Introdução

Passava da meia-noite e muitos dos convidados haviam já ido para a cama, deixando ficar os copos sujos com os restos ambarinos de uísque de qualidade. A distribuidora de jogo contratada a um casino local saíra meia hora antes, mas os jogadores resistentes haviam-na convencido a deixar-lhes a mesa e as cartas, de modo a que pudessem continuar a jogar. O grupo que ainda se debruçava sobre o feltro e as fichas parecia inexistente debaixo das traves de madeira do teto abobadado de três metros de altura. A enorme parede de janelas no outro lado da mesa dava para um longo cais que se agitava com as águas do lago Tahoe.

Sentado num dos extremos da mesa, de costas para o lago, o jovem Erik Voorhees, de vinte e nove anos de idade, não parecia alguém que estivera desempregado meros três anos antes, atolado em dívidas dos cartões de crédito e que fazia biscates para pagar um apartamento no New Hampshire. Naquela noite, nos seus sapatos de verniz e *jeans* de marca, Erik enquadrava-se na perfeição com todos os outros e conversava tranquilamente com o gestor de fundos de cobertura ao seu lado. O cabelo começava a rarear, algo notório nas entradas sobre a testa, mas Erik continuava com uma expressão caracteristicamente pueril. De covinhas juvenis em riste, Erik gracejou quanto ao seu mau desempenho no jogo de póquer da véspera, chamando-lhe parte da sua «estratégia de vida».

«Estava a preparar-me para hoje», comentou, com um sorriso rasgado, empurrando depois uma pilha de fichas para o centro da mesa.

Erik podia dar-se ao luxo de ter perdas desse montante. Vendera recentemente um *site* de jogo financiado pela enigmática moeda digital e rede de pagamentos conhecida como Bitcoin. Comprara o *site* por cerca de $225 em 2012, recriara-o como SatoshiDice, e vendera-o um ano depois por $11 milhões. Era ainda detentor de uma reserva de Bitcoins que começara a adquirir anos antes, quando cada Bitcoin valia apenas uma mancheia de dólares. Uma Bitcoin valia agora cerca de $500, dando-lhe um acervo de milhões. Inicialmente menosprezado pelos investidores e pelos homens de negócios sérios, Erik atraía agora bastante interesse vindo do topo. Fora convidado para o lago Tahoe por Dan Morehead, o gestor de fundos ao seu lado na mesa de póquer, cujo objetivo era sondar quem já fizera fortunas na corrida ao ouro pela Bitcoin.

O impulso que levara Voorhees, e para muitos dos outros presentes na casa de Morehead, a entrar na tal corrida ao ouro tivera tudo e nada que ver com a vontade de enriquecer. Pouco depois de ficar a par da existência da tecnologia a partir de uma publicação no Facebook, Erik previu que o valor de cada Bitcoin viria a crescer astronomicamente. Claro que desde há muito que acreditava que esse crescimento seria uma consequência do complexo código informático da Bitcoin que vinha a recriar muitas das principais estruturas de poder do mundo, entre elas os bancos de Wall Street e os governos internacionais – fazendo ao dinheiro o que a Internet fizera aos serviços postais e à indústria dos *media*. Para Erik, o crescimento da Bitcoin não serviria apenas para o tornar abastado; levaria igualmente a um mundo mais justo e pacífico em que os governos não teriam meios para financiar guerras e os indivíduos controlariam o seu dinheiro e o seu destino.

Com tais ambições, não admirava que Erik tivesse tido um progresso atribulado desde os tempos de indigência em New Hampshire. Depois de se mudar para Nova Iorque, ajudara a convencer os gémeos Winklevoss, Tyler e Cameron, de fama facebookiana, a investirem quase um milhão de dólares numa *startup* chamada BitInstant que ele ajudara a criar. Todavia, essa relação terminou violentamente, após o que Erik se despediu da empresa e se mudou para o Panamá com a namorada.

Mais recentemente, Erik vinha a passar grande parte do seu tempo no gabinete no Panamá, a lidar com investigadores da Comissão de Títulos e Câmbios americana – uma das principais agências reguladoras financeiras – que averiguavam um negócio em que ele vendera ações de uma das suas *startups* em troca de Bitcoins. As ações haviam garantido avultados dividendos aos investidores. E, segundo a opinião de Erik, as entidades reguladoras nem sequer compreendiam a tecnologia, mas estavam certas ao afirmar que ele não registara as ações junto delas. Não obstante, uma investigação era melhor que a situação vivida por um dos antigos sócios de Erik na BitInstant, que fora detido dois meses antes, em janeiro de 2014, acusado de lavagem de dinheiro.

Entretanto, Erik deixara de se assustar com facilidade, algo facilitado pelo facto de, ao contrário de muitos dos seus semelhantes, ter um bom sentido de humor em relação a si próprio e ao movimento quixotesco no qual se vira envolvido.

«Faço por me lembrar de que é provável que a Bitcoin venha a colapsar», diria. «Por mais envolvido que eu esteja, faço por me controlar e por me recordar de que é normal que as novas coisas inovadoras falhem. Ajuda a manter a sanidade.»

Claro que Erik prosseguiu, e não só por causa do dinheiro que lhe enchera a conta. Foi também devido ao novo dinheiro que ele e os outros presentes no lago Tahoe estavam a ajudar a criar – um novo tipo de dinheiro que ele acreditava poder vir a mudar o mundo.

—

O conceito da Bitcoin vira a luz do dia cinco anos antes, em circunstâncias mais modestas, quando fazia parte de uma lista de correspondência obscura de um autor indistinto que dava pelo nome de Satoshi Nakamoto.

Logo à partida, Satoshi imaginou uma analogia digital para o velhinho ouro: um novo tipo de moeda universal que pudesse ser detida por todos e gasta em qualquer ponto do globo. À semelhança do ouro, estas novas moedas digitais valeriam apenas o que alguém estivesse disposto a pagar por elas: inicialmente, nada. Mas o sistema fora concebido

para que, à semelhança do ouro, as Bitcoins fossem sempre escassas (só se emitiriam 21 milhões de Bitcoins) e difíceis de falsificar. Tal como o ouro, para libertar moedas novas da fonte era preciso algum trabalho, no caso das Bitcoins, trabalho informático.

A Bitcoin tinha ainda vantagens óbvias em relação ao ouro enquanto sítio onde armazenar valor. Não era preciso um navio para transportar Bitcoins de Londres para Nova Iorque – bastava um código digital pessoal e o clique de um rato. Como segurança, Satoshi confiava em fórmulas matemáticas inquebráveis no lugar de guardas armados.

Claro que a comparação com o ouro não explicava por completo o motivo por que a Bitcoin acabou por chamar tanta atenção. Cada barra de ouro sempre existiu independentemente de todas as outras barras. As Bitcoins, à semelhança de todos os *sites* do mundo, que só existem na rede descentralizada conhecida como Internet, foram concebidas para se encontrarem numa rede descentralizada de arquitetura inteligente. À semelhança da Internet, a rede Bitcoin não era gerida por uma autoridade central. Ela era, isso sim, construída e mantida por todas as pessoas que a ela ligassem o computador, algo que qualquer indivíduo, em qualquer parte do mundo, poderia fazer. No caso da Internet, aquilo que ligava toda a gente era um conjunto de regras de *software*, conhecido como protocolo da Internet, que regiam o modo como a informação se deslocava. A Bitcoin contava com um protocolo de *software* próprio – as regras que ditavam o funcionamento do sistema.

Os pormenores técnicos do funcionamento deste sistema são de uma complexidade atordoante – envolvem matemática e criptografia avançadas. Contudo, desde os primeiros tempos que um pequeno grupo de seguidores dedicados viu que, na sua base, a Bitcoin era, pura e simplesmente, uma forma nova de criar, manter e enviar dinheiro. As Bitcoins não eram como os dólares e os euros, criados por bancos centrais e mantidos e transferidos por instituições financeiras poderosíssimas. Tratava-se, isso sim, de uma moeda criada e sustentada pelos utilizadores, com dinheiro novo a ser distribuído lentamente por quem ajudava a manter a rede.

