecendo atualmente em países com menos liberdade, como bancos sendo fechados durante colapsos da moeda na Grécia, bancos em Chipre usando depósitos para roubar fundos de seus clientes ou o governo declarando certas notas como sendo sem valor de um dia para o outro, como na

Índia, privando as pessoas de sua riqueza, causando corridas em caixas eletrônicos e pessoas morrendo de fome devido à incapacidade de acessar seu capital.

A antiga URSS, onde cresci, tinha uma economia fortemente controlada de modo centralizado, levando a uma escassez massiva de bens. Quando queríamos sair, só podíamos trocar uma quantia limitada de dinheiro por pessoa sob uma taxa de câmbio oficial, controlada pelo governo, que era amplamente desconectada da verdadeira taxa de livre mercado. Efetivamente assim o governou tirou de nos a pouca riqueza q tínhamos através de um controle rígido da economia e movimentos de capitais.

Quando as economias começam a falhar em países autocráticos, elas tendem a implementar controles econômicos rígidos, impedindo as pessoas de sacar seu dinheiro dos bancos, carregá-lo para fora do país ou trocá-lo por moedas que ainda possuem valor, como o dólar americano no livre mercado. Isso da carta branca ao governo para implementar experimentos econômicos insanos como por exemplo o sistema socialista da URSS.

O Bitcoin fornece um sistema de segurança que não depende da confiança de terceiros para proteger o seu dinheiro. Em vez disso, o Bitcoin torna suas moedas *impossíveis de serem acessadas por outros* sem uma chave especial que só você possui, *não importa por que razão, não importa quão boa seja a desculpa, não importa o quê façam.* Possuindo Bitcoin, você possui a chave para sua liberdade financeira. Bitcoin separa dinheiro do estado.

*A solução do Bitcoin é usar uma rede ponto a ponto para verificar se há gastos duplos[...] como um servidor de carimbo de data/hora distribuído, carimbando a primeira transação para gastar uma moeda.*

Uma rede simplesmente se refere à ideia de que vários computadores estão conectados e podem enviar mensagens uns aos outros. A palavra distribuído significa que não há uma entidade central controladora, mas que todos os participantes se coordenam para tornar a rede bem-sucedida.

Em um sistema sem controle central, é importante saber que ninguém está trapaceando. A ideia de *gasto duplo* refere-se à capacidade de gastar o mesmo dinheiro duas vezes. Isso não é um problema com dinheiro físico pois ele sai da sua mão quando o utiliza. Entretanto, transições digitais podem ser copiadas, de maneira similar a musicas ou filmes. Quando movimentas dinheiro através de um banco, o banco garante que o dinheiro não sera movido duas vezes. Em um sistema sem entidade central é necessário encontrar uma maneira de impedir o gasto duplo que na pratica é a mesma coisa que forjar dinheiro.

Satoshi está descrevendo que os participantes da rede Bitcoin trabalham juntos para *marcar o tempo* (colocar em ordem) as transações para que saibamos o que aconteceu primeiro, a fim de evitar que seja possível forjar o dinheiro de maneira digital. Nos próximos capítulos, construiremos esse sistema do zero. Isso nos permitirá detectar falsificações sem depender de nenhum emissor central ou validador de transações.

Bitoin não foi uma invenção do dia para a noite, em seu artigo Satoshi cita diversas tentativas importantes de implementar sistemas similares ao Bitcoin, incluindo o b-money do Wei Dai e o Hashcash do Adam Back. A invenção do Bitcoin foi realizada sobre os ombros de gigantes, mas ninguém ate então havia juntado todas as peças corretas, criando o então primeiro sistemas de criação e transferência de dinheiro digital verdadeiramente

escasso, sem a necessidade de um controle central.

A invenção do Bitcoin resolveu uma série de problemas técnicos interessantes relacionados a privacidade, degradação e controle central nos sistemas monetários atuais. Alguns deles são:

1. Como criar uma rede ponto a ponto na qual qualquer pessoa pode ingressar e participar voluntariamente;

2. Como um grupo de pessoas que não precisam revelar suas identidades ou confiar umas nas outras pode manter uma contabilidade compartilhada de valores, mesmo que algumas delas sejam desonestas;

3. Como criar uma verdadeira escassez digital sem um intermediário;

4. Como criar um ativo digital que não seja forjável e seja verificável instantaneamente e resistente a roubo e hacking.

Quando Bitcoin foi lançado apenas um punhado de pessoas utilizavam e rodavam um *node* do software Bitcoin nos seus computadores para alimentar a rede Bitcoin. A grande maioria das pessoas da época pensavam que era uma piada, ou que o sistema iria apresentar serias falhas de projeto que o fariam não funcional.

Com a passagem do tempo mais pessoas se juntaram a rede, utilizando seus computadores a rede se tornou mais segura e reforçando que rede tinha valor ao trocar outras moedas por ela, ou bens e serviços. Hoje dez anos depois a rede é utilizada por milhões de pessoas com dezenas a

centenas de milhares de *nodes* rodando o software gratuito do Bitcoin, que foi desenvolvido por centenas de voluntários e empresas ao redor do mundo.

Vamos descobrir como podemos construir este sistema!

# 2 Removendo o intermediário

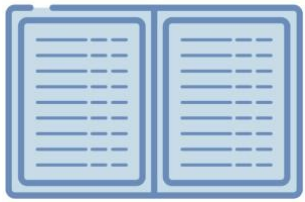
No capítulo anterior, comentamos que o Bitcoin fornece um sistema ponto a ponto para a transferência de valor. Antes de nos aprofundarmos em como isso funciona, vamos primeiro entender como um banco tradicional ou empresa de pagamento lida com o rastreamento da propriedade e das transferências de ativos.

## Os bancos são apenas livros contábeis

Como funciona um pagamento digital feito por seu banco, PayPal ou ApplePay? Muito simples, essas entidades intermediárias atuam como um livro-razão de contas e transferências glorificado.

O proposito de um banco é armazenar seus depósitos e guardar-los. Porem depósitos hoje em dia são primariamente eletrônicos em vez de papeis ou moedas. Então o trabalho de um banco é manter e guardar esse banco de dados bancários. visto que a informação é eletrônica, os seguranças são majoritariamente eletrônicos. Bancos utilizam softwares que detectam intrusos, fazem backups contra perda de informação e fazem auditorias com terceiros para ter certeza que seus processos internos não estão comprometidos, além de seguros para se protegerem caso algo de errado nesse processo.

Neste exemplo, vamos utilizar a expressão *banco*, mas queremos dizer realmente qualquer outra entidade que processa pagamentos. Começamos com um livro-razão de



*Livro-razão*

contas que mostra que Ana e Bruno depositaram dinheiro no banco.

**Livro razão do banco**

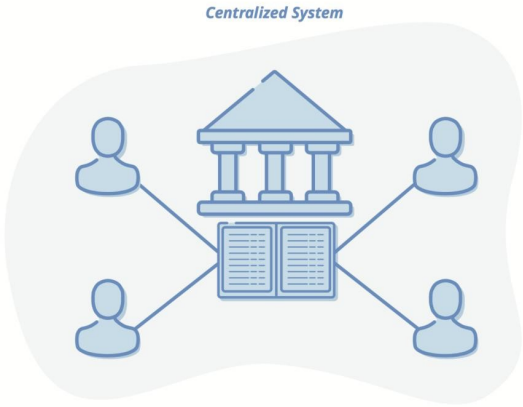
1. Ana: Crédito por depósito em dinheiro $+R\$2,00$
2. Bruno: Crédito por depósito em dinheiro $+R\$10,00$

Quando Ana deseja enviar $R\$2,00$ para Bruno, ela liga para seu banco ou usa o *internet banking* ou um aplicativo disponibilizado pela empresa, autentica-se usando um nome de usuário e senha ou um código PIN e, em seguida, faz a solicitação de transferência. O banco, então, registra em seu livro-razão.

**Livro razão do banco**

1. Ana: Crédito para depósito em dinheiro $+R\$2,00$
2. Bruno: Crédito para depósito em dinheiro $+R\$10,00$
3. Ana: Débito $-R\$2,00$
4. Bruno: Crédito $+R\$2,00$

Portanto, o banco registrou os novos débitos e créditos e agora o dinheiro foi movido de uma conta para outra. Simples!




*Sistema centralizado*

## O problema de gasto duplo

O que acontecerá se Ana tentar gastar esses dois dólares novamente? Isso é chamado de problema de gasto duplo. Ela envia a solicitação para o banco, mas o banco diz "Desculpe, vemos que você já gastou R$2,00 para pagar Bruno, você não tem mais dinheiro para enviar".

Quando você tem uma autoridade central como um banco, é muito fácil para ele dizer que você está tentando gastar um dinheiro que já gastou. Isso porque eles são os únicos que podem modificar o livro-razão e têm processos internos, incluindo sistemas de backup e auditorias feitas por computadores e seres humanos para se certificar de que está correto e nada foi adulterado.

Chamamos isso de *sistema centralizado* porque possui um único ponto de controle.

### Vamos descentralizar o livro razão

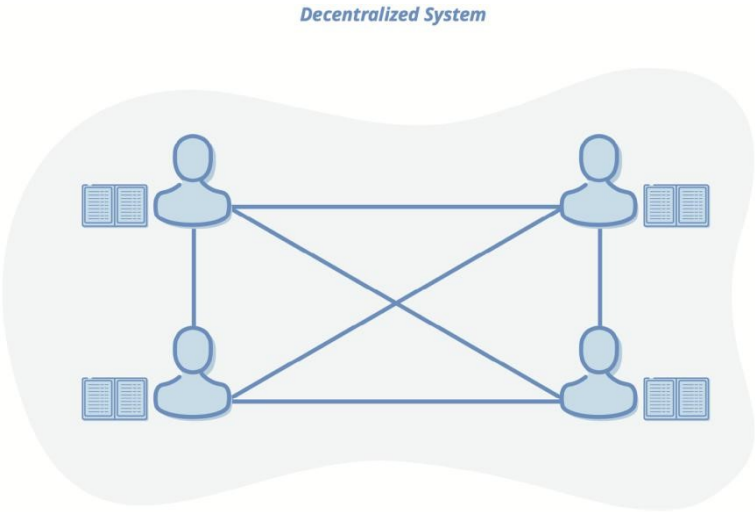
O primeiro problema que o Bitcoin visa resolver é a remoção de um intermediário confiável criando um sistema *ponto a ponto*. Vamos imaginar que os bancos desapareceram e precisamos recriar nosso sistema financeiro. Mas desta vez, não vamos ter um ente central. Como podemos manter um livro-razão sem nenhum centralizador?

Se não temos um guardião do livro-razão, precisaremos que o livro-razão pertença ao povo. *Vive la révolution.* É assim que fazemos.

Primeiro, vários nos reunimos e criamos uma *rede*. Isso apenas significa que temos um jeito de conversar uns com os outros. Digamos que trocamos números de telefone ou contas de Snapchat. Quando Ana quiser enviar dinheiro para Bruno, ao invés de ligar para o banco, ela vai no Snapchat de todos os seus amigos e diz a eles: "Estou enviando R$2,00 para Bruno". Todos a reconhecem, respondendo "Legal, entendemos!", e escrevem em suas cópias do livro-razão. A imagem agora tem a seguinte aparência:

Portanto, ao invés de um único banco, temos uma cópia do livro-razão nas mãos de todos. Sempre que alguém quer gastar o dinheiro, basta ligar ou fazer um snapchat a todos os seus amigos e informá-los de que isso está acontecendo. Todos registrarão as transações. Como o livro-razão não está mais em apenas um lugar, nós o chamamos de *distribuído* e, como nenhum ente centralizado é responsável, o chamamos de *descentralizado*. Isso resolve o problema do intermediário confiável

Agora que não temos intermediário, como isso resolve o problema do gasto duplo? Quem devemos consultar invés do banco para verificar se dinheiro já foi gasto ou não? Bem, uma vez que todos possuem uma cópia do




*Sistema descentralizado*

livro-razão, todos devem ser consultados. Esse sistema é conhecido como sistema baseado com consentimento porque ele precisa que todos concordem com uma versão particular da verdade.

se Ana tentar gastar novamente os R$2,00 que ela já enviou para Bruno, sua transação será rejeitada por todos na rede, já que eles consultariam seus livros-razão e diriam a ela que de acordo com seus registros, ela já gastou o dinheiro. Portanto, eles não iriam registrar sua segunda tentativa de gastar o dinheiro. Agora temos uma rede ponto a ponto para registrar propriedade e transferências de fundos.

Este sistema funciona muito bem entre um grupo de amigos que têm motivos sociais para não enganar uns aos outros, mas isso não se aplica quando as redes possuem milhões de pessoas. À medida que mais e mais pessoas começam a usar o sistema, há um incentivo para trapa-

cear para obter dinheiro extra no livro-razão.

Como mantemos todos honestos?

## O ataque de gastos duplos

Se eu for a Ana, posso *conspirar* com algumas das outras pessoas e dizer a elas: "Quando eu gastar o meu dinheiro, não escreva em seus livros. Finja que essa transação nunca aconteceu". Veja como Ana pode realizar um ataque de gasto duplo.

Começando com um saldo de $R\$2,00$, Ana faz o seguinte:

1. Ela manda seus $R\$2,00$ para Bruno, para comprar uma barra de chocolate. Agora ela deve ter $R\$0,00$ sobrando;

2. Danilo, Evandro e Fernanda estão conspirando com Ana e não registram a sua transação para Bruno em seus livros. Em sua cópia, Ana nunca gastou seu dinheiro;

3. Carol é uma honesta guardiã do livro-razão. Ela anota a transação de Ana para Bruno. Em seu livro-razão, Ana tem $R\$0,00$;

4. Henrique estava de férias por uma semana e não ouviu falar de nenhuma dessas transações. Ele se junta à rede e pede uma cópia do livro-razão;

5. Henrique obtém 4 cópias falsas (Danilo, Evandro, Fernanda, Ana) e uma cópia honesta (Carol). Como ele determina qual é a real? Sem um sistema melhor, ele busca a maioria dos votos e é enganado ao aceitar o livro-razão falso como sendo o correto;

6. Ana compra uma barra de chocolate de Henrique usando os $R\$2,00$ que ela realmente não tem. Henrique aceita porque, pelo que sabe, Ana ainda tem $R\$2,00$ em sua conta (de acordo com o livro-razão que ele obteve de todos os outros;

7. Ana agora tem 2 barras de chocolate e $R\$4,00$ de dinheiro falso foram criados no sistema. Ela paga seus amigos em barras de chocolate, e eles repetem o ataque 100 vezes a cada nova pessoa que entra na rede;

8. Agora, Ana tem todas as barras de chocolate e todos os outros estão segurando grandes quantias de dinheiro falso;

9. Quando eles tentam gastar o dinheiro que Ana supostamente enviou para eles, Danilo, Evandro e Fernanda que controlam a maioria da rede, rejeitam esses gastos porque sabem que o dinheiro é falso desde o começo.

Nós temos um problema. Isso é chamado de *falha de consenso*. As pessoas na rede não chegaram a um consenso sobre qual é o estado real. Não tendo um sistema melhor, eles seguiram a regra da maioria, o que levou a pessoas desonestas controlando a rede e gastando dinheiro que não tinham.

Se quisermos fazer um sistema *sem permissão* onde qualquer um pode participar sem pedir, então ele também deve ser resiliente a usuários desonestos.

## Resolvendo o problema de consenso distribuído

Agora vamos resolver um dos problemas mais difíceis da ciência da computação: consenso distribuído entre as partes, onde alguns são desonestos ou não confiáveis. Este problema é conhecido como Problema dos Generais Bizantinos e é a chave que Satoshi Nakamoto usou para criar a invenção do Bitcoin. Vamos começar de forma simples.

Precisamos fazer com que várias pessoas concordem com os dados do livro-razão sem saber se os responsáveis pelo livro-razão têm anotado todas as transações de maneira correta e honesta.

Uma solução ingênua é simplesmente nomear os representantes honestos do livro-razão. Em vez de todos começarem a escrever nele, escolhemos um punhado de amigos como Carol, Giovana, Fernanda e Zélia para fazer isso, porque eles não mentem e todo mundo sabe que nunca vão para as festas nos fins de semana.

Então, toda vez que temos que fazer uma transação, em vez de contar a todos os nossos amigos, apenas ligamos para Carol e a sua gangue. Eles ficam felizes em manter o livro-razão para nós por uma pequena taxa. Depois de escreverem no livro-razão, eles ligam para todos os outros e informam sobre as novas linhas incluídas, que todos ainda mantêm como backup.

Este sistema funciona muito bem, exceto que um dia, agentes do governo aparecem e querem saber quem está administrando este sistema financeiro paralelo. Eles prendem a Carol e seus amigos e os levam embora, pondo fim ao livro-razão distribuído. Todos nós temos backups não confiáveis, não podemos confiar uns nos outros e não po-

demos descobrir de quem é o backup que deve ser usado para iniciar um novo sistema.

Em vez de um fechamento total, o governo também pode ameaçar discretamente os responsáveis pelo registro com pena de prisão se eles aceitarem as transações da Ana (que é suspeita de vender drogas). O sistema agora está efetivamente sob controle central e não podemos mais dizer que ele não tem permissão.

E se tentarmos a democracia? Vamos encontrar um grupo de 50 pessoas honestas e realizaremos eleições todos os dias para manter a rotação de quem escreve no livro-razão. Todos na rede têm direito a voto.

Este sistema funciona muito bem até que as pessoas apareçam e usem violência ou coerção financeira para alcançar os mesmos objetivos de antes:

1. Forçar o eleitorado a votar nos contadores de sua escolha;

2. Forçar os detentores do livro-razão eleitos a escreverem lançamentos falsos nele.

Nós temos um problema. Sempre que designamos pessoas específicas para manter o livro-razão, devemos confiar que elas são honestas, e não temos como defendê-las de serem coagidas por alguém a cometer atos desonestos e corromper nosso livro-razão.

## Identidade equivocada e ataques Sybil

Até agora, examinamos dois métodos fracassados de garantir a honestidade: um usava contadores específicos e conhecidos e o outro usava contadores eleitos e rotativos.

A falha de ambos os sistemas foi que a base de nossa confiança estava ligada à identidade do mundo real: ainda tínhamos que identificar especificamente os indivíduos que seriam responsáveis por nosso livro-razão.

Sempre que assumimos confiança com base na identidade, nos abrimos para algo chamado *Ataque Sybil*. Este é basicamente um nome chique para personificação; tem o nome de uma mulher com transtorno de personalidade múltipla.

