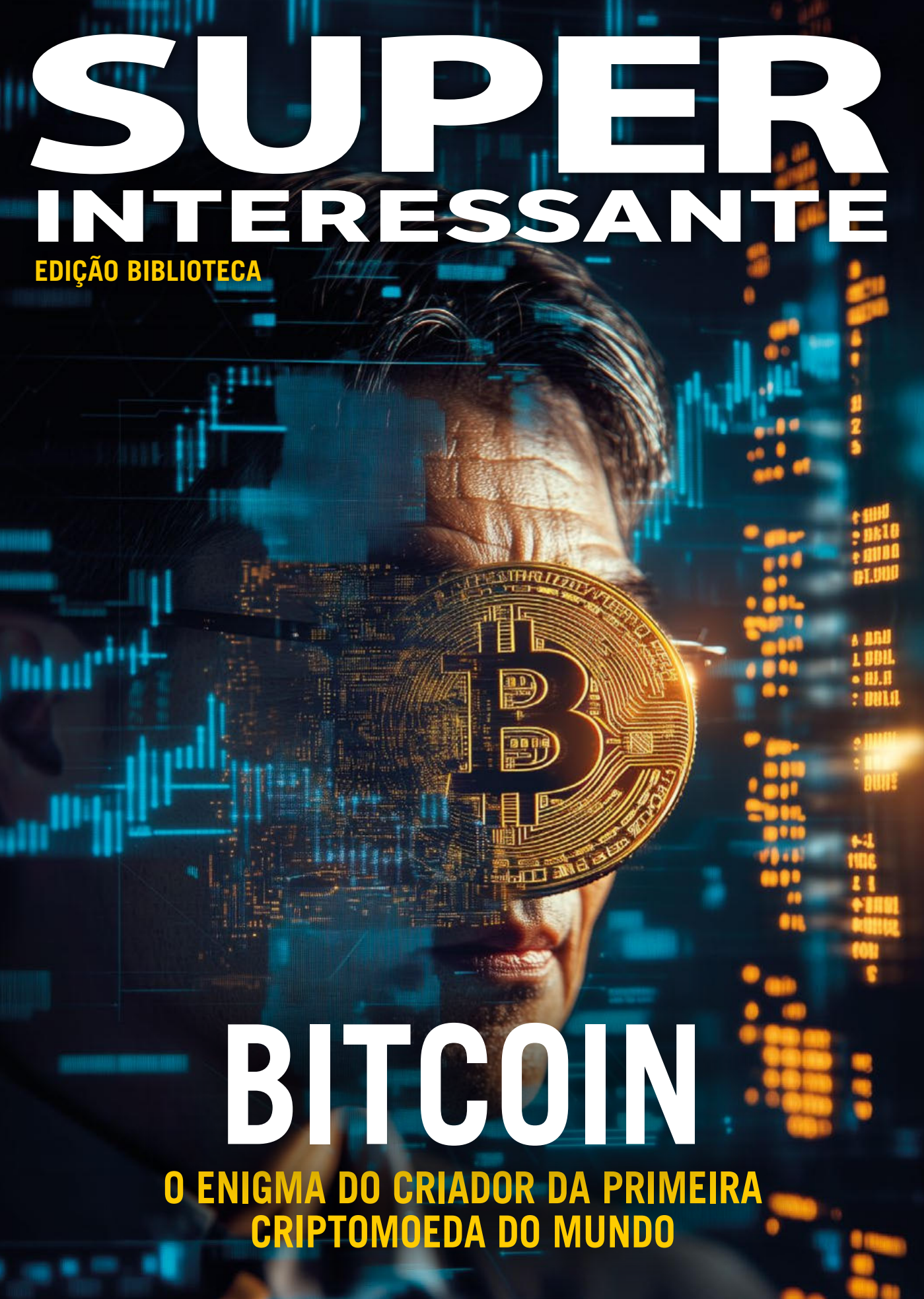
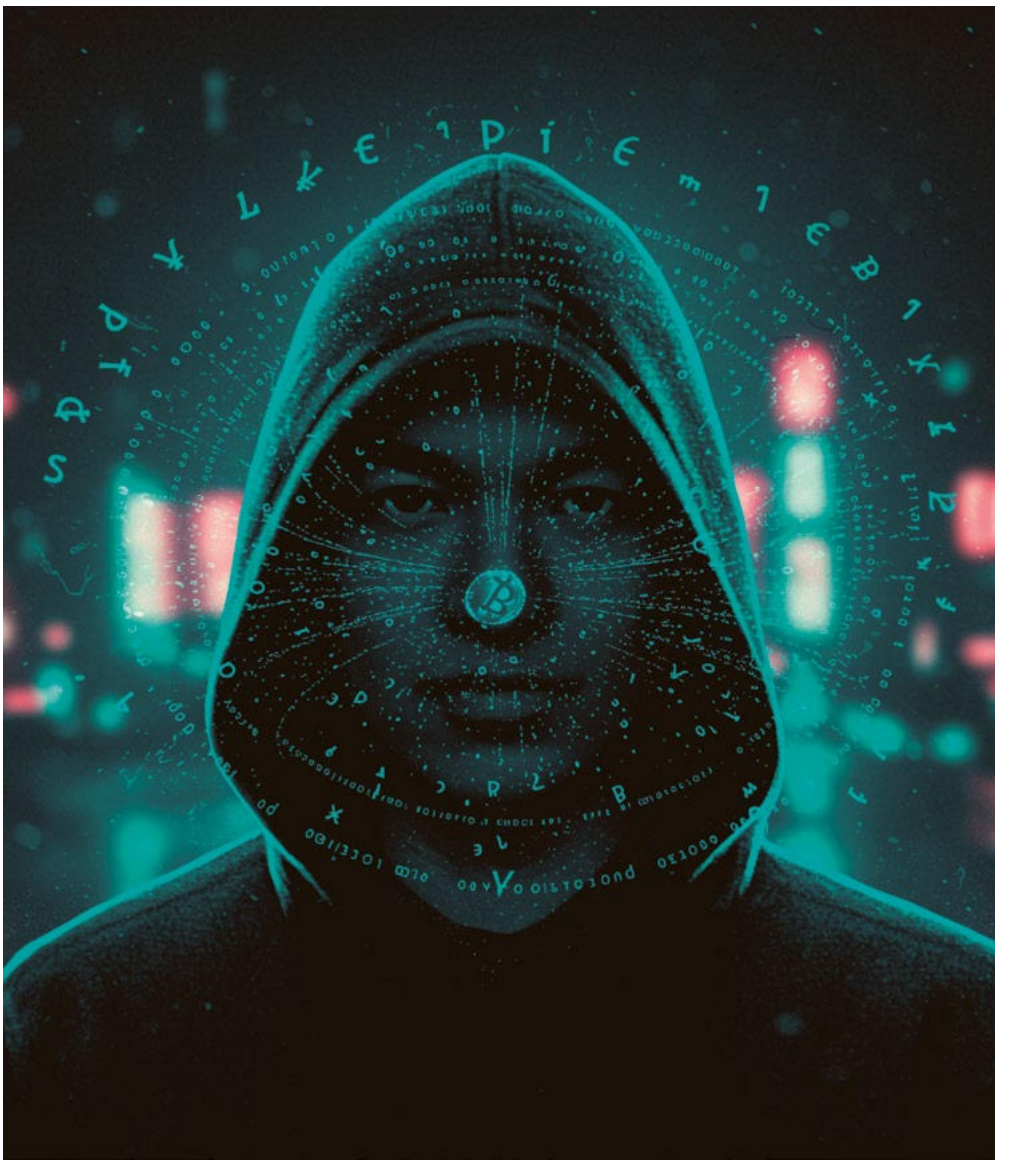
SUPER INTERESSANTE

EDIÇÃO BIBLIOTECA



BITCOIN

O ENIGMA DO CRIADOR DA PRIMEIRA CRIPTOMOEDA DO MUNDO



SHUTTERSTOCK

Sob um pseudónimo indecifrável, alguém concebeu um sistema capaz de desafiar as maiores potências financeiras do planeta. Em 2008, entre linhas de código e e-mails encriptados, nasceu uma moeda sem dono e, com ela, um nome que ninguém conseguiu desvendar: Satoshi Nakamoto.

«NÃO COMPREENDO POR QUE MOTIVO
AS PESSOAS ESTÃO TÃO OBCECADAS
EM SABER QUEM É REALMENTE NAKAMOTO.
TALVEZ A QUESTÃO RESIDA PRECISAMENTE
EM QUE NÃO O SAIBAMOS.»

Edward Snowden (1983),
ex-analista da Agência Central de Inteligência
e da Agência de Segurança Nacional dos EUA.

SHUTTERSTOCK

O mito da era digital

Embora vivamos num mundo que tudo revela, existem mistérios que escapam mesmo ao olhar clínico da tecnologia. Satoshi Nakamoto, o nome por de trás da criação do bitcoin, mantém-se como uma sombra lúcida entre linhas de código. Génio solitário, coletivo oculto ou mito necessário?

Esta revista, inspirada no livro de Benjamin Wallace, *Mr. Nakamoto. O enigmático criador do bitcoin* (Pinolia), explora esta figura enigmática e a fascinante busca pela sua identidade. Mas não se limita ao universo das criptomoedas: mergulha nos dilemas da privacidade, do anonimato na era digital, na revolução descentralizada e nas mudanças sociais e tecnológicas que a moeda do futuro implica.

Entre pistas, silêncios e miragens, o leitor entra num labirinto onde se cruzam criptografia, utopias digitais, paranoias libertárias e comunidades que confundem fé com sistema operativo. O que começa como uma investigação transforma-se num retrato: não do homem, mas da era que o gerou. Sem dúvida, o que aqui lemos é uma radiografia do nosso tempo.

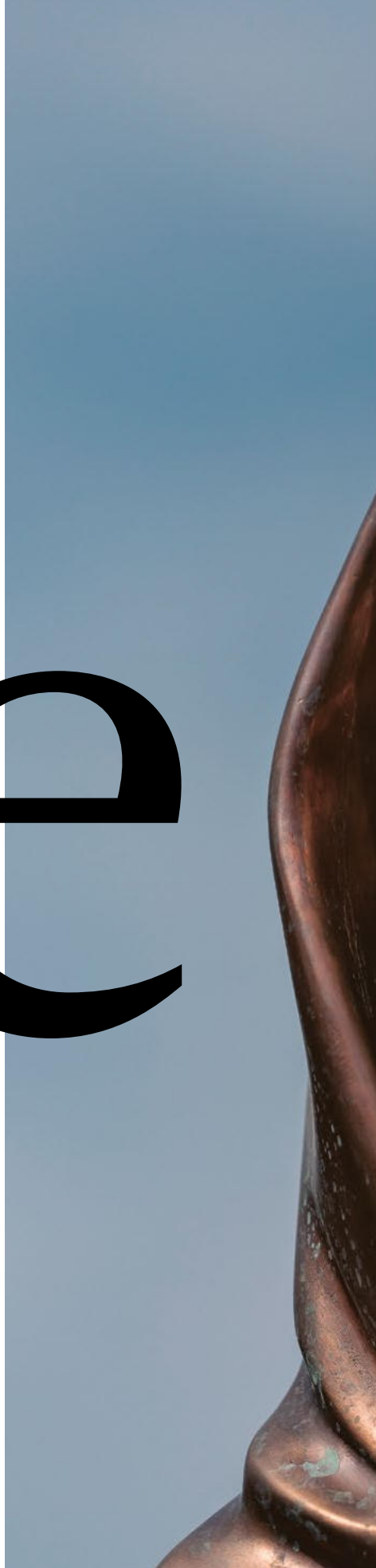
No ponto de encontro entre anonimato, poder e tecnologia desenha-se o pulso de uma nova época. O seu silêncio é, por si só, um gesto radical, uma declaração de intenções perante um sistema que quer tudo visível, etiquetado e classificado. O anonimato é hoje um manifesto. Compreender esta personagem esquiva é também reconhecer que existem indivíduos que recusam entrar pelo aro e que têm a coragem de desafiar governos e bancos. Sem pretensões de exemplo, são matéria de mito.

CRISTINA ENRÍQUEZ
SUBDIRETORA

CONTEÚDOS

SHUTTERSTOCK

É ele



Sob o enigmático pseudónimo de Satoshi Nakamoto, o criador do bitcoin permanece nas sombras da história financeira moderna. Estátua de Satoshi Nakamoto, em Budapeste, Hungria. SHUTTERSTOCK

Se Satoshi Nakamoto, o inventor do bitcoin que se escondia por detrás desse pseudónimo, fosse quem eu achava que era, não o iria reconhecer. Provavelmente, nem sequer falaria comigo. E vê-lo implicava sentar-me num avião durante vinte horas e conduzir outras oito. Mas precisava de tentar manter uma conversa com ele — e tinha de ser frente a frente.

Nakamoto desaparecera na primavera de 2011. Soube da sua existência nesse verão, quando escrevi o primeiro artigo na *Wired* sobre o bitcoin, a moeda baseada na internet que operava para lá do controlo de qualquer governo ou banco. Doze anos depois, o criador do bitcoin continuava um desconhecido e a sua enorme fortuna permanecia intacta. O anonimato e a moderação constituíam uma desconcertante recusa do reconhecimento e da riqueza que obteria se decidisse sair das sombras. Na história moderna da ciência não havia precedentes de alguém que, tendo criado uma tecnologia revolucionária e, depois de a lançar no mundo, não reclamasse o mérito.

O ÚLTIMO GRANDE MISTÉRIO

Privados de um ser humano de carne e osso a quem venerar, os adeptos do bitcoin tinham conferido ao pseudónimo uma aura lendária. Em 2022, podia ver-se Kanye West a sair de um Escalade em Beverly Hills com um boné de basebol de Satoshi Nakamoto. Em Budapeste, os seus seguidores inauguraram a primeira estátua de Nakamoto, uma representação em bronze de uma figura espectral encapuzada. No arquipélago de Vanuatu, no sul do oceano Pacífico, promotores imobiliários venderam participações num paraíso utópico chamado ilha Satoshi. Um trio de libertários comprou um navio de cruzeiro desativado, batizou-o como MS *Satoshi* e recrutou colonos para a primeira sociedade soberana do mundo movida a bitcoin. Mais do que um colega tecnólogo fez campanha para que Satoshi Nakamoto recebesse um Prémio Nobel.

Mas o enigma da identidade de Nakamoto teimava em resistir a qualquer solução. Elon Musk e Peter Thiel, entre outros, especulavam sobre o assunto. Os obcecados caçadores de Nakamoto esforçavam-se por desenterrar novas pistas ou recompor as existentes de forma mais convincente. Àquela altura, já tinham sido apontados mais de uma centena de suspeitos distintos.

A intriga transcendia a tecnologia. Num mundo em que a internet lançava luz sobre todos os recantos, restavam muito poucas perguntas deste tipo por responder. Descobríramos quem era a fonte secreta de Bob Woodward. Conhecíamos, por fim, a demonstração do último teorema de Fermat. Já se sabia que Thomas Pynchon provavelmente comprava os seus *bagels* na Zabar's.