Uma vez que o seu objetivo era pôr em causa algumas das mais poderosas instituições da nossa sociedade, desde o início que a rede Bitcoin

foi descrita pelos seguidores em termos utópicos. Tal como a Internet roubou poder às grandes organizações dos *media*, deixando-o nas mãos de *bloggers* e de dissidentes, a Bitcoin prometia roubar poder aos bancos e aos governos e distribuí-lo pelas pessoas que usavam o dinheiro.

Era uma conversa altaneira e atraiu muito desprezo – quando sequer ouvia falar disso, a maior parte dos comuns mortais imaginou este dinheiro digital algures entre um *Tamagotchi* e um esquema de Ponzi.

Todavia, a Bitcoin teve a felicidade de entrar no mundo num momento utópico, na sequência de uma crise financeira que expusera muitos dos problemas do nosso sistema financeiro e político, o que criou o desejo de alternativas. O Tea Party, o Occupy Wall Street e o WikiLeaks, entre outros, tinham objetivos díspares, mas estavam unidos na vontade de expropriar a elite privilegiada do seu poder, entregando-o aos indivíduos. A Bitcoin garantia uma solução tecnológica potencial para tais sonhos. A variedade de pessoas que abandonaram as suas vidas anteriores em busca da promessa trazida por essa tecnologia mostra até que ponto a Bitcoin apelava aos seus seguidores – entusiastas como Erik Voorhees e muitos dos seus novos amigos. A juntar a tudo isso, se a Bitcoin resultasse, os primeiros utilizadores tornar-se-iam fabulosamente abastados. Tal como Erik gostava de dizer, «Nunca se vira uma coisa que nos pudesse deixar ricos, ao mesmo tempo que mudava o mundo.»

Uma vez que trazia em si a oportunidade de fazer dinheiro, a Bitcoin não se limitava a atrair revolucionários descontentes. Antes de criar o seu fundo de cobertura, o anfitrião de Erik, Dan Morehead, estudara em Princeton e trabalhara no Goldman Sachs. Morehead era uma figura destacada entre os interesses abastados que nos últimos tempos vinham a injetar dezenas de milhões de dólares no ecossistema da Bitcoin, sempre de olho em grandes dividendos. Em Silicon Valley, os investidores e os empreendedores ansiavam por formas de usar a Bitcoin para melhorar os sistemas de pagamento existentes, como o PayPal, o Visa e a Western Union, e roubar o negócio a Wall Street.

Mesmo quem nutria pouco afeto pelo Occupy Wall Street ou pelo Tea Party compreendia as vantagens de uma moeda mais universal que não tivesse de ser convertida em cada fronteira; um método de

pagamento digital que não nos obrigasse a fornecer as informações de identificação de cada vez que o usássemos; a justiça de uma moeda que mesmo os mais pobres do mundo pudessem manter numa conta digital sem terem de pagar comissões exorbitantes, ao invés de terem de depender apenas de dinheiro vivo; e a conveniência de um sistema de pagamento que possibilitasse aos serviços *online* cobrarem um ou dois cêntimos – para ver um único artigo ou saltar um anúncio –, contornando os atuais limites impostos pela cobrança mínima de 20 ou 30 cêntimos por uma transação feita com cartão de crédito.

Claro que muitos dos interessados nas aplicações mais práticas da Bitcoin acabaram a falar da tecnologia em termos revolucionários: uma oportunidade de fazer dinheiro perturbando o *status quo* existente. Ao jantar, algumas horas antes do jogo de póquer tardio, Morehead gracejara quanto ao facto de, na altura, todas as Bitcoins no mundo valerem aproximadamente o mesmo que a empresa Urban Outfitters, fornecedora de *jeans* rasgados e decorações de residências universitárias – cerca de $5 mil milhões.

«É de loucos, não?» comentou Morehead. «O mais certo será que daqui a uns séculos, quando andarem a investigar a nossa sociedade, à *Planeta dos Macacos*, a Bitcoin tenha tido mais impacto no mundo do que a Urban Outfitters. Ainda estamos nos primeiros dias.»

Muitos banqueiros, economistas e agentes do governo ignoraram os fanáticos da Bitcoin como promotores ingénuos de um frenesim especulativo semelhante à loucura holandesa das túlipas, quatro séculos antes. Em várias ocasiões, a história da Bitcoin deu razão aos alertas dos críticos, ilustrando os riscos contidos no progresso para um mundo mais digitalizado sem uma autoridade central. Poucas semanas antes do encontro promovido por Morehead, a maior empresa Bitcoin do mundo, o posto de câmbio conhecido como Mt. Gox anunciara a perda do equivalente a cerca de $400 milhões de Bitcoins dos utilizadores e o seu colapso – era o mais recente de uma série escândalos do género a afligir os utilizadores de Bitcoin.

Claro que nenhuma das crises destruiu o entusiasmo dos fiéis da Bitcoin, com o número de utilizadores a crescer, mesmo com todas as adversidades. Na altura do encontro de Morehead haviam sido abertas

mais de cinco milhões de carteiras Bitcoin em vários *websites*, a maioria fora dos Estados Unidos. Os indivíduos em casa de Morehead representavam a grande variedade de personagens que haviam sido atraídas: entre eles estavam um antigo executivo da Wal-Mart que viera propositadamente da China, um recém-licenciado da Eslovénia, um banqueiro de Londres e dois antigos elementos de uma associação estudantil da Georgia Tech. Alguns eram motivados pelo ceticismo contra o governo, outros pelo ódio contra os grandes bancos e outros ainda por experiências pessoais mais íntimas. O executivo chinês da Wal-Mart, por exemplo, crescera com avós que haviam escapado à revolução comunista apenas na posse da fortuna que haviam acumulado em ouro. Num mundo inconstante, a Bitcoin parecia-lhe uma alternativa bastante mais portátil.

Esta narrativa centra-se nestas pessoas que, em lugares diferentes e com motivações diversas, haviam criado a Bitcoin e continuam a fazê-lo. Satoshi, o criador da Bitcoin, desapareceu em 2011, deixando *software* de código aberto que os utilizadores da Bitcoin podiam atualizar e melhorar. Cinco anos depois estimava-se que apenas 15 por cento do código informático básico da Bitcoin fora escrito por Satoshi. À parte o trabalho no *software*, o poder da Bitcoin, à semelhança do que acontece com todo o dinheiro, dependia do número de pessoas a usá-la. Cada pessoa nova a juntar-se aumentava a probabilidade de sobrevivência.

Assim sendo, esta não é uma normal história sobre uma *startup*, sobre um génio solitário a moldar o mundo à sua imagem e a ganhar resmas de dinheiro. O que temos aqui é, isso sim, a história de uma invenção conjunta que se aproveitou de muitas das principais correntes do nosso tempo: a fúria contra o governo e Wall Street; as batalhas entre Silicon Valley e a indústria financeira; e as esperanças que depositámos na tecnologia para que esta nos salve da nossa fragilidade humana, a par do medo gerado pelo poder da tecnologia. Cada indivíduo abordado neste livro teve um motivo muito pessoal para se dedicar a esta nova ideia, mas todas as suas vidas foram enformadas pelas ambições, pela ganância, pelo idealismo e pela fragilidade humana que transformaram a Bitcoin de obscuro artigo académico em indústria multimilionária.