Você já recebeu uma mensagem estranha de um de seus amigos apenas para descobrir que o telefone dele havia sido pego pelo irmão? Quando se trata de bilhões ou mesmo trilhões de dólares em jogo, as pessoas justificam todo tipo de violência para roubar aquele telefone e enviar aquela mensagem. É fundamental evitarmos que as pessoas que mantêm nosso livro-razão sejam coagidas de alguma forma. Como podemos fazer isso?

## Vamos construir uma loteria

Se não queremos a possibilidade de pessoas serem comprometidas por ameaças de violência ou suborno, precisamos de um sistema com tantos participantes que seria impraticável para alguém coagi-los. Deve ser o caso de que qualquer pessoa possa participar de nosso sistema, e que não tenhamos que introduzir nenhum tipo de votação, que está sujeita à coerção pela violência e compra de votos.

E se fizéssemos uma loteria onde escolheríamos alguém aleatoriamente sempre que quiséssemos escrever no livro-

razão? Aqui está nosso primeiro rascunho deste design:

1. Qualquer pessoa no mundo pode participar. Dezenas de milhares de pessoas podem aderir à nossa rede de loteria de contadores;

2. Quando queremos enviar dinheiro, anunciamos para toda a rede as transações que pretendemos realizar, tal como o fizemos anteriormente;

3. Invés de todas as pessoas anotarem a transação, fazemos uma loteria para ver quem ganha o direito de adicionar as transações no livro razão.

4. Quando selecionamos um vencedor, essa pessoa escreve todas as transações sobre as quais acabou de ouvir no livro razão;

5. Se a pessoa gravar transações válidas (conforme considerado por todos os outros participantes da rede) no livro-razão, ela receberá uma taxa;

6. Todos mantêm uma cópia do livro-razão, adicionando as informações que o último ganhador da loteria produziu;

7. Usamos o intervalo de dez minutos para garantir que a maioria das pessoas tenha tempo para atualizar seus livros contábeis entre os sorteios da loteria.

Este sistema é uma melhoria. É impraticável comprometer os participantes deste sistema porque é impossível saber quem são os participantes e qual será o próximo vencedor.

Porem, não temos uma clara resposta para como administrar uma loteria sem alguém no comando, ou por

que deveríamos confiar que o vencedor da loteria irá agir honestamente quando for escrever no livro-razão. Vamos descobrir como solucionar isso a seguir.

# 3 Prova de Trabalho

Este sistema de loteria, conforme projetado, tem dois problemas principais:

1. Quem vai vender os bilhetes da loteria e escolher os números vencedores, se já determinamos que não podemos ter nenhum tipo de centralização que possa comprometer sua administração?

2. Como podemos garantir que o vencedor da loteria realmente registre boas transações no livro-razão, ao invés de tentar enganar o resto de nós?

Se quisermos um sistema *sem permissão* ao qual qualquer pessoa possa ingressar, temos que remover o requisito de confiança do sistema deixando-o totalmente *sem necessidade de confiança*. Temos que criar um sistema que tenha as seguintes propriedades:

1. Deve ser possível para todos os integrantes gerar seus próprios bilhetes de loteria, uma vez que não podemos confiar em uma autoridade central;

2. Precisamos de alguma maneira para que haja custo ao gerar um bilhete, assim evitando que alguém possa monopolizar a loteria gerando um numero alto de bilhetes de graça. Como fazemos que uma possa precise gastar dinheiro para gerar um bilhete quando não há de quem comprar o bilhete? Faremos você comprar o bilhete do universo, queimando energia, um recurso custoso;

3. Deve ser fácil para todos os outros participantes verificar se você ganhou na loteria apenas examinando seu bilhete, uma vez que não podemos confiar em ninguém para manter um registro da combinação vencedora, se ao invés disso, combinamos com antecedência uma faixa de valores se seu bilhete estiver dentro dessa faixa você ganha a loteria, usaremos uma ferramenta criptográfica chamada 'função Hash' para fazer isso;

Vamos falar de todos eles, um de cada vez. A explicação completa de como essa loteria funciona é provavelmente a coisa mais difícil de entender no Bitcoin, então vamos dedicar os próximos três capítulos para cobrir a solução em profundidade.

Sistemas de loteria centralizados padrão como Megasena são executados por alguém gerando um conjunto aleatório de números e um monte de bilhetes com números aleatórios neles. Normalmente, apenas um jogo possui os números que correspondem exatamente ao número aleatório secreto conhecido apenas pela organização que administra a Megasena. Uma vez que não podemos confiar na autoridade central, devemos permitir que qualquer um gere seus próprios números aleatórios.

Como iremos verificar o vencedor? Na Megasena, os proprietários da loteria conhecem a combinação vencedora. Já que não podemos ter isso em um sistema descentralizado, podemos então, criar um sistema onde todos possam concordar em uma faixa de números com antecedência, e se o seu número aleatório cair dentro da faixa, você ganha na loteria. Usaremos um truque criptográfico chamado função hash, para fazer isso. Vamos mergulhar em uma leve introdução a como usar o hash no próximo capítulo.

Finalmente, devemos encontrar uma maneira de puni-lo se você trapacear. Gerar números aleatórios, ou seja, bilhetes de loteria, é basicamente gratuito. Como fazemos para que você realmente tenha que gastar dinheiro para comprar bilhetes quando não há ninguém para vendê-los? Faremos você comprá-los do universo, gastando energia, um recurso escasso que não pode ser criado do nada. Isso será abordado no Capítulo 5.

## Prova de trabalho: um quebra-cabeça assimétrico com uso intensivo de energia

A solução para esses três problemas é chamada de Prova de Trabalho. Na verdade, foi inventado muito antes do Bitcoin, mais precisamente, em 1993.

Precisamos tornar caro a "compra de bilhetes" para a loteria, caso contrário, as pessoas poderiam gerar um número ilimitado de bilhetes. O que é algo comprovadamente caro, mas isso não precisaria vir de nenhuma autoridade central?

Eu mencionei a física no início do livro, e é aqui que a física joga com o Bitcoin: a primeira lei da termodinâmica diz que a energia não pode ser criada nem destruída. Em outras palavras, não existe almoço grátis quando se trata de energia. A eletricidade é sempre cara porque é um recurso escasso que custa dinheiro real. Você tem que comprá-la dos produtores de energia ou operar sua própria usina. Em qualquer caso, você não pode obter algo do nada.

O conceito por trás da Prova de Trabalho é que você participa de um processo aleatório, semelhante a lançar um dado. Mas, em vez de um dado de seis lados, este tem tantos lados quanto a quantidade de átomos que existem

no universo. Para lançar o dado e gerar números de loteria, seu computador deve realizar várias operações, que custam em termos de eletricidade.

Para ganhar na loteria, você deve produzir um número especial que é matematicamente derivado das transações que deseja gravar no livro-razão, mais um número aleatório (explicaremos os detalhes de como isso funciona no próximo capítulo).

Para encontrar esse número vencedor, você pode ter que rolar esse dado bilhões, trilhões ou quatrilhões de vezes, queimando centenas ou milhares de dólares em energia. Como o processo é baseado na aleatoriedade, é possível que todos gerem seus próprios bilhetes de loteria sem uma autoridade central, usando basicamente apenas um número aleatório que pode ser gerado por um software ou hardware e uma lista de transações que desejam gravar no livro-razão.

Agora, embora possa ter levado milhares de dólares para utilizar energia suficiente para encontrar o número aleatório correto, para que todos os outros na rede validem que você é um vencedor, eles precisam realizar algumas verificações básicas:

1. O número que você forneceu é menor ou maior do que o limite mágico com o qual todos concordaram?

2. O número é de fato derivado matematicamente de um conjunto válido de transações que você deseja gravar no livro-razão?

3. As transações que vocês esta registrando são validas perante as regras do Bitcoin: sem gasto duplo, não gerando novos Bitcoin além do previsto e etc.

Prova de trabalho é um processo aleatório que requer

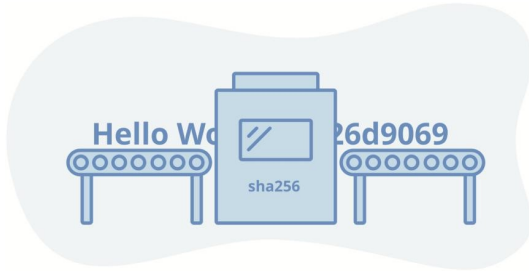
muitas computações para achar o numero vencedor. Entretanto requer apenas uma única operação para verificar esta solução. Pense nele como palavras cruzadas ou sudoku. Pode demorar muito tempo para achar uma solução, mas dado as solução é de rápida verificação. Isso torna o sistema de Prova de Trabalho *assimétrico*: é muito difícil de gerar, mas muito fácil de ser validado.

Como você consumiu uma quantidade considerável de energia, e por sua vez, dinheiro jogando na loteria, deseja que todos aceitem o seu bilhete de loteria premiado. Portanto, você é incentivado a se comportar bem escrevendo apenas transações válidas no livro-razão.

Se você, por exemplo, tentar gastar um dinheiro que já foi gasto, então seu bilhete de loteria "vencedor"será rejeitado por todos os outros, e você perderá todo o dinheiro que gastou comprando a energia para criar o bilhete. Por outro lado, se você escrever transações válidas no livro-razão, iremos recompensá-lo em bitcoin para que você possa pagar suas contas de energia e ainda ter algum lucro.

O sistema de Prova de Trabalho tem a importante propriedade de ser *caro no mundo real*. Assim, se você quisesse atacar a rede coagindo alguns de seus participantes, não só teria que vir à casa deles e assumir o hardware, mas também pagar suas contas de luz.

Antes de podermos discutir como a Prova de Trabalho é validada, precisaremos de uma introdução rápida em Ciência da Computação sobre dois conceitos: bits e criação de hash.




*Fazendo o hash de um string*

## Criando um Hash

O quebra-cabeça de Prova de Trabalho assimétrico do Bitcoin envolve o uso de uma função hash. Da álgebra básica, sabemos que uma função é uma caixa onde você *insere* um valor de entrada $x$ e obtém um valor de saída $f(x)$. Por exemplo, a função $f(x)=2x$ pega um valor e o multiplica por dois. Portanto, a entrada $x=2$ nos dá a *saída* $f(x)=4$.

Uma função hash é uma função especial, onde você insere qualquer sequência de letras, números ou outros dados, como “Olá, mundo”, e obtém um número gigante que parece algo totalmente aleatório:

> 111181171325821924266132935775749045845 5
> 489044664361600112658434663354150209 5

A função hash particular usada acima na string "Hello, World"é chamada de sha256 e, por acaso, é a que o Bitcoin usa.

A função hash sha256 tem as seguintes propriedades que são úteis para nós:

1. A saída é determinística: você sempre obtém a mesma saída para a mesma entrada;

2. A saída é imprevisível: alterar apenas uma letra ou adicionar um espaço à string de entrada mudará drasticamente a saída, tanto que você não pode encontrar nenhuma correlação com os dados de entrada original;

3. É rápido calcular o hash para dados de entrada de qualquer tamanho;

4. É impossível encontrar duas strings que geram hash para a mesma saída;

5. Dado o hash de saída de sha256, é impossível retornar à string de entrada. Chamamos isso de função unilateral;

6. A saída é sempre um tamanho específico (256 bits para sha256).

## Uma introdução rápida sobre bits

O sistema numérico que você conhece e adora, composto dos números de 0 a 9, é chamado de *decimal* porque possui dez dígitos. Os computadores, por outro lado, preferem um sistema numérico diferente, feito de uns e zeros, indicando a presença ou ausência de um sinal elétrico. Este sistema numérico é chamado de *binário*.

No sistema decimal, você usa apenas os dígitos de 0 a 9. Se você usar apenas um dígito, poderá representar dez números diferentes, de 0 a 9. Se usar dois dígitos, poderá representar 10x10=100 números diferentes: 00, 01,... a 99. Para três dígitos, você pode ter 10x10x10=1000 números: 000, 001,... a 999.

Espero que você esteja começando a ver um padrão. Para descobrir o tamanho de um número que podemos representar com N dígitos, multiplicamos dez por ele mesmo N vezes. Em outras palavras, $10^N$, ou 10 elevado à potência de N.

O binário funciona da mesma maneira. A única coisa que muda é o número de dígitos que estão disponíveis para nós. Embora estejamos acostumados com decimais com dez dígitos, um *dígito binário* ou *bit* só pode ter dois valores: zero e um.

Se 1 bit pode representar dois valores, então dois bits podem representar 4 valores: 00, 01, 10, 11. Você pode calcular isso multiplicando 2x2, pois cada dígito pode ter dois valores.

Três bits podem representar 2 x 2 x 2 = $2^3$ = 8 valores, que são 000, 001, 010, 011, 100, 101, 110, 111.

Portanto, um número *binário* de N *bits* pode ser representado como $2^N$ valores diferentes.

Portanto, o número de valores exclusivos que você pode representar com 256 bits, o tamanho da função de hashing sha256, é $2^{256}$. Esse é um número gigante, quase inconcebível para a mente humana. Representado em decimal, esse número tem 78 dígitos. Para colocar isso em perspectiva, isso é mais ou menos o número estimado de átomos em todo o universo conhecido.

$$\begin{aligned} 2^{256} =& 115.792.089.237.316.195.423.570.985.008. \\ & 687.907.853.269.984.665.640.564.039.457. \\ & 584.007.913.129.639.936 \end{aligned} \tag{3.1}$$

Este é o número de saídas possíveis quando você faz o hash de qualquer string com a função de hash sha256.

Portanto, é efetivamente impossível prever como será o número produzido por essa função. Seria como prever 256 jogadas de moeda em sequência ou adivinhar a localização de um átomo específico que escolhi em algum lugar do universo.

Este número é muito longo para continuar escrevendo, então diremos apenas $2^{256}$ de agora em diante, mas espero que isso acione uma imagem mental de um universo de possibilidades para você.

## Vamos transformar algumas strings em hash

Aqui estão algumas strings de exemplo e seus hashes sha256. O resultado está em números decimais, embora dentro de um computador eles apareceriam como uma sequência binária de uns e zeros.

O objetivo aqui é demonstrar como o número muda drasticamente com base em uma pequena mudança na string de entrada. Você não pode prever a saída produzida pela função hash com base no que você colocou nela:

"Hello World!"
52740724284578854442640185928423074974
81806529570658746454048816174655413720

"Hello World!!"
95863319874939535731602344194643497258 3
74513872780665335270495834770720452323

Não há como ninguém, nem mesmo um computador, olhar para o número de aparência aleatória resultante e

descobrir a string que o criou. Se você quiser brincar com o sha256, há alguns sites online onde você pode experimentar fazer o hash de qualquer informação que desejar. por exemplo `https://passwordsgenerator.net/sha256-hash-generator/`

## Criando um hash para ganhar na loteria de prova de trabalho

Tudo bem, agora estamos prontos para falar sobre a parte chave da magia. Dissemos que há $2^{256}$ valores de saída de sha256 possíveis no total. Para tornar mais fácil de entender, vamos fingir que há apenas um total de 1000 saídas hash possíveis.

O nosso sistema de loteria funciona assim:

1. Ana anuncia que deseja enviar R$2,00 para Bruno;

2. Todo mundo que quer tentar a sorte na loteria pega esta transação "Ana envia R$2,00 para Bruno", adicionando um número aleatório chamado *nonce* (número usado apenas uma vez) no final. Isso é para ter certeza de que a string que eles estão fazendo o hash é diferente de qualquer outra pessoa, ajudando-os a encontrar um número vencedor na loteria;

3. Se esse número for menor do que o *Número Alvo* (veremos isso em um segundo), eles ganham na loteria;

4. Se o número que eles obtiverem for maior do que o número alvo, eles tentam fazer o hash novamente, adicionando nonces aleatórios: "Ana envia R$2,00 para Bruno com nonce = 12345", "Ana envia R$2,00

para Bruno com nonce = 92435", "Ana envia R$2,00 para Bruno nonce = 132849012348092134" e assim por diante, até que o número hash resultante seja menor que o *Número Alvo*.

Pode levar muitas, muitas tentativas para encontrar um hash que seja menor que o número alvo. Portanto, a ideia aqui é esta: se houver 1000 hashes possíveis e definirmos o número alvo como 100, qual porcentagem de hashes está abaixo do alvo?

Esta é a matemática básica: de 1000 números possíveis, de zero a 999, existem 100 números que são menores que 100 e 900 números que são maiores. Portanto, 100/1000 ou 10% dos hashes são menores que o destino. Então, se você fizer um hash com qualquer string e sua função hash produzir 1000 saídas diferentes, você espera obter um hash abaixo do alvo limitado a 100, cerca de 10% do tempo.

É assim que a loteria funciona: nós definimos um *alvo* e todos concordamos com ele (falaremos sobre como isso funciona em breve). Então, pegamos as transações sobre as quais as pessoas estão nos contando e fazemos o hash, adicionando um nonce aleatório no final. Assim que alguém encontra um hash que está dentro do limite imposto pelo alvo, nós o anunciamos para todos na rede:

Olá pessoal:

- Peguei as transações: "Ana envia R$2,00 para Bruno, Carol envia R$5,00 para Ana";
- Adicionei o nonce "32895";
- O resultado foi um hash com retorno 42, que é menor que o alvo limite de 100;

- Aqui está minha prova de trabalho: os dados da transação, o nonce que usei e o hash que foi produzido com base nessas entradas.

Para isso, talvez seja necessário bilhões de tentativas de hash para conseguir o resultado, gastando milhares de dólares em energia, mas todos podem imediatamente validar que fiz certo porque eles podem fazer o hash em uma única tentativa, já que dei a entrada e o saída esperada. Lembre-se de que os hashes são impossíveis de serem revertidos, mas são fáceis de serem calculados!

Como isso está ligado ao gasto de energia? Bem, já dissemos que o conjunto de todos os hashes possíveis é na verdade um número gigante que é quase tão grande quanto o número de átomos no universo. Agora podemos definir o *alvo* como baixo para que apenas uma pequena fração dos hashes sejam válidos. Isso significa que qualquer pessoa que quiser encontrar um hash válido terá que gastar uma grande quantidade de tempo e processamento o que significa que terá que gastar eletricidade, para encontrar um número de hash menor que nosso alvo.

Quanto menor o alvo, mais tentativas serão necessárias para encontrar um número que funcione. Quanto maior o alvo, mais rápido podemos encontrar um hash vencedor.