Quando me propus escrever sobre Nakamoto, não podia prever que, mais de uma década depois, a sua identidade continuaria a ser o último grande mistério.

ATÉ O *60 MINUTES*, COM GRANDES RECURSOS E UMA EQUIPA DE JORNALISTAS DE INVESTIGAÇÃO, SE DEU POR VENCIDO

Teria sido ainda mais absurdo imaginar que o fantasma escondido por detrás da primeira criptomoeda do mundo — e o afã por o desmascarar — traria consigo ações judiciais, uma perseguição automóvel, uma recompensa, uma fortuna de 75 mil milhões de dólares, tentativas de extorsão, ameaças de morte, uma equipa SWAT, um suicídio, um traficante de armas foragido, um falsificador em série, uma sociedade secreta de paranoicos que se identificavam apenas por pseudónimos, um génio de grande coração preso no próprio corpo por uma doença, um bunker nuclear na Europa, cadáveres congelados no deserto do Arizona e um espião britânico metido num saco de lona.

ERA ALGUÉM PERIGOSO... TINHA ARMAS

As tentativas anteriores de desmascarar Nakamoto tinham falhado, por vezes de forma espetacular. Até o *60 Minutes*, com recursos incalculáveis e uma sólida equipa de experientes jornalistas de investigação, se deu por vencido ao declarar o desafio como «missão impossível». No entanto, agora, contra todas as probabilidades, eu acreditava tê-lo resolvido.

Estava nervoso com o que isso poderia significar. O mundo do bitcoin mostrava-se hostil a projetos como o meu. Porém, essa não era a minha principal preocupação. Quando descobri a verdadeira identidade de Nakamoto, surpreendeu-me que não fosse um suspeito habitual. Tratava-se de alguém que tomara medidas extraordinárias para se tornar impossível de encontrar. E o que descobri sobre ele era inquietante. Nada tinha a ver com a imagem que as pessoas faziam de Satoshi Nakamoto. Descrevera-se repetidamente como alguém perigoso. Tinha armas.

SHUTTERSTOCK

Bob Woodward, conceituado jornalista de investigação, no Centro de Política da Universidade da Virgínia, numa entrevista para a CBS.

SHUTTERSTOCK

Notas que representam Dorian Satoshi Nakamoto, o engenheiro nipo-americano que foi erroneamente identificado pela revista *Newsweek*, em 2014, como o criador do bitcoin.

EM BUDAPESTE ERGUE-SE A PRIMEIRA ESTÁTUA DE NAKAMOTO, A REPRESENTAÇÃO DE UMA FIGURA ESPECTRAL ENCAPUZADA

Antes de voar meio mundo para me encontrar com ele, tinha de estar seguro de que sabia onde se encontrava. Possuía pelo menos quatro propriedades em dois continentes. Ao princípio, pensei que se escondia numa zona remota da ilha do Havai. Mas ultimamente passara a acreditar que vivia na costa leste da Austrália, numa pequena comunidade costeira a norte de Brisbane. Percebi então que teria de contratar uma equipa de investigadores privados para vigiar a propriedade e confirmar a sua presença.

Estava no meio de todas estas divagações quando combinei jantar com a minha irmã num restaurante mexicano de Manhattan e lhe contei o que tinha descoberto na minha investigação.

SHUTTERSTOCK

Agências como o FBI seguiram pistas, analisaram padrões e estudaram transações para chegar ao criador do bitcoin.

—É ele —afirmou, com uma certeza que eu não sentia.

Enquanto a minha irmã saboreava calmamente a sua margarita, eu remoía as minhas dúvidas.

—É ele —repetiu.

Contei-lhe as minhas inquietações, pois ela tinha mais experiência com este tipo de situações. Fora produtora de informação televisiva durante vinte anos. Quando trabalhava no programa *48 Hours*, esteve em Montana depois de o FBI invadir a propriedade do Unabomber e o deter.

Sugeriu que fosse acompanhado por segurança profissional, que usasse um colete à prova de bala e que avisasse a polícia local.

—Obrigado —murmurei.

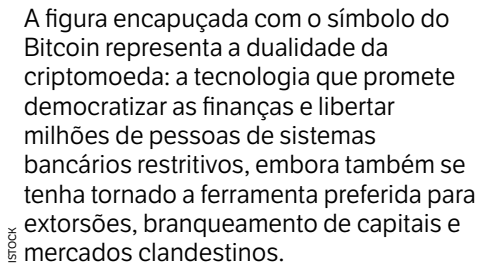
Senti-me um pouco melhor. Pelo menos, tinha um plano. Os profissionais dos noticiários de televisão faziam isto a toda a hora. Se ela não estava preocupada, eu não tinha por que me inquietar.

Mais tarde, nessa mesma noite, enviei uma mensagem de texto à minha irmã: «Não consigo dormir, não sei porquê».

Eram 4h09 da madrugada.

«Duas ideias: talvez fosse boa ideia tentares encontrá-lo num lugar público, caso alguma vez saia de casa. Além disso, alguém, a uma distância prudente, deveria filmar o encontro como prova». ■

Uma lenda em toda a linha



ISTOCK

A figura encapuçada com o símbolo do Bitcoin representa a dualidade da criptomoeda: a tecnologia que promete democratizar as finanças e libertar milhões de pessoas de sistemas bancários restritivos, embora também se tenha tornado a ferramenta preferida para extorsões, branqueamento de capitais e mercados clandestinos.

SHUTTERSTOCK

A teoria que liga Elon Musk a Satoshi Nakamoto é das mais fascinantes no universo das criptomoedas. Na imagem, a SpaceX, empresa do sul-africano.

Dezoito meses antes, na Passagem de Ano de 2021, tinha recebido um e-mail com o seguinte assunto: «Nova informação sobre o Satoshi». Desde que escrevi o artigo para a *Wired*, passara a deparar-me periodicamente com e-mails como este. O bitcoin, e a indústria mais vasta das criptomoedas que gerou, ainda era tão recente que bastava ter investido um pouco em 2017 para se ser considerado veterano; por isso, os jornalistas que tinham acompanhado a história nos seus primeiros anos eram já especialistas consagrados e alvos naturais para quem tivesse uma teoria sobre Satoshi para vender. E havia sempre alguém a vender uma nova teoria sobre Satoshi. Regra geral, dava pouca atenção a esses e-mails. As notícias sobre Nakamoto reacendiam uma fugaz esperança de descobrir algo novo, mas acabavam inevitavelmente por não convencer. Já me habituara à ideia de um mistério sem solução. Além disso, aquele e-mail em particular não me inspirava confiança porque não vinha assinado. Ainda assim, cliquei para o abrir. Não havia texto, apenas uma ligação que remetia para um artigo de blogue intitulado «Sou o estagiário da SpaceX que especulou que o Satoshi é o Elon Musk. Há mais nesta história». O autor, Sahil Gupta, causara algum burburinho na internet quatro anos antes com outro texto em que defendia que Musk era «provavelmente» Nakamoto.

NAKAMOTO ERA UM FAMOSO ENIGMA

Agora apresentava mais indícios: o relato de uma interação que tivera com o chefe de gabinete de Musk, Sam Teller. Soava inócuo e ambíguo, pelo que não respondi.

Dois dias depois, recebi outro e-mail sem assinatura do mesmo endereço.

Este continha uma ligação para uma página do GitHub, um sítio onde os programadores de *software* partilham o seu trabalho, com uma análise detalhada do caso de Gupta sobre Musk como Nakamoto. Talvez por Musk já ser presença constante nas notícias, passei as semanas seguintes a matutar sobre a teoria de Gupta. Não sabia bem o que pensar dos seus argumentos, oscilando entre a ambiguidade e o tecnicismo. Acabei por escrever a Gupta, que era quem claramente me enviara os e-mails. Afinal, parecia ter-me escolhido para amplificar a sua história.

— Obrigado por responder à minha mensagem — disse Sahil. — Enviei e-mails a centenas de jornalistas.

Estava em casa, perto de San Jose, e falávamos por videochamada. Usava uma T-shirt magenta e auscultadores prateados, e no rosto adivinhava-se a sombra de uma barba.

— É incrível quão negativa é a caricatura que fizeram do Musk — continuou Sahil, com uma energia inquieta. — Acham que montou uma empresa de foguetões e outra de automóveis por acaso.

Sahil descreveu então como chegara a descobrir a verdadeira identidade de Nakamoto.

Em 2015, quando Sahil era estudante universitário em Yale, ficou impressionado com o que a SpaceX fazia, pelo que conseguiu um estágio de verão a escrever *software* de gestão de inventário na sua fábrica de foguetões, em Hawthorne, Califórnia.

— Foi uma experiência incrível — recordou Sahil.

Musk estava no escritório uns três dias por semana e Sahil via-o ocasionalmente nos corredores. Após uma «desmontagem rápida não programada», o termo que a empresa usava para se referir à explosão de um dos seus foguetões, Sahil esteve presente quando Musk proferiu um discurso sobre como a SpaceX seria capaz de melhorar a tecnologia para resolver o problema.

— Um discurso verdadeiramente inspirador — disse-me Sahil.

Foi depois de terminar o estágio que estabeleceu a ligação ao bitcoin. Sahil especializava-se em Informática e, para a tese de final de curso, colaborou com outros dois estudantes para propor uma moeda digital do banco central chamada Fedcoin. «E se os Estados Unidos pudessem melhorar o dólar aproveitando os melhores aspetos do bitcoin?», explicava. Nos agradecimentos do trabalho, mencionava-se «Satoshi Nakamoto por ser uma autêntica lenda». Enquanto investigava para a tese, Sahil mergulhou na literatura sobre criptomoedas, a começar pelo documento técnico de nove páginas em que Nakamoto descreveu o bitcoin pela primeira vez. Nessa altura, soube que a verdadeira identidade de Nakamoto era um famoso enigma e, ao ler os escritos do criador do bitcoin, chamou-lhe a atenção a semelhança com a linguagem de Musk. Ambos fala-

EM 2015, SAHIL GUPTA ERA ESTUDANTE UNIVERSITÁRIO EM YALE E ESTAVA IMPRESSIONADO COM O QUE FAZIA A SPACEX

vam em raciocínio de «ordem de grandeza» e usavam a palavra «maldito». Ambos argumentavam a partir de primeiros princípios. Nakamoto falava do dinheiro de forma conceptual, como fez Musk quando era executivo na PayPal no início dos anos 2000. Sahil descobriu que Musk, tal como Nakamoto, tinha experiência de programação em C++ e conhecimentos de economia e criptografia. Nakamoto também demonstrara uma espécie de abnegação movida por uma missão.

— É assim o Musk — disse-me Sahil.

A partir de todas essas semelhanças, começou a perguntar-se: poderá o inventor do bitcoin ter estado à nossa frente todo este tempo, oculto pelo esplendor da sua própria celebridade?

«É ELON O SATOSHI?»

Quando Sahil se licenciou, decidiu que queria trabalhar diretamente para Musk, no gabinete do diretor-executivo. Depois de enviar vários e-mails a Musk, conseguiu uma entrevista telefónica com Teller, o chefe de gabinete. Sahil falou-lhe da sua formação académica, mas este disse-lhe que não era um bom candidato, pois procuravam um assistente administrativo. Acrescentou que, com a sua experiência, tinha estofo para fundar a própria empresa.

— Foi um bom conselho — disse Sahil.

Quando a conversa estava a chegar ao fim, Sahil decidiu arriscar: «O Elon é o Satoshi?».

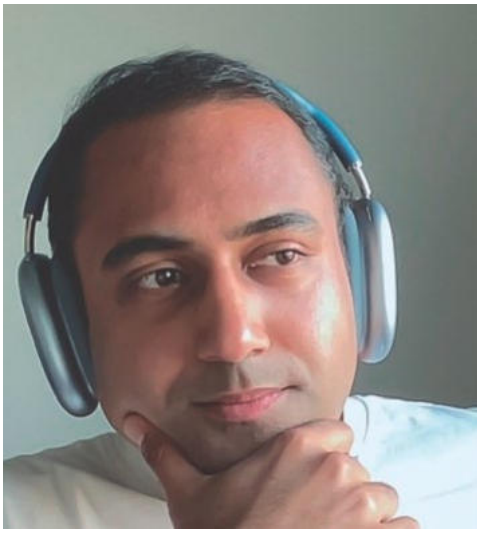
SHUTTERSTOCK

Em 2021, Elon Musk revelou que a Tesla tinha comprado milhões de bitcoins e anunciou que passaria a aceitar a criptomoeda como pagamento pelos seus veículos.

SAHIL DESCOBRIU QUE MUSK, TAL COMO NAKAMOTO, TINHA EXPERIÊNCIA DE PROGRAMAÇÃO EM EM LINGUAGEM C++

— Teller ficou em silêncio cerca de quinze segundos. E depois respondeu: «Bem, que é que eu posso dizer?». Essa resposta pareceu-me uma boa pista. Para mim, ficou bastante claro: apanhado de surpresa pela minha pergunta, Teller deu-me uma resposta bastante reveladora — contou-me Sahil.

Meses depois, Sahil escreveu o texto de blogue «Elon Musk provavelmente inventou o bitcoin». Omitiu o conteúdo da conversa privada com Teller, mas descreveu os paralelismos que encontrara. E defendeu que a comunidade do bitcoin, dividida por disputas sobre se a tecnologia deveria abrir-se ao grande público e como o deveria fazer, beneficiaria do regresso do seu fundador para a guiar. Alguns blogues de criptomoedas pegaram na teoria de Sahil e a *Bloomberg News* deu-lhe cobertura. O próprio Musk tuitou: «Não é verdade. Um amigo enviou-me parte de um [bitcoin] há uns anos, mas não sei onde está». Sahil acabaria por trabalhar para Musk: em 2018 foi contratado para ajudar a programar o *software* na nuvem da Tesla. Durante o aumento da produção do Model 3, achou empolgante e fascinante ver como Musk, desafiando as normas da indústria, colocava os engenheiros de *software* a partilhar espaço com os operários da produção. Musk manteve-se firme na ideia, apesar do ceticismo. Sahil disse-me que a sua teoria de que o Elon era o Satoshi nunca lhe trouxe problemas no trabalho na Tesla.



ASC

Sahil Gupta (na imagem) afirmou, num artigo no *HackerNoon*, que Nakamoto era provavelmente Musk.

— Fui franco quanto à minha posição. Considero mesmo que o Elon é comparável a Benjamin Franklin. Creio que o meu chefe me perguntou uma vez sobre a teoria.