Alguns dos participantes acabaram com o tipo de fortuna exposta na casa de Morehead, onde a entrada de pedra está decorada com o seu timbre pessoal. Outros acabaram na pobreza e mesmo na prisão. A Bitcoin propriamente dita está sempre a um passo de ser um fracasso absoluto. Claro que mesmo que venha a colapsar, ela já serviu como um dos mais fascinantes testes sobre como o dinheiro funciona, quem lucra com ele e como pode ser melhorado. É improvável que venha a substituir o dólar em cinco anos, mas ela deixa-nos vislumbrar onde poderemos acabar quando o governo deixar, inevitavelmente, de imprimir as caras de presidentes mortos em papel caro.

Na manhã a seguir ao grande jogo de póquer, enquanto os convidados faziam as malas para voltarem a casa, Voorhees sentou-se no extremo do cais atrás da mansão de Morehead, ligeiramente acima da água depois de um inverno com pouca neve. A alegria exibida à mesa de jogo na véspera desaparecera. Parecia contrariado ao falar sobre a recente decisão de se afastar do cargo de CEO da *startup* de Bitcoin que vinha a gerir no Panamá. Receoso de prejudicar a empresa, a sua posição impedira-o de falar acerca do potencial revolucionário da Bitcoin.

«O meu sonho não é gerir um negócio, é construir o mundo da Bitcoin», explicaria.

A juntar a isso, a namorada fartara-se de viver no Panamá e Erik tinha saudades da família nos Estados Unidos. Dali a algumas semanas, tencionava regressar ao Colorado, onde crescera. Todavia, a Bitcoin fez com que se tornasse alguém muito diferente da pessoa que era ao partir. Uma situação com que muitos dos seus camaradas *bitcoiners* se identificavam.

PARTE UM

Capítulo 1

10 de janeiro de 2009

Era sábado. Dia de aniversário do filho. O tempo em Santa Bárbara estava lindo e a cunhada chegara de França. Mas Hal Finney precisava de estar ao computador. Era um dia que vinha antecipando há meses e, em certa medida, há décadas.

Hal nem sequer tentou explicar à mulher, Fran, aquilo que o mantinha ocupado. Ela era fisioterapeuta e raramente compreendia o seu trabalho ao computador. Mas, por onde sequer começar com aquele trabalho? «Querida, vou tentar fazer um tipo novo de dinheiro.»

Essa era, na essência, a sua intenção, quando, depois de uma longa manhã, se sentou no modesto escritório caseiro: um canto da sala com uma velha secretária, ocupada principalmente por quatro monitores de vários tamanhos e marcas, todos ligados a computadores diferentes que usava para trabalho e assuntos pessoais. Todos os espaços que não estivessem ocupados por computadores estavam cobertos por um montão de papéis, livros de exercícios e manuais de programação velhos. Não parecia nada de especial mas, ali sentado, Hal via o pátio além da sala de estar, banhado pelo sol da Califórnia, mesmo no meio de janeiro. Na alcatifa à esquerda estava *Arky*, o seu fiel leão-da-rodésia, batizado com o nome de uma estrela da constelação do Boieiro. Ali sentia-se em casa e ali fizera muito do seu trabalho criativo enquanto programador.

Ligou o enorme *IBM ThinkCentre*, acomodou-se e abriu o *website* que recebera por *email* na véspera, enquanto estava no trabalho: www.bitcoin.org.

A Bitcoin surgira-lhe pela primeira vez no monitor meses antes, numa mensagem enviada para uma das muitas listas de difusão que

subscrevia. As trocas ocorriam habitualmente entre as personalidades familiares com as quais ele vinha a falar há anos e que povoavam o cantinho relativamente especializado da programação em que trabalhava. Não obstante, aquele *email* em particular chegara de um nome pouco familiar – Satoshi Nakamoto – e descrevia o que era referido como «e-dinheiro» com o apelativo nome Bitcoin. O dinheiro digital era algo com que Hal vinha fazendo experiências há muito tempo, o bastante para o deixar cético perante a ideia de que pudesse vir a funcionar. Mas algo se destacava naquele *email*. Satoshi prometia um tipo de dinheiro que não precisaria de um banco, nem de qualquer outra entidade externa para o gerir. Era um sistema que podia viver inteiramente na memória de computação coletiva das pessoas que o usassem. Hal sentiu-se particularmente atraído pela asserção de Satoshi, segundo a qual os utilizadores podiam deter e trocar Bitcoins sem providenciarem informação identificadora a quaisquer autoridades centrais. Hal passara a maior parte da vida profissional a trabalhar em programas que permitiam às pessoas furtar-se à cada vez mais atenta vigilância do governo.

Depois de ler as nove páginas da descrição, contida no que se assemelhava a uma tese académica, Hal respondeu entusiasticamente no grupo:

> «Quando a Wikipedia começou, nunca pensei que fosse funcionar, mas ela revelou-se um grande sucesso por muitas das mesmas razões.»

Perante o ceticismo de outros na lista de *emails*, Hal instara Satoshi a escrever algum código para o sistema que descrevera. Meses depois, nesse sábado de janeiro, Hal descarregou o código de Satoshi a partir do *website* Bitcoin. Um simples ficheiro.exe instalou o programa Bitcoin e abriu automaticamente uma janela de aspeto limpo no ambiente de trabalho.

Ao ser aberto pela primeira vez, o programa gerou automaticamente uma lista de endereços Bitcoin que seriam os números da conta de Hal no sistema, bem como a senha, ou chave privada, que lhe daria acesso a cada endereço. A par disso, o programa continha apenas umas

quantas funções. A principal, «Enviar moedas», não parecia ser uma opção para Hal, dado que ele não tinha moedas para enviar. No entanto, antes que pudesse investigar mais, o programa teve um erro fatal.

Isso não deteve Hal. Depois de verificar os registos do computador escreveu a Satoshi a explicar o que acontecera quando o seu computador tentara ligar-se a outros computadores da rede. Além de Hal, o registo mostrava apenas outros dois computadores na rede, ambos com o mesmo endereço IP, supostamente de Satoshi e ligado a um fornecedor de serviços internet (ISP) na Califórnia.

Satoshi respondera menos de uma hora depois, manifestamente desapontado com a falha; ele afirmou ter estado a testar intensivamente o código, sem nunca encontrar qualquer problema. Todavia, disse ainda a Hal que aligeirara o programa para que fosse mais fácil descarregá-lo, o que poderia ter causado o problema.

«Acho que tomei uma decisão errada», escreveu Satoshi com uma frustração palpável.

Satoshi enviou a Hal uma nova versão do programa, reaproveitando algum do material antes descartado, e agradeceu a Hal pela ajuda. Quando também esse código falhou, Hal persistiu. Finalmente, conseguiu fazê-lo funcionar com recurso a um programa que operava fora do Microsoft Windows. Assim que ficou operacional, Hal clicou na função com o nome mais empolgante presente no menu: «Gerar moedas». Quando o fez, o processador do computador entrou audivelmente em modo acelerado.

Com tudo a funcionar, Hal pôde fazer uma pausa e dedicar-se aos deveres familiares, incluindo um jantar de família num restaurante chinês das redondezas e uma pequena festa de aniversário para o filho. As instruções que Satoshi incluíra com o *software* afirmavam que a criação de moedas poderia levar «dias ou meses, dependendo da velocidade do computador e da competição presente na rede».

Hal redigiu uma breve nota para informar Satoshi que estava tudo operacional: «Tenho de sair, mas vou deixar esta versão a correr durante um bocado.»

Hal já lera o suficiente para compreender as bases do trabalho que o computador estava a realizar. Assim que o programa Bitcoin estivesse

a correr, ligava-se a um canal de *chat*, cuja função era encontrar outros computadores que também estivessem a correr o *software* – nessa altura, basicamente apenas os computadores de Satoshi. Todos os computadores estavam a tentar capturar novas Bitcoins, que eram lançadas no sistema em lotes de cinquenta moedas. Cada novo lote de Bitcoins era atribuído ao endereço de um utilizador, que se ligava à rede e vencia uma espécie de corrida para resolver um quebra-cabeças informático. Quando um computador ganhava uma ronda da corrida e capturava novas moedas, todas as outras máquinas na rede atualizavam o registo partilhado do número de Bitcoins detidas pelo endereço Bitcoin daquele computador. Em seguida, os computadores na rede recomeçariam automaticamente a corrida, de modo a resolver um novo problema que disponibilizasse o próximo lote de cinquenta moedas.