# 4 Minerando

O processo de jogar na loteria de Prova de Trabalho para ganhar acesso e escrever o livro-razão do Bitcoin é popularmente conhecido como *mineração*. Agora estamos prontos para ver como a loteria de prova de trabalho do Bitcoin realmente funciona:

1. Qualquer pessoa que desejar participar, entra na rede Bitcoin conectando seu computador e ouve as transações;

2. Ana anuncia sua intenção de enviar algumas moedas para Bruno. Os computadores da rede ficam conversando entre si para espalhar essa transação para todos demais usuários;

3. Todos os computadores que desejam participar da loteria começam a fazer o hash das transações que ouviram falar, acrescentando os nonces aleatórios à transação e executando as funções do hash sha256;

4. Aproximadamente a cada dez minutos, algum computador a encontra um número hash menor que o número alvo atual ganha a loteria;

5. Este computador anuncia o número vencedor que eles encontraram e a entrada (transações e nonce) que eles usaram para produzi-lo. Pode ter levado horas para conseguir, ou alguns minutos. Essas informações juntas (transações, nonce e hash da Prova de Trabalho) são chamadas de *bloco*;

6. Todos os outros validam o bloco verificando se as transações junto com o nonce do hash de fato geram aquele determinado hash, e se ele é de fato menor que o *Número Alvo* e se o bloco não contém nenhuma transação inválida, e que a história dentro dele não conflita com blocos anteriores;

7. Todos escrevem o bloco em sua cópia do livro-razão, acrescentando-o à cadeia de blocos existente, produzindo uma *blockchain*.

É isso. Produzimos nosso primeiro bloco e nossa primeira entrada em nossos livros-razão.

Talvez você já tenha lido em algum lugar da mídia que minerar Bitcoins envolve solucionar equações complexas. Agora você entende que isso é falso. Invés de solucionar equações, a loteria de mineração de Bitcoin é sobre jogar um dado gigante repetidas vezes para produzir um hash dentro de um dado intervalo. É simplesmente um jogo de azar, que força os participantes a gastarem uma certa quantia de eletricidade.

## Como são minerados novos bitcoins?

Até agora, discutimos como Ana pode enviar R$2,00 para Bruno. Vamos parar de falar em reais, porque o Bitcoin não sabe nada sobre essa moeda. O que temos são os próprios bitcoins - unidades digitais que representam valor na rede Bitcoin.

Para revisitar nosso exemplo, o que realmente está acontecendo é que Ana está enviando 2 bitcoins para Bruno, anunciando que ela está movendo bitcoins que estão registrados na sua "conta" para a conta de Bruno.

Alguém então ganha na loteria de Prova de Trabalho e escreve sua transação no livro-razão.

Mas onde Ana conseguiu esses 2 bitcoins para começo de conversa? Como o Bitcoin começou e como alguém adquiriu o Bitcoin antes de haver lugares para comprá-lo com a moeda fiduciária tradicional, como o real brasileiro?

Quando Satoshi criou o Bitcoin, ele podia ter criado um banco de dados no qual ele seria o dono de 21 milhões de moedas e pedido a pessoas comprarem isso dele. Porem, teria-se pouco motivo para pessoas atribuírem valor a um sistema que apenas uma pessoa controla toda a riqueza. Ele poderia criar um registro, onde algumas pessoas poderiam se cadastrar com um e-mail para ter uma chance de ganhar algumas moedas, mas isso seria suscetível a um ataque de Sybil(impersonificação) visto que da para gerar milhões de endereços de e-mails quase que gratuitamente.

Acontece que o processo de mineração de bitcoin, que é o processo de jogar na loteria de Prova de Trabalho e obter direitos de acesso ao livro-razão, é exatamente o que produz mais unidades de bitcoin. Quando você encontra um bloco válido (utilizando uma grande quantidade de energia e encontrando um número que é válido e que te faz vencedor da loteria), você pode escrever todas as transações sobre as quais ouviu falar naquele Bloco e, portanto, no livro-razão.Mas você também pode gravar uma transação adicional muito especial, chamada de transação *coinbase* (ou transação de cunhagem no português) no livro-razão. Essa transação basicamente diz: "12,5 Bitcoins foram criados e dados a Maria, a mineradora, para compensá-la por gastar toda aquela energia para minerar este bloco".

É assim que novos bitcoins são minerados a existência. esse processo permite absolutamente qualquer pessoa no mundo de minerar seus próprios bitcoins sem a existência de uma autoridade central, e sem identificar a eles mesmos, contanto que estejam dispostos a pagar pelo custo da eletricidade necessário para participar da loteria. Isso torna Bitcoin resistente a ataque de Sybil. Se você quiser moedas terás que gastar energia e pagar um dinheiro para minerar elas.

## A recompensa do bloco

Assim, a pessoa que ganha na loteria pode dar a si mesma alguns bitcoins recém criados. Mas por que 12,5 bitcoin e não 1000? Por que ela não pode enganar o sistema e dar a si mesma qualquer quantia?

Aqui está a parte principal: O Bitcoin é um sistema de consenso distribuído. Isso significa que todos devem concordar sobre o que é válido. A maneira que se faz isso é através de rodar um software no computador que aplica um grupo de regras bem definidas, conhecidas como as regras de consenso do Bitcoin. Qualquer bloco produzido por mineradores é validado por essas regras. Se ele passar, todos irão escrever em seus livros razão e aceitar como a verdade. Se não o bloco é rejeitado.

embora a lista completa de regras de consentimento seja um tanto complexa, aqui estão alguns exemplos.

- Um bloco valido pode criar uma quantia especifica de Bitcoins, determinada pelo cronograma de emissão que esta escrito no código

- Transações precisam ter assinaturas corretas, indicando que as pessoas que estão gastando aquelas

moedas tem a autorização devida.

- Não é permitido ter transações que gastam moedas que haviam sido gastas anteriormente nesse bloco ou qualquer outro bloco anterior.

- A informação contida em um bloco não pode ser maior que um determinado tamanho.

- O hash de prova de trabalho precisa ser inferior ao atual tamanho alvo, provando a improbabilidade estatística desse bloco ter sido minerado utilizando qualquer outro método que não o gasto de uma certa quantidade de energia.

Se Maria criar um bloco e decidir dar a si mesma algo além desta quantidade, o computador de todos os outros *rejeitará* o bloco como sendo inválido, porque dentro do software do Bitcoin Client que todos estão executando, há um trecho de código que diz "a recompensa do bloco atual é exatamente 12,5 bitcoin. Se você receber um bloco que concede a alguém mais do que isso, não aceite".

Se Maria tentar trapacear e produzir um bloco *inválido*, o bloco não será gravado no livro-razão de ninguém e ela terá desperdiçado milhares de dólares em eletricidade produzindo algo que ninguém aceitará, ou seja, uma falsificação. Isso concede ao Bitcoin uma custo infalsificável(*unforgeable costliness*), um termo usado primeira vez pelo pioneiro em moedas digitais, Nick Szabo, no seu artigo *Shelling Out*. Intuitivamente sabemos que se dinheiro fosse fácil de falsificar, não seria muito útil como dinheiro. Bitcoin é tão impossível de se falsificar, quanto é fácil de testar, através de um simples verificação matemática.

O primeiro bloco minerado foi criado por Satoshi. O código é de código aberto - isso significa que qualquer pessoa pode dar uma olhada em como ele funciona e validar que nada de suspeito está acontecendo por detrás dos panos. Até o Satoshi teve que fazer cálculos e jogar na loteria de Prova de Trabalho para extrair o primeiro bloco. Ele mesmo não poderia produzir uma falsificação, fraudando o custo de energia, embora ele seja o criador do sistema.

Qualquer pessoa que se juntou a rede depois dele pode verificar o hash que ele gerou com alvo inicial e os dados da transição para notar que ele havia atingindo o alvo estatisticamente raro através do gasto de energia. Imagine ser capaz de auditar a criação de dinheiro do tradicional sistema bancário fiat nesse nível de precisão e em tempo real.

## O Halving

O processo de mineração produz novos Bitcoins. Mas Satoshi queria um sistema que não era possível de ser depreciar. Ele não queria que a oferta monetária pudesse ser perpetuamente expandida. Invés, ele projetou um cronograma de emissão de novas moedas que começava muitas e tendia a zero novas moedas por ano.

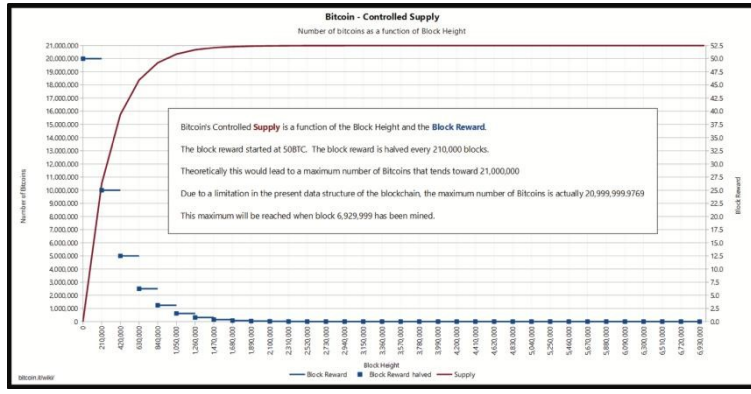
No início, a recompensa do bloco era de 50 bitcoin, então foi isso que Satoshi ganhou por minerar o primeiro bloco, assim como as outras pessoas que se juntaram à rede nos primeiros dias depois dos primeiros blocos serem criados.

O código Bitcoin impõe que cada recompensa do bloco seja reduzida pela metade a cada quatro anos aproximadamente. Isso se baseia na quantidade de blocos minera-

dos, e não na passagem do tempo, mas eles são quase os mesmos devido aos blocos sendo produzidos aproximadamente a cada dez minutos.

A Recompensa por Bloco em 2009 foi de 50, em 2012 foi de 25, em 2016 foi de 12,5. A partir de hoje, 15 de janeiro de 2019 - foram minerados 558.688 blocos, desde o início da história do Bitcoin, e a recompensa é de 12,5 bitcoin por bloco.

71.312 blocos a partir deste momento, ou aproximadamente no final de maio de 2020, a recompensa será reduzida para 6,25 bitcoins por bloco, levando a uma inflação do fornecimento anual de moedas para aproximadamente 1,8%. Uma década depois, após dois halvings, mais de 99% de todo o Bitcoin terá sido minerado e menos de 1 bitcoin será produzido por bloco. Você pode monitorar o processo de halving em `https://www.bitcoinblockhalf.com/`




*https://en.bitcoin.it/w/images/en/4/42/Controlled_supply-supply_over_block_height.png*

Eventualmente, por volta do ano 2140, a Recompensa por Bloco desaparecerá totalmente, e os mineradores se-

rão incentivados apenas pelas taxas pagas por aqueles que realizam as transações.

Esses números de emissão e de recompensa de bloco são aplicados no código Bitcoin - que, para reiterar, é totalmente de código aberto e pode ser validado por qualquer pessoa - dependendo de quão longe estamos na história do Bitcoin, produzindo um bloco que não siga essas regras fará com que você seja rejeitado por todos os outros que estão verificando as mesmas que estão escritas em seus códigos.

## Controlando a Emissão e Intervalo de Mineração

A mineração requer hardware e eletricidade, portanto, quanto mais hardware e eletricidade você controlar, maior será a probabilidade de encontrar o resultado mais rápido, em comparação às demais pessoas. Por exemplo, se houver 100 computadores com velocidade e custo energético igual na rede e você controlar 10 deles, encontrará o bloco vencedor em *aproximadamente* 10% das vezes. No entanto, a mineração é um processo baseado no acaso e na aleatoriedade, então é possível que horas ou mesmo dias possam se passar sem que você encontre um bloco.

Como foi falado na seção anterior, os mineradores não podem simplesmente conceder a si mesmos recompensas de blocos arbitrárias, ou seriam rejeitados pelos demais nodes. Mas e se eles gastarem muita energia para adiantar os blocos de mineração e colocarem as mãos em um monte de bitcoins, violando a restrição do projeto de que o cronograma de emissão deve ser conhecido com antecedência?

Vamos novamente ao exemplo de que há apenas 1000

hashes possíveis e nosso número de alvo sendo 100. Isso significa que 10% das vezes vamos lançar um número menor que 100 e encontrar um bloco.

Digamos que leve 1 segundo para calcular cada hash. Se a cada segundo "lançarmos nosso dado" misturando as transações atuais e nosso nonce aleatório, e 10% das vezes atingirmos um número menor que o alvo, então esperamos que leve cerca de 10 segundos, em média, para encontrar um hash válido.

O que acontece se dois computadores estiverem apostando nessa loteria? Eles têm duas vezes mais hashes sendo tentados, então esperamos que um hash válido seja encontrado em 5 segundos. E se 10 computadores estiverem jogando? Um deles encontrará um hash válido aproximadamente a cada segundo.

Isso cria um problema: se mais pessoas estão minerando, os blocos serão produzidos muito rapidamente. Isso gera dois resultados que não queremos:

1. Isso atrapalha a ideia de ter um cronograma de emissão pré-determinado. Queremos que seja emitido um número relativamente consistente de bitcoins por hora para ter certeza de que emitiremos todos eles até o ano 2140, e não antes disso;

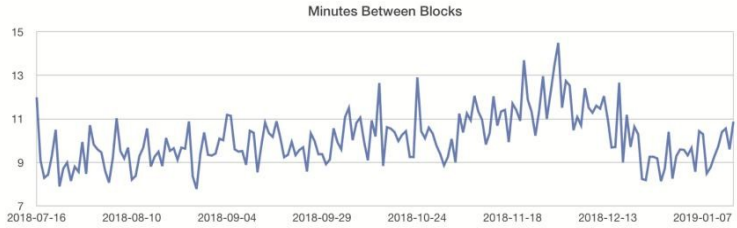
2. Isso cria problemas de rede: se os blocos são extraídos tão rapidamente que não têm tempo de alcançar toda a rede antes que o próximo seja extraído, então não podemos chegar a um consenso sobre uma história linear de transações, uma vez que vários mineradores podem incluir a mesma transação em seus blocos, fazendo com que os blocos sejam inválidos por conterem transações que já foram gastas em outros blocos.

E se menos pessoas estão minerando, criamos o problema oposto:

1. Os bitcoins estão sendo emitidos muito lentamente, novamente interferindo na emissão pré-determinada;

2. A blockchain pode se tornar inutilizável conforme as pessoas esperam horas, dias ou até mesmo semanas, para obter uma transação gravada no livro-razão.

O número total de hashes por segundo executado por todos os mineradores da rede Bitcoin é conhecido como *hash rate*.




*Minutos entre blocos minerados*

## Ajustes de dificuldade: concordando com o alvo

Como Bitcoin é um sistema voluntario e sem permissão que pessoas podem participar quando desejarem, sem ninguém comandando, o numero de mineradores ativos em um dado momento pode variar drasticamente. Precisamos de uma maneira de manter a produção de blocos estável impedindo aumentos ou reduções no cronograma


*Estamos tentando acertar esse pequeno espaço, o numero de possíveis resultados é grande, que irá demorar uma quantidade grande quantia de tempo para acerta la aleatoriamente.*

toda vez que um minerador novo entra na rede ou um minerador existente saia.

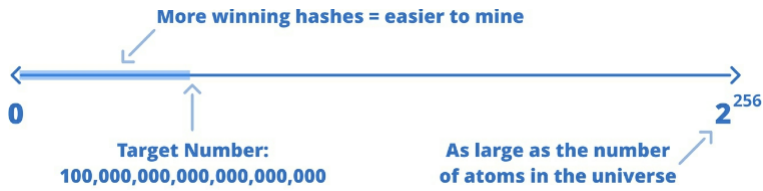
Como podemos tornar mais difícil encontrar hashes válidos se mais jogadores entrarem na loteria e mais fácil se os jogadores saírem dela, a fim de manter os tempos de emissão e de blocos estáveis?

Lembre que mineração de Bitcoin é uma loteria para tentar produzir um numero aleatório menor que um alvo.

O Bitcoin resolve esse problema com um *ajuste de dificuldade de mineração*. Como todos estão executando o mesmo código, que impõe as mesmas regras, e todos têm uma cópia de todo o histórico de blocos até este ponto, todos podem calcular de forma independente a rapidez com que os blocos estão sendo produzidos.

A cada 2016 blocos, o que leva aproximadamente o equivalente a duas semanas, olhamos para trás e descobrimos quanto tempo levou para produzir esses blocos e, em seguida, ajustamos nosso *Número Alvo* para acelerar ou desacelerar a produção de blocos.

Todos os usuários pegam os últimos 2016 blocos e os dividem pelo tempo que levaram para produzir, criando assim uma média. Demorou mais de dez minutos? Estamos indo muito devagar. Demorou menos de dez minu-




*Estamos tentando acertar esse pequeno espaço, o numero de possíveis resultados é grande, que irá demorar uma quantidade grande quantia de tempo para acerta la aleatoriamente.*

tos? Estamos indo rápido demais.

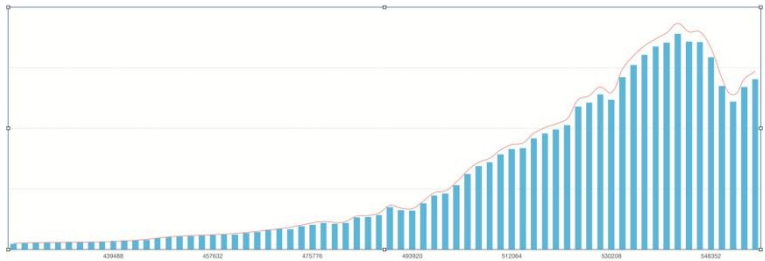
Agora podemos fazer um ajuste no *Número Alvo* para que seja aumentado ou diminuído proporcionalmente a quanto mais rápido ou mais devagar queremos ir com base no intervalo de 10 minutos que está escrito no código fonte.

Podemos aumentar o *Número Alvo* para um número mais alto, criando um espaço maior de hashes válidos, dando aos mineradores uma chance maior de encontrar um hash vencedor, gastando menos energia. Isso é chamado de *redução da dificuldade*.

De maneira contrária, podemos diminuir o *Número Alvo* para que menos hashes sejam válidas e os mineradores tenham que gastar mais energia para encontrar um hash válido. Isso é chamado de *aumento de dificuldade*.