Com o tempo, Sahil saiu para montar a sua própria empresa, dedicada à modelação virtual em 3D para sites como a Shopify. Mas, com o passar dos anos e à medida que ia juntando peças, a sua crença de que Musk era Nakamoto tornou-se convicção. Deparou-se com declarações de Luke Nosek, cofundador da PayPal, proferidas num painel em Davos: o objetivo original da empresa era desenvolver uma moeda livre de bancos. Sahil recebeu a dica de que Musk, tal como Nakamoto, tinha o hábito de colocar dois

espaços após um ponto final nos seus escritos. Um colega referiu que Musk voava regularmente de e para o aeroporto de Van Nuys, o que coincidia, de forma inquietante, com talvez a única falha de segurança que Nakamoto cometera: no início da história do bitcoin, um e-mail de Nakamoto a outro programador de *software* revelou inadvertidamente um endereço IP no norte de Los Angeles. Sahil soube que os primeiros programadores do bitcoin consideravam Satoshi um «mandão» — e Musk, certamente, também o era. E qual era a marca distintiva de Musk antes da era Twitter? Enfrentar desafios impossíveis: tornar os carros elétricos apelativos; fazer um foguetão aterrar numa plataforma marítima.

POR QUE NEGARIA SER NAKAMOTO?

No final de 2021, Sahil decidiu que chegara o momento de fazer nova investida pública. Nakamoto era então visto quase universalmente como um génio benevolente e Sahil sentiu que se abrira uma oportunidade para que os meios de comunicação aceitassem finalmente que Nakamoto e Musk eram a mesma pessoa. A SpaceX acoplara com sucesso uma cápsula à Estação Espacial Internacional e Musk fora recentemente nomeado «Personalidade do Ano» pela revista *Time*. Chegara até a tuitar, em tom de brincadeira, sobre a dogecoin, uma criptomoeda meme. Quando Sahil publicou a nova entrada no blogue, a que o levou a enviar-me a mim e a tantos outros jornalistas um e-mail, relatou pela primeira vez a história da interação com o chefe de gabinete de Musk.

Agora, no ecrã do meu computador, Sahil dizia estar «99% seguro» da sua teoria. Atribuía as dúvidas dos outros aos preconceitos contra Musk.

— Surpreende-me que as pessoas sejam céticas quanto às capacidades de Musk. Isso indica uma profunda estagnação na sociedade, pois as pessoas são incapazes de avaliar os factos com objetividade.

Da minha parte, tinha algumas perguntas. Musk era uma pessoa invulgarmente capaz, mas chegou a descrever 2008 — quando contraiu dívidas, divorciou-se e viu falhar o terceiro lançamento consecutivo de um Falcon — como o pior ano da sua vida. Nakamoto publicara o documento técnico do bitcoin em 2008. Teria Musk tido tempo e energia para criar a primeira criptomoeda viável do mundo e depois gerir pessoalmente o projeto de *software* durante quase dois anos, enquanto montava uma indústria de carros elétricos e uma empresa espacial bem-sucedida?

Sahil tinha respostas. Disse-me que vira uma entrevista em que Musk recordava que, em 2007, dedicava apenas três dias por mês à Tesla. E não demonstrara Musk uma capacidade prodigiosa para trabalhar em vários projetos sem relação entre si ao mesmo tempo? Além disso, já apresentara produtos revolucionários através de um documento técnico. De facto, em 2013, Musk, sem

OBJETIVO DE SAHIL ERA GERAR «PRESSÃO PÚBLICA SUFICIENTE PARA QUE MUSK FINALMENTE ASSUMISSE O MÉRITO»

SHUTTERSTOCK

Se Musk fosse realmente Satoshi, a Tesla teria sido a jogada-mestra final: usar a própria empresa para conferir credibilidade institucional à sua criação criptográfica.

grandes alardes, publicara um documento de 58 páginas em que descrevia um novo sistema de transporte a que chamou Hyperloop.

Certo, mas fizera-o em seu próprio nome; além disso, não era propriamente uma pessoa modesta. Portanto, se fosse realmente o criador do bitcoin, por que negaria ser Nakamoto? Para Sahil, isto não era uma contradição, mas antes mais uma prova da inteligência de Musk.

— Ao contrário de uma empresa que precisa de marketing, o bitcoin era mais forte e poderia crescer mais depressa, nos primeiros tempos, sob a aura de um fundador anónimo.

E por que considerava Sahil importante partilhar o segredo de Musk com o mundo?

— Porque é uma história incrível — respondeu-me.

Queria que Musk recebesse a glória que merecia. O objetivo de Sahil era gerar «pressão pública suficiente para que Musk finalmente assumisse o mérito».

Se Sahil tinha razão ou não, não o saberia dizer, mas conseguia compreender a sua obsessão. O bitcoin atingira recentemente um máximo histórico de quase 70 000 dólares por moeda, e o valor de mercado de todos os bitcoins em circulação ultrapassara o bilião de dólares. El Salvador reconhecera o bitcoin como moeda de curso legal. Em 2011, não parecia tão importante que alguém soubesse quem era Nakamoto. Mas como era possível que, ainda agora, continuasse a ser uma incógnita?

Seis meses depois, deixei o meu emprego para me dedicar a tempo inteiro a desvendar o mistério que me cativara pela primeira vez há uma década. ■

Dinheiro fictício da internet

O que começou como uma «experiência de internet» movimenta hoje milhares de milhões diários em volume de *trading*, supera o PIB de muitos países e é adotado por nações inteiras. O «dinheiro fictício» está a tornar-se mais real do que o dinheiro real.

ISTOCK


THIS NOTE IS LEGAL TENDER
FOR ALL DEBTS, PUBLIC AND PRIVATE
Treasurer of the United States.
SERIES
2003
A
100

Já ouviste falar do bitcoin? —perguntou-me Jason Tanz.

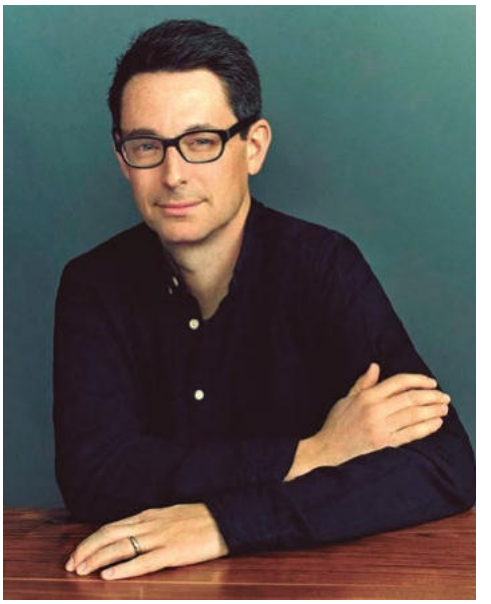
—Sinceramente, não.

—Conheces a Silk Road?

—Também não.

Jason era o diretor da *Wired*. Era junho de 2011.

Jason mencionou um artigo recente no Gawker sobre a Silk Road, o mercado da *dark web*, onde o bitcoin —apresentado como uma «moeda digital impossível de rastrear»— era a moeda de eleição. Com menos de três anos de vida, já traçara uma narrativa em três atos: de um projeto de *software* utópico a um improvável mercado de cento e trinta milhões de dólares por dia, passando por uma rede obscura fustigada pelo crime, pelo escândalo e por uma queda de preços. E, com o movimento Occupy Wall Street a poucos meses de distância, parecia o momento certo. Jason explicou-me porque é que o bitcoin era, de facto, algo novo. As tentativas anteriores de criar dinheiro digital tinham falhado porque a mesma caraterística que tornara a internet revolucionária (distribuição instantânea, sem fronteiras e sem uma autoridade central) também dera origem ao chamado problema do duplo gasto. Se a internet fosse uma fotocopiadora e o dinheiro digital apenas uma cadeia de bits, o que impediria alguém de copiar e colar o mesmo bit vezes sem conta? O arquiteto do bitcoin, Satoshi Nakamoto, resolvera esse problema de forma engenhosa.



WIRED

Jason Tanz, ex-diretor da *Wired online*, escreveu artigos sobre a economia colaborativa, criptomoedas...

—Interessa-te? —perguntou Jason.

Eu tinha estudado Filologia Inglesa, não percebia nada de informática e aderira à era digital com um atraso atroz. Quando a internet começou a popularizar-se na década de noventa, senti-me desconcertado: porque é que toda a gente tratava aquilo que, a meu ver, não passava do último de uma longa série de inventos tecnológicos como se fosse algo revolucionário? «Não passa de uma torradeira», costumava dizer em tom sarcástico.

—Soa incrível —respondi.

A IDEIA DE UM SISTEMA MONETÁRIO DESONESTO EVOCAVA O SERVIÇO POSTAL CLANDESTINO DE THOMAS PYNCHON

SHUTTERSTOCK

Moeda comemorativa que representa um dos capítulos mais controversos da história do bitcoin: a Silk Road, o primeiro grande mercado da *dark web*.

O LEILÃO DO LOTE 49

The Economist publicara uma análise detalhada do funcionamento do bitcoin. Fred Wilson, um destacado investidor de capital de risco, comparara-o ao WikiLeaks e à Primavera Árabe pelo seu potencial transformador. E a história era irresistível. A ideia de um sistema monetário paralelo e desonesto evocava o serviço postal clandestino do romance de Thomas Pynchon *O Leilão do Lote 49*. Os mais acérrimos partidários do bitcoin eram uma vívida mistura ciberpunk de hackers, fanáticos do ouro, anarquistas e seguidores de Ayn Rand. E eu estava cativado pelo enigma de Satoshi Nakamoto.

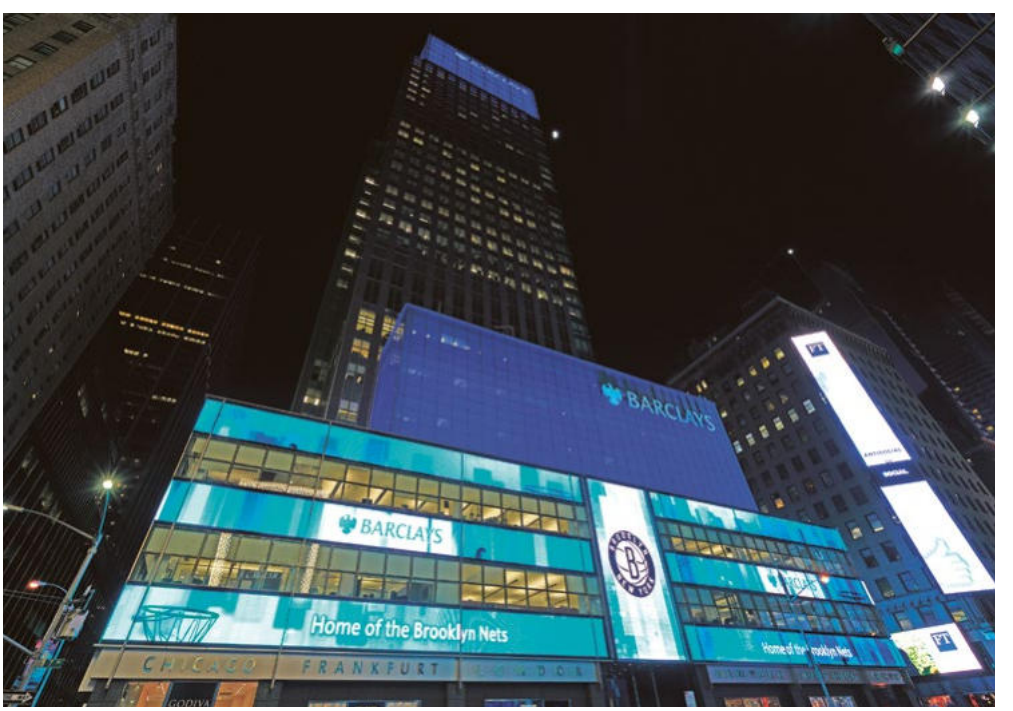
A ideia de que, por muito detalhados que fossem os nossos mapas, ainda havia zonas em branco, por explicar, fascinava-me. Em criança, guardava debaixo da mesa de cabeceira um livro de grande formato, repleto de ilustrações extravagantes e fotos granuladas a preto e branco, que reunia mistérios inexplicáveis como o monstro do lago Ness e o Triângulo das Bermudas. Com o tempo, o meu interesse por essas lendas, com o seu toque de irrealidade, deu lugar à fascinação por uma espécie de figura pública que abundava no final dos anos setenta e início dos oitenta: o icónico fugitivo. Terroristas da Weather Underground ou da Fração do Exército Vermelho (Baader-Meinhof). Partidários do Terceiro Reich escondidos na selva paraguaia. Patty Hearst, uma sequestrada de sangue azul transformada em assaltante de bancos de metralhadora em punho. O guerrilheiro Carlos, o Chacal. Escritores alérgicos aos meios de comunicação, como Pynchon e J. D. Salinger. Estávamos rodeados e impregnados por essas histórias. Talvez, como jovem leitor devoto de cada novo romance de Robert Ludlum, eu

fosse particularmente impressionável. Mas agora, a meu ver, Satoshi Nakamoto —essa figura esquiva que podia ou não existir— fizera algo mais extraordinário do que qualquer um deles.

Comecei a telefonar a pessoas do mundo do bitcoin e a apanhar o metro a partir de Brooklyn, onde vivia, para me encontrar com elas. Algumas reuniões tinham lugar num escritório lúgubre no quinto andar de um prédio no centro de Manhattan, onde funcionava uma pequena produtora de vídeos para a web cujo proprietário era obcecado pelo bitcoin; outras, numa cafetaria de *bubble tea* perto de Union Square.

Fiquei a saber que três anos antes, no Halloween de 2008, Nakamoto publicara um breve artigo em que descrevia «um sistema de dinheiro eletrónico entre pares», numa lista de correio eletrónico especializada em criptografia, pouco conhecida e moderada, que era informalmente conhecida como Metzdowd. A sua proposta descrevia um novo tipo de moeda que operaria numa rede de computadores gerida por voluntários, a que qualquer pessoa poderia aderir ou da qual se poderia desligar livremente. Resolveria o problema do duplo gasto através de um registo público e transparente, mantido coletivamente pela rede, em vez de depender da base de dados de débitos e créditos de um banco ou de um governo. Nakamoto incluiu uma ligação para uma descrição formal mais detalhada que ficaria conhecida como «o white paper ou documento técnico do bitcoin», mas essa era a ideia geral.

O momento escolhido por Nakamoto para lançar uma moeda alternativa foi muito astuto. Na altura, muita gente estava furiosa com os bancos: no mês ante-



SHUTTERSTOCK

Antiga sede mundial da Lehman Brothers na cidade de Nova Iorque, agora rebatizada como Barclays Capital.

rior, a Lehman Brothers declarara a maior falência da história dos Estados Unidos e a Reserva Federal utilizara dinheiro dos contribuintes para resgatar a AIG, uma das maiores companhias de seguros do mundo. A descentralização —a ideia de não pôr todos os ovos no mesmo cesto— era mais apelativa do que nunca.