Quando Hal regressou ao computador, ao final da tarde, viu imediatamente que já obtivera cinquenta Bitcoins, agora registadas ao lado de um dos seus endereços Bitcoin e registadas também no balanço público que mantinha o rasto de todas as Bitcoins. Estas, o septuagésimo oitavo lote de moedas geradas, contavam-se entre as primeiras 4000 Bitcoins a serem lançadas no mundo real. Nessa época não valiam rigorosamente nada, mas isso não fez esmorecer o entusiasmo de Hal. Num *email* de felicitações a Satoshi, enviado a toda a lista de contactos, permitiu-se um toque de imaginação.

«Imaginem que a Bitcoin tem sucesso e se torna o sistema de pagamento dominante em todo o mundo», escreveu. «Nesse caso, o valor total da moeda será igual ao valor total da riqueza presente no mundo.»

Pelos seus cálculos, isso faria com que cada Bitcoin valesse uns dez milhões de dólares. «Mesmo que as probabilidades de a Bitcoin vir a ter êxito a esse nível sejam escassas, serão mesmo de uma hipótese em cem milhões? É algo em que pensar», escreveu, antes de se desligar.

Já há muito que Hal Finney acreditava que o futuro seria diferente do passado em inúmeros aspetos.

Um de quatro filhos de um engenheiro petrolífero itinerante, Hal devorara os clássicos da ficção científica, mas também lera livros de cálculo por

diversão e acabara por estudar no Instituto de Tecnologia da Califórnia (Cal Tech). Nunca recuara perante um desafio intelectual. Durante o ano de caloiro tirou um curso em teoria de campo gravítico que se destinava a estudantes já licenciados.

Não obstante, ele não era o típico marrão – homem grande e atlético, que adorava esquiar nas montanhas da Califórnia, não padecia da falta de competências sociais comum entre os estudantes do Cal Tech. Este espírito ativo passou para as suas demandas intelectuais. Quando leu os romances de Larry Niven, que debatiam a possibilidade de congelar criogenicamente humanos e devolvê-los mais tarde à vida, Hal não se limitou a ponderar o potencial na sua residência. Localizou uma fundação dedicada a tornar esse processo uma realidade e inscreveu-se para receber a revista da Fundação de Extensão da Vida Alcor. Acabaria por se decidir a pagar para ter o seu corpo, bem como o dos familiares nas câmaras geladas da Alcor, perto de Los Angeles.

O surgimento da Internet fora uma benesse para Hal, permitindo-lhe ligar-se a pessoas em lugares distantes com ideias igualmente obscuras, porém radicais. Ainda antes da invenção do primeiro *browser*, Hal já se juntara a algumas das comunidades *online* pioneiras, com nomes como *cypherpunks* e *extropianos*, onde se lançou em debates sobre como a nova tecnologia poderia ser usada para moldar o futuro com que todos eles sonhavam.

Mais do que qualquer outro, um tema em particular obcecava este grupo: como viria a tecnologia a alterar o equilíbrio de poder entre corporações e governos, de um lado, e, do outro, entre os indivíduos. A tecnologia dava claramente aos indivíduos novos poderes. A incipiente Internet permitia a estas pessoas comunicar com mentes semelhantes e espalhar as suas ideias de um modo até então impossível. No entanto, assistia-se a uma discussão constante sobre a forma como a insidiosa digitalização da vida também proporcionava aos governos e às empresas um maior domínio sobre aquele que talvez seja o bem mais valioso e perigoso na era da informação: a própria informação.

Tal como seria óbvio, os governos já mantinham registos acerca dos cidadãos antes dos computadores, mas a maior parte das pessoas

tinha estilos de vida que impossibilitava a obtenção de muita informação. Porém, na década de 1990, muito antes de a Agência de Segurança Nacional (NSA) ser apanhada a espiar os telemóveis de cidadãos comuns e de as políticas de privacidade do Facebook se terem tornado matéria de debate nacional, os *cypherpunks* viram que a digitalização da vida tornava muito mais fácil às autoridades recolher dados sobre os cidadãos, deixando os dados vulneráveis à captura por agentes mal-intencionados. A questão que consumia os *cypherpunks* era como proteger a informação pessoal e salvaguardar a privacidade. *O Manifesto Cypherpunk*, difundido em 1993 pelo matemático de Berkeley Eric Hughes, abria assim: «Para uma sociedade aberta na era eletrónica é necessário privacidade.»

Esta linha de pensamento era, em parte, produto das políticas libertárias que se haviam popularizado na Califórnia nas décadas de 1970 e 1980. Suspeitar do governo era quase natural para programadores como Hal, que trabalhavam para criar um novo mundo através do código, sem precisar de depender de mais ninguém. Hal interiorizara estas ideias no Cal Tech e através da leitura dos romances de Ayn Rand. Não obstante, o tema da privacidade na era da Internet era igualmente apelativo além dos círculos libertários, entre os ativistas dos direitos humanos e de outros movimentos de protesto.

Nenhum dos *cypherpunks* viu como solução para o problema a simples fuga à tecnologia. Em vez disso, Hal e os outros procuraram encontrar respostas na tecnologia e, particularmente, na ciência da encriptação da informação. Historicamente, as tecnologias de encriptação haviam sido um privilégio reservado, em grande medida às instituições mais poderosas. Os indivíduos privados podiam tentar encriptar as suas comunicações, mas os governos e as forças armadas dispunham quase sempre do poder para quebrar esses códigos. Todavia, nas décadas de 70 e 80 do século passado, os matemáticos de Stanford e do MIT desenvolveram uma série de progressos que possibilitaram, pela primeira vez, que as pessoas comuns encriptassem, ou empastelassem, as mensagens de um modo que só podia ser desencriptado pelo destinatário pretendido, sem poder ser decifrado nem pelos mais poderosos supercomputadores.

Cada utilizador da nova tecnologia, designada por «criptografia com chave pública», receberia uma chave pública – uma mistura única de letras e números que serve como uma espécie de endereço que pode ser livremente distribuído – e uma chave privada correspondente, que supostamente só é conhecida do utilizador. As duas chaves estão relacionadas, matematicamente, de uma maneira que assegura que apenas a utilizadora (chamemos-lhe Alice, como os criptógrafos faziam amiúde), munida da sua chave privada, pode descodificar mensagens enviadas para a sua chave pública, e só ela pode assinar mensagens associadas com a sua chave pública. A relação única entre cada chave pública e privada era determinada por complexas equações matemáticas construídas de modo tão inteligente que ninguém com uma chave pública específica seria alguma vez capaz de recuar no processo para determinar a correspondente chave privada – nem mesmo o mais poderoso supercomputador. Toda esta construção viria mais tarde a desempenhar um papel central no *software* Bitcoin.

Hal teve o primeiro contacto com o potencial da cifragem com chave pública em 1991, graças ao criptógrafo pioneiro David Chaum, que se dedicava a experimentar maneiras de usar a cifragem com chave pública para proteger a privacidade individual.

«Parecia-me óbvio», afirmou Hal aos outros *cypherpunks* acerca do seu primeiro contacto com os escritos de Chaum. «Eis-nos perante os problemas da perda de privacidade, informatização insidiosa, bases de dados massivas, mais centralização – e Chaum oferece um rumo completamente diferente, uma direção que põe o poder nas mãos dos indivíduos e não dos governos e das corporações.»