Isso também significa que, para qualquer bloco, com base em quantos blocos vieram antes dele (a *altura do bloco*), sabemos exatamente qual é o número alvo. Isso nos permite saber o limite mágico sob o qual o número do hash da Prova de Trabalho deve cair para um bilhete de loteria vencedor naquele bloco específico ser dado como válido.

O ajuste de dificuldade e numero alvo é possivelmente



*Hash Rate em relação a dificuldade*

a inovação central do Bitcoin, permitindo a qualquer, independentemente, verificar o números da loteria baseados no alvo que eles podem independentemente calcular da mesma maneira que qualquer outra pessoa. É isso que permite a gente rodar uma loteria sem que ninguém nos diga a combinação vencedora.

O gráfico abaixo mostra a *hash rate* como uma linha e a dificuldade como barras ao longo do tempo. A dificuldade parece uma escada porque é ajustada a cada 2016 blocos. Você pode ver que toda vez que a *hash rate* sobe acima da dificuldade, a dificuldade aumenta para alcançar a *hash rate*. Quando a *hash rate* cai, como aconteceu entre outubro e dezembro de 2018, a dificuldade diminui. O ajuste de dificuldade sempre fica atrás do que quer que a *hash rate* faça.

Como há uma defasagem de 2016 blocos entre os ajustes de dificuldade, é possível que haja picos massivos de aumento ou diminuição na *hash rate* para mais ou menos produção de Bitcoin durante o período e isso pode violar levemente o cronograma da emissão.

Como adicionar *hash rate* normalmente significa produzir uma grande quantidade de novo hardware, isso é relativamente incomum e não afeta muito as coisas, e esperamos que isso se mantenha assim no futuro. As con-

sequências de qualquer pico são limitadas a uma janela de 2016 blocos, no qual esses picos ocorreram, pois com o próximo ajuste de dificuldade voltaremos a media de 10 blocos por minuto.

## Segurança e o valor em moeda fiduciária do Bitcoin

Determinamos que o Bitcoin recalcula automaticamente a dificuldade com base no número de jogadores da loteria, ou seja, os mineradores consomem energia quando fazem o hash. É aqui que o mundo real começa a tocar nosso mundo digital. O preço do Bitcoin, o preço do hardware e da energia e o valor de dificuldade criam ciclos de feedback complexos:

1. Os especuladores compram bitcoin porque acham que ele está subindo, elevando o preço para R$X;

2. Os mineiros gastam até R$X de energia e hardware para tentar extrair um bitcoin;

3. Uma alta demanda dos compradores e um aumento no preço levam mais mineradores a minerar o bitcoin;

4. Mais mineradores significa mais energia consumida em bitcoin e a rede fica ainda mais segura, tranquilizando os compradores sobre a segurança do Bitcoin, às vezes levando a um ciclo de feedback que aumenta ainda mais o preço;

5. Após a passagem de 2016 blocos, a presença de mais mineradores e, portanto, maior quantidade de hash, causa um ajuste de dificuldade para cima;

6. Uma dificuldade maior significa um Número Alvo menor - os mineradores estão encontrando blocos com menos frequência - fazendo com que pelo menos alguns deles gastem mais R$X em custos operacionais para extrair uma moeda;

7. Alguns mineradores se tornam não lucrativos, consumindo mais energia na mineração do que podem encontrar de bitcoin, fazendo com que rejeitem ser mineradores;

8. Outros 2016 blocos se passam. A dificuldade é recalculada para ficar mais fácil, já que alguns mineradores saíram do jogo;

9. Uma dificuldade menor significa que os mineiros que antes não eram lucrativos podem voltar a ficar online e fazer a mineração, ou novos mineiros podem entrar no jogo;

10. Vá para o item 1.

Em um mercado em queda, o ciclo pode ir na outra direção, com os usuários vendendo as moedas, fazendo com que o preço caia e os mineiros se tornem não lucrativos.

O algoritmo de ajuste de dificuldade garante que sempre haverá algum tipo de equilíbrio entre o preço e o número de mineradores na rede. Mesmo que preços despenquem e acabem por remover metade do taxa de hash da rede, na próximo ajuste de dificuldade tornaria mineração lucrativo novamente em torno do novo equilíbrio de preços.

A natureza do ajuste de dificuldade é retirar os mineradores ineficientes em favor dos que operam com a energia mais barata possível. Ao longo do tempo, isso

força mineradores de bitcoin a partes mais remotas do mundo onde recursos energéticos são abundantes. Uma reportagem da *Coinshares* de 2019 estima que 75% é feito com energias renováveis.

Na prática, nos últimos anos, o preço subiu rapidamente, assim como a taxa total de hash. Quanto mais alta a taxa de hash, mais difícil é atacar a rede porque, para controlar o que é gravado apenas no próximo bloco, é necessário ter muita energia e hardware sob seu controle, pois precisa ter mais da metade de toda a rede. Hoje, a energia utilizada pela rede de mineradores do Bitcoin é estimada como sendo maior do que um país de médio porte.

## Taxas e o fim da recompensa de mineração

Se a recompensa de bloco vai eventualmente acabar, como vamos continuar incentivando mineradores a continuamente gastar energia para manter o livro-razão seguro? A resposta do Bitcoin é taxas de transação financeira. Não só eles substituem a recompensa de bloco mas incentivam o minerador a incluir transações nos blocos ao invés de minerar blocos vazios.

As taxas são determinadas por um sistema de livre mercado, no qual os usuários pagam por espaço escasso em um bloco. Os usuários que enviam transações indicam quanta taxa estão dispostos a pagar aos mineradores, e eles podem ou não incluir as transações que são informadas, dependendo do quanto irão ganhar. Quando há poucas transações esperando para entrar no próximo bloco, as taxas tendem a ser muito baixas, pois não há competição. À medida que o espaço do bloco é preenchido,

os usuários estão dispostos a pagar taxas mais altas para que suas transações sejam confirmadas rapidamente (no próximo bloco). Aqueles que não querem pagar, podem sempre definir taxas baixas e esperar mais para serem minerados em um momento com baixa demanda, quando o espaço do bloco estiver mais disponível.

Ao contrário dos sistemas financeiros tradicionais, onde as taxas tendem a se basear em uma porcentagem do valor que está sendo transferido, no Bitcoin o valor transferido não tem relação com as taxas. Tornamos as taxas proporcionais ao recurso escasso que consomem: espaço em bloco. Portanto, as taxas são medidas em satoshis por byte (bytes são 8 bits, basicamente apenas uma medida de quantos dados há em sua transação). Assim, uma transação que envia um milhão de bitcoins de um endereço para outro pode ser mais barata do que uma que consolida 1 bitcoin espalhado por 10 contas, porque o último requer mais espaço de bloco.

No passado, houve períodos em que o Bitcoin tinha uma demanda muito alta, como o que aconteceu no final de 2017, onde as taxas se tornaram extremamente altas. Desde então, alguns novos recursos foram implementados para reduzir a pressão sobre as taxas na rede.

Uma dessas implementações se chama *Segregated Witness*(ou Testemunha Segregada), que reorganiza como dados no bloco são representados separando as assinaturas digitais dos dados da transação, criando mais espaço para esses dados. Transações que utilizam esse upgrade podem usar mais que 1MB de espaço através de uns truques que estão além do escopo desse livro.

O outro alívio para as taxas veio através do *batching*: As exchanges e outros participantes de alto volume no ecossistema começaram a combinar transações de bitcoin

para vários usuários em uma transação. Ao contrário de um pagamento tradicional em seu banco ou PayPal que é feito de uma pessoa para outra, uma transação de Bitcoin pode combinar um grande número de entradas e produzir um grande número de saídas. Assim, uma exchange que precisa enviar bitcoin para saque para 100 pessoas pode fazê-lo em uma única transação. Este é um uso muito mais eficiente do espaço do bloco, transformando o que é ostensivamente apenas um punhado de transações de bitcoin por segundo em milhares de pagamentos por segundo.

*Segragated Witness* e *Batching* já fizeram um bom trabalho em reduzir a demanda por espaço de bloco. Ainda haverá outras melhorias que estão na etapa de desenvolvimento para tornar o espaço no bloco mais eficiente. Mas de qualquer maneira, haverá outros momentos onde as taxas de transações de Bitcoin serão altas novamente devido a alta demanda por espaço de bloco.

Quase concluímos a invenção de todo o Bitcoin:

1. Substituiu um banco central por um livro-razão distribuído;

2. Instituiu um sistema de loteria para selecionar quem escreve no livro-razão;

3. Os participantes da loteria são forçados a consumir energia para comprar bilhetes por hash e torna mais fácil para todos poderem verificar os bilhetes vencedores, verificando os números hash produzidos pelos jogadores;

4. Diz aos jogadores da loteria que se eles não jogarem de acordo com as regras, rejeitamos os blocos, incluindo as *transações de criação de moedas*,

chamadas de *coinbase*, para que eles não fossem pagos quando ganhassem, criando assim um desincentivo econômico para trapacear e um incentivo econômico para jogarem de acordo com as regras;

5. Controlou o tempo e a seleção do *Alvo* para a loteria, permitindo que todos calculassem por si mesmos qual o *Alvo* deveria ser, baseado nas regras codificadas e no histórico dos últimos 2016 blocos;

6. Aplicou o cronograma de emissão usando ajustes de dificuldade que são alterados de acordo com o aumento ou diminuição da *hash rate*;

7. Usou o código-fonte aberto para garantir que todos pudessem verificar por si mesmos se estavam aplicando as mesmas regras em relação à validade da transação, recompensa do bloco e cálculo de dificuldade.

Não há mais entidade centralizada. Temos um sistema totalmente distribuído e descentralizado. Quase temos a imagem completa do funcionamento da rede. Resta apenas um problema. Quando alguém se junta à rede e pede cópias do livro-razão, eles podem obter diferentes históricos de nodes diferentes. Como podemos impor uma história única e linear e como podemos evitar que os mineradores reescrevam o passado?

# 5 Protegendo o livro-razão

Até agora, falamos como gerenciamos e mantemos as cópias e gravamos no livro-razão distribuído sem que possa haver coerção ou corrupção, utilizando um sistema de loteria e a validação por consenso.

Mas o que acontece quando um ganhador da loteria quer ser malicioso? Ganhar o direito de escrever em livro-razão significa que eles podem alterar lançamentos históricos no livro-razão? Evandro, Danilo e Fernanda podem conspirar para reescrever a história ou alterar os saldos das contas e dar a si mesmos moedas extras?

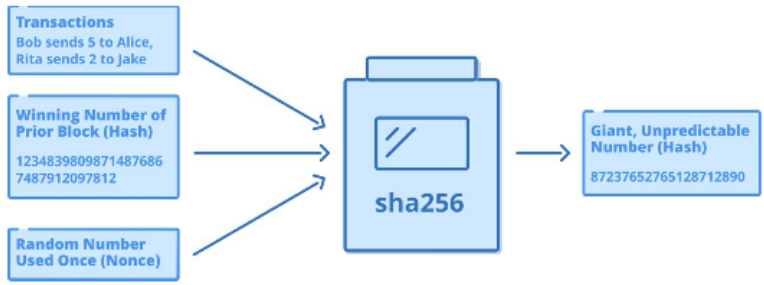
Ai vem a *blockchain*. Um termo de marketing que permeou grande parte do setor de tecnologia, a blockchain nada mais é do que a ideia de que os *blocos* do Bitcoin são *encadeados* para fornecer links de um conjunto de transações para o próximo bloco. Isso cria uma registro histórico linear de cada bloco desde o bloco gênesis extraído por Satoshi em 2009 ate hoje.

Mentimos um pouco no capítulo anterior para manter as coisas mais simples. Quando você minera jogando na loteria de Prova de Trabalho, você não está apenas fazendo o hash das transações que querem ir para o próximo bloco junto com o nonce. Na verdade, você também está fornecendo o hash do último bloco como entrada em sua função hash, vinculando assim seu bloco ao bloco anterior.

Lembre-se de que a saída de uma função hash é aleatória e dependente de todos os dados de entrada que nela constam. Agora modificamos nossos hashes do bloco para

incluir três entradas diferentes:

1. As transações que queremos incluir no livro-razão;
2. Um nonce aleatório;
3. O hash do bloco anterior que estamos usando como sendo a base do histórico do livro-razão.




*As três entradas usadas para construir o hash para participar da loteria, agora incluindo o hash ganhador anterior, fazendo um cadeia entre um bloco e outro.*

Isso nos permite construir um registro histórico de cada bloco desde o Bloco gênesis (primeiro bloco do Bitcoin) extraído por Satoshi. Quando escrevemos um novo bloco na blockchain, temos que validar que este bloco não contém nenhuma transação que gaste bitcoins que já foram gastos em blocos anteriores.

Se alguma dessas três entradas forem alteradas, o hash de saída mudará drasticamente e de maneira imprevisível. Esse comportamento cria uma propriedade interessante: se você adulterar os dados de qualquer bloco antigo, alterará seu hash. Se você alterar o hash de qualquer bloco antigo, alterará o hash de cada bloco que vier depois,

atuando como uma especie de foto de toda a historia da rede ate esse ponto!

Você não pode adulterá a prova de trabalho, como todos sabem a quantidade de energia que precisa ser gasta em cada bloco baseado no numero alvo para esse bloco. Se alguém for tentar mudar um bloco mais velho, eles precisariam computar o hash de prova de trabalho daquele bloco e de todos os bloco que vieram depois. Não só a blockchain deixa adulterações evidentes, como ela torna extremamente caro realizar a adulteração.

Efetivamente, cada novo bloco minerado no Bitcoin aumenta a segurança dos blocos que vieram antes dele, por conta do aumento da quantidade de energia necessária para recalcular todos os hashes para modificar um ponto anterior da rede. Uma transação em um bloco que possui 6 blocos posteriores a ele é considerada definitivamente inalterada. Seria necessária uma enorme quantidade de energia para recalcular os últimos seis blocos na taxa de hash total atual. Alterar um bloco a 100 blocos atrás? Nem pense nisso, esquece.

Quando fazes o download de uma copia da *blockchain* todas as transições são completamente transparentes e você pode verificar os hashes da prova de trabalho para garantir que nada foi alterado por alguém que lhe enviou o livro-razão.

## Quando Blocos Collidem

Falta uma peça no sistema de consenso. Como podemos forças todos a utilizar a mesmo histórico das transações se ocorrer o caso de dois mineradores simultaneamente minerar dois blocos e anunciam eles a rede?

Imagine que agora estamos administrando uma rede

mundial. Pessoas em todo o mundo, dos Brasil ao Japão, estão conectadas a essa rede global e todas estão jogando na loteria da Prova de Trabalho.

Alguém em São Paulo encontra um bloco válido. Eles o anunciam na rede e todos os computadores do Brasil começam a detectá-lo. Enquanto isso, alguém em Tókio também encontra um bloco a poucos segundos depois do bloco de São Paulo. Seus vizinhos ainda não ouviram falar do bloco brasileiro, então eles ficam sabendo primeiramente do bloco japonês.

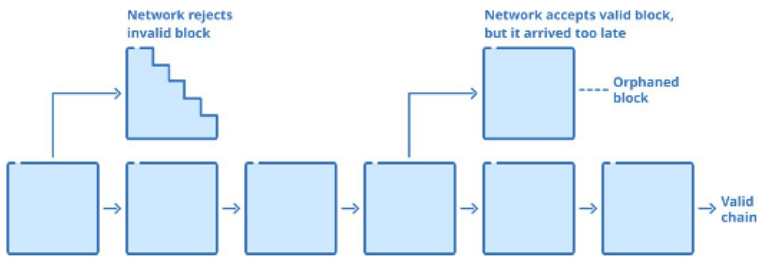
Ambos os blocos contem uma transação de 1 bitcoin de Ana a Bruno. Mas logo na sequencia Bruno envia o bitcoin para Carol. Devido a diferença de tempo o bloco brasileiro o próximo bloco brasileiro vai refletir essa transação e o Bruno vai ter um saldo na conta de zero. Entretanto, o bloco japonês minerou seu bloco antes de ver a transação de Bruno para Carol. O bloco japonês mostra que Bruno tem o saldo de um bitcoin.

A rede está dividida por não saber qual a blockchain é a cópia correta do livro-razão, uma vez que ambos contêm quantidades equivalentes de Prova de Trabalho e ambos contêm transações válidas. Isso é conhecida como *chain split*. Você não pode contar com nenhum ente central para lhe dizer qual deles é o verdadeiro. O que você faz?

O Bitcoin fornece uma solução bem simples para este problema: vamos apenas esperar para ver o que acontece. Existem agora duas versões concorrentes da blockchain, e os mineradores estão livres para escolher qual versão desejam participar. No próximo período de aproximadamente dez minutos, outro bloco será minerado. Os brasileiros estarão minerando no topo do bloco de que ouviram falar pela primeira vez, e os japoneses estarão minerando no topo de seu bloco.

Dado um tempo de mais ou menos dez minutos, outro bloco será minerado.Qualquer que seja o lado que minere primeiro, será o escolhido como sendo o verdadeiro. Como? Porque no código do Bitcoin há uma regra que diz que a cadeia de Prova de Trabalho Cumulativa Mais Longa resolve qualquer divisão que ocorra na cadeia. Quem consome mais energia vence. A regra de resolução de inconsistências entre cadeias com base em sua Prova de Trabalho cumulativa total agora é chamada de Consenso de Nakamoto, em homenagem a Satoshi Nakamoto.

Digamos que os japoneses minerem o próximo bloco. A rede deles está agora um bloco à frente da brasileira. Quando eles divulgarem essa descoberta, os nodes brasileiros do Bitcoin reconhecerão que os nodes japoneses produziram uma cadeia de Prova de Trabalho cumulativa mais longa e se reorganizarão (ou farão o que chamamos de "*reorg*"). Isso significa que eles vão jogar fora o bloco que mineraram em favor dos japoneses porque a blockchain deles é maior.




*O chain split é um processo natural que ocorre quando dois mineradores encontram blocos simultaneamente. A rede que se tornar mais pesada pela prova de trabalho se dita valida e a outra rede é feita órfão.*

O bloco brasileiro agora é chamado de *órfão*. Uma vez

que foi rejeitado, significa que o minerador que o encontrou não foi recompensado, e as transações não entraram no livro-razão. Porem as transações rejeitada não estão perdidas. Algumas dela podem ter entrado na rede japonesa competidora, e as que eventualmente não entrarão, podem ser escritos no próximo bloco.