VERSÃO ALFA NO SOURCEFORGE

A escolha do fórum por parte de Nakamoto para anunciar o bitcoin também foi hábil. Os libertários com conhecimentos técnicos —pessoas versadas em informática e hostis à autoridade— estavam amplamente representados em Metzdowd, com o seu enfoque na criptografia. Que nenhum dos subscritores tivesse ouvido falar de Satoshi Nakamoto não surpreendeu ninguém. Metzdowd era frequentado por entusiastas dos fundamentos matemáticos da encriptação e, por isso, estavam habituados a pseudónimos.

Alguns membros da lista, particularmente interessados na promessa do dinheiro digital, fizeram-lhe comentários sobre o *software* que estava a escrever, e Nakamoto recebeu-os de bom grado. «Obrigado por levantar essa questão», disse a uma pessoa. «Agradeço as suas perguntas», respondeu a outra num e-mail privado, antes de acrescentar: «Na verdade, fiz isto ao contrário. Tive de escrever todo o código antes de me convencer de que podia resolver cada problema, e só depois redigi o documento.» No início de janeiro de 2009, Nakamoto lançou uma versão alfa no SourceForge. Na altura, era um site popular para projetos de *software* de código aberto, esforços colaborativos que acolhiam qualquer programador que quisesse participar. No primeiro dia, segundo um dos primeiros bitcoiners, 127 pessoas transferiram o *software* do bitcoin.

O DINHEIRO 2.0

Muitos dos primeiros participantes eram programadores que achavam que o dinheiro tradicional precisava urgentemente de uma atualização. As notas de papel perdiam cor, amarrotavam-se, rasgavam-se, gastavam-se, sujavam-se e ainda por cima propagavam germes. Só estavam disponíveis em denominações fixas, podiam ser falsificadas e eram difíceis de movimentar em quantidades significativas. O bitcoin era o dinheiro 2.0: duradouro, infalsificável, quase infinitamente divisível. Poderia concretizar o sonho do comércio online das microtransações. Podias enviar qualquer montante, para qualquer lugar, de imediato.

Muitas pessoas dessa primeira vaga tinham convicções firmes sobre a sua autonomia pessoal. O bitcoin, como moeda baseada em zeros e uns numa infraestrutura digital mantida por pessoas comuns em qualquer ponto do planeta, era imune à intromissão dos poderes centrais. Ao contrário dos lingotes de ouro, o bitcoin não podia ser confiscado. Ao contrário de uma conta bancária, não podia

«TIVE DE ESCREVER TODO O CÓDIGO ANTES DE ME CONVENCER DE QUE PODIA RESOLVER CADA PROBLEMA»

NO CORAÇÃO DA CRIAÇÃO ESTAVA A BLOCKCHAIN, UM REGISTO EM CONTÍNUO CRESCIMENTO DE TODAS AS TRANSAÇÕES

ser congelado. Ao contrário de uma moeda nacional, não podia ser desvalorizado por capricho de um banco central, nem sujeito a controlos de capitais por parte de um ditador. Ao contrário dos cartões de crédito e das transferências bancárias, não impunha comissões de transação excessivas.

Os primeiros adeptos exibiam frequentemente uma mistura idiossincrática de motivos e crenças. Um exemplo que reflete a singularidade desses pioneiros foi Dustin Trammell, que se fazia chamar Druid na rede. Dustin era um hacker de trinta anos a quem agradava aprender fazendo; longe do computador, era um entusiasta do *cosplay*. Experimentara moedas alternativas com lastro em metais, como uma chamada Liberty Dollar, e doava os ciclos de processamento sobrantes dos seus computadores ao SETI@home, um projeto de longa duração da Universidade da Califórnia, em Berkeley, que aproveitava a capacidade de computação de milhares de computadores pessoais para analisar dados de radiotelescópios na busca por inteligência extraterrestre. Depois de conhecer o bitcoin, Dustin destinou metade desses computadores a executar o *software*, apenas porque lhe parecia um projeto tecnológico genial. Mais tarde, interessar-se-ia por ideias monetárias libertárias. Dustin trocou alguns e-mails com Nakamoto em que lhe confessou que «a moeda eletrónica e a criptografia são duas coisas que me interessam muito» e ofereceu a sua ajuda no projeto. «Temos definitivamente interesses semelhantes! —respondeu-lhe Nakamoto— Sabes, creio que havia muito mais gente interessada nos anos noventa mas, depois de mais de uma década de sistemas falhados baseados em terceiros de confiança (DigiCash, etc.), veem isto como uma causa perdida. Espero que consigam perceber que esta é a primeira vez, que eu saiba, que estamos a experimentar um sistema não baseado na confiança.»

«PROVA DE TRABALHO»

No coração da criação de Nakamoto estava algo chamado *blockchain*, um registo em contínuo crescimento de todas as transações (compra, venda, etc.) efetuadas no sistema. Aproximadamente a cada dez minutos, o mais recente conjunto de registos de transações era reunido num «bloco», e o bloco era «encadeado» ao bloco anterior através de uma matemática engenhosa que tornava impraticável alguém voltar atrás e manipular o conteúdo do bloco. Este registo, ou livro-razão, que nas finanças tradicionais seria mantido por uma instituição como um governo ou um banco, no bitcoin era mantido por uma rede de computadores de voluntários, cada um dos quais executava o *software* do bitcoin, comunicava com os demais computadores da rede e armazenava cópias mais ou menos idênticas e em constante atualização do livro-razão. O preço

de entrada nessa rede, para um computador, consistia em tentar resolver um quebra-cabeças matemático gerado pelo sistema a cada dez minutos. Tal como os sites distinguem humanos de *bots* pedindo aos utilizadores que indiquem quantas pontes há numa grelha de fotografias de paisagens, esse requisito, chamado «prova de trabalho», dissuadia agentes mal-intencionados de se apoderarem do sistema. Porque é que alguém se daria ao trabalho de desperdiçar a capacidade do seu computador nessa atividade estranha? Nakamoto concebeu o sistema de forma inteligente para que o primeiro computador a resolver cada quebra-cabeças recebesse uma recompensa de vários bitcoins. De uma penada, encontrara uma forma de atrair participantes sinceros e dissuadir os desonestos, ao mesmo tempo que criava um mecanismo previsível para libertar novos bitcoins para a oferta monetária. Embora o objetivo principal dessa corrida à resolução de quebra-cabeças fosse garantir a integridade do sistema, acabou por se chamar «mineração» devido à recompensa de vários bitcoins. (A enorme energia utilizada por centenas de milhares de computadores a trabalhar constantemente para resolver estes quebra-cabeças é também o que granjeou ao bitcoin a sua má reputação entre os ecologistas).

«MOEDA FIDUCIÁRIA»

Tudo isto pode soar arcano para leigos, mas um dinheiro descentralizado era algo que o mundo nunca tinha visto. A sua invenção foi uma proeza intelectual. Zooko Wilcox, cuja obsessão com a ideia de dinheiro descentralizado começou quando era um programador de dezenove anos com inclinações políticas e fre-

ISTOCK

Desde a criação do bitcoin, um dos avanços mais relevantes foi reconhecer que a tecnologia *blockchain* pode aplicar-se para lá das criptomoedas.

quentava a Universidade do Colorado, em Boulder, praticamente não pensara noutra coisa durante a década anterior ao aparecimento do bitcoin. «Durante doze anos, mais ou menos, um dos meus passatempos favoritos antes de adormecer era tentar descortiná-lo —disse-me—. A minha sensação é que o mecanismo de consenso criado por Nakamoto, e a forma como o combinou com sistemas de incentivos, não teria sido descoberto por mais ninguém. Teriam sido precisos outros cem anos para lá chegar.» Quer extraísses bitcoins, quer os comprasses a alguém que o tivesse feito, entrar desde cedo tinha um apelo inegável. O *software* de Nakamoto estabelecia um limite máximo de 21 milhões de bitcoins cunhados, quantidade que o sistema previa atingir por volta do ano 2140. Em vez de estar em risco de inflação ou hiperinflação, o bitcoin era deflacionário: se a tecnologia se disseminasse, terias na mão um ativo que se valorizaria. Numa publicação na rede social da Fundação P2P, Nakamoto comentou: «Adoro a ideia de comunidades virtuais e não geográficas a experimentar novos paradigmas económicos».

Para mim, o bitcoin era alucinante, como um portal para um mundo —ou uma visão do mundo— cuja existência eu desconhecia. Os libertários alienados já viam o dinheiro do dia a dia como mera «moeda fiduciária» —pronunciavam a expressão com umas sonoras e desdenhosas aspas—, que só tinha valor por decreto governamental. Mas, para o resto de nós, descobrir uma moeda que funcionava fora dos parâmetros habituais era como aquela metáfora de David Foster Wallace sobre uns peixes que não se dão conta de estar na água até que, retirados bruscamente do seu meio, a arfar, contemplam pela primeira vez a realidade.

O que é que fazia com que o bitcoin valesse alguma coisa? O dólar norte-americano era de curso legal e estava respaldado por um dos governos mais estáveis do mundo. Podias usá-lo para pagar impostos. Os comerciantes eram obrigados

SHUTTERSTOCK

A crise financeira de 2008 não foi apenas o pano de fundo, mas o catalisador direto para a criação das criptomoedas.

NO MESMO MÊS EM QUE SOUBE DA EXISTÊNCIA DESTA CRIPTOMOEDA, PERDEU MAIS DE 99 % DO SEU VALOR

a aceitá-lo. Mas o que poderia atribuir valor a uma cadeia de números e letras? Quando foi lançado um serviço de câmbio de bitcoins chamado New Liberty Standard, em outubro de 2009, fixou o preço de um único bitcoin (BTC) em menos de um décimo de um cêntimo de dólar, com base no custo de eletricidade necessário para o extrair. Mas o preço do bitcoin ganhou vida própria. No início de 2011, a cotação de mercado ultrapassou o dólar e, quando Jason me telefonou, um bitcoin valia mais de 17 dólares. Grande parte do valor, naqueles primeiros tempos, parecia derivar da crença no potencial do bitcoin como uma espécie de ouro digital com um mercado mundial —e de pura especulação financeira.

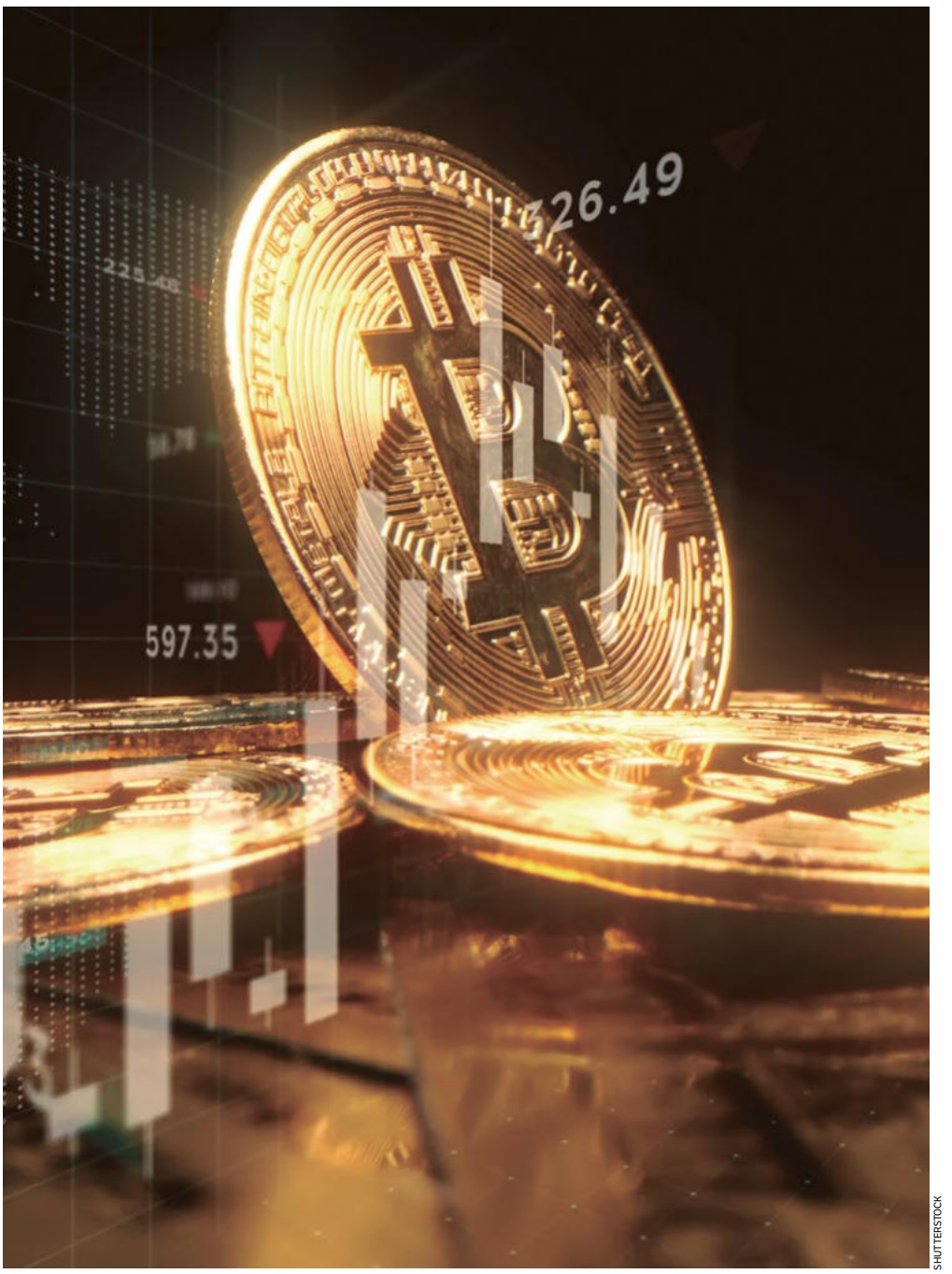
O QUE É QUE ESTAS PESSOAS TINHAM CONTRA OS BANCOS?

Senti-me atraído pelo fascínio de estar em terreno virgem. «É fascinante criar uma nova moeda —contou-me Jeff Garzik, um programador de bitcoin que vivia e trabalhava numa autocaravana Fleetwood Southwind de 1984 na Carolina do Norte—. Pode dizer-se que é a primeira moeda global do mundo.» Em Brooklyn, conheci Mark Suppes, um faz-tudo que estava a construir uma caixa automática de bitcoins no seu *loft* em Bedford-Stuyvesant, a poucos metros do reator de fusão nuclear caseiro que também montava. Um anarquista barbudo, de lenço ao estilo pirata na cabeça e que publicava no YouTube como The Real Plato, viajava do Connecticut à Califórnia, à maneira de Jack Kerouac, e tentava financiar a aventura unicamente com bitcoins. Colecionadores de moedas raras falavam de um tempo futuro em que as pessoas trocariam bitcoins invulgares, como os do chamado bloco Génesis, o primeiro da cadeia, com tanto entusiasmo como se fossem Águias Duplas de 1933.