Tal como era hábito, quando encontrava algo especialmente interessante, Hal não se limitava a ler passivamente sobre o assunto. À noite e ao fim de semana, depois do trabalho como criador de *software*, começou a trabalhar num projeto voluntário, conhecido como Pretty Good Privacy (PGP), que permitia o envio de mensagens que podiam ser encriptadas com recurso a cifragem com chave pública. O fundador do projeto, Phil Zimmerman, era um ativista antinuclear que pretendia proporcionar aos dissidentes uma forma de comunicar ao abrigo

da vigilância dos governos. Não demorou para que Zimmerman fizesse de Hal o primeiro funcionário da PGP.

Os projetos idealistas como o PGP contavam, regra geral, com uma audiência pequena, mas o potencial da tecnologia tornou-se notório quando procuradores federais lançaram uma investigação criminal à PGP e a Zimmerman. O governo categorizou as tecnologias de encriptação, como a PGP, como armas de guerra, o que tornava a sua exportação ilegal. Ainda que tivessem acabado por abandonar o caso, Hal passou anos a ser discreto acerca do envolvimento com a PGP, sem nunca poder assumir o crédito de muitos dos seus importantes contributos para o projeto.

Os *extropianos* e os *cypherpunks* estavam a trabalhar em várias experiências diferentes que podiam ajudar a dar poder aos indivíduos contra as fontes tradicionais de autoridade; não obstante, o dinheiro sempre esteve no centro dos esforços de recriação do futuro.

O dinheiro é para qualquer economia de mercado aquilo que a água, o fogo ou o sangue são para o ecossistema humano: uma substância básica essencial para que o resto funcione. Para os programadores, as moedas existentes, válidas apenas dentro de fronteiras nacionais e sujeitas a bancos de uma grande incompetência tecnológica, pareciam desnecessariamente limitadas. A ficção científica com que Hal e outros haviam crescido apresentava quase sempre um qualquer tipo de divisa universal que podia abranger galáxias: na saga *Guerra das Estrelas* era o crédito galáctico; na trilogia *Night's Dawn* era o crédito joviano.

Além destas ambições mais delirantes, o sistema financeiro existente era encarado pelos *cypherpunks* como uma das maiores ameaças à privacidade individual. Poucos tipos de informação revelam mais sobre Alice, a favorita dos criptógrafos, do que as suas transações financeiras. Se tivesse acesso aos extratos do seu cartão de crédito, um coscuvilheiro poderia seguir todos os seus movimentos ao longo do dia. Não é por acaso que os registos financeiros são uma das principais maneiras de apanhar fugitivos. *O Manifesto Cypherpunk* de Eric Hughes alongara-se sobre este problema: «Quando a minha identidade é revelada pelo mecanismo subjacente da transação, eu não tenho

privacidade. Não posso revelar-me seletivamente; tenho de me revelar sempre», escreveu Hughes.

«A privacidade numa sociedade aberta requer sistemas de transação anónimos», acrescentou.

Há muito que o numerário garantia uma forma anónima de fazer pagamentos, mas esse sistema pecuniário não fez a transição para o reino digital. Assim que o dinheiro se tornou digital, passou a estar sempre envolvida uma entidade terceira nas transações, sendo, por conseguinte, capaz de a rastrear. Aquilo que Hal, Chaum e os *cypherpunks* pretendiam era um tipo de dinheiro para a era digital, algo que pudesse ser seguro e infalsificável, sem sacrificar a privacidade dos utilizadores. No ano do manifesto de Hughes, Hal enviou um *email* ao grupo, imaginando um tipo de moeda digital em relação à qual «não fossem mantidos registos de onde gasto o dinheiro. Tudo o que o banco sabe é quanto levantei mensalmente.»

Um mês depois, Hal até se lembrou de um nome provocador: «Pensei hoje num novo nome para o dinheiro digital: CRASH, a partir de Crypto cASH».

Quando os *cypherpunks* finalmente se interessaram, Chaum já desenvolvera a sua versão. A partir de um instituto em Amesterdão criara o DigiCash, uma divisa *online* que podia ser gasta em qualquer parte do mundo sem que os utilizadores precisassem de divulgar qualquer informação pessoal. O sistema tirava partido da cifragem com chave pública para possibilitar o que Chaum designava como assinaturas digitais cegas, as quais permitiam efetuar transações sem divulgar qualquer informação identificativa. Quando o americano Mark Twain Bank começou a fazer experiências com o DigiCash, Hal criou uma conta.

O esforço de Chaum viria a criar anticorpos em Hal e outras pessoas. Com o DigiCash, uma organização central, nomeadamente a empresa de Chaum, precisava de confirmar todas as assinaturas digitais. Isso significava que era necessário confiar até certo ponto que essa organização central não manipularia as contas ou abriria falência. Com efeito, quando, em 1998, a empresa de Chaum faliu, o DigiCash evaporou-se com ela. Estas preocupações levaram Hal e outros a

trabalhar para criar uma moeda digital que não dependesse de uma instituição central. Obviamente, o problema era ter quem verificasse que as pessoas não estavam simplesmente a copiar e colar o dinheiro digital, gastando-o mais de uma vez. Alguns *cypherpunks* desistiram do projeto, pura e simplesmente, mas Hal não era pessoa de desistir tão facilmente.

Ironicamente, para alguém ansioso por criar um novo tipo de divisas, o interesse de Hal não era prioritariamente financeiro. Os programas que vinha a escrever, como o PGP, eram explicitamente destinados a ficarem disponíveis para qualquer um, sem custos. A sua desconfiança política em relação ao governo não era movida pelo pagamento de impostos. Durante a década de 1990, Hal calculou sempre o maior valor aplicável ao seu escalão fiscal, enviando um cheque com esse valor, a fim de evitar o incómodo de preencher os impressos; adquiriu a sua modesta casa nos arredores de Santa Barbara e nela se manteve ao longo dos anos; não parecia importar-se por ter de trabalhar a partir da sala de estar, nem com o desgaste dos sofás azuis à frente da secretária. Hal não era motivado por interesse próprio; pelo contrário, o seu trabalho parecia movido por uma curiosidade intelectual que fervilhava em cada *email* que escrevia e pela perceção daquilo que os outros mereciam.

«Grosso modo, o nosso objetivo é tornar obsoleto o Big Brother. É um trabalho importante», escreveu ele aos seus companheiros de viagem. «Se as coisas correrem bem, talvez sejamos capazes de olhar para trás e ver que foi o trabalho mais importante que alguma vez fizemos.»

Capítulo 2

1997

A ideia de criar um novo tipo de dinheiro surgirá, aos olhos de muitos, como uma tarefa algo estranha e, quiçá, fútil. Para a maioria das pessoas atuais, o dinheiro significa o mesmo em todo o lado: notas e moedas emitidas por estados soberanos. O poder de cunhar moeda é um dos direitos que definem uma nação, mesmo no caso de países tão pequenos como o Vaticano ou a Micronésia.

Não obstante, esta é uma situação relativamente recente. Até à Guerra Civil, o grosso do dinheiro em circulação nos Estados Unidos era emitido por bancos privados, dando origem a uma manta de retalhos tresloucada de notas concorrentes que podiam deixar de valer o que quer que fosse, caso os bancos que as haviam emitido colapsassem. Nessa época, muitos países dependiam das moedas estrangeiras em circulação.

Este estado de coisas dava continuação a uma longa tradição humana: o esforço aparentemente incessante para encontrar melhores formas de dinheiro, recorrendo pelo caminho a ouro, conchas, discos de pedra e casca de amoreira.

A demanda por um formato melhor de dinheiro teve sempre que ver com a busca de um modo mais fiável e uniforme de valorizar o que nos rodeia – uma única métrica que nos permita comparar de modo fiável o valor de um pedaço de madeira, de uma hora de trabalho de carpintaria ou da pintura de um quadro. Como dizia o sociólogo Nigel Dodd, o bom dinheiro é aquele que «consegue converter as diferenças qualitativas entre as coisas em diferenças quantitativas que nos permitem comercializá-las».