Mineradores armazenam todas as transações que eles escutam num lugar especial em seus computadores chamado de como *mempool*. Qualquer transação que esta no bloco que foi rejeitado é colocado de volta na mempool. Que são então minerados por alguém no futuro contanto que elas entrem em conflito a histórico do livro-razão produzido pelo bloco mais recente.

Você pode notar que, embora tenha me referido aos nodes como brasileiros e japoneses, na realidade os nodes não sabem nada sobre a identidade uns dos outros, localização geográfica e assim por diante. A única prova de validade de que precisam é que alguém tenha a cadeia de Prova de Trabalho Cumulativa Mais Longa e que as transações na cadeia sejam todas válidas (sem gastos duplos, etc.).

A probabilidade de ocorrer essa divisão da cadeia é muito baixa - costumava acontecer uma vez por mês ou menos, mas recentemente não aconteceu muito devido a melhorias na tecnologia de propagação de bloco e conectividade de rede entre os mineradores. Hoje e no futuro previsível, o Bitcoin tem um limite para a quantidade de informação que um bloco pode ter, definido no seu código. Parte da razão pela qual o Bitcoin produz blocos relativamente pequenos aproximadamente a cada dez minutos é para garantir que os blocos órfãos sejam extremamente raros. A outra razão é manter os requisitos de hardware para executar um node relativamente baixos

para encorajar mais nodes no sistema.

Mineração é probabilística. As vezes blocos estão a dez minutos um do outro, as vezes alguns segundos. Se nodes produzíssemos blocos a cada segundo ou tivéssemos blocos muito grandes, teríamos uma probabilidade muito alta de que os blocos brasileiros e japoneses entrariam em conflito porque eles estão geograficamente distantes e levam mais tempo para se alcançarem. Se os órfãos acontecessem com muita frequência, a cadeia de blocos se desfaria porque haveria órfãos em órfãos e os nodes não seriam capazes de concordar sobre um histórico linear de transações antes do próximo bloco ser minerado.

É importante manter pequeno o tamanho do bloco para aumentar a chance da rede inteira possa receber o bloco mais recentes antes que um novo seja minerado. O outro e talvez mais importante motivo, é para manter os requisitos de hardware relativamente baixos para rodar um node, encorajando mais nodes, e mineradores descentralizados a participarem da rede. Blocos grandes encorajam a utilização de data centers e dadas regiões geográficas para minimizar blocos órfão, que impactam negativamente no lucro das operações.

## A única verdadeira rede

Vamos voltar ao nosso exemplo do Capítulo 3, onde Henrique se junta a uma rede pela primeira vez.

O node do Henrique vai conectar a alguns outros node na rede e perguntar se conhecem outros nodes e depois conectar-se a eles. Esse processo é conhecido como descoberta de nodes.

Alguns desses nodes vão ser descaradamente malignos e dar a ele uma copia falsa do livro-razão, com assinatu-

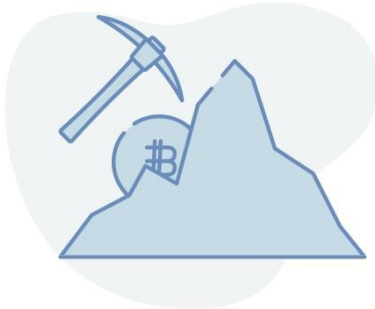
ras incorretas para transações ou com Bitcoins forjados através de mineração impropria, sem hashes de prova de trabalho validos. Essas copias serão rejeitadas de cara e esses nodes proibidos de conectar ao Henrique no futuro.

Outros nodes que ele conectar serão honestos, porem terão versões conflitantes da verdade. Por exemplo, talvez esses node tenha ficado offline e perdido a mineração de alguns blocos. Se ele baixar varias versões da blockchain e todas estão equivalentemente validas, o software no seu node vai utilizar o consenso de Nakamoto. Medindo a quantidade acumulada de prova de trabalho, qualquer das redes que tiver medido o maior valor será considerada a única verdadeira rede.

Os nodes constantemente conversam uns com os outros para garantir que tenham os blocos mais recentes. Se o seu node quiser saber qual cópia da blockchain é verdadeira, ele só precisa procurar a cadeia com a Prova de Trabalho mais cumulativa. Sendo assim Henrique não depende do voto da maioria, que seria fácil de trapacear utilizando uma maioria de nodes malignos

Mesmo que Henrique se conecte a duzias de nodes desatualizados ou malignos e apenas um node correto, o software do Bitcoin saberá qual é a copia correta devido da quantidade de prova de trabalho acumulada e a validade das transações. A importância disso é subestimada, Henrique não depende de confiança em nenhum partida; o node vai performar todas as validações para garantir que a rede que eles ta procurando é a única verdadeira rede.

É extremamente difícil, portanto, para hackers malintencionados fornecer a um node uma cópia falsa do blockchain, pois isso exigiria cortar a conexão desse node com qualquer outro node honesto e conectá-lo apenas a



*Ao contrário da mineração de ouro, que também consome energia, o processo de mineração de Bitcoin na verdade protege a rede para tornar o livro-razão à prova de adulteração.*

nodes malignos.

## Reversibilidade das transações

Duas redes competindo normalmente são produzidas ao acaso e resolvidas rapidamente. Porem uma pessoa que deseja atacar a rede bitcoin pode se aproveitar do consenso de Nakamoto controlando mais do que 50% da taxa de hash total. Assim eles produziriam a rede com prova de trabalho acumulado mais longa, que poderia conter transações de suas escolhas contanto que ele estejam dispostos a gastar a energia para tal. Quando eles publicarem nessa cadeia, os outros nos da rede aceitariam ele como o única verdadeira rede. Isso é conhecido como ataque de 51% porque requer o controle centralizado de mais da metade da rede.

É importante entender que não há finalidade real de transação no Bitcoin, visto que ataques de 51% ou a chance de criar blocos órfãos são sempre teoricamente possíveis. Por conta disso, recipientes de transações tipi-

camente esperam algumas blocos serem minerados sobre a transação para considerar ela escrita em pedra. Nesse ponto, a quantidade de energia requerida para reverter a transação é tao cara, que ela provavelmente não vai acontecer.

Blocos minerados apos um bloco contendo uma transação de interesse a você normalmente são chamados de confirmações, então quando ouvires que uma dada transação possui seis confirmações isso quer dizer que foram minerados seis blocos depois da transação. Se você está vendendo um livro digital que tem custo marginal para você como comerciante, pode querer apenas 1 confirmação, ou mesmo zero confirmações, entregando o bem digital assim que vir a transmissão da transação na rede. Se você está vendendo uma casa, talvez queira esperar por doze confirmações, ou cerca de duas horas de mineração. Quanto mais você espera, mais Provas de Trabalho são empilhadas no topo do bloco que contém suas transações e mais caro se torna no mundo real para reverter a transação. Cada comerciante ou processador de pagamentos decide por si mesmo o que considera final. Hoje, a maioria das pessoas aceita 6 confirmações - seis blocos extraídos depois daquele que contém a transação - como sendo definitivo, mas os comerciantes podem definir isso como quiserem.

Se a taxa de hash do Bitcoin cair significativamente, o que significa que menos energia está protegendo cada bloco, pode-se sempre aumentar o número de confirmações necessárias para a liquidação final. Embora isso possa parecer muito complicado no início, é importante ter em mente que as transações com cartão de crédito normalmente podem ser revertidas 120 dias após serem feitas.

Por outro lado, o Bitcoin é um dinheiro de liquidação final que não pode ser retirado de você, como dinheiro ou ouro. Deste ponto de vista, a reversibilidade e a finalidade das transações no Bitcoin é, na verdade, uma vasta melhoria em relação à maioria das redes de pagamento tradicionais.

A estimativas de hoje mostram que se tivesse toda a energia da rede Bitcoin ao seu dispor - o que é uma presunção e tanto, visto que terias ao que ter ao seu dispor a energia de um pais, e todas as equipamentos especializados do mundo - ainda seria necessário mais de um ano de mineração para reescrever a histórico de transações da rede. É possível ver tais dados em `http://bitcoin.sipa.be/`

Em um mercado em queda, o ciclo pode ir na outra direção, com os usuários vendendo as moedas, fazendo com que o preço caia e os mineiros se tornem não lucrativos. No entanto, ao contrário do que se pode ler na mídia sobre uma "espiral da morte", o algoritmo de ajuste de dificuldade garante que sempre haverá algum tipo de equilíbrio entre o preço e o número de mineradores na rede. Também retira os mineradores ineficientes em favor dos que operam com a energia mais barata possível.

# 6 Forks e ataques de 51%

No início, Satoshi minerou os primeiros bitcoins usando a unidade de processamento central (CPU) do computador. Como a dificuldade inicial de mineração no sistema era baixa, era relativamente barato gerar essas moedas usando a CPU.

Com o tempo, as pessoas começaram a ajustar o software de mineração para torná-lo cada vez mais eficiente. Eventualmente, eles escreveram um software que começou a tirar proveito de processadores especializados chamados unidades de processamento gráfico (GPUs) que existem nas placas de vídeo e geralmente são usados para jogos.

Com as GPUs, a mineração tornou-se milhares de vezes mais eficiente do que a mineração usando a CPU. A dificuldade rapidamente se ajustou para cima para equivaler ao novo taxa de Hash que havia enchido a rede pelo uso de GPUs. Nesse ponto, qualquer pessoa que minerava em uma CPU fornecia uma fração tão pequena da taxa de hash que rapidamente se tornou não lucrativo e tiveram que desligar seus mineradores.

Conforme as GPUs assumiram o controle e as pessoas começaram a comprar toneladas de placas gráficas, a eficiência da mineração foi aprimorada ainda mais por meio da produção de ASICs (Application Specific Integrated Circuits, ou Circuitos Integrados Específicos de Aplicações em português). São chips de hardware de computador que são criados com um objetivo específico - a função bitcoin sha256 e nada mais. Sendo especializados neste

algoritmo em particular, os ASICs foram capazes de ser milhares de vezes mais eficientes do que as GPUs para mineração e rapidamente tornaram as GPUs não lucrativas, assim como as GPUs fizeram com as CPUs. Em poucos anos, a nova geração de dispositivos ASIC coloca suas versões anteriores fora do mercado com grandes melhorias de eficiência.

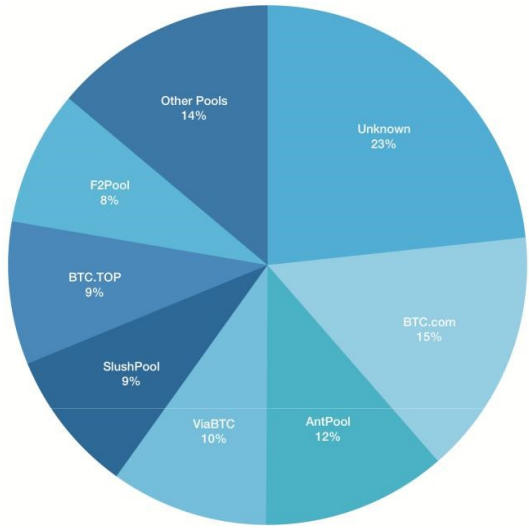
Os primeiros mineradores da rede gastaram apenas alguns centavos de eletricidade para produzir seus bitcoins. À medida que o preço do bitcoin subia e mais e mais mineradores aderiam a rede, a dificuldade aumentava e ficava cada vez mais caro gerar bitcoins. Hoje, o preço gira em torno de $ 8000.00 por moeda, e pessoas queimam milhares de reais em eletricidade por unidade de bitcoin criado.

## Pools de mineração

Um problema com a mineração de bitcoin é que ela não é determinística, como jogar um dado. Isso significa que você pode acabar gastando centenas de dólares em eletricidade e nunca encontrar um bloco válido.

Em 2010, uma inovação chamada pool de mineração (conhecida como Slushpool) surgiu para resolver o problema de mineradores consumindo energia sem receber recompensa. Um pool de mineração é um pool de risco compartilhado, semelhante ao funcionamento do seguro médico.

Todos os mineradores contribuem com a mineração, fazendo com que todos os participantes pareçam um grande minerador. Se alguém na pool encontrar um bloco válido, a recompensa pelo bloco é dividida proporcionalmente entre todos os mineradores com base na taxa de




*Pools de mineração*

hash com que contribuíram. Isso permite que até mesmo pequenas operações de mineração, como indivíduos, recebam recompensa pela pequena taxa de hash com que contribuem. Para fornecer este serviço de coordenação, o pool fica com uma parte das recompensas.

Os pools de mineração causaram um efeito de centralização, os usuários tendem a migrar para pools maiores. Porem, é importante lembrar que usuários estão minerando para a pool e que a pool não é detentora da taxa de hash que eles representam. Usuários podem trocar de pool de mineração ao longo do tempo e fazem isso. O diagrama abaixo mostra a distribuição aproximada da mineração em janeiro de 2019.

Na verdade, há um precedente histórico para mineradores individuais deixarem uma pool que se tornou muito poderosa: em 2014, a Ghash.io tinha quase metade do poder de mineração total. Os mineiros viram que ele estava

se tornando muito centralizada e partiram para outras pools de maneira voluntaria.

Embora pools de mineração relativamente centralizadas sejam a realidade atual, há melhorias constantes na tecnologia de mineração, incluindo uma proposta chamada BetterHash, que permite que os mineradores individuais tenham mais controle sobre o que estão minerando e reduza a dependência da coordenação das pools.

## Ataques de 51%

A centralização do pool de mineração leva à preocupação de que eles possam conspirar para o ataque de 51% da rede. Se você olhar o gráfico acima, verá que as 5 principais pools, em conjunto, têm mais de 50% da taxa de hash de mineração total. Vamos examinar como esse ataque é realizado e quais perigos ele carrega.

Quando você possui pouco mais de 50% da taxa de hash, pode dominar as gravações no livro-razão porque pode produzir uma cadeia mais longa do que a outra taxa de hash inferior a 50% combinada ao longo do tempo. Lembre-se de que o Consenso de Nakamoto diz que os nodes devem aceitar a cadeia de Prova de Trabalho cumulativa mais longa que chegar até eles.

Aqui está um exemplo de como um ataque simples de 51% é realizado:

1. Digamos que a rede como um todo esteja produzindo 1000 hashes/segundo;

2. Você compra um monte de hardware de mineração e eletricidade para produzir 2.000 hashes/segundo. Agora você tem 66% da taxa total de hash (2000/3000);

3. Você começa a minerar uma cadeia que contém apenas blocos vazios;

4. Daqui a duas semanas, você transmitirá sua blockchain vazia. Como você está minerando aproximadamente duas vezes mais rápido que os mineradores honestos, sua cadeia será duas vezes mais longa focando na Prova de Trabalho cumulativa. A transmissão para todos os nodes existentes fará com que eles se reorganizem e percam as últimas duas semanas de história escrita na blockchain.

Além de minerar blocos vazios, o que torna a blockchain inutilizável, você também pode realizar um ataque de gasto duplo:

1. Envie algum bitcoin para uma exchange;

2. Troque por USD e retire o USD;

3. Mais tarde, transmita na blockchain que você minerou secretamente e que não contém o envio para a exchange;

4. Você reescreveu a história e agora tem o bitcoin original e os dólares;

Com o consumo de energia da taxa de hash do Bitcoin hoje sendo mais ou menos a de um pais de médio porte. Adquirir hardware e eletricidade suficientes para realizar tal ataque é extremamente caro. Estimativas mostram que custaria para você aproximadamente $700k Dólares por hora para realizar um ataque de 51% hoje, e o custo continua a subir. Essa estimativa não leva em conta a reação que mineradores honestos terão ao a tal ataque,

que a tudo indica fariam ele custar ainda mais. Você pode explorar o custo de um ataque ao Bitcoin ou outras criptomoedas em `https://www.crypto51.app`.

Também é muito difícil escapar impune com um ataque de gasto duplo dessa proporção sem deixar pegadas que poderiam ser usadas para descobrir quem você é. Afinal, você estaria consumindo a energia de um país de porte médio e comprando milhões de dólares em hardware e enviando milhões de dólares para a exchange para fazer todo este processo.

Manter esse tipo de ataque por qualquer período de tempo razoável é inviável, mas digamos que uma entidade mal-intencionada com financiamento ilimitado decidisse fazer isso e fosse capaz de sustentar esse ataque além do nível de um incômodo. A rede poderia se adaptar alterando a sua função de prova de trabalho (usando alguma coisa diferente do sha256). Isso tornaria todos os ASICs de hardware usados pelo invasor completamente inúteis. Essa, no entanto, é a opção nuclear, pois também tiraria do mercado imediatamente todos os mineradores honestos.No entanto, a rede sobreviveria e surgiria das cinzas, como a Fênix.

Além da inviabilidade do ataque, ter a maioria da taxa de hash não dá direito a ser dono da rede:

1. Você não pode criar moedas do nada. Isso viola a regra de consenso de recompensa de blocos, sendo eles rejeitados, mesmo se tivessem Prova de Trabalho suficiente;

2. Você não pode gastar moedas que não são suas. Você não seria capaz de fornecer uma assinatura digital válida, o que viola as regras;

Assim, os nodes que aceitam Bitcoin como pagamento manteriam a rede honesta mesmo em face de uma maioria desonesta de mineradores, simplesmente seguindo as regras do Bitcoin. Portanto, um ataque de 51% é mais um incomodo do que um problema de segurança. O mais provável, pior cenário possível aqui seria um estado, que possui bolso fundo que esteja tentando tornar o bitcoin não utilizável. No entanto tal ataque não pode se manter por muito tempo. Quando o Bitcoin se recuperar de um ataque como esse apenas provaria a resiliência e tornaria o bitcoin um problema ainda maior para aqueles que desejam atacar ele.

Enquanto ate a presente data o Bitcoin nunca foi realizado um ataque de 51% com sucesso, o ataque já foi realizado em outras *blockchains* que possuem taxa de hash pequena protegendo elas. Nestes casos, exchanges foram vitimas de ataques de gasto-duplo e perderam dinheiro nessas moedas de pouca taxa de hash, que eles provavelmente não deveriam ter listado em primeiro lugar.

# 7 Contas Sem Identidade

Até agora, construímos um livro-razão distribuído sem autoridade central, um sistema de loteria para selecionar quem escreve, um sistema para recompensar bons mineradores e punir os que se comportam mal, uma forma de ajustar a dificuldade de mineração para garantir um cronograma de cunhagem consistente e reduzir conflitos, e um sistema para verificar a validade da cadeia, examinando a prova cumulativa de trabalho e o histórico de transações.