Mas, embora me deixasse levar pela emoção, havia aspetos que me escapavam. Eu conseguia perceber que este novo dinheiro fosse apelativo num país como a Argentina, onde a hiperinflação e os controlos cambiais eram reais, bem como no México, nas Filipinas ou em grande parte de África, onde mais de 60 % da população não tinha contas bancárias. Mas não entendia o problema que os bitcoiners norte-americanos tinham com as instituições financeiras tradicionais. O seguro federal de depósitos funcionava bastante bem. Os caixas automáticos eram práticos. O que é que estas pessoas tinham contra os bancos?

Também me custava entender os fundamentos técnicos do bitcoin e como interagiam as partes do sistema. Nas reuniões, costumava anuir enquanto as pessoas falavam de «funções *hash* unidirecionais» e de «equilíbrios de *Nash*» e depois, em casa, passava horas a ler sobre o tema até me arderem os olhos. Quando finalmente achava que o tinha percebido, a clareza recém-adquirida esvaía-se assim que tentava explicá-lo a outra pessoa. Senti-me um pouco menos estúpido depois de Garzik, um dos principais programadores de *software* do projeto, me dizer: «O bitcoin é muito, muito difícil de entender».

A ALTERNATIVA A GUARDAR O TEU BITCOIN NUMA PLATAFORMA ERA A «AUTOCUSTÓDIA» DE UMA CHAVE PRIVADA



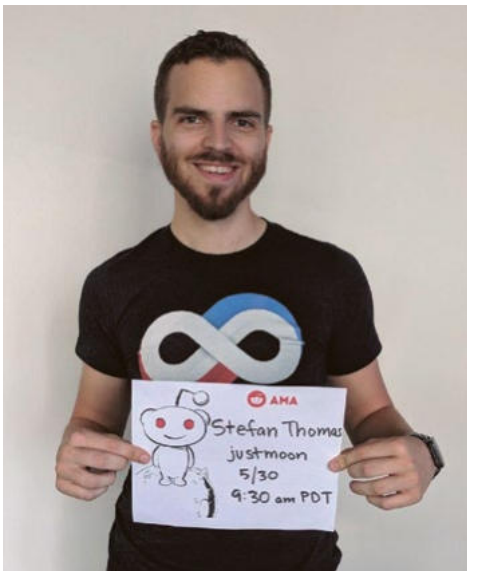
SHUTTERSTOCK

O bitcoin, criado especificamente para eliminar intermediários financeiros, é agora comercializado por esses mesmos intermediários.

O bitcoin também era difícil de comprar, de guardar, de usar e de custodiar. Era extremamente volátil: no mesmo mês em que soube da sua existência, perdeu, por momentos, mais de 99 % do seu valor, caindo de 17 para 0,01 dólares. As plataformas de câmbio de bitcoins, não reguladas e sem prestar contas, revelavam-se frequentemente negócios pouco fiáveis, com proprietários anónimos que recebiam os depósitos dos clientes e, um dia, simplesmente fugiam com eles. Até a Mt. Gox, a maior plataforma, sofrera o roubo de 25 000 BTC, no valor, à época, de 500 000 dólares, às mãos de piratas informáticos; precisamente isso precipitou o colapso repentino do preço do bitcoin.

AUTOCUSTÓDIA

A alternativa a guardares o teu bitcoin numa plataforma era a «autocustódia» de uma chave privada, normalmente uma cadeia de 51 carateres de números e letras que era o equivalente criptográfico de uma palavra-passe, numa «carteira» de bitcoin, que na realidade se assemelhava mais a um porta-chaves. Podias rabiscar a tua chave num pedaço de papel, gravá-la numa placa de aço e enterrá-la no jardim, guardá-la num computador limpo ou simplesmente decorá-la. A última opção parecia o auge da autosoberania e havia algo de excitante na ideia de que podias atravessar uma fronteira internacional com a tua chave na cabeça e transferir o teu dinheiro de uma forma tão simples.



ASC

Stefan Thomas possui 7002 bitcoins mas perdeu a palavra-passe e só tem duas tentativas antes de que se bloqueie permanentemente.

Ninguém aconselhava fazê-lo, pois um único algarismo mal recordado poderia custar-te todos os teus ativos. A autocustódia —um ideal que acabaria consagrado no mantra cripto «Sem as tuas chaves, não são as tuas moedas»— acarretava o seu próprio conjunto de problemas. Stefan Thomas, um programador suíço, guardara cópias das chaves de 7002 bitcoins em três locais, colocando a sua carteira principal numa «máquina virtual» isolada da internet e fazendo uma cópia de segurança tanto com o *software* TrueCrypt como numa IronKey, um *hardware* seguro semelhante a uma pen USB. Mas então, ao atualizar o sistema operativo, apagou acidentalmente a máquina virtual. E, quando iniciou sessão no seu TrueCrypt, que estava armazenado na Dropbox, também desaparecera; afinal, podia ser sobrescrito se houvesse mais de duas máquinas ligadas ao mesmo tempo. Quanto ao seu IronKey, simplesmente perdera a palavra-passe. O valor das moedas perdidas, nessa altura, era de 140 000 dólares. «Passei uma semana a tentar recuperá-las

sem sucesso —disse-me Stefan—. Foi bastante doloroso.» No final de 2021, essas moedas valeriam 473 milhões de dólares. Mas Stefan não foi o único na desgraça. A empresa de dados Chainalysis estimava que 20 % de todos os bitcoins em circulação se tinham perdido.

«COMO É QUE ISTO PODE FUNCIONAR?»

Gavin Andresen pareceu-me um primeiro guia afável neste mundo esotérico. A ponto de completar quarenta e um anos, trazia uma franja castanha colada à testa e a etiqueta «geek» literalmente no peito, cosida num emblema sobre uma camisa de manga curta. Era um homem de classe média, pai de duas crianças e de tom de voz suave. Enquanto alguém que desprezasse a própria memória te diria algo como «a minha mulher podia contar-te muita coisa sobre a minha má memória» e ficaria por aí, Gavin provavelmente expressá-lo-ia assim: «Li uma investigação sobre o quão defeituosa é a memória humana» e lançar-se-ia a explicar-te tudo em detalhe. Além disso, andava de monociclo.

O bitcoin surgira na vida de Gavin num momento oportuno. Em 2009, a sua esposa, Michele, professora de Geologia na Universidade de Massachusetts, tirou um ano sabático, Gavin deixou o seu posto estável na área da aprendizagem automática na universidade e a família mudou-se para a Austrália. Gavin passou os seis meses seguintes em Queensland a fazer malabarismos com cocos, a correr na praia, a fazer mergulho, a guerrear-se com mosquitos, a resgatar uma serpente-do-mar de focinho pontiagudo, a beber cerveja XXXX e a rapar a pêra que usara nos últimos dezassete anos, entre outros passatempos. Planeava lançar

STEPHEN MCCARTHY / SPORTSFILE / WEB SUMMIT

Gavin Andresen foi a pessoa escolhida pessoalmente por Satoshi Nakamoto para liderar o desenvolvimento do protocolo antes do seu misterioso desaparecimento em 2011.

O BITCOIN FAUCET ENQUADRAVA-SE BEM NO ENCANTO ARTESANAL DO BITCOIN NESSA PRIMEIRA FASE

uma *start-up* quando a família regressasse aos Estados Unidos, mas, em maio de 2010, ainda não encontrara uma ideia que o convencesse.

Então leu uma entrada num blogue de tecnologia sobre um punhado de projetos de *software* de código aberto, incluindo o bitcoin. Gavin formara-se na Universidade de Princeton e trabalhara na Silicon Graphics. Era membro do órgão legislativo da sua pequena cidade da Nova Inglaterra, interessava-se ativamente pela política escolar local e oferecera-se como voluntário para ajudar com o site da Liga das Mulheres Eleitoras de Amherst.

Mas atraía-o a ideia de que o dinheiro não estivesse controlado por uma elite da Reserva Federal. Gostava da liberdade individual, da sabedoria coletiva, dos processos orgânicos de base em vez do controlo a partir de cima. Acreditava mais na evolução do que na revolução, em «pequenos passos rumo a um mundo melhor».

Contudo, a sua principal reação perante o bitcoin, como me contou mais tarde, foi: «Como é que isto pode funcionar?». Perguntava-se como é que o sistema criava novas moedas e como evitava o duplo gasto. Pesquisou «bitcoin» no Google e obteve apenas quatro páginas de resultados. Depois transferiu o código e começou a lê-lo. Era claro que o programador sabia o que fazia. Gavin executou o *software* e minou algumas moedas. Ainda assim, «tive de pensar muito para me convencer de que o sistema não apresentava falhas». Quando falámos, estava «bastante seguro de que não havia nenhuma falha fundamental».

Um mês depois de conhecer o bitcoin, Gavin criou o Bitcoin Faucet. Nessa altura, um bitcoin valia meio cêntimo, e Gavin gastou cinquenta dólares para comprar 10 000 e configurar um site para os oferecer. Qualquer pessoa podia resolver um CAPTCHA e receber cinco bitcoins gratuitos. A ideia era tornar esta experiência apelativa para novos utilizadores. Gavin compreendia que o dinheiro só adquire valor quando as pessoas o utilizam.

SUBSTITUIR O DÓLAR COMO MOEDA DE RESERVA MUNDIAL

O Bitcoin Faucet encaixava bem no encanto artesanal do bitcoin naquela primeira fase. Numa ocasião, Gavin almoçou com David Forster, um agricultor que vivia perto da sua casa em Massachusetts e que trocava meias de alpaca por bitcoins. Os bitcoiners rejubilaram quando Laszlo Hanyecz, que vivia na Florida, pagou 10 000 bitcoins por duas pizzas grandes da Papa John's. Anos mais tarde, as pessoas não se cansavam de reavaliar essas pizzas ao preço atual do bitcoin: 690 milhões de dólares por pizza! «Não me sinto mal por isso —disse-me Laszlo quando esses bitcoins valiam apenas uns 85 000 dólares—. A pizza estava ótima.»

Uns dias depois, Gavin colocava e respondia a perguntas no fórum do bitcoin enquanto enviava fragmentos de código a Nakamoto para colmatar os inevitáveis buracos presentes em qualquer *software* novo. Sabia pouco sobre Nakamoto.

Nunca se tinham encontrado pessoalmente nem falado ao telefone. A ideia que Gavin tinha do seu principal colaborador de trabalho baseava-se unicamente na correspondência escrita. Através de e-mails e mensagens privadas, Gavin interpretou que Nakamoto era sério e picuinhas, autossuficiente e brilhante. A Gavin preocupavam-no os problemas legais. O governo processara criadores anteriores de moedas alternativas. Poderia ser preso? Michele gostava de gracejar com ele sobre esse «dinheiro fictício da internet», mas depressa Gavin começou a dedicar-lhe todo o seu tempo.

Trabalhava no projeto porque lhe interessava, mas também admirava o modo como Nakamoto adaptara o bitcoin à natureza humana. Assim que possuías algumas dessas moedas digitais, querias ajudar o sistema, fosse a minerá-las, a usá-las, a promovê-las ou a trabalhar no código, para que os teus bitcoins valessem mais amanhã do que ontem. À medida que o preço subia, Gavin recebia uma recompensa material em tempo real. A sua participação era um «interesse próprio esclarecido». Achava que o bitcoin poderia tornar-se numa importante moeda mundial e, com o tempo, eventualmente até substituir o dólar como moeda de reserva mundial.

GAVIN TORNOU-SE O PROGRAMADOR PRINCIPAL

Apesar de o bitcoin ser um projeto de código aberto, um esforço coletivo que, em teoria, era imune a interesses particulares, alguém tinha de assumir a direção, e durante os primeiros vinte meses esse alguém fora Satoshi. Nakamoto publicava o código, outros programadores sugeriam correções e ele incorporava as que considerava adequadas.

Quatro meses depois de Gavin começar a colaborar, a sua dedicação, os seus conhecimentos informáticos e a atitude sincera pareceram granjear-lhe a confiança de Nakamoto. Primeiro, deu a Gavin acesso direto ao código-fonte. Depois, por volta de setembro de 2010, Nakamoto disse-lhe que estava ocupado com outros projetos e que, nos meses seguintes, lhe entregaria o controlo tanto do repositório de código no SourceForge como da «chave de alerta» do projeto, que permitia transmitir mensagens urgentes a todas as máquinas que executavam o *software* do bitcoin. Para um projeto de código aberto, estes elementos eram os símbolos de autoridade mais evidentes e, nesse momento, Gavin tornou-se efetivamente o programador principal do projeto, a liderar uma equipa de cinco programadores voluntários.

Nos meses seguintes, Nakamoto continuou a intervir ocasionalmente em questões técnicas, mas a sua natureza reservada chocava com a abordagem aberta de Gavin. Depois de a PayPal e a Visa terem congelado as contas do WikiLeaks, uma fação de bitcoiners sustentou que o WikiLeaks poderia beneficiar do bitcoin e que, por sua vez, essa colaboração serviria para dar a conhecer a moeda digital.

ALGUNS BITCOINERS CELEBRARAM COM ENTUSIASMO A ATENÇÃO MEDIÁTICA, MAS NAKAMOTO NÃO

SHUTTERSTOCK

O WikiLeaks começou a aceitar doações em bitcoin em 2011, tornando-se numa das primeiras organizações a fazê-lo.

«Avancem», escreveu alguém num fórum chamado BitcoinTalk. Mas Nakamoto irritou-se: «Não, não o façam. O projeto precisa de crescer gradualmente para que o *software* se possa fortalecer pelo caminho. Apelo ao WikiLeaks para que não tente utilizar bitcoins. O alvoroço que provocariam provavelmente destruir-nos-ia nesta fase».

A ideia de o WikiLeaks aceitar doações em bitcoins deu origem a um artigo na *PC Magazine*. Alguns bitcoiners celebraram com entusiasmo a atenção mediática, mas Nakamoto não: «Teria sido bom receber esta publicidade noutro contexto qualquer, mas o WikiLeaks abriu a caixa de Pandora e a avalanche dirige-se para nós».

NAKAMOTO PARECIA CADA VEZ MAIS DESCONFORTÁVEL

Para os jornalistas que cobriam o bitcoin, Gavin tornara-se a pessoa natural a quem recorrer em primeiro lugar. Tinha um caráter afável e sensato, uma tendência natural para posições políticas moderadas e a vontade de usar o seu verdadeiro nome, o que fazia dele o embaixador do bitcoin que Nakamoto nunca fora. Mas Nakamoto parecia cada vez mais desconfortável com as interações de Gavin com os meios de comunicação. No final de abril de 2011, enviou-lhe um e-mail: «Quem me dera que não continuasses a falar de mim como uma figura misteriosa nas sombras, ou a imprensa acabará por interpretar o bitcoin como se fosse uma moeda pirata». Foi a última vez que Gavin soube de Nakamoto. Quando falei pela primeira vez com Gavin, nesse julho, disse que não se comunicava com Nakamoto «havia um par de meses». Depois de, a 26 de abril, Gavin ter dito ingenuamente a Nakamoto, num e-mail, que aceitara dar uma palestra sobre o bitcoin à CIA, curiosa pelas criptomoedas, na sua sede em Langley, Virgínia, Nakamoto nunca respondeu. Quase na mesma altura, escreveu e-mails a pelo menos mais um programador que trabalhara no projeto.