O dinheiro imaginado pelos *cypherpunks* parecia levar a padronização característica do dinheiro à sua lógica extrema, favorecendo a existência de uma moeda universal de uso massificado, ao contrário das moedas nacionais limitadas que atualmente levamos para todo o lado e que carecem de câmbio em cada fronteira.

No seu esforço para criar uma nova moeda, os *cypherpunks* estavam cientes das características que habitualmente encontramos na cunhagem bem-sucedida. A tendência tem sido para o bom dinheiro ser resistente (imaginemos uma nota de dólar impressa em lenços de papel), portátil (imaginemos um cêntimo que pesasse dez quilos), divisível (imaginemos que só tínhamos notas de cem dólares e nenhuma moeda), uniforme (imaginemos que todas as notas de dólar eram diferentes) e difícil de copiar (imaginemos notas que pudessem facilmente ser copiadas por todos).

No entanto, além destas características, o dinheiro sempre careceu de algo muito menos tangível, que é a fé das pessoas que o utilizam. Se deve aceitar notas de dólar pelas colheitas que tanto lhe custaram a desenvolver, um agricultor tem de acreditar que esse dólar, mesmo sendo apenas um pedaço de papel verde, valerá alguma coisa no futuro. Ao longo do tempo, a qualidade fundamental do dinheiro bem-sucedido nunca se prendeu unicamente com quem o emitiu, nem com a sua portabilidade ou durabilidade física, mas sim com o número de pessoas dispostas a usá-lo.

No século XX, o dólar serviu de moeda global e isso deveu-se (em grande medida) ao facto de a maioria das pessoas em todo o mundo acreditarem que os Estados Unidos, e o respetivo sistema financeiro, tinham mais hipóteses de sobreviver do que praticamente qualquer outro. Assim se explica o motivo que levou a que as pessoas vendessem a sua moeda nacional para manter as suas poupanças em dólares.

Há muito que a relação entre moeda e fé transformou os indivíduos capazes de criar e proteger o dinheiro em figuras semirreligiosas. A palavra *moeda* deriva do deus romano Juno Moneta, em cujos templos a moeda era cunhada. Nos Estados Unidos, os administradores do Banco Central (a Reserva Federal), cuja função é gerir o fornecimento de dinheiro, são tratados como uma espécie de oráculo; as suas

declarações são escrutinadas como as entranhas das cabras em tempos idos. Aos agentes federais atribui-se um nível de poder e independência que não se compara ao de quase qualquer outro líder governamental. A tarefa de proteger a moeda nacional é confiada a uma agência criada especialmente para o efeito, os Serviços Secretos, que só mais tarde acumularam também a responsabilidade de proteger a vida do presidente.

O anterior presidente da Reserva Federal, Alan Greenspan (que, apesar das suas imperfeições, será, porventura, o mais famoso dos oráculos da Reserva Federal) sabia que o dinheiro era algo que podia ser criado não apenas pelos bancos centrais. Num discurso proferido em 1996, quando os *cypherpunks* avançavam com as suas experiências, Greenspan declarou que imaginava a revolução tecnológica a trazer de volta o potencial para o dinheiro privado, algo que até poderia ser uma coisa boa:

> «Num futuro próximo poderíamos desenvolver propostas para que os emissores de obrigações de pagamentos eletrónicos (como cartões de débito ou "dinheiro digital") estabelecessem empresas especializadas nessa função com fortes balanços e notações de risco públicas.»

Nos anos que se seguiram às declarações de Greenspan assistiu-se a uma atividade frenética no mundo *cypherpunk*. Em 1997, um investigador britânico chamado Adam Back publicou na lista de distribuição *cypherpunk* o seu plano para aquilo que apelidava de *hashcash*, uma solução que resolvia um dos principais problemas que impedia o projeto do dinheiro digital: a impossibilidade aparente de criar um tipo de ficheiro digital que não pudesse ser copiado indefinidamente.

Para resolver o problema, Back teve uma ideia inteligente, que mais tarde viria a ser uma importante base do *software* Bitcoin. O conceito de Back usava criativamente um dos pilares centrais da criptografia assimétrica: funções de dispersão criptográficas. Estamos a falar de equações matemáticas que se resolvem com facilidade, porém, são difíceis de inverter, do mesmo modo que é relativamente fácil multiplicar 2903 por 3571 recorrendo a lápis e papel, mas é muito mais difícil

descobrir os dois números que multiplicados um pelo outro tenham o resultado de 10 366 613. Com o protocolo *hashcash*, os computadores tinham essencialmente de descobrir os dois números que se podem multiplicar para obter 10 366 613, embora os problemas do protocolo fossem bastante mais complicados do que isto. A tal ponto que a única coisa que os computadores podiam fazer era tentar várias vezes, com o objetivo de, com o tempo, conseguirem chegar à resposta certa. Quando um computador encontrava a resposta certa, ganhava *hashcash*.

A criação de *hashcash* através deste método foi muito útil no contexto do dinheiro digital, uma vez que garantia a dificuldade da sua reprodução, uma característica da maioria do bom dinheiro, mas não dos ficheiros digitais, que podem facilmente ser duplicados. Um computador tinha de executar imensas tarefas para criar cada nova unidade de *hashcash*; a este processo foi dado o nome de «protocolo prova-de-trabalho», algo que mais tarde se tornaria uma inovação essencial subjacente à Bitcoin. O principal problema do sistema de Back como forma de dinheiro digital era o facto de cada unidade de *hashcash* apenas poder ser usada uma vez, obrigando todos os envolvidos no sistema a desenvolver novas unidades sempre que precisavam de utilizar dinheiro. Outro problema era o facto de alguém que possuísse uma capacidade ilimitada de processamento conseguir produzir cada vez mais *hashcash*, reduzindo assim o valor total de cada unidade.

Um ano após Back divulgar o seu programa, dois outros membros independentes da lista *cypherpunk* inventaram sistemas que resolviam algumas das fraquezas do *hashcash*, através da criação de *tokens* digitais que careciam do protocolo prova-de-trabalho, mas que também podiam ser reutilizados. Um destes sistemas, um conceito denominado *bit gold*, foi inventado por Nick Szabo, um *cypherpunk* especializado em segurança, que confidenciou a ideia a colaboradores próximos (como Hal Finney, em 1998), embora nunca a tenha realmente posto em prática. Outro sistema, conhecido como *b-money*, foi inventado por um americano de nome Wei Dai. Hal criou a sua própria variante, com um nome definitivamente menos sensual: provas de trabalho reutilizáveis ou RPOW.

No seio da lista *cypherpunk* e de grupos relacionados, a conversa em torno destas ideias parecia, por vezes, uma discussão entre irmãos rivais, sempre a tentarem ficar por cima. Szabo disparava contra outras propostas, dizendo que, em vez de *software*, dependiam todas demasiado de *hardware* especializado. No entanto, estes homens (e eram realmente todos homens) também foram desenvolvendo um respeito profundo uns pelos outros. E apesar do fracasso das suas experiências, as suas ambições foram-se tornando maiores do que a simples criação de dinheiro anónimo. Entre outras coisas, Back, Szabo e Finney queriam contornar os custos e frustrações do sistema financeiro de então, através do qual os bancos cobravam taxas em cada transação e dificultavam a movimentação de dinheiro através das fronteiras internacionais.

«Queremos unidades de câmbio transferíveis completamente anónimas, com custos de transação muito baixos. Se o conseguirmos (e é evidente que algumas pessoas estão a usar a DigiCash e algumas outras criptomoedas), os bancos tornar-se-ão os dinossauros obsoletos que bem merecem ser», diria Back à lista *cypherpunk* imediatamente após a divulgação do *hashcash*.

Os *cypherpunks* ganharam um ideal platónico pelo qual ansiar quando, em 1999, o escritor de ficção científica Neal Stephenson publicou o seu livro *Cryptonomicon*. O romance, que se tornou lendário nos círculos *hackers*, imaginava um mundo subterrâneo alimentado por um tipo de dinheiro digital que permitia a manutenção da identidade privada. O romance incluía descrições extensas da criptografia que tornava esta realidade possível.