Agora vamos lidar com a identidade. Em um sistema bancário tradicional, você envia dinheiro identificando-se ao banco, seja por meio da apresentação de um código ou PIN pessoal ou da apresentação do nome de usuário e senha, no aplicativo. O banco garante que duas pessoas não compartilhem uma só identidade.

Já que agora não temos uma entidade central para rastrear os indivíduos, como podemos abrir contas em nosso novo sistema financeiro baseado em Bitcoin? Como podemos encaminhar para objetivo de Satoshi de remover identidade de transações financeiras, afim de evitar furto de identidades e entidades centrais.Como podemos garantir que, quando Anaanunciar que deseja pagar Bruno, seja realmente ela e, tenha a autoridade de enviar esses fundos?

## Gerando uma "Conta Bitcoin"

Já que não podemos contar com um intermediário central como um banco para manter um registro de todas as contas. E se permitirmos que todos registrem seu próprio nome de usuário e senha? Um banco normalmente verifica se um nome de usuário ainda não está em uso, mas isso não é possível neste caso, já que não temos um ator central distribuindo identidades. Portanto, precisamos de algo maior, mais forte e mais exclusivo do que um nome de usuário e uma senha. Esta técnica deve ser semelhante aos capítulos anteriores. Mais uma vez, precisamos de um número aleatório gigante.

Assim como possibilitamos que todos comprassem bilhetes de loteria gerando grandes números aleatórios, podemos usar o mesmo truque para gerar contas. Para criar uma "Conta Bitcoin", também conhecida como endereço, primeiro geraremos um par de números de 256 bits matematicamente vinculados, conhecido como *par de chaves pública/privada*. Novamente, $2^{256}$ é tão grande quanto o número de átomos no universo, então duas pessoas gerando acidentalmente o mesmo par de chaves é quase impossível. Daremos o nosso endereço a qualquer pessoa que queira nos enviar moedas. Usaremos a chave privada para gastar as moedas.É assim que elas funcionam.

Criptografia é um método para pegar dados e obscurecer eles, de tal maneira que só quem tem acesso a chave consegue ler a mensagem original através de descriptografar. Como crianças alguns de nos brincávamos com brinquedos codificadores e decodificadores para converter uma mensagem em lero-lero e retornar ela a uma mensagem normal depois. Esse tipo de criptografia é chamada de simétrica pois usa apenas uma chave. O par de chaves tem algumas propriedades interessantes. Você pode usar

qualquer uma das chaves para criptografar uma mensagem e a outra para descriptografá-la.

Você está convidado a compartilhar sua chave pública com o mundo inteiro. Saber essa chave não permite que eles tenham acesso à sua chave privada. Pessoas que queiram te enviar uma mensagem podem criptografar elas com tua chave publica. Porque apenas você tem a chave privada, você é o único que consegue descriptografar a mensagem.

Vamos dar uma olhada qual o processo que Anafaz para enviar as moedas para Bruno. Para receber uma transação, Brunogera um par de chaves privadas/públicas e mantém sua chave privada em segredo. Ele produz um *endereço*, um grande número com base no hash da sua chave pública. Bruno, então, compartilha esse número de endereço com Anapara que ela possa enviar moedas para ele.

você pode pensar que endereços são caixas postais. Invés de cartas, Anapode depositar moedas nesse caixa postal. Mas apenas Brunopossui a chave privada que vai abrir o caixa postal, liberando ele à gastar essas moedas.

Quando movimentas dinheiro dentro de um banco, você fornece a eles um usuário e senha. Quando escreves um cheque, você assina seu nome para autenticar que você escreveu o cheque. Quando movimentas bitcoins, você fornece uma prova que es o dono da chave para o endereço que detêm as moedas.

Anaagora precisa informar à rede que está enviando moedas para o endereço público de Brunoà partir de seu próprio endereço público. Como ela prova que está autorizada a gastar naquele endereço público? Ela faz isso fornecendo prova de que possui a chave privada desse endereço, mas sem realmente revelar sua chave privada.

Essa prova de propriedade é chamada de *assinatura digital*. Ana constrói uma transação, que essencialmente é apenas um pedaço de dados que parece algo como:

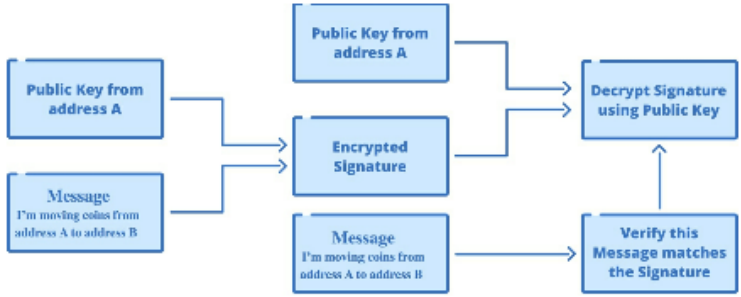
> "o endereço 12345 que contem 2.5 bitcoins,
> está enviando 2 bitcoins para o endereço 56789
> e 0.5 bitcoins de volta ao endereço 12345",

Exceto que os números do endereço são, na verdade, números gigantes de 160-bits. Ela então faz o hash de sua transação e criptografa o hash com sua chave privada, criando uma *assinatura digital*.

Quando ela publica sua transação na rede, ela revela sua chave pública (de onde ela está enviando). Uma vez que todos possuem a chave pública, todos podem facilmente descriptografar a assinatura digital. Anaanuncia o seguinte:

- estou enviando moedas do endereço 12345.
- Aqui esta a chave publica do endereço 12345, e vocês podem de fato ver que é a chave publica pelo hashando a chave publica e vendo que chegas no endereço.
- Aqui esta a assinatura digital que eu criptografei com a chave privada correspondendo a esse endereço. você pode usar a chave publica para descriptografar ele e verificar que é idêntica a transação que estou enviando.

Visto que agora todos tem a chave publica da Ana, eles conseguem facilmente descriptografar a assinatura digital. Pela virtude de ser capaz de descriptografar corretamente a assinatura utilizando a chave publica permite que todos saibam que Anatem a chave privada para




*A transação que movimenta as moedas esta criptografada usando uma chave privada para criar um assinatura digital. Ela é descriptografada usando uma chave publica, que todos conhecem.*

aquele endereço. Caso não tivesse, a descriptografia teria falhado, pois a chave publica pode apenas descriptografar mensagens criptografada pela chave privada. É importante ressaltar que não foi revelado sua chave privada, eles tem apenas a prova que ela foi capaz de utilizar a chave privada criptografando a assinatura.

Ao contrário de uma assinatura em um cheque ou de sua senha de banco, sua assinatura digital é específica para os dados de transação exclusivos que você está assinando. Portanto, não pode ser roubada e reutilizada em uma transação diferente. Cada transação recebe uma assinatura diferente, mesmo que seja baseada na mesma chave privada, visto que qualquer informação modificada muda o hash da assinatura.

## Você consegue adivinhar uma chave privada?

Vamos descobrir as chances de adivinhar uma chave privada, o que lhe daria a capacidade de mover as moedas no endereço público correspondente. Lembre-se de que uma chave é composta por 256 bits. Cada bit possui apenas dois valores (um ou zero). Isso significa que você pode visualizar cada bit como um cara ou coroa.

Se tivéssemos uma chave privada de 1 bit, seria como jogar uma moeda. Cara ou coroa, um ou zero? Você tem uma chance em duas de acertar.

Revisão rápida de probabilidade básica: A probabilidade de ocorrência de vários eventos é calculada multiplicando-se a probabilidade individual de cada evento. Se um lançamento de moeda tem $1/2$ chance de dar cara, então a chance de dois lançamentos de moeda consecutivos dar cara é $1/2x1/2 = 1/4$ ou 1 em 4.

Se você adivinhasse o resultado de 8 lançamentos consecutivos de moeda, seria $(2^8)$, ou uma chance em 256.

Uma placa de carro americana tem 6 letras e números. Existem 26 letras e 10 números, portanto, um total de 36 caracteres. Como há seis deles, o número de placas de carros possíveis = $(36^6)$, então suas chances de adivinhar a minha são de uma em 2.176.782.336 (uma em dois bilhões).[1].

Um cartão de crédito tem dezesseis dígitos. Cada dígito pode ter 10 valores, e há 16 deles, então suas chances de adivinhar meu cartão de crédito são de uma em $(10^{16})$,

[1] A inspiração para esta seção veio de uma excelente postagem no Medium que detalha as probabilidades de uma variedade de eventos. Recomendo a leitura da postagem completa para contexto: `https://medium.com/breathe-publication/a-dance-with-infinity-980bd8e9a781`

que é uma em 10.000.000.000.000.000.000 ou aproximadamente uma em dez quintilhões.

Existem cerca de ($10^{50}$) átomos na Terra. Se estou pensando em um ao acaso, suas chances de adivinhar exatamente qual átomo, é de:

> Um em 1.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.

Uma chave privada tem 256 bits, que é $2^{256}$ ou cerca de $10^{77}$. Na verdade, está mais perto em magnitude de adivinhar um átomo específico de todo o universo ou de ganhar na Mega Sena 9 vezes seguidas usando apenas 6 números:

> Uma chance em 115.792.089.237.316.195.423.570.985.008.687.907.853.269.984.665.640.564.039.457.584.007.913.129.639.936

Mas e se você tivesse um computador superpoderoso para fazer as suposições? Não posso fazer mais justiça a este assunto do que a este post[2] do Reddit, que recomendo a leitura na íntegra. Embora seja técnico, o parágrafo final dá uma boa ideia do que seria necessário para listar todas as chaves de 256 bits possíveis:

[2] A postagem completa do Reddit que descreve como adivinhar uma chave de 256 bits está disponível aqui: `https://bit.ly/2Dbw9Qd`

> "Então, se você pudesse usar o planeta inteiro como um disco rígido, armazenando 1 byte por átomo, usando estrelas como combustível e percorrendo 1 trilhão de chaves por segundo, você precisaria de 37 octilhões de Terras para armazená-lo e 237 bilhões de sóis para alimentar o dispositivo capaz de fazer isso, o que levaria 3,6717 octodecilhões de anos."
>
> – U/PSBLAKE EM R/BITCOIN

Basicamente, é impossível adivinhar a chave privada de alguém. Não apenas isso, mas o número de endereços de Bitcoin é tão grande que as melhores práticas realmente exigem a geração de um novo endereço para cada transação que você fizer. Então, em vez de ter uma conta bancária, você pode ter milhares ou até milhões de contas Bitcoin, uma para cada transação que já recebeu.

Pode ser desconcertante que sua conta Bitcoin seja protegida apenas por acaso, mas espero que a ilustração acima dê a você uma ideia de que isso é muito mais seguro do que a senha de sua conta bancária, armazenada em um servidor centralizado, disponível para hackers.

## Rastreamento de saldos

É hora de corrigir uma última mentira inofensiva que já dissemos em capítulos anteriores. Na verdade, não há saldos mantidos no livro-razão. O Bitcoin usa um modelo chamado UTXO: Unspent Transaction Outputs. A UTXO é simplesmente a palavra para uma saída de transação - uma moeda produzida por uma transação anterior, incluindo uma *transação do tipo coinbase* de

recompensa em bloco - que ainda não foi gasta em outro endereço.

Diferente de moedas metálicas que podem vir com uma determinada denominação, como por exemplo centavos, dezenas de centavos, 25 centavos, bitcoins são divisíveis em ate 100,000,000 unidades chamados de satoshis. Então dependendo do valor que recebeste nos seus endereços, talvez você precise combinar moedas de múltiplos endereços para gerar um UTXO maior, ou separar um UTXO para tornar ele menor. A ideia do UTXO é que cada transação é um conjunto de entradas que são consumidas para produzir novas saídas. Pense nisso como enviar um monte de moedas para uma máquina que derrete e cunha novas moedas de qualquer valor que quisermos. Carteira, que discutiremos mais tarde nesse capitulo, geralmente administram isso por trás das cenas, para que você precise apenas especificar a quantidade que deseja enviar.

Digamos que Anatenha um endereço que contém 1 bitcoin. Ela deseja enviar $0,3$ bitcoins para Bruno. Ela gera uma transação que mostra seu endereço com 1 bitcoin com o seu UTXO como entrada e duas saídas: um novo endereço bitcoin UTXO que vale $0,3$ como saída para o endereço do Brunoe um novo UTXO que vale 0,7 como saída para seu próprio endereço como troco. O troco pode ir para o endereço de envio original ou, para melhor privacidade, ela pode enviá-la para um novo endereço que foi gerado instantaneamente.

Já que não há nenhuma maneira de dizer quem controla qual endereço na blockchain. Para isso, você precisa saber as chaves privadas correspondentes e vinculá-las às identidades do mundo real. O modelo UTXO incentiva um mecanismo de privacidade muito bom, permitindo a

criação de novos endereços sempre que as moedas são movidas. Então uma pessoa pode ter centenas ou milhares de endereços se eles enviam ou recebem moedas com frequência Softwares de carteira fazem a gestão de tudo isso para a gente, evitando que precisamos nos preocupar com os detalhes.

Assim, para verificar o "saldo" de um determinado endereço, na verdade temos que somar todos os UTXOs que possuem este endereço como saída. O conjunto total de UTXOs atuais no Bitcoin aumenta quando as pessoas enviam de um endereço para vários e diminui quando as pessoas realizam transações de "consolidação" em que moedas de vários endereços são gastas em um endereço.

O modelo UTXO permite a validação fácil e eficiente de gastos duplos, uma vez que qualquer UTXO em particular só pode ser gasto uma vez. Não precisamos saber todo o histórico de gastos de uma conta específica.

Também podemos criar e destruir qualquer número de UTXOs de uma vez, criando transações complexas que misturam diferentes entradas e saídas. Isso permite a ideia de "mistura de moedas"[3], em que várias partes participam de uma única transação de Bitcoin que mistura qualquer número de entradas para produzir qualquer número de saídas, obscurecendo assim o histórico dos UTXOs. A popularidade de tais técnicas esta aumentando e é importante para privacidade e fungibilidade, que é um termo que dita que qualquer um bitcoin é equivalente a outro bitcoin. Dessa maneira se alguns bitcoins caírem nas mãos de uma entidade desagradável, as moedas não são marcadas por toda a eternidade só porque foram utilizadas para algum ato nefasto.

[3] `https://en.bitcoin.it/wiki/CoinJoin`

## Carteiras

Como gerar uma conta nada mais é do que gerar um número aleatório de 256 bits para ser sua chave privada, e podemos criar milhares ou milhões de contas, precisamos de um mecanismo para rastreá-las. No Bitcoin, a palavra *carteira* é usada para se referir a qualquer tipo de dispositivo que rastreia suas chaves. Pode ser tão simples como um pedaço de papel ou tão complexo como uma peça de hardware.

O software original do Bitcoin publicado por Satoshi veio com uma carteira de software. Essa carteira geraria seu par de chave pública/privada, geraria endereços e selecionaria UTXOs para você possa enviar bitcoins em qualquer valor.

Ao contrário da carteira do seu banco, que normalmente tem a forma de um único aplicativo móvel ou internet banking, o Bitcoin é um sistema completamente aberto. Portanto, existem centenas de carteiras, a maioria das quais é gratuita, sendo muitas delas também de código aberto, bem como meia dúzia de implementações de carteiras de hardware, com outras sendo produzidas. Qualquer pessoa com conhecimento de programação de computadores pode construir sua própria carteira ou ler o código de uma carteira de código aberto para garantir que nada de suspeito esteja acontecendo.

Este é outro lugar no Bitcoin onde a inovação sem permissão está acontecendo em um ritmo rápido, ao contrário do aplicativo móvel do seu banco.

Visto que sua chave privada é a única coisa de que você precisa para gastar suas moedas, você deve guardá-la bem. Se alguém roubar seu cartão de crédito, você pode ligar para a empresa e registrar uma reclamação de fraude e tentar obter seu dinheiro de volta. No Bitcoin,

não há intermediário. Se alguém tem sua chave privada, eles controlam suas moedas e não há ninguém que você possa ligar.

As chaves privadas também são altamente suscetíveis a perdas. Se você armazenar sua carteira no computador e ele for roubado ou pegar fogo, você tem um problema. Se você seguir as práticas recomendadas do Bitcoin para gerar um novo endereço toda vez que receber um pagamento, armazenar e fazer backup com segurança dessas chaves privadas se tornará algo muito custoso.

Com o tempo, o ecossistema Bitcoin desenvolveu uma série de soluções para esse problema. Em 2012, o BIP32 (Bitcoin Improvement Proposals ou Proposta de Melhoria do Bitcoin, um mecanismo para as pessoas espalharem ideias sobre como melhorar o Bitcoin) foi proposta para criar Carteiras Determinísticas Hierárquicas. A ideia por trás disso é que usando apenas um único número aleatório (seed), podemos gerar uma cadeia inteira de pares de chaves públicas/privadas: endereços de Bitcoin e chaves de assinatura para eles.

Hoje em dia, se você usar qualquer um dos softwares comumente disponíveis ou carteiras de hardware, eles gerarão automaticamente novas chaves para você para cada transação e permitirão que você faça backup de apenas uma única seed.

Em 2013, o BIP39 veio para tornar o backup de chaves ainda mais fácil. Em vez de usar um número completamente aleatório, as chaves seriam geradas a partir de um conjunto aleatório de palavras que seriam legíveis por seres humanos. Aqui está um exemplo de seed:

> witch collapse practice feed shame open despair creek road again ice least

Com esse método, o backup das chaves se tornou muito

fácil: você pode escrever a seed em um pedaço de papel e colocá-la em um cofre. Você pode até memorizar a frase e sair de um regime econômico decadente como a Venezuela, sem que ninguém saiba que você está carregando sua riqueza na cabeça.

Além disso, um endereço Bitcoin pode exigir mais de uma chave privada para ser acessado. Endereços multisignature ou *multisig* podem empregar uma grande variedade de esquemas de segurança. Por exemplo, duas pessoas podem compartilhar uma conta usando multisig 1 de 2, onde qualquer uma das partes pode assinar as transações e gastar as moedas.

Um multisig 2 de 2, que exige que ambas as partes forneçam as chaves privadas para gastar, impedindo de qualquer uma pessoas possa controlar as moedas, utilizada por exemplo entre parceiros comerciais.

Você pode fazer um sistema de depósito simples usando um multisig 2 de 3. O comprador obtém uma chave, o vendedor obtém outra chave e uma terceira chave é dada a um verificador. Se o comprador e o vendedor concordarem, eles podem desbloquear os fundos sem a necessidade do verificador. Em caso de litígio, o verificador pode agir em conjunto com uma das partes para desbloquear os fundos.