Depois, ficou em silêncio. ■

Uma miragem deslumbrante

Depois de anos de existência, o bitcoin permanece nesta tensão entre ser uma revolução monetária legítima e um ativo especulativo: nem o paraíso prometido pelos maximalistas, nem a fraude proclamada pelos detratores, mas uma tecnologia complexa, com capacidades reais e limitações significativas.

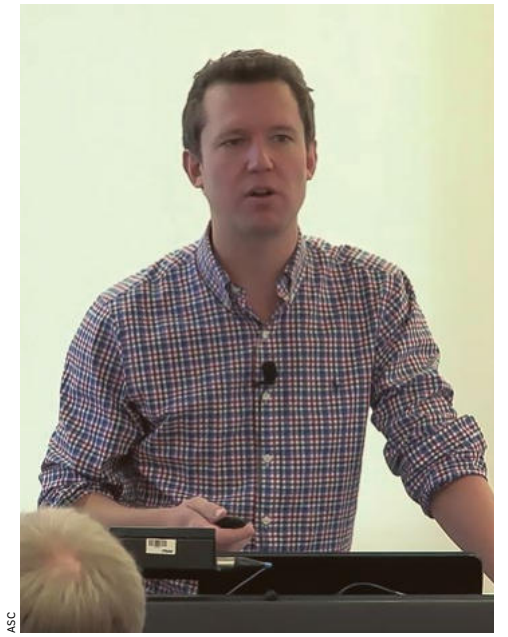
ISTOCK

Então, sabes quem é o Satoshi? —perguntei.

Se alguém o sabia, esse era o Gavin.

—Não sei o seu verdadeiro nome. Espero que um dia decida deixar de ser anónimo e o possa conhecer, mas não creio —respondeu-me.

O Gavin e os outros programadores estavam de acordo em alguns pontos. O segundo sítio onde Nakamoto anunciara o seu documento técnico foi o site da Fundação P2P, uma organização idealista sem fins lucrativos dedicada a redes entre pares de todo o tipo. No seu perfil no site, Nakamoto assinalou o Japão como local de residência. Mas ninguém acreditava, de facto, que fosse japonês. O seu inglês era impecável, com a segurança descontraída de um falante nativo. Soava britânico, ou pelo menos de um país da Commonwealth. O bloco Génese incluía uma manchete do *Times* e, tanto no código-fonte do bitcoin como nas suas publicações no fórum BitcoinTalk, Nakamoto privilegiava a ortografia britânica, em palavras como *colour* e *optimise*. A manchete do Times sugeria a motivação de Nakamoto: «O ministro das Finanças à beira do segundo resgate bancário».



ASC

O irlandês Mike Hearn passou de peça-chave a tornar-se o crítico mais acérrimo do bitcoin.

UM GEEK DA PROGRAMAÇÃO

Chamava a atenção o zelo com que Nakamoto guardava a sua identidade. Registou o domínio bitcoin.org através de um serviço de mascaramento chamado anonymousspeech.com, que, por sua vez, fora registado por um agente de alojamento temporário em Tóquio. Esse serviço forneceu-lhe um endereço de correio eletrónico em vistomail.com, que oferecia a opção de manipular a data e a hora de envio de um e-mail. Um terceiro endereço de correio eletrónico que Nakamoto usou era do gmx.com, outro fornecedor de webmail gratuito. Michael Marquardt, que dirigia o *BitcoinTalk* sob o nome de Theymos, estava convencido de que Nakamoto ocultava o seu endereço IP recorrendo ao TOR, o mesmo *software* de navegação anónima necessário para aceder a sites da web obscura como a *Silk Road*. E

NAKAMOTO REGISTOU O DOMÍNIO BITCOIN.ORG ATRAVÉS DO SERVIÇO DE MASCARAMENTO ANONYMOUSSPEECH.COM

Nakamoto exprimia-se com uma opacidade estudada. Respondia a perguntas técnicas, segundo Gavin, como «um geek da programação a falar com outro geek da programação». Qualquer tentativa de lhe arrancar informação pessoal era habilmente ignorada.

O código de Nakamoto contava a sua própria história. Gavin achava que os programadores tinham estilos literários tão distintos como os de Kurt Vonnegut e Jackie Collins. Havia indícios de que Nakamoto poderia ser um pouco mais velho. A Gavin, o seu estilo de programação parecia-lhe algo antiquado, e um programador irlandês chamado Mike Hearn, que trabalhava para a Google, na Suíça, observou que Nakamoto usava notação húngara, uma convenção de nomenclatura de variáveis popular entre programadores de Windows nos anos 90. Também era bastante invulgar ver alguém do mundo Windows a liderar um projeto de código aberto, já que o movimento de código aberto surgira em grande medida como reação a sistemas fechados como o Windows.

ASC

Amir Taaki, anarquista, *hacktivista* e programador britânico-iraniano, conhecido pelo seu papel destacado no projeto bitcoin.

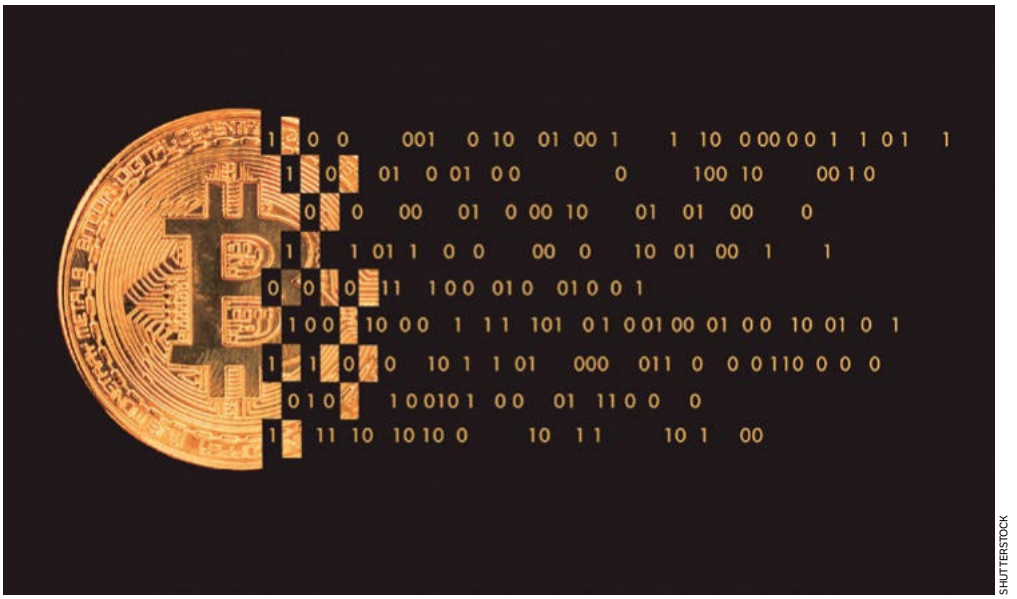
Os programadores de bitcoin divergiam noutros aspetos. Para Gavin, Nakamoto figurava entre os 10% de programadores mais destacados pela sua destreza. Mas Amir Taaki, um dos primeiros programadores de bitcoin e hacker anarquista —vivia num prédio ocupado em Londres e mais tarde tornar-se-ia ativista das armas impressas em 3D e lutaría a favor dos curdos na frente da guerra civil da Síria— disse-me que não acreditava que Nakamoto tivesse sequer formação em informática. Embora Amir considerasse sólido o conceito do bitcoin, achava que o código estava mal escrito, com tudo amontoado em dois ficheiros pouco manejáveis, em vez de dividido em componentes modulares, como o organizaria um profissional. Isto levou-o a pensar que Nakamoto poderia ser professor. «Quando programas durante muitos anos e trabalhas com uma equipa, começas a pensar: "Como posso escrever este código-fonte de forma compreensível para um grande número de pessoas?". Aprendes a abstrair as coisas de maneira a torná-las óbvias e compreensíveis, aprendes padrões de design básicos, formas padrão de fazer as coisas, mas estes são aspetos que os académicos não aprendem. Os engenheiros preocupam-se com questões deste tipo, isto é, com responder à pergunta: "Como posso construir isto sem erros e de um modo fácil de entender?"». Amir tinha formação em Matemática, e o que detetou ao ler o documento técnico foi um domínio perito de ferramentas matemáticas e estatísticas.

Gavin tinha a impressão de que o código do bitcoin fora escrito por um pequeno grupo ou até por uma única pessoa. Quando os programadores colaboram, costumam inserir comentários regulares no código para explicarem uns aos outros o que é suposto este ou aquele bloco de instruções fazer. O *software* do bitcoin continha poucos comentários. Outros defendiam que o bitcoin era excessivamente sofisticado e funcionara bem demais desde o momento do seu lançamento para ser produto de um único cérebro. Além disso, o livro branco empregava o pronome nós, pelo que Satoshi Nakamoto poderia ser, na realidade, o nome coletivo de um grupo ou de uma instituição.

Quando tomei conhecimento da existência do bitcoin, os membros da sua jovem comunidade já se interrogavam sobre a identidade de Nakamoto. As especulações precederam o seu desaparecimento. Em janeiro de 2011, mesmo antes de Nakamoto se evaporar, já começava a ser venerado. Quando ficou claro que o bitcoin precisava de unidades mais pequenas, a comunidade começou a chamar satoshi à centésima parte de um bitcoin. Nesse mesmo mês, alguém reparou que a última publicação de Nakamoto no *BitcoinTalk* fora a 13 de dezembro. Instalou-se o pânico. Tinha Nakamoto abandonado o projeto? Estaria morto? Quem os lideraria? Pela primeira vez, algumas pessoas começaram a questionar abertamente quem era realmente Nakamoto.

NEAL STEPHENSON, GRIGORI PERELMAN, JULIAN ASSANGE...

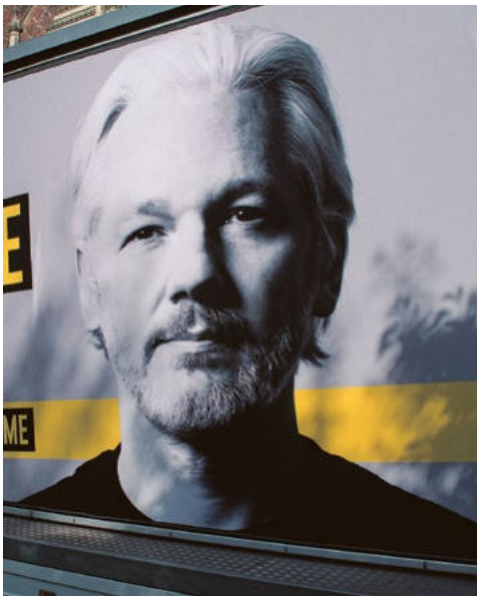
Alguém avançou com a teoria de que Nakamoto era «parecido a Nicolas Bourbaki», referindo-se a um pequeno grupo de matemáticos franceses que começou a publicar artigos na década de 1930 usando um pseudónimo coletivo. Outros assinalaram que o mistério conferia ao bitcoin um glamour útil. Outra pessoa sugeriu



SHUTTERSTOCK

A transformação de código binário em valor económico. Satoshi Nakamoto conseguiu algo que os economistas consideravam impossível: criar escassez digital recorrendo à matemática e ao consenso.

que «o tipo só quer alguma privacidade. E isso é bom, porque mostra claramente que não é fama o que procura, mas ideais. Na minha humilde opinião, deveríamos respeitar isso e deixar a sua identidade em paz». Mas as pessoas não conseguiram evitar propor candidatos: poderia ser Neal Stephenson, o romancista cujo *Criptonomicon* antecipara o dinheiro digital? Julian Assange, o fundador australiano da WikiLeaks? Grigori Perelman, um génio russo eremita que recusara um prémio de Matemática de um milhão de dólares?



SHUTTERSTOCK

Londres, Inglaterra. 11 de setembro de 2020. Um painel publicitário com o fundador da WikiLeaks, Julian Assange.

O pânico revelou-se injustificado. A 13 de janeiro, Gavin sossegou a comunidade: Nakamoto enviara-lhe um e-mail nesse dia «sobre um erro complicado... Está ocupado». Mas, a 16 de abril de 2011, um utilizador do *BitcoinTalk* chamado Wobber, assinalando que «já fazia muito tempo desde a última vez que publicara aqui», abriu um novo tópico: «Quem é Satoshi Nakamoto?». Wobber destacou a variedade da experiência de Nakamoto e o quão invulgar fora o seu comportamento: criar algo tão inovador, não se atribuir o mérito nem explorar a notoriedade e ir-se embora sem dizer a ninguém. Alguém comparou Nakamoto ao Zorro ou a um David mascarado que apontara a sua funda ao Golias dos bancos e dos governos. Outro perguntou-se se Nakamoto poderia ser Gavin Andresen. Gavin tinha ligação à Austrália, pois nascera lá antes de se mudar para os Estados Unidos em criança, o que explicaria porque é que Nakamoto alternava caraterísticas da ortografia americana e da Commonwealth. Outra pessoa perguntou-se se Nakamoto teria criado uma personalidade falsa para interagir consigo próprio.

«SATOSHI PODERIA SER QUALQUER UM»

Com tão poucas pistas a seguir, os detetives agarravam-se aos detalhes mais insignificantes. Poderia o nome conter uma pista? *Sato shi Nakamoto*, traduzido aproximadamente do japonês, poderia significar «inteligência central». Talvez

O BITCOIN PRECISAVA DE UNIDADES MAIS PEQUENAS E A COMUNIDADE COMEÇOU A CHAMAR SATOSHI À CENTÉSIMA PARTE DE UM BITCOIN

isto apontasse para o papel dos espiões na criação do bitcoin. Talvez a Agência de Segurança Nacional estivesse a executar uma estratégia de longo prazo, lançando uma rede financeira não oficial que poderia usar para pagar ativos no terreno em qualquer parte do mundo, ou como um isco onde os adversários realizariam transações com uma falsa sensação de segurança enquanto os espiões de Fort Meade vigiavam todos os seus movimentos.

Não era uma ideia totalmente descabida. O Laboratório de Investigação Naval dos Estados Unidos criara o The Onion Router, o *software* de anonimato conhecido como TOR24 que tornou possível a web obscura. Mais tarde, o FBI criaria em segredo a sua própria linha de telefones cifrados e um serviço de mensagens, o ANOM, que foram adotados inadvertidamente por criminosos organizados, resultando em mais de oitocentas detenções. E, no verão de 1996, três investigadores da Divisão de Criptologia da Direção de Investigação e Tecnologia de Segurança da Informação da NSA publicaram internamente um extenso artigo, que posteriormente se tornaria público, intitulado «Como fazer dinheiro: a criptografia do dinheiro eletrónico anónimo».