Não obstante, as experiências destes ciberativistas continuavam a deparar-se com obstáculos práticos no mundo real. Ninguém conseguia descobrir uma forma de criar dinheiro sem depender de uma instituição central, vulnerável ao erro ou à supervisão governamental. As experiências sofriam igualmente uma dificuldade fundamental, que era convencer as pessoas a usar e a valorizar estes novos *tokens* digitais. Quando Satoshi Nakamoto entrou em cena, a história já desmoralizara muitos dos fãs mais prováveis da Bitcoin. O objeto de criar uma criptomoeda parecia um sonho semelhante ao de transformar carvão em diamantes.

Em agosto de 2008, Satoshi emergiu do nevoeiro com um *email* enviado ao criador do *hashcash*, Adam Back, pedindo-lhe que visse um pequeno ensaio a descrever uma coisa chamada Bitcoin. Back nunca ouvira falar daquilo, nem de Satoshi, e não perdeu muito tempo com o *email*, limitando-se a apontar a Satoshi outras experiências *cypherpunk* que lhe houvessem escapado.

Seis semanas depois, por altura do Halloween, Satoshi enviou uma proposta mais bem composta para uma lista de distribuição especializada em criptografia que era fortemente académica, uma das principais sucessoras da defunta lista *cypherpunk*. Como era habitual nesta comunidade, Satoshi não forneceu detalhes quanto à sua identidade e contexto e ninguém perguntou. O que importava era a ideia, não a pessoa. Em linguagem cuidadosa e assertiva, Satoshi abria com a declaração ousada de que resolvera grande parte dos problemas que há muito dificultavam a longa demanda pelo Santo Graal do dinheiro universal.

«Tenho estado a trabalhar num novo sistema de dinheiro eletrónico que é absolutamente ponto-a-ponto, sem necessidade de uma terceira entidade externa de confiança», lia-se no início do *email*.

O PDF de nove páginas anexado ao *email* deixava claro que Satoshi conhecia perfeitamente todos os esforços anteriores para criar uma criptomoeda autossustentável. O ensaio de Satoshi citava Back e Wei Dai, bem como várias publicações de criptografia obscuras. Contudo, Satoshi juntara todas as inovações anteriores e criara um sistema bastante diferente de tudo que surgira antes.

Em vez de depender de um banco central ou de uma empresa para emitir e monitorizar o dinheiro (como faziam o sistema financeiro corrente e o DigiCash de Chaum), este sistema estava construído de modo a que cada transação de Bitcoin e os bens de cada utilizador fossem monitorizados e registados pelos computadores de todas as pessoas a utilizar a criptomoeda ou por uma base de dados gerida comunitariamente, que viria a ser conhecida como cadeia de blocos, ou *blockchain*.

O processo que levou a esta invenção reveste-se de várias camadas e até os especialistas demorariam meses a entender como todas funcionam em conjunto. Não obstante, é possível delinear em termos gerais

os elementos básicos do sistema, sendo que tal era feito no ensaio de Satoshi, que viria a ficar conhecido como «Bitcoin White Paper», o Livro Branco da Bitcoin.

De acordo com este ensaio, cada utilizador do sistema podia ter um ou mais endereços públicos de Bitcoin (uma espécie de números de conta bancária designados por chave pública) e uma chave privada para cada endereço. As moedas associadas a determinado endereço só podiam ser gastas pela pessoa que detivesse a chave privada desse endereço. A chave privada era ligeiramente diferente da palavra-chave tradicional, que tem de ser mantida por alguma autoridade central para verificar que o utilizador está a utilizar a palavra-chave correta. No caso da Bitcoin, Satoshi recorreu às maravilhas da criptografia assimétrica para tornar possível que um utilizador – voltemos a chamar-lhe Alice – assinasse digitalmente a transação e provasse que detinha a chave privada, sem mais ninguém precisar de ver ou conhecer essa chave privada[1].

Assim que Alice assinava digitalmente a transação com a sua chave privada, esta era comunicada a todos os computadores da rede Bitcoin, que confirmavam que Alice dispunha das moedas que estava a tentar gastar. Isso era feito através da consulta do registo público de todas as transações de Bitcoin, do qual todos os computadores da rede tinham uma cópia. Assim que os computadores confirmassem que o endereço de Alice tinha, de facto, o dinheiro que estava a tentar gastar, a informação sobre a transação de Alice era registada na lista das transações mais recentes, denominada como bloco na *blockchain*.

O método concreto para adicionar blocos à *blockchain* era, possivelmente, a parte mais complicada do sistema. No nível mais simples, consistia numa espécie de corrida computacional entre todos os computadores da rede, baseada no modelo que Adam Back inventara para o *hashcash*. O computador vencedor era responsável pela inscrição do bloco de transações mais recente na *blockchain*. Igualmente importante, o vencedor também recebia um conjunto de novas Bitcoins: 50 Bitcoins quando a rede começou a operar a sério.

[1] Para mais pormenores sobre este e outros elementos básicos do funcionamento da rede Bitcoin ver o Apêndice Técnico, na página 334.

Esta era, de facto, a única maneira de trazer novas Bitcoins ao mundo. A recompensa de novas moedas ajudou a encorajar os utilizadores de Bitcoin a configurarem os seus computadores de modo a participarem no trabalho comunitário de registo de transações.

Se surgissem conflitos quanto ao computador vencedor da «corrida», prevalecia o registo de transações já adotado pela maioria dos computadores da rede. Se, por exemplo, a maioria dos computadores da rede acreditasse que Alice vencera a última corrida, mas um número menor de computadores acreditasse que fora Bob a vencer, os computadores que haviam usado o registo de transações de Bob seriam ignorados pelos outros computadores da rede até que se juntassem à maioria. Este método de decisão democrático era importante, pois evitava que alguns computadores maus se rebelassem e atribuíssem a si próprios imensas Bitcoins novas; os elementos rebeldes teriam de capturar a maioria dos computadores da rede para alcançar este fim.

As alterações ao *software* Bitcoin que correria nos computadores de todos os utilizadores seriam igualmente decididas com base neste modelo democrático. Qualquer utilizador podia fazer uma alteração ao *software* Bitcoin de código aberto, mas as alterações só teriam efeito quando a maioria dos computadores da rede adotasse a versão alterada do *software*. Se um computador solitário começasse a utilizar uma versão diferente do *software* Bitcoin, seria ignorado pelos outros computadores e deixaria de fazer parte de rede Bitcoin.

Recapitulemos os cinco passos básicos do processo Bitcoin:

- Alice dá início a uma transferência de Bitcoins da sua conta, assinando digitalmente a transação com a sua chave privada e comunicando-a aos restantes utilizadores.
- Os outros utilizadores da rede certificam-se de que o endereço Bitcoin de Alice tem fundos suficientes e depois adicionam a transação de Alice, conhecida como bloco, a uma lista de transações recentes.
- Os computadores envolvem-se numa corrida informática para adicionar a sua lista de transações, ou bloco, à *blockchain*.

- O computador que conseguir adicionar o seu bloco à *blockchain* é recompensado com um conjunto de novas Bitcoins.
- Os computadores da rede começam a compilar uma nova lista de transações recentes não confirmadas, tentando ganhar o próximo pacote de Bitcoins.