Você pode usar um esquema multisig 3 de 5 para se proteger contra a perda de chaves, permitindo-se perder até 2 das 5 chaves e ainda ser capaz de desbloquear a conta. Você pode armazenar duas das chaves em lugares diferentes, duas com amigos de confiança diferentes que não se conhecem e uma com um serviço de custódia especializado como o BitGo que assina suas transações, tornando seu Bitcoin muito difícil de ser roubado enquanto se protege das perdas das chaves.

Você pode ir ainda mais longe e criar endereços que são desbloqueados por condições bastante complexas utilizando construtos de programação como frases condicionais por exemplo "se isso então aquilo"(*if this then that*). Você pode, por exemplo, fazer um endereço de bitcoin do qual você não pode gastar por 10 anos, não importa o quanto alguém queira forçá-lo a mudá-lo.

Mais e mais soluções semi custodiais estão surgindo de empresas como Casa ou Unchained capital, que te ajudam a armazenar suas chaves de uma maneira segura. Diferente de um banco que pode congelar sua conta, essas soluço es parcialmente custodiais atuam como um backup ou coassinante de confiança, mas não podem eles mesmos tirar os fundos sem suas chaves. Carteira estão constantemente evoluindo porque não requer a permissão de ninguém para fazer isso, diferente do aplicativo do seu banco. Por conta disso vemos novas entidade surgindo e mais inovação o tempo todo.

Isso é profundo e transforma o mundo. Nunca antes foi possível transportar seus bens de uma forma completamente segura contra apreensão ou roubo.

# 8 Quem faz as regras?

Agora temos um sistema distribuído funcional para acompanhar e transferir valor. Vamos revisar o que criamos até agora:

1. Um livro-razão distribuído, uma cópia que é mantida por todos os participantes;

2. Um sistema de loteria baseado em Prova de Trabalho e ajustes de dificuldade para manter a rede segura e o cronograma de emissão consistente;

3. Um sistema de consenso que garante que cada participante possa validar todo o histórico da blockchain para si, usando um software de código aberto chamado Bitcoin Client;

4. Um sistema de identidade usando assinaturas digitais que permite a criação arbitrária de caixas de correio semelhantes a contas que podem receber bitcoins sem uma autoridade central.

Agora é hora de enfrentar uma das coisas mais interessantes e contra-intuitivas do Bitcoin: De onde vêm as regras, como são aplicadas e como elas podem ser modificado ao longo do tempo.

## O software do Bitcoin

Ao longo dos capítulos anteriores, presumimos que todos na rede estavam validando as mesmas regras: ou seja, es-

tão rejeitando gastos duplos, garantindo que cada bloco contenha a quantidade adequada de Prova de Trabalho, que cada bloco aponte para o bloco anterior da blockchain atual e que cada transação contida no bloco esta devidamente assinada pelo proprietário daquele endereço, entre um monte de outras coisas com as quais as pessoas concordaram ao longo do tempo.

Também dissemos que o Bitcoin é um software de código aberto. O código aberto significa que qualquer pessoa pode ler seu código e também que qualquer pessoa pode atualizar sua própria cópia com o código que quiser. Como as mudanças chegam ao Bitcoin?

O Bitcoin é um *protocolo*. Em software de computador, este termo se refere a um conjunto de regras que o software segue. No entanto, contanto que você siga o conjunto de regras que todos estão seguindo, você é livre para modificar seu software como desejar. Quando dizemos que as pessoas "executam nodes de Bitcoin", o que realmente queremos dizer é que elas executam um software que se comunica usando o protocolo Bitcoin. Este software pode conversar com outros nodes Bitcoin, transmitir transações e blocos para eles, descobrir outros nodes para fazer se conectar e assim por diante.

Os detalhes reais de como o software é implementado dependem de qualquer pessoa que o execute. Na verdade, existem muitas implementações do protocolo Bitcoin. O mais popular deles é chamado Bitcoin Core e é a extensão do trabalho lançado pela primeira vez por Satoshi Nakamoto.

Existem outros clientes também, alguns até mesmo escritos em outras linguagens de computador e mantidos por pessoas diferentes. Como o consenso em Bitcoin é crítico, o que significa que todos os nodes devem concor-

dar sobre quais blocos são ou não válidos, a grande maioria dos nodes executa o mesmo software (Bitcoin Core) para evitar quaisquer bugs acidentais que podem fazer com que alguns nodes discordem sobre o que é válido ou não. Na verdade não existe uma lista de especificações completas e escritas do protocolo bitcoin, então a melhor aposta para implementar um novo software do bitcoin é ler o código original e ter certeza que não desviaste do que ele faz, mesmo com bugs.

## Então, quem faz as regras?

As regras que compõem o Bitcoin são codificadas no cliente Bitcoin Core. Mas quem decide essas regras? Por que dizemos que o Bitcoin é escasso se alguém pode entrar e fazer uma modificação no software que muda o limite de 21 milhões de bitcoins para 42 milhões?

Sendo um sistema distribuído, todos os nodes deste sistema devem concordar com as regras. Se você for um minerador e decidir mudar o software para conceder a você o dobro de Bitcoins que lhe é permitido pela configuração atual de recompensa por bloco, então, quando você minerar seu bloco, todos os outros nodes da rede rejeitarão seu bloco. Fazer uma mudança nas regras é extremamente difícil porque existem milhares de nodes distribuídos em todo o mundo, cada um aplicando as regras do Bitcoin.

O modelo de governança do Bitcoin é contra-intuitivo, especialmente para aquelas pessoas que vivem em uma democracia ocidental. Estamos acostumados à governança pelo voto - a maioria das pessoas pode decidir fazer algo, aprovar uma lei e impor sua vontade à minoria. Mas o sistema de governo do Bitcoin está muito

mais próximo de uma anarquia do que da democracia.

Cada Pessoa que aceita pagamentos em Bitcoin decide por ela mesma o que ela considera ser o Bitcoin. Se alguém roda um software que diz que à 21 milhões de bitcoins, e você tenta enviar a eles bitcoins produzidos pelo seu software pirata que desafia esse limite, suas moedas aparentarão ser falsificadas para eles logo serão rejeitadas.

Vamos dar uma olhada nos entes que compõe este sistema:

**Node**: Cada participante da rede Bitcoin executa um node. Eles escolhem qual software executar. Embora a maioria das pessoas execute o Bitcoin Core, a principal implementação do protocolo bitcoin que foi iniciado pelo Satoshi e agora é desenvolvido por centenas de desenvolvedores independentes e diversas empresas ao redor do mundo. Se essa implementação do software se tornar malicioso e tentar introduzir algo como inflação, ninguém o executará. Exemplos de nodes incluem aqueles executados por qualquer pessoa que aceite Bitcoin - comerciantes, exchanges, empresas que oferecem carteiras e pessoas comuns que usam o Bitcoin para qualquer propósito que desejem.

**Mineradores**: Alguns nodes também mineram bitcoins, gravando transições e tornando muito custoso para alguém adulterar o livro-razão. Se os mineradores são os únicos que escrevem nele, pode ser tentador considerá-los os criadores das regras, mas não são. Eles estão simplesmente seguindo as regras definidas pelos nodes que aceitam os bitcoins. Se os mineradores começarem a produzir blocos que contenham recompensa extra, eles não serão aceitos por outros nodes, tornando essas moedas inúteis. Assim, cada usuário executando um node está

participando de uma governança anárquica - eles estão escolhendo quais regras as moedas que eles consideram Bitcoin devem seguir, e qualquer violação é rejeitada imediatamente.

**Usuários/investidores**: Os usuários são as pessoas que compram e vendem a moeda bitcoin e bem como também rodar nodes. Muitos usuários atualmente não executam seus próprios nodes, mas dependem de um node hospedado pelo provedor da carteira, onde atua como uma espécie de proxy para os desejos e vontades do usuário. Os usuários decidem o valor da moeda no livre mercado através da oferta e demanda. Mesmo que os mineradores e exchanges conspirassem e introduzissem algum tipo de mudança radical, como a inflação, os usuários provavelmente se livrariam da moeda que seguisse essas regras, baixando o preço e colocando as empresas que aceitaram essa regra à falência. Uma minoria intolerante de usuários sempre poderia manter sua própria versão do Bitcoin viva, que ainda seguisse as regras originais

**Desenvolvedores**: O software do Bitcoin Core é o maior projeto do Bitcoin Client que existe. Ele atraiu um rico ecossistema de centenas dos melhores desenvolvedores e empresas de criptografia. O projeto central é muito conservador, pois o software alimenta uma rede que agora protege centenas de bilhões de dólares. Cada ideia de mudança passa por um processo chamado *Bitcoin improvement proposal*[1] e qualquer modificação no código é cuidadosamente revisada por pares. O processo de propostas e revisão de código é feito de maneira totalmente

[1]leia mais sobre o desenvolvimento do Bitcoin Core é gerido em *Who controls Bitcoin Core?* por Jameson Loop:https://medium.com/@lopp/who-controls-bitcoin-core-c55c0af91b8a

aberta. Qualquer pessoa pode participar, comentar ou enviar o código. Se os desenvolvedores se tornarem mal intencionados e introduzirem algo que ninguém deseja executar, os usuários simplesmente executarão softwares diferentes. Talvez versões mais antigas, ou começarão a desenvolver algo novo. Por causa disso, os desenvolvedores principais devem desenvolver mudanças que os usuários geralmente desejam, ou arriscam perder seu status de implementação de referência se ninguém quiser executá-la.

## Forks Modificadores de regras

Esperamos que agora você tenha um boa ideia sobre como o software Bitcoin impõe as regras que as pessoas concordaram e como as pessoas podem decidir qual software executar para aplicar as regras em que acreditam.

Também falamos que os mineradores decidem as regras que seguirão ao produzir blocos e que devem minerar o tipo de blocos que os usuários desejam, ou arriscar que seus blocos não sejam aceitos e, assim, perder a recompensa da mineração.

Finalmente, sabemos que o software do Bitcoin aceitará a mais longa cadeia de prova cumulativa de trabalho como sendo a única verdadeira rede, e que forks (ou bifurcações em português), às vezes, ocorrem naturalmente devido à mineração dos mineradores usando as cadeias desatualizadas.

Devido a vasta diversidade de participantes na rede, as regras do Bitcoin estão quase que escritas em pedra desde o começo. As únicas melhorias que foram executadas no bitcoin ate então foram feitas de maneira retro compatível, preservando as regras de consenso para nodes que

não aplicaram as melhorias.

Agora vamos falar sobre como regras podem ser modificadas. Um fork intencional é quando alguns usuários e/ou mineradores decidem que não concordam com as regras atuais do Bitcoin e que precisam mudar as regras. Existem dois tipos de forks, que mudam as regras que foram encontrados na natureza: soft forks, que são compatíveis com versões anteriores, e hard forks, que não são compatíveis com versões anteriores. Vamos ver como isso ocorre na teoria e, em seguida, ver alguns exemplos históricos[2].

Um soft fork é uma mudança retro compatível com as regras de consenso do Bitcoin que aperta as regras. Isso significa que se você executar um node antigo que não foi atualizado para as novas regras, ele ainda verá os blocos produzidos sob as novas regras como válidos. Vejamos um exemplo para deixar claro:

Em 12 de setembro de 2010, uma nova regra foi introduzida no software: Os blocos devem ter no máximo 1 MB de tamanho. Esta regra foi introduzida para resolver problemas de spam na blockchain. Antes dessa regra, todos os blocos de qualquer tamanho eram válidos. Com a nova regra, apenas blocos menores eram válidos, logo as regras ficaram mais rígidas. Se você estava executando um node antigo e não o atualizou, os blocos menores ainda eram válidos de acordo com suas regras, então você não foi afetado.

Um soft-fork é uma maneira de atualizar o sistema sem interrupções porque permite que os operadores dos nodes atualizem para o novo software lentamente ao longo do

[2]A historia completa de forks modificadores de regras podem ser analisados aqui `https://blog.bitmex.com/bitcoins-consensus-forks/`

tempo, de forma voluntária. Se eles não fizerem a atualização, eles ainda serão capazes de processar todos os blocos que chegam como sempre fizeram. Apenas os mineradores que produzem os blocos precisam se atualizar para começar a produzir blocos usando as novas regras. Depois que os mineradores atualizaram para o novo fork de 1 MB, todos os blocos daquele ponto em diante tinham no máximo 1 MB de tamanho. Os usuários que executam versões antigas do software não precisavam saber disso.

No caso de um hard fork, uma alteração não compatível com versões anteriores é introduzida. Um hard fork é uma expansão do banco de regras na qual os blocos que eram originalmente inválidos agora são considerados válidos. Os nodes antigos que não foram atualizados não serão capazes de processar os blocos produzidos sob as novas regras. Assim, eles ficarão presos na blockchain antiga, a menos que façam a atualização.

Hard forks com concordância quase unânime de todos os nodes da rede não causaria problemas. Cada node seria atualizado imediatamente para as novas regras. Se alguns retardatários fossem deixados para trás, eles não obteriam novas atualizações de bloco e teoricamente notariam que seu software parou de funcionar e seriam forçados a atualizá-los.

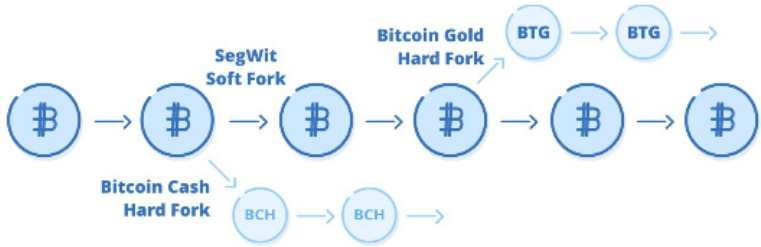
Na prática, os hard forks nunca são feitos de maneira suave. Em um sistema anárquico verdadeiramente descentralizado, você não pode coagir todos a mudarem para as novas regras. Em agosto de 2017, algumas pessoas que não estavam felizes com o progresso da rede Bitcoin em relação a pagamentos baratos decidiram que queriam fazer um fork para criar uma rede com blocos maiores. Como o Bitcoin tinha uma regra sobre os blocos não ultrapassarem 1 MB, devido a um soft fork ocorrido em

2010. Essas pessoas queriam criar uma nova cadeia com blocos maiores. Este fork ficou conhecido como Bitcoin Cash.

Um hard fork fora do consenso como Bitcoin Cash, que não é seguido por todos os mineradores e nodes, cria uma nova blockchain. Essa blockchain compartilha alguma história com a blockchain original incluindo as UTXO(saldo de conta) existentes ate o ponto da divisão. Mas, a partir do ponto de divisão em diante, as moedas criadas no fork não são mais Bitcoin, pois não são aceitas por nenhum node da rede Bitcoin.

O assunto o que "é" ou "não é" Bitcoin foi calorosamente debatido no ano seguinte ao fork do Bitcoin Cash. Houve algumas pessoas em favor do Bitcoin Cash que propuseram uma narrativa de que o Bitcoin deve ser definido pelo que está escrito no white paper original, escrito por Satoshi há dez anos. Escolhendo a dedo as palavras específicas no documento para provar seu ponto. Mas um sistema baseado em consenso não funciona com apelo a autoridades. Funciona pela ação coletiva de muitos indivíduos incluído por optarem que software executar, e que moeda comprar ou vender no mercado livre.

No caso deste fork, as pessoas que executam a grande maioria dos nodes economicamente significativos - ou seja, carteiras, exchanges e comerciantes não queriam trocar seu software por algo suportado por uma equipe de desenvolvimento muito menor e menos experiente e em uma quantidade muito menor de hash. Nem as pessoas achavam que tal "atualização" valesse a pena quando comparado a possibilidade de interrupção do ecossistema. O problema com os hard forks é que eles só funcionam quando todos aceitam a troca. Se houver retardatários, duas moedas são criadas. Assim, o Bitcoin permaneceu




*Moedas de um soft-fork podem ser enviada a nodes antigos. Um Hard-fork produz um novo retro incompatível UTXOs que não será aceito por nodes antigos*

como sendo o Bitcoin e o Bitcoin Cash tornou-se uma moeda separada. Como todos que já tinham bitcoin receberam bitcoin Cash livre de custo, muitos apenas venderam a moeda por "dinheiro gratuito"o que empurrou o preço do bitcoin Cash para baixo

Hoje, existem dezenas de outros forks de Bitcoin, como Bitcoin SV(que por se só é um fork do Bitcoin Cash) Bitcoin Gold, Bitcoin Diamond e Bitcoin Private. Todos eles com um pequeno hash protegendo-os, baixo suporte ao desenvolvedor, com atividade na rede quase inexistente e baixa liquidez em exchange. A sua falta de liquidez faz dessas moedas um ótimo alvo para subidas e quedas manipuladas, que frequentemente levam a subidas meteóricas de preço e iguais quedas espetacularmente devastadoras. Muitas foram sujeitas a hacks em suas carteiras, ataques de 51% e outros desastres. Muitos são golpes ou campo de batalha para apostadores. A maioria tem um algo grau de centralização em algum aspecto do seu projeto. O site `forkdrop.io` esta atualmente acompanhando 74 tentativas de Bitcoin.

Centenas de moedas semelhantes ao Bitcoin usam código semelhante, mas não compartilham o histórico de

saldo da conta do Bitcoin (conjunto UTXO), como Litecoin ou Dogecoin. Essas não são tipicamente consideradas divisões do Bitcoin embora dividam muito do mesmo código, pois elas não compartilham o histórico de saldo nas carteiras do bitcoin.

Um fork do Bitcoin não impacta sua oferta máxima de 21 milhões de Bitcoins. Imagine que você tem as reservas de ouro do mundo em um forte ultra seguro com segurança pesada. Você construir uma pequena, mal montada cabana e chamar ela de forte lite, protegendo ela com um único segurança. Podes pintar umas pedras de ouro e colocar elas dentro da cabana. Quando anunciares ao mundo que você "forkou"o ouro e todos que detêm ouro podem deter a mesma quantia de pedras douradas em sua cabana.