Também se podia ler o nome de Nakamoto como um acrónimo dos nomes de grandes empresas tecnológicas: samsung, toshiba, nakamichi, motorola, pelo que talvez uma conspiração empresarial estivesse por detrás deste mistério. Os utilizadores do Reddit juntaram as suas habilidades de decifração e acabaram por descobrir que Satoshi Nakamoto era um anagrama de, entre outras frases, *Ma, I took NSA's oath* («Mamã, fiz o juramento da Agência de Segurança Nacional») e *So a man took a shit* («Assim, um homem cagou»).

Pela primeira vez, as pessoas perguntaram-se por que razão Nakamoto usara um pseudónimo. Ter-se-ia devido aos incómodos da fama? À história de os Governos perseguirem os criptógrafos? A evitar o assédio? Aos inimigos que o bitcoin poderia gerar? Talvez quisesse simplesmente permanecer anónimo. Talvez não quisesse misturar este empreendimento com outros negócios.

Em maio, Gwern Branwen, um programador e escritor que também usava um pseudónimo, com seguidores em certos blogues populares em Silicon Valley, traçou a sua própria ideia sobre Nakamoto. «O Satoshi podia ser qualquer um», escreveu. O bitcoin não exigia «grandes avanços intelectuais de tipo matemático ou criptográfico», mas antes uma combinação inteligente de tecnologias existentes, pelo que «o Satoshi podia ser um simples programador autodidata, já que não precisava de conhecimentos profundos de criptografia!».

A CRIPTOMOEDA É MAIOR DO QUE SATOSHI

Stefan Thomas, o bitcoiner suíço que perdera mais de sete mil moedas, abordou a questão metodicamente, representando graficamente os dados temporais das mais de quinhentas publicações de Nakamoto no fórum. Estes revelaram uma que-

THE ONION ROUTER, UM SOFTWARE DE ANONIMATO CONHECIDO COMO TOR24, TORNOU POSSÍVEL A WEB OBSCURA

ASC

O investigador de segurança Dan Kaminsky, conhecido pelo seu trabalho na descoberta de falhas de segurança do DNS.

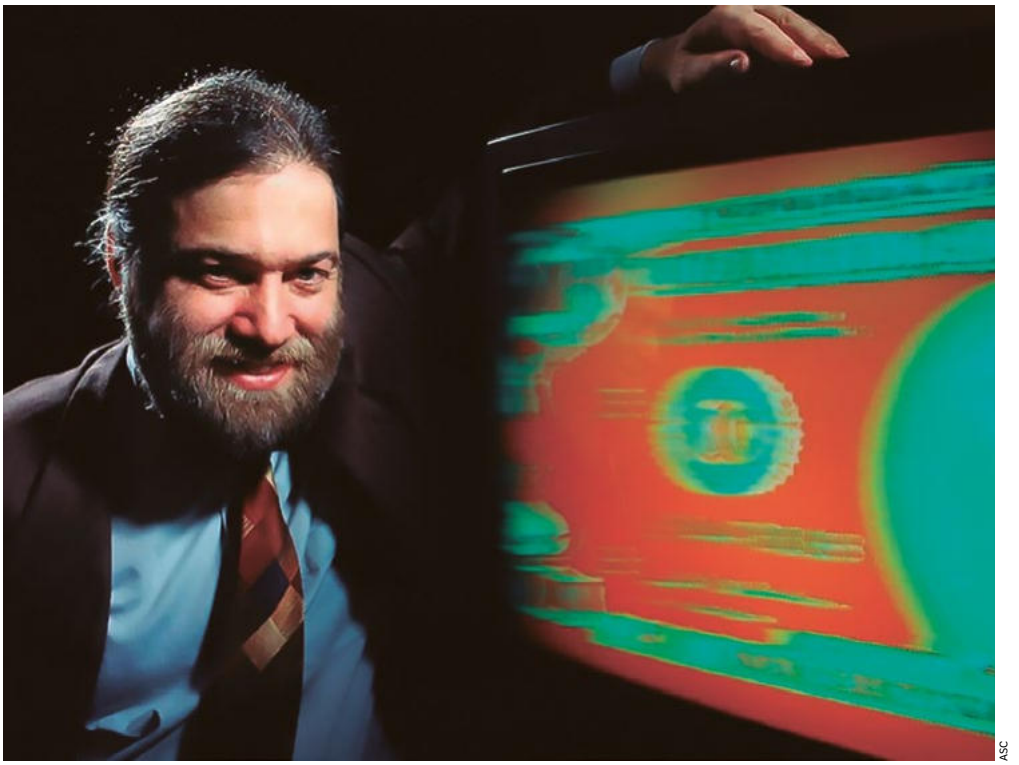
da acentuada na atividade de publicação durante as horas correspondentes à noite na América do Norte. «O Mike jura que tem sotaque britânico», disse-me Stefan, referindo-se a Mike Hearn, o programador de bitcoin. Stefan tinha em mente um perfil vago de Nakamoto: uma única pessoa que vivia nos Estados Unidos, embora não fosse norte-americano. «A navalha de Ockham», disse. Uma explicação simples superava uma complicada.

Quando Stefan publicou o seu gráfico no *BitcoinTalk*, este foi recebido com um coro de discordâncias: não seria mais provável que Nakamoto dedicasse tempo ao bitcoin quando não estava a trabalhar? Nesse caso, as horas de publicação poderiam corresponder à Europa Ocidental. «Desde quando é que um hacker dorme à noite?», protestou alguém. Outro notou que o padrão deveria mudar aos fins de semana, mas não mudava.

Dan Kaminsky, um investigador de segurança informática de trinta e dois anos que ganhara notoriedade três anos antes quando descobriu uma vulnerabilidade crítica capaz de comprometer toda a infraestrutura da internet, pensou que Nakamoto poderia ser um grupo de um banco. «Suspeito que o Satoshi seja uma pequena equipa de uma instituição financeira —disse-me o Dan—. Tenho esse pressentimento».

A identidade de Nakamoto era «uma miragem deslumbrante. Mas não creio que seja assim tão importante para o que é o bitcoin. A criptomoeda é maior do que Satoshi», acrescentou Dan. Isto reforçava um argumento que eu já ouvira antes: o anonimato de Nakamoto e o seu eventual desaparecimento não eram acidentais, mas elementos-chave da conceção original do bitcoin.

Não conseguia parar de pensar no bitcoin. Não conseguia parar de pensar no seu criador. Talvez não tivesse de ser assim tão difícil. Às vezes, parecia que a internet



David Chaum inventou quase todos os conceitos fundamentais do dinheiro digital, mas a sua empresa, a DigiCash, faliu em 1998.

era, em grande medida, um eco constante das mesmas ideias. Os Sherlocks informáticos que desenhavam gráficos temporais e escrutinavam nomes de variáveis não se tinham dado ao trabalho de levantar o telefone. Crenças tomadas por factos na internet dissolviam-se muitas vezes ao contacto com a realidade. Talvez Nakamoto estivesse a mexer, impaciente, os polegares calejados de tanto teclar, sentado numa cadeira ergonómica para *gamers*, à espera de que alguém como eu lhe ligasse. Escrevi para satoshin@gmx.com, o endereço que Gavin disse ter usado, e pedi uma entrevista.

MATEMÁTICOS COM ARMAS

Enquanto esperava resposta, contactei um par de possíveis candidatos a ser Nakamoto. Um deles era Adam Back, um criptógrafo britânico que, na década de 1990, escrevera o Hashcash, um *software* de prevenção de *spam* que utilizava quebra-cabeças computacionais, a chamada «prova de trabalho», para obrigar as máquinas a demonstrar que eram «honestas». Era a mesma tecnologia que Nakamoto viria a incorporar mais tarde no bitcoin. De facto, Back foi a primeira pessoa, publicamente conhecida, a quem Nakamoto contactou. Em agosto de 2008, alguém de quem nunca ouvira falar escreveu-lhe para perguntar como citar corretamente o Hashcash no livro branco do bitcoin, como Back viria a revelar mais tarde.

Trocámos e-mails, mas convenci-me do que Amir Taaki me dissera: «O Adam

ADAM BACK FOI A PRIMEIRA PESSOA, PUBLICAMENTE CONHECIDA, A QUEM NAKAMOTO CONTACTOU

tem um estilo coerente em todos os seus projetos. O seu estilo não coincide com o do Satoshi». Amir explicou-me que Back seguia as convenções de programação padrão, escrevia em C e era um programador de Unix/Linux, enquanto Nakamoto tinha um estilo errático, escrevia em C++ e era um tipo do Windows. Back era também conhecido, então, como um fanático da privacidade, alguém propenso a rejeitar as concessões de anonimato do bitcoin; a essência —e a principal contradição— de uma blockchain era que qualquer pessoa podia ver tudo o que acontecia. Além disso, parecia-me incrivelmente desastrado que alguém empenhado em passar despercebido, que mal citara duas ou três referências, incluísse entre elas o seu próprio trabalho.

O candidato a Nakamoto mais óbvio era David Chaum, um corpulento empresário do dinheiro eletrónico que usava Birkenstocks e que tivera um dos seus primeiros momentos eureka enquanto conduzia uma carrinha Volkswagen no norte da Califórnia, e outro enquanto estava sentado numa banheira de hidromassagem. Chaum concebera os protocolos criptográficos que viabilizaram transações anónimas, detinha várias patentes de dinheiro digital impossível de rastrear e, através da sua empresa DigiCash, nos Países Baixos, estivera mais perto do que ninguém de o tornar realidade. Também dava a impressão de ser alguém dado a pseudónimos. Quando um repórter da *Wired*, anos antes, lhe perguntou inocentemente quantos anos tinha, Chaum disse: «Não é algo que partilhe com as pessoas». Quando lhe enviei um e-mail, respondeu-me: «Estou um pouco atrapalhado», e não voltou a responder.

Mas, quando telefonei a Stefan Brands, um criptógrafo holandês que trabalhara de perto com Chaum durante muitos anos, estava convicto de que o bitcoin não era de Chaum. «Ele não fará nada que não tenha, de facto, um anonimato robusto», afirmou Stefan. Assinalou também que Chaum tinha um doutoramento e «um currículo académico brilhante», ao passo que, no entender de Stefan, quem quer que criara o bitcoin era «provavelmente um engenheiro de segurança ao nível de licenciatura». Stefan considerava que o bitcoin revelava uma sofisticação notável no seu desenho, mas o que realmente o fascinava eram os sofisticados mecanismos de incentivos integrados no sistema. Perguntava-se se Gavin Andresen poderia ser Nakamoto.

—O Gavin negou —retorqui.

—Obviamente, quem quer que tenha feito isto fez um esforço deliberado para ocultar a sua identidade. Portanto, se for ele, não o admitirá assim, de mão beijada —respondeu Stefan.

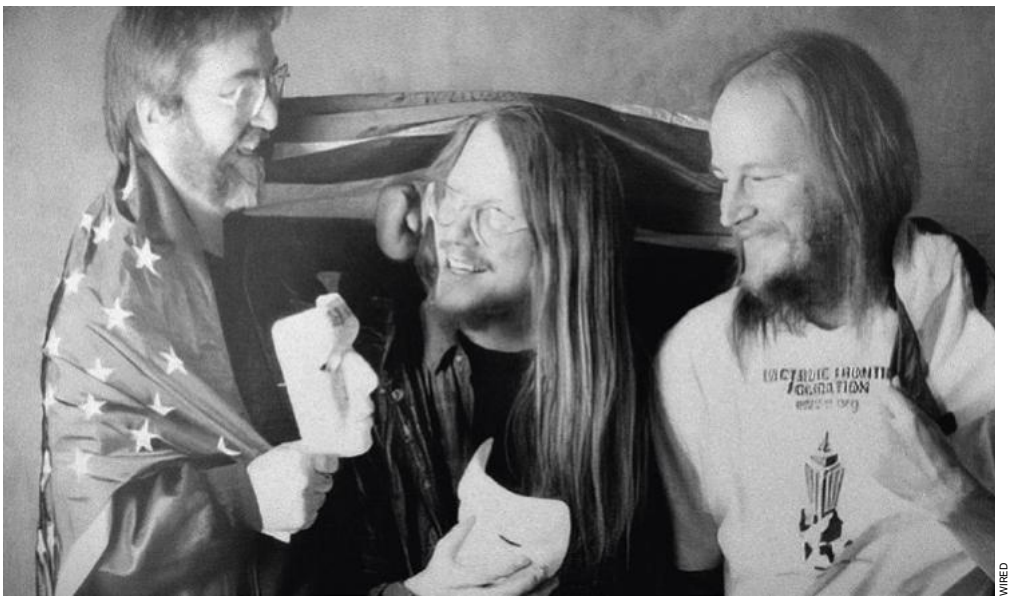
Stefan tinha algo claro: dado que o bitcoin exigia conhecimentos básicos de criptografia e parecia ser motivado pela ideia económica libertária da descentralização, o seu criador estava quase com total certeza ligado a um grupo radical ativo no início dos anos 90. Stefan não foi a única pessoa a apontar-me esse grupo que um antigo membro descreveu como «matemáticos com armas». ■

Matemáticos com pistolas

Os *cypherpunks* dos anos 90, como Tim May, Eric Hughes e Wei Dai, perceberam que a criptografia era uma arma mais poderosa do que qualquer arsenal militar. As suas «balas» eram funções de hash, assinaturas digitais e protocolos de consenso.

ISTOCK


progres
setProgre
laplaci
realForwardPlan = BBL
(double*)
realForwardKernelPlan
realBackwardPlan = BBLw_p
forwardLaplacianPlan = BBLw_plan_df
backwardLaplacianPlan = BBLw_p



WIRED

Esta fotografia icónica a preto e branco capta os três arquitetos intelectuais do *cypherpunk* que lançaram as bases do bitcoin: Timothy C. May, John Gilmore e Eric Hughes.

Num sábado de setembro de 1992, ao meio-dia, vinte revolucionários reuniram-se numa sala de estar em Oakland, Califórnia. A sala era de Eric Hughes, um estudante de pós-graduação em Matemática, de cabelo comprido, criado no seio dos mórmons, que apreciava casacos de camurça com franjas. Hughes acabara de comprar a casa e ainda não a tinha mobilado, pelo que as pessoas traziam almofadas para se sentarem.