O resultado deste processo complicado era algo aparentemente simples, mas que nunca antes fora alcançado: uma rede financeira que podia criar e movimentar dinheiro sem uma autoridade central. Sem bancos, sem empresas de cartões de crédito, sem reguladores. O sistema foi criado para que ninguém, além do detentor da chave privada, pudesse gastar ou retirar dinheiro associado a um endereço específico de Bitcoin. Mais ainda, cada utilizador do sistema podia ter a certeza de que, a cada momento, apenas existiria um registo público inalterável daquilo que cada um dos utilizadores possuía. Para confiar nisto, os utilizadores não tinham de confiar em Satoshi, como os utilizadores de DigiCash tinham de confiar em David Chaum ou os utilizadores do dólar na Reserva Federal; apenas tinham de confiar nos seus próprios computadores a correr o *software* Bitcoin e no código escrito por Satoshi, que era um código aberto e, consequentemente, estava à disposição para ser revisto por qualquer pessoa. Se os utilizadores não gostassem de alguma coisa relativamente às regras definidas no *software* de Satoshi, podiam alterá-las. Quem aderia à rede Bitcoin era, ao mesmo tempo, cliente e dono tanto do banco, como da cunhagem.

Todavia, até então, Satoshi apenas descrevera esta grande ideia.

Apesar dos avanços descritos no ensaio sobre a Bitcoin, quando Hal Finney finalmente o leu, uma semana após a publicação, só havia duas respostas na lista de divulgação de criptografia, ambas definitivamente negativas. John Levine, um conhecido especialista em cibersegurança, disse que o sistema facilmente ficaria assoberbado com *hackers* que podiam disseminar uma versão da *blockchain* diferente da que era usada por todo os outros.

«As pessoas boas revelam, de longe, muito menor capacidade informática do que as pessoas más», escreveu Levine a 2 de novembro. «Também tenho dúvidas quanto a outras questões, mas esta é a fatal.»

A preocupação de Levine era legítima. O sistema Bitcoin descrito por Satoshi assentava na premissa de que os computadores tomariam decisões por maioria. Ao início, quando eram menos os computadores na rede, seria fácil tornar-se a maioria e dominar. No entanto, a esperança de Satoshi era que, inicialmente, enquanto a rede fosse pequena, não houvesse muito incentivo para a dominar. Se tal acontecesse mais tarde, Satoshi esperava que isso se devesse ao facto de a rede ter atraído membros suficientes, cujo número dificultaria o controlo.

James Donald, outro veterano dos debates *cypherpunk*, declarou que «carecemos muito, mesmo muito, de um sistema», embora a sua interpretação do ensaio fosse de que a base de dados de transações, a *blockchain*, rapidamente se tornaria demasiado grande para os utilizadores a conseguirem descarregar.

Nas semanas seguintes, Hal foi praticamente o único defensor de Satoshi. Na lista de criptografia escreveu que não estava muito preocupado com a pirataria referida por Levine, embora admitisse que não sabia bem como funcionaria tudo aquilo na prática, manifestando a vontade de ver o código real e não apenas uma descrição concetual.

«Esta parece ser uma ideia muito promissora e original e estou ansioso para ver como se desenvolverá o conceito», escreveu Hal no grupo.

Graças ao apoio de Hal, Satoshi enviou-lhe antecipadamente uma versão beta. Na fase de testes, em novembro e dezembro, resolveram alguns dos defeitos iniciais. Pouco depois, em janeiro de 2009, Satoshi enviou o código completo aos elementos da lista. O *software* final apresentava certas alterações interessantes em relação ao sistema descrito no ensaio original. Determinava-se que seriam atribuídas novas moedas aproximadamente de dez em dez minutos, tornando a «corrida» das funções de dispersão mais difícil, caso os computadores estivessem a gerar moedas com maior frequência.

O *software* definia ainda que o vencedor de cada bloco receberia cinquenta moedas nos primeiros quatro anos, vinte e cinco nos quatro anos seguintes e metade disso a cada quatro anos consecutivos, até serem

libertados no mundo 21 milhões de moedas, altura em que cessaria a criação de novas moedas.

No primeiro dia, quando Hal descarregou o *software*, a rede já estava ativa e em funcionamento. Nos dias seguintes, pouca atividade foi adicionada à *blockchain*, à exceção de um computador da rede (habitualmente propriedade de Satoshi) que obtinha cinquenta moedas mais ou menos a cada dez minutos. Na tarde de domingo registou-se a primeira transação, quando Satoshi enviou dez moedas a Hal, para se certificar de que esta parte do sistema estava a funcionar sem problemas. Para terminar a transação, Satoshi assinou digitalmente com a chave privada associada ao endereço onde as moedas estavam armazenadas. A transação foi comunicada à rede (composta, essencialmente, por Hal e Satoshi) e foi registada na *blockchain* uns minutos depois, quando os computadores de Satoshi venceram a jornada seguinte da corrida da função de dispersão. A partir daqui, quem descarregasse o *software* descarregaria toda a *blockchain* até ao momento, que incluía um registo das dez moedas enviadas por Satoshi a Hal, bem como das cinquenta moedas que Hal ganhara no sábado.

Nas primeiras semanas, a movimentação de dinheiro por parte das outras pessoas que aderiram ao sistema foi lenta. Satoshi recorria aos seus computadores para ajudar a alimentar a rede. Estava ainda a envidar todos os esforços para vender a tecnologia, respondendo com celeridade a qualquer pessoa que mostrasse o mínimo interesse. Certa noite, um programador do Texas escreveu a Satoshi, revelando grande familiaridade com criptomoeda e criptografia; Satoshi respondeu-lhe na manhã seguinte.

«Temos, sem dúvida, interesses semelhantes!» escreveu Satoshi com inocente entusiasmo, antes de descrever o desafio que a Bitcoin enfrentava:

> «Sabe, acho que havia muito mais gente interessada nos anos 90, mas depois de uma década de sistemas falhados com base numa terceira parte de confiança (DigiCash, etc.), todos encaram isto como uma causa perdida. Espero que consigam fazer a distinção e perceber que esta é a primeira vez, que eu saiba, que estamos a tentar um sistema que não se baseia na confiança em terceiros.»

Contudo, o programa de Satoshi não passava de um monte de código alojado num servidor, como tantos outros sonhos desenvolvidos por programadores. A maioria destes sonhos morria, esquecida algures num disco rígido. O sistema Bitcoin carecia de mais utilizadores e defensores como Hal para poder sobreviver, e não se encontravam muitos. Uma semana após o lançamento do programa, um membro da lista de divulgação de criptografia comentou: «É pouco provável que algum dos principais governos permita que a Bitcoin, na forma atual, circule em larga escala.»

Hal reconhecia que era provável que o autor estivesse certo, mas, não obstante, lançou-se uma vez mais em defesa de Satoshi: «A Bitcoin tem alguns pontos a seu favor: um deles é o facto de ser distribuída sem qualquer ponto de rutura, sem "cunhagem", sem empresas com escritórios que possam ser alvo de intimações, detenções ou encerramento.»

Claro que até o entusiasmo de Hal parecia, por vezes, esmorecer. Enquanto o computador ia trabalhando em máxima capacidade, tentando gerar novas moedas, começou a preocupar-se com as emissões de dióxido de carbono oriundas de todos os computadores em disputa pela criação de moedas. Depois de o seu filho, Jason, se queixar do desgaste provocado no computador, Hal desligou a opção «Gerar Moedas». Começou ainda a temer que, devido à existência de um registo público de todas as transações (embora os utilizadores fossem representados por um endereço de aspeto confuso), o sistema Bitcoin não fosse afinal tão anónimo como inicialmente pensara.

Foi então que aconteceu algo muito pior. O discurso de Hal começou a ficar desarticulado. Durante o treino para a maratona começou a ficar cada vez mais fraco. Em breve, todo o tempo livre que tinha era passado a consultar médicos, na tentativa de identificar a misteriosa maleita. Acabou por ser diagnosticado com a doença de Lou Gehrig, uma doença degenerativa que provocaria gradualmente a atrofia de todos os músculos do corpo. Quando recebeu a notícia, Hal retirou-se da aventura Bitcoin. Quando finalmente regressou, a sua condição física estava muito pior e a condição da Bitcoin muito melhor.