Nos precisamos de muitos mineradores protegendo o bitcoin, tornando ele custoso a ataques de 51%. Um fork do Bitcoin que só possui alguns mineradores, semelhantes a sua cabana mal protegida, é fácil de atacar. O código é provavelmente estruturalmente inseguro, construído por uma equipe de desenvolvedores sem experiencia, com péssima revisão por pares, igual a sua cabana. Moedas de forks não são aceitas por nodes porque quebram as regras do Bitcoin. Da mesma maneira que pessoas que tem testes químicos para o ouro não irão aceitar suas pedras douradas. O custo de manufaturar as pedras e as moedas do fork é zero visto que deste elas de graça para todos os proprietários de ouro. Isso é limita o interesse do mercado em forks do Bitcoin.

Enquanto você considera as milhares de copias do Bitcoin que já foram criadas, e nenhuma os quais possui valor de mercado significativo, pense nesse paradoxo: Criar forks do Bitcoin é gratuito e fácil. Porem, mudar as re-

gras do Bitcoin ou criar Bitcoin novos é tudo menos fácil. A próxima vez que você ouvir alguém com conhecimento limitado sobre o bitcoin perguntar porque o Bitcoin é especial responda com isso.

A natureza descentralizadas do ecossistema do Bitcoin cria uma forte preferencia ao modelo atual. Mudanças significativas precisam de meses ou anos de muito debates, construções de consenso e revisão por pares para ser implementado. Isso é algo bom, e algo que almejamos de um sistema que visa ser a moeda do planeta. Bitcoin é uma dança delicada entre milhares de participantes, todos agindo de forma egoísta e muitas vezes com necessidades concorrentes. É um sistema anarquista de mercado verdadeiramente livre, sem ninguém em particular no comando.

# 9 O que vem depois

## O Bitcoin é o Orkut das Cripto?

Por que eu escolhi escrever um livro sobre Bitcoin quando eu poderia ter escrito um sobre o ecossistema cripto como um todo? Não existe milhares de outras moedas? O que faz o Bitcoin ser tão especial, Além que foi a primeira criptomoeda descentralizada. Ela não é mais lenta que seus competidores?

Isso é o que muitas pessoas novas ao bitcoin perguntam. Depois de entender o básico de como Bitcoin funciona, a próxima pergunta logica tende a ser: "Tecnológica blockchain parece interessante. Como sabemos que uma versão melhor não vai surgir e transformar meu Bitcoin no Orkut das cripto?"

O fosso é uma vantagem competitiva que um negocio construí para impedir a entrada de novos concorrente. Para o Orkut esse fosso era uma enorme base de usuários que mantinham relações amigáveis. Pessoas não utilizariam um serviço competidor que seus amigos também não estivessem la. Mas tanto um fosso quanto um grafo social bem conectado não foram o suficiente para impedir o Facebook de comer o almoço do Orkut ao longo de alguns poucos anos.

O fosso do Bitcoin é muito mais muito maior que o do Orkut. Para entender isso precisamos examinar o que um competidor precisaria fazer para deslocar o Bitcoin

## Seja o dinheiro mais comercializado e liquido

A primeira coisa a entender é que a comparação com Orkut versus Facebook é ruim porque você pode ter uma conta no Orkut e no Facebook ao mesmo tempo sem custo. Isso na verdade é o que muitas pessoas fizeram durante a fase de transição de uma rede social a outra. Quando a massa critica de pessoas haviam migrado para o Facebook, as pessoas pararam de usar o Orkut.

Não é assim que dinheiro funciona, entretanto. Se você tem o valor de um dólar em bitcoin, isso é um dólar de valor que você não pode ter em nenhuma outra moeda. você esta tomando a decisão de maneira consciente de vender uma moeda por outra. você não pode guardar o mesmo valor em ambas as moedas ao mesmo tempo. Agora se pergunte: Por que você iria segurar qualquer coisa se não a moeda mais liquida e mais amplamente aceita? A resposta é apenas especulação. Se você não consegue mudar a economia inteira ao seu redor para também guardar essa moeda, então não existe maneira dessa moeda se tornar dominante.

A liquidez do Bitcoin é muito além de qualquer um dos seus competidores. No dia de hoje, o valor de mercado do Bitcoin é de $160B de acordo com `https://messari.io/screener`. O segundo maior competidor, o Etherium, tem apenas $30B de valor de mercado. Isso nem é uma mensura da verdadeira liquidez observando quanto você consegue efetivamente vender antes do preço começar a decair significativamente.

Liquidez é uma bola de neve. Segurar o dinheiro mais liquido significa que mais gente quer ele, que aumenta ainda mais a liquidez dele. Retendo qualquer outra coisa

que não seja o dinheiro mais liquido, você esta ativamente punindo a se mesmo enquanto espera todas as outras pessoas fazerem o mesmo. Os incentivos econômicos não se alinham em favor da liquidez do concorrente em uma noite.

## Demonstração de $100B+ de valor seguro por dez anos

Através das circunstancias, foi permitido o Bitcoin crescer de um experimento geek na internet que ninguém se importava, para, comprar uma pizza por 10,000 bitcoins, para, um preço pico de $20K USD por bitcoin. Ele fez tudo isso de maneira relativamente quieta, sem ninguém enchendo o saco. Durante esse período, ele desenvolveu um sistema imunológico de nível mundial, devido a anos de ataques e cresceu para a rede de maior taxa de hash do mundo. Em dez anos, assegurando mais que 100 bilhões de dólares, e se tornou impossível de hackear.

É quase impossível lançar uma nova criptomoeda quietamente hoje. Hoje a coisa está em alta, e todo mundo está ligado neste mercado. Vamos analisar uma blockchain alternativa, o EOS, que valeu aproximadamente 10 bilhões de dólares no seu lançamento e hoje vale menos da metade. Ele travou dois dias apos seu lançamento devido a uns bugs no seu código. Esses bugs foram atualizado dentro de horas com mínima supervisão ou revisão. você vai colocar $ 100B de valor numa rede assim? Talvez o EOS ainda esteja por aqui em uns 10 anos mas, talvez nessa época, O Bitcoin vai ter 20 anos de idade, e segurará trilhões em valor.

## Congele ataque vindo taxa de hash

Visto que das milhares das moedas la fora estão usando uma duzia de algoritmos de hash diferentes, quais quer novas moedas que surjam estão sobre constante ameaça de ataques de 51% pela taxa de hash já disponível. Isso já aconteceu com o Bitcoin Gold e diversas outras moedas.

Qualquer novo competidor precisa sobreviver ataque do poder de hash já existe ou usar um algoritmo que não possui nenhuma ASIC. Se não possui nenhuma ASIC então o sistema vai ser facilmente atacado, utilizando um serviço de aluguel de GPU, já amplamente disponíveis. Ele também não pode começar assegurando um valor alto, como o EOS fez um dia, que é imprudente e uma boa maneira de ser obrigado a fazer atualizações centralizadas. Então eles não podem se financiar, então a única maneira que sobra é um lançamento justo similar ao bitcoin e crescer de valor lentamente para que eles possam desenvolver seu sistema se segurança proporcionalmente. Porem se eles crescerem muito lentamente eles não vão alcançar o numero de usuários e liquidez do Bitcoin devido ao decorrer do tempo.

## Ser altamente descentralizado

A grande do modelo de segurança do bitcoin vem do seu alto grau de descentralização. Isso significa que o protocolo é difícil de ser modificado e por consequência pode ser confiado a honrar as propriedades escritas em seu código(Oferta limitada,etc). Essa propriedade foi testada quando um numero alto de empresários e mineradores se juntaram e queriam mudar o tamanho do bloco para

conduzir o protocolo em uma dada direção[1]. Esse fork foi rejeitado pelos usuários e falhou espetacularmente.

Um competidor que é altamente descentralizado basicamente elimina qualquer empresa ou equipe que são formadas por pessoas conhecidas visto que isso cria um ponto central de falha e coerção. também exclui qualquer moeda que queria "sair quebrando tudo", pois só podes fazer isso quando es centralizado. Qualquer competidor ou esta indo rápido demais e fica centralizado, ou esta se movendo muito lentamente e nunca vai alcançar.

## Atrair os melhores desenvolvedores do mundo

Muito semelhante a Linux criou que criou um redemoinho de atividade que impediu o surgimento de outros sistemas *Nix de competir, O bitcoin também. Todo dia a comunidade cresce e novas empresas são montadas em cima do Bitcoin, oferecendo serviços. Um competidor precisa roubar uma parcela das mentes desenvolvedoras de um núcleo exponencialmente crescente, que inclui duzias de empresas, programas educacionais e conferencias.

## Cresça uma rede financeira global

Bitcoin é apoiado por centenas de exchanges mundo a fora, mercados futuros e outros produtos financeiros derivativos em lugares de grande capital como o *Chicago Mercantile Exchange*, centenas de fundos financeiros e

[1] Leia mais sobre o tal fork chamado de Segwit2x que foi planejado através de acordos obscuros e consequentemente abortado aqui:`https://bitcoinmagazine.com/technical/now-segwit2x-hard-fork-has-really-failed-activate`

painéis de trading, e ainda uma rede de pessoas que já usam o bitcoin como alternativa a moedas fracassadas como o bolívar venezuelano. Todas essas coisas precisaram ser construídas para um competidor do Bitcoin deslocar ele.

Instituição como *Chicago Mercantile Exchange* não vão listar cada um dos novos competidores sem que tenha toneladas de volume em exchanges apoiando o competidor. você precisaria convencer negócios a aceitarem esse competidor no lugar do Bitcoin. Um competidor esse que provavelmente é menos seguro, menos liquido, possui uma equipe de desenvolvedores menos competentes e por definição menos adoção mundial. É uma subida bastante ingrime a trilhar.

## Seja dinheiro mais forte

Existe um grotesco equivoco que o Bitcoin é a maneira mais rápida e barata de se enviar dinheiro. Isso claramente não pode ser baseado em suas propriedades fundamentais que envolvem um Livro-razão replicável em escala mundial. Entretanto, principal caso de uso já demonstrada é ser dinheiro forte resistente a censura, esta crescendo.

Qualquer outra como, como fazer transferências remetentes mais baratas são cerejas em cima do bolo. A maioria dos tais competidores do Bitcoin ainda pensam que precisam solucionar o caso de uso para pagamentos rápidos, que já foi solucionado por dezenas de empresas centralizadas mudo a fora, e solucionado relativamente bem. Além que também já esta sendo solucionado pelo crescimento acelerado da rede lightning em cima da rede Bitcoin.

Competir na arena de dinheiro forte requer um comprometimento surreal a descentralização e propriedades que são verdadeiramente difíceis de serem modificadas e atacadas. Infelizmente outras moedas não conseguem competir nessa arena visto que na realidade elas foram construídas tipicamente por equipes centralizadas visando o lucro, e não como um bom acidente de um ecossistema lentamente crescente construído por cypherpunks.

## Desenvolvimentos Futuros no Bitcoin

Neste ponto, já passamos por toda a questão de *inventar o Bitcoin* e cobrimos como a rede evoluiu ao longo do tempo. Agora olhamos para o futuro e cobrimos algumas das melhorias de curto prazo que virão para o Bitcoin.

O Bitcoin é uma camada de dinheiro programável sobre a qual podemos construir muitos serviços. Este é um conceito totalmente novo e estamos apenas começando a ter conhecimento do que é possível ser feito.

### Lightning Network

Como discutimos acima, o Bitcoin teve problemas com taxas altas à medida que o espaço em bloco se tornou cada vez mais procurado. Hoje, o Bitcoin é capaz de apenas cerca de 3 a 7 transações por segundo com base no número de transações que cabem em um bloco. Lembre-se que cada transação pode, na verdade, ser um pagamento para centenas de pessoas por lote. Ainda assim, não tem a capacidade suficiente para se tornar uma rede global de pagamentos.

Uma solução ingênua pode ser aumentar o tamanho do bloco, e de fato várias moedas concorrentes, incluindo

o Bitcoin Cash, tentaram essa abordagem. O Bitcoin não segue esse caminho porque aumentar o tamanho do bloco impactaria negativamente as características de descentralização, como o número de nodes e a dispersão geográfica. Mesmo que um aumento no tamanho do bloco fosse possível devido a melhorias no hardware, há também o problema de que a natureza descentralizada do Bitcoin significa que um hard fork que tenta mudar o tamanho do bloco causaria muitos problemas, e provavelmente ocorreria outra divisão da blockchain, criando assim, uma moeda diferente.

Um aumento no tamanho do bloco também não resolveria o problema de tornar o Bitcoin adequado como um sistema de pagamento mundial - ele simplesmente não seria tão escalável. É aqui que entra a Lightning Network: Outro protocolo e conjunto de implementações de software que criam transações offchain de Bitcoins. The Lightning Network pode ser o assunto de todo um livro, mas vamos discuti-la brevemente.

A ideia da Lightning é que nem todas as transações precisam ser registradas na blockchain. Por exemplo, se você e eu estamos em um bar comprando bebidas, podemos abrir uma conta no bar e resolver no final da noite. Realmente não faz sentido cobrarmos de nosso cartão de crédito por cada bebida, pois é uma perda de tempo. Com o Bitcoin, usar a energia equivalente à de um país inteiro ao confirmar a compra de um café ou cerveja e ter essa compra registrada o tempo todo em milhares de computadores em todo o mundo não é escalonável nem particularmente bom para a privacidade.

A Lightning Network, se for bem-sucedida, melhorará muitas das desvantagens do Bitcoin:

1. Transferência de transações virtualmente ilimitada.

Centenas de milhares de micro transações poderiam ser realizadas usando a blockchain Bitcoin uma vez, como liquidação final;

2. Confirmações instantâneas; não há necessidade de esperar que os blocos sejam minerados;

3. Taxas de transação de menos de um centavo adequadas para micro pagamentos, como pagar um centavo para ler um blog;

4. Maior privacidade. Apenas as partes que participam da transação precisam saber sobre ela, ao contrário de uma transação em rede que é transmitida para o mundo inteiro.

A Lightning usa o conceito de canais de pagamento, que são transações reais de Bitcoin na blockchain que bloqueiam uma certa quantidade de Bitcoin e o tornam disponível na Lightning Network para transferência instantânea e quase gratuita. A Lightning Network está nos estágios iniciais, mas já se mostra promissora. Você pode verificar o site https://yalls.org/ que usa micro pagamentos baseados na Lightning para disponibilizar a leitura de artigos.

### Bitcoin no Espaço

O Bitcoin faz um excelente trabalho de ser resistente à censura, pois é resistente ao confisco (você pode carregá-lo em sua cabeça) e resistente à censura de transferência, uma vez que requer apenas um minerador honesto na rede para garantir suas transações (e você pode minerar você mesmo).

No entanto, sendo o Bitcoin transmitido pela Internet, é suscetível de censura em nível de rede. Os regimes autoritários que querem reprimir a atividade podem tentar bloquear o tráfego de Bitcoin que entra e sai de seu país.

O Blockstream Satellite é o primeiro esforço para contornar a censura de rede em nível estadual, bem como alcançar áreas remotas que podem não ter conexões com a Internet. Este satélite permite que qualquer pessoa com uma antena parabólica e equipamento relativamente barato conecte e baixe a blockchain do Bitcoin, com comunicação bidirecional em breve. Agora também existem esforços como o TxTenna para construir redes fora da rede elétrica. Quando acoplado a uma conexão via satélite, esse tipo de configuração seria quase imparável[2].

## Pesquisa Futura

Então é isso. Você passou pelo exercício de *Inventar o Bitcoin* e, com sorte, emergiu do outro lado do espelho, pronto para explorar mais sobre o assunto. Onde você conseguirá mais informações? Aqui estão alguns recursos para ajudá-lo a explorar a toca do coelho:

Para saber mais sobre a economia por trás do Bitcoin:

- O padrão Bitcoin do Saifedean Ammous;
- Criptoativos do Chris Burniske e Jack;
- Pesquisar no Google: Economia Austríaca;

[2]Nota do tradutor: Atualmente um grupo de brasileiros usou ondas de rádio para colocar uma transação na rede usando a Lua como ponto de reflexo. Veja mais em `https://livecoins.com.br/brasileiros-enviam-bitcoin-a-lua-na-frente-de-elon-musk/`

- Bitcoin Investment Theses do Pierre Rochard;
- The Bullish Case for Bitcoin do Vijay Boyapati;
- For kids: Bitcoin Money do michael Caras.

Para se aprofundar na ciência da computação:

- O whitepaper do Bitcoin escrito por Satoshi Nakamoto;
- Mastering Bitcoin do Andreas Antonopulous;
- O Seminário do Jimmy Song;
- Programming Blockchain também do Jimmy Song.

Para se aprofundar na história e filosofia do Bitcoin:

- Planting Bitcoin por Dan Held;
- Bitcoin Governance do Pierre Richard;
- Bitcoin Past and Future do Murad Mahmudov;
- Todos os vídeos feitos por Andreas Antonopulous, especialmente Currency Wars e The Monument of Immutability.

Uma grande parte do ecossistema Bitcoin vive no Twitter. Deixarei aqui um punhado de pessoas, sem uma ordem específica, que seria interessante seguir. Comece nesta lista e vá diversificando conforme for encontrando novas mentes que caíram na toca do coelho:

- @lopp
- @pwuille

- @adam3us
- @danheld
- @TraceMayer
- @pierre_rochard
- @bitstein
- @Melt_Dem
- @theonevortex
- @WhatBitcoinDid
- @stephanlivera
- @TheBlock__
- @TheLTBNetwork
- @real_vijay
- @jimmysong
- @Excellion
- @starkness
- @roasbeef
- @saifedean
- @giacomozucco
- @Snyke
- @aantonop

- @MustStopMurad
- @peterktodd
- @skwp (Autor do livro)
- @KoreaComK (Tradutor do livro)

Você pode encontrar mais textos do autor do livro em `https://yanpritzker.com`. Vejo você do outro lado.

# Agradecimentos

Obrigado às diversas pessoas que me deram feedback durante os primeiros rascunhos deste livro. Em particular: Joe Levering, Phil Geiger, Yury Pritzker, Jonathan Wheeler e Walter Rosenberg.

Obrigado ao Jimmy Song por seu seminário de programação na Blockchain, que me deu o chute necessário que precisava para montar este texto.

# Sobre o Autor

Yan Pritzker é desenvolvedor e empreendedor em startups há 20 anos. Mais recentemente, ele foi o CTO cofundador da Reverb.com, onde administrou a tecnologia e a infraestrutura durante o período de 2012 a 2018. Hoje ele está focado em educação e consultoria em Bitcoin para startups no estágio inicial.

Yan escreve sobre Bitcoin e tópicos relacionados em yanpritzker.com.

Você também pode segui-lo no Twitter: @skwp.