Tim May, amigo de Hughes, dirigiu-se aos presentes. May era um físico alto e barbudo que, sendo um dos primeiros funcionários da Intel, resolvera um problema crítico que levou ao redesenho dos seus chips; com os ganhos das ações, pôde reformar-se aos trinta e quatro anos, o que lhe deu muito tempo para ler e escrever. Entre as inspirações que fervilhavam na sua cabeça havia duas obras de ficção. Uma era o romance de Ayn Rand *A Revolta de Atlas*, com a sua fantasia libertária e elitista de um enclave montanhoso chamado Galt's Gulch onde os intelectuais do mundo podiam ignorar o mundo aborrecido e a civilização medíocre. A outra era o romance de ficção científica de Vernor Vinge *True Names*, que contava a história de um grupo de *hackers* que tinha de operar, na realidade virtual, sob o disfarce de *nyms* (pseudónimos), contra uma variedade de adversários — incluindo o Verdadeiro Inimigo (o Governo) — para se proteger no mundo físico. May convenceu-se de que a tecnologia para concretizar estas visões já existia: o dinheiro digital anónimo idealizado por David Chaum e os avanços na criptografia que haviam tornado possível o seu sonho.

A CRIPTOGRAFIA SIMÉTRICA NÃO BASTAVA

Durante mais de dois mil anos, a criptografia, a ciência da escrita secreta, fora simétrica: a chave secreta utilizada para codificar uma mensagem era a mesma utilizada para a decifrar. Isto significava que a chave tinha de ser transmitida entre

DURANTE MAIS DE DOIS MIL ANOS, A CRIPTOGRAFIA, A CIÊNCIA DA ESCRITA SECRETA, FORA SIMÉTRICA

as partes em comunicação, o que representava ao mesmo tempo uma vulnerabilidade e uma limitação: a interceção da chave era um risco e remetente e destinatário tinham de se conhecer de antemão. Isto funcionara, ainda que de forma imperfeita, durante séculos, quando as partes eram, por exemplo, um imperador a comunicar com um dos seus comandantes. Mas, nos alvores da internet, tecnólogos visionários começaram a imaginar um mundo em que milhares de milhões de desconhecidos quereriam cifrar as suas comunicações online, e a criptografia simétrica deixaria de bastar. Na década de 1970, Whitfield Diffie e Martin Hellman, em Stanford, e Ralph Merkle, em Berkeley, fizeram separadamente uma descoberta notável: um procedimento para criar pares de chaves matematicamente ligadas. A primeira permaneceria oculta. A segunda, gerada a partir da primeira, mas sem possibilidade de lhe rastrear a origem, partilhar-se-ia abertamente. Qualquer pessoa poderia então cifrar uma mensagem com a chave pública, que só poderia ser decifrada com a chave privada. Pela primeira vez, desconhecidos poderiam comunicar em segurança. Também se podia inverter o processo. Um documento podia ser «assinado» (na realidade, codificado) com a chave privada e qualquer pessoa poderia comprovar a autoria verificando se era possível decifrá-lo com a chave pública. Assim nasceram as assinaturas digitais, ou a capacidade de atestar a identidade online.

CHUCK PAINTER/ STANFORD NEWS SERVICE

Martin Hellman (ao centro), Whitfield Diffie (à direita) e Ralph Merkle (à esquerda), vencedores do Prémio Turing de 2015 por terem revolucionado a criptografia moderna.

O GOVERNO DOS EUA EQUIPARAVA A CRIPTOGRAFIA A UMA ARMA DA MESMA CATEGORIA QUE OS TOMAHAWK

May sintetizou estas ideias num manifesto que, agora, na sala de Hughes, leu em voz alta perante uma multidão sentada no chão, de pernas cruzadas: «Um espectro assombra o mundo moderno: o espectro da criptoanarquia». May dizia-o num sentido positivo. Descreveu um futuro com pagamentos e mensagens em linha seguros e impossíveis de rastrear, imunes ao escrutínio ou à intervenção governamental. Imaginou os possíveis usos criminosos dessa tecnologia, a maioria dos quais pouco pareciam preocupá-lo, mas considerou a criptografia de chave pública tão revolucionária como fora a imprensa ao abalar as instituições medievais, ou o arame farpado ao transformar a fronteira americana. «Deste modo, a descoberta aparentemente menor de um ramo arcano da matemática há-de tornar-se a tesoura que corta o arame farpado suspenso sobre a propriedade intelectual».

ASC

Philip R. Zimmermann é o criador do Pretty Good Privacy, um pacote de *software* de cifragem de correio eletrónico.

PRETTY GOOD PRIVACY

Para lá desta utopia, que May chamou «Libertária no ciberespaço», a sua ação era também movida por uma ameaça iminente. Phil Zimmermann, um ex-ativista antinuclear barbudo, lançara o PGP, que significava Pretty Good Privacy («privacidade bastante boa») e era um programa gratuito que punha a criptografia de chave pública ao alcance de qualquer pessoa. Bastava instalar uma cópia no computador para cifrar os correios eletrónicos antes de os enviar. O Governo dos Estados Unidos, que equiparava a criptografia avançada a uma arma da mesma categoria dos mísseis de cruzeiro Tomahawk, ponderava avançar com uma ação judicial contra ele. May, Hughes e John Gilmore, um dos primeiros funcionários da Sun Microsystems que também pôde reformar-se antecipadamente e depois cofundou a Electronic Frontier Foundation, queriam pôr a criptografia nas mãos das massas. Depois de May ter lido o seu manifesto, uma das poucas participantes, uma mulher chamada Jude Milhon, conhecida como St. Jude, propôs que o grupo se chamasse *cypherpunks*. Concentrar-se-iam na ação concreta no mundo real: «Os *cypherpunks* escrevem código», nas palavras de Hughes.

UM GRUPO MUITO ECLÉTICO

Depois, passaram horas mergulhados no Jogo da Criptoanarquia, um exercício que May e Hughes tinham concebido para materializar protocolos matemáticos e abstrações como o anonimato e o dinheiro digital e provocar novas formas de pensar. A cada participante foi atribuído um papel: uns atuavam como traficantes de droga a tentar ocultar os seus movimentos, outros como agentes de contra-informação no encalço de infiltrados, e alguns como corretores de informação. May e Hughes distribuíram dinheiro falso que representava «dinheiro eletrónico» e envelopes vazios dentro de outros envelopes vazios para simular *remailers*, serviços que despojavam os correios eletrónicos de toda a informação identificativa e dificultavam a terceiros rastrear remetentes e destinatários. O dia foi caótico, com mensagens extraviadas e participantes a cometer erros com os selos, mas o grupo divertiu-se à grande.

Quase todos os *cypherpunks* eram homens, mas, fora isso, era um grupo bastante eclético. Um membro afirmava ser o príncipe do Liechtenstein. Outro aparecia às reuniões vestido de cabedal. Um *cypherpunk* chamado John Draper era mais conhecido como «Captain Crunch» porque, na década de 1970, descobrira um método para fazer chamadas telefónicas gratuitas de longa distância. A sua descoberta foi tão simples quanto engenhosa: os apitos incluídos nas caixas de cereais Cap'n Crunch emitiam uma frequência de 2600 hertz que permitia iludir o sistema de encaminhamento da AT&T. (Por isso, Draper cumpriu pena numa prisão federal). Juntar-se-iam também ao grupo o inventor do BitTorrent, Bram Cohen, o letrista dos Grateful Dead e cofundador da Electronic Frontier Foundation, John Perry Barlow, o criador do Signal, Moxie Marlinspike, e Julian Assange. Embora os *cypherpunks* da área da Baía de São Francisco se reunissem pessoalmente uma vez por mês, o seu principal ponto de encontro era uma lista de correio eletró-

SCALAR.USC.EDU

Bob Gudgel, Dee Pritchard e John Draper em 1971. Draper, «Captain Crunch», é o elo perdido entre os primeiros hackers e os fundadores do movimento *cypherpunk*.

A ADMINISTRAÇÃO CLINTON PRESSIONOU OS FABRICANTES PARA QUE EQUIPASSEM OS SEUS PRODUTOS COM O CLIPPER CHIP

nico que qualquer pessoa podia subscrever. Muitos participantes usavam os seus nomes reais, mas havia também habituais muito respeitados conhecidos apenas por pseudónimos como Black Unicorn e Pr0duct Cypher. Usar pseudónimos para publicar na lista com múltiplas identidades tornou-se um jogo para alguns e uma ferramenta para outros. A internet continuava a ser uma fronteira inexplorada, aberta à descoberta dos novos tipos de relações com desconhecidos que possibilitava. Os pseudónimos representavam, além disso, uma ideia: ser julgado pelas ideias e não pelas credenciais.

Os *cypherpunks* estavam longe de ser pessoas que olhavam para a web embrionária e pensavam «bah». Pelo contrário, viam uma enorme oportunidade e partilhavam quer uma acentuada previsão de como um mundo digitalmente interligado colocaria em risco a privacidade pessoal, quer a convicção de que só a criptografia a poderia salvaguardar. Isto era relevante tanto para os defensores de uma intervenção estatal mínima, que só queriam ser deixados em paz, como para ativistas de direitos civis preocupados com a segurança de dissidentes em países autocráticos, e até para pessoas comuns que simplesmente queriam escrever correios eletrónicos sem olhares indiscretos. A criptografia, como Hughes gostava de dizer, era «a consequência matemática de pressupostos paranoicos». (O próprio Hughes, segundo um *cypherpunk* chamado Jim McCoy, «mantinha o carro imaculadamente limpo, para que, se fosse mandado parar, a polícia não tivesse pretexto para o registar»).

BIG BROTHER INSIDE

Dado que um princípio fundamental dos *cypherpunks* sustentava que «o código é discurso», qualquer restrição a ele era entendida como uma violação da Primeira Emenda. O Governo queria criminalizar um programa informático? Adam Back punha-se a vender T-shirts estampadas com uma fórmula de encriptação proibida para exportação e qualquer *cypherpunk* respeitável podia envergá-la alegremente ao embarcar num voo internacional. Outros *cypherpunks*, pelo mesmo motivo, tatuaram os algoritmos proibidos. Quando um grande júri ponderava acusar Zimmermann, o criador do PGP, os *cypherpunks* ajudaram a difundir o seu *software* exportando versões impressas e digitais, para que se espalhasse no estrangeiro a tal ponto que o Governo dos Estados Unidos ficasse sem meios de o travar. Depois de a Administração Clinton ter pressionado, em 1993, os fabricantes de telefones a equiparem os seus produtos com o Clipper Chip, uma porta traseira para permitir a vigilância governamental, os *cypherpunks* entravam nas lojas de eletrónica e colavam autocolantes com a legenda *Big Brother Inside* («Grande Irmão no interior») nos aparelhos comprometidos. Para certos *cypherpunks*, a defesa da privacidade respondia também a inquietações mais pessoais. Gene Hoffman, antigo executivo da PGP, disse-me que o grupo não estava unido unicamente por ideais abstratos.

Os direitos de privacidade são «algo de que é difícil cuidar. Muita gente do movimento *cypherpunk* desejava proteger certos aspetos da sua vida privada. A confluência entre *cypherpunks* e praticantes de BDSM era notavelmente elevada», confidenciou-me Hoffman. Quando mencionei isto a um *cypherpunk* chamado Doug Barnes, de vinte e dois anos, a quem Neal Stephenson atribuiu a invenção do termo *meatspace*, ele discordou: «A maioria dos *cypherpunks* que conheço é um pouco excessiva na partilha. Havia muita gente notoriamente poliamorosa».

LIBERTÁRIA NO CIBERESPAÇO

A combinação de revolução e tecnologia por vezes produzia um composto instável; assim, entre os *cypherpunks* havia uma fação radical que se autodenominava criptoanarquista. Eram mais radicais do que os libertários e acreditavam que a tecnologia podia eliminar a necessidade de qualquer Governo. Tim May imaginou um mercado de informação anónimo, a que chamou BlackNet, onde se podiam vender ilicitamente segredos corporativos e incitar à partilha de informação privilegiada. Outros *cypherpunks* falavam com esperança do uso de dinheiro digital para fugir aos impostos. Um chamado Jim Bell escreveu um ensaio intitulado *Política de Assassinato*, no qual propunha um sítio na internet onde pessoas que usassem dinheiro digital anónimo pudessem financiar uma grande recompensa para quem adivinhasse corretamente a data da morte de um determinado funcionário público; isso, presumivelmente, incentivaria outra pessoa a «adivinhar» uma data e a tentar fazer com que a morte ocorresse nesse momento, enquanto, em teoria, os financiadores originais ficariam livres de responsabilidade penal. Bell viria a passar anos numa prisão federal, primeiro por evasão fiscal e depois por perseguir e assediar agentes da autoridade tributária. Phil Zimmermann, um homem afável que enfrentava a ameaça de um processo penal e usava fato todos os dias nos últimos três anos para projetar uma imagem respeitável perante a opinião pública, ficou em choque quando, numa reunião de *cypherpunk* organizada pela PGP, um membro que se fazia chamar Lucky Green meteu a mão no saco de lona e anunciou: «O Cypherpunks Gun Club vai praticar tiro no próximo sábado e estão todos convidados». De seguida, retirou uma espingarda de assalto AR-15 com um carregador. «Os escritórios da PGP ficavam num edifício bancário», recordou Phil.

TRAVIS GOODSPEED

Chip VLSI de 1993. Representa um dos momentos mais cruciais na guerra entre a privacidade individual e a vigilância.

Alguns *cypherpunks* eram bastante dogmáticos e tendiam a manter discussões intermináveis que irritavam tanto criptógrafos profissionais como programadores

Os ataques às Torres Gémeas desencadearam uma expansão do poder governamental de vigilância que viria a validar muitas das previsões mais sombrias do movimento *cypherpunk*.

e *hackers* no ativo. «Na altura dizia-se: "Os *cypherpunks* escrevem código" — recorda Jon Callas, que trabalhou para a PGP e, mais tarde, para a Apple, e que assistiu a muitas dessas primeiras reuniões —. E eu pensava: "Estou demasiado ocupado a programar para ser um *cypherpunk*"». Quando Bram Cohen organizou mais tarde uma convenção de *hackers*, anunciou que excluiria explicitamente temas como a «criptografia matemática sem aplicação prática» e o «debate político sobre o depósito de chaves». Ainda assim, a sensação de estar a escrever um capítulo decisivo da história era inescapável. Ser um *cypherpunk* era sentir a emoção dos pioneiros. Estava-se a liderar a marcha para um futuro ousado, movida por uma causa justa. Devido à ênfase nos pseudónimos, na descentralização e na economia libertária, era evidente o ar *cypherpunk* que Satoshi Nakamoto exalava. Mas a principal razão pela qual Stefan Brands e outros me tinham apontado os tecnólogos rebeldes era o facto de estes se referirem constantemente à necessidade do dinheiro digital. Muitos *cypherpunks* viam-no como o seu objetivo final, a pedra angular da «Libertária no ciberespaço» de May. Enquanto os números de série e os banqueiros tornavam rastreável o dinheiro antigo, o dinheiro do futuro seria anónimo. Enquanto o dinheiro antigo estava ligado à política e aos Governos, o dinheiro do futuro seria independente. A moeda digital privada tornou-se uma obsessão para os *cypherpunks* mais radicais, porque representava uma ameaça para os Governos, com o seu controlo exclusivo sobre a criação de moeda e a sua capacidade de impor impostos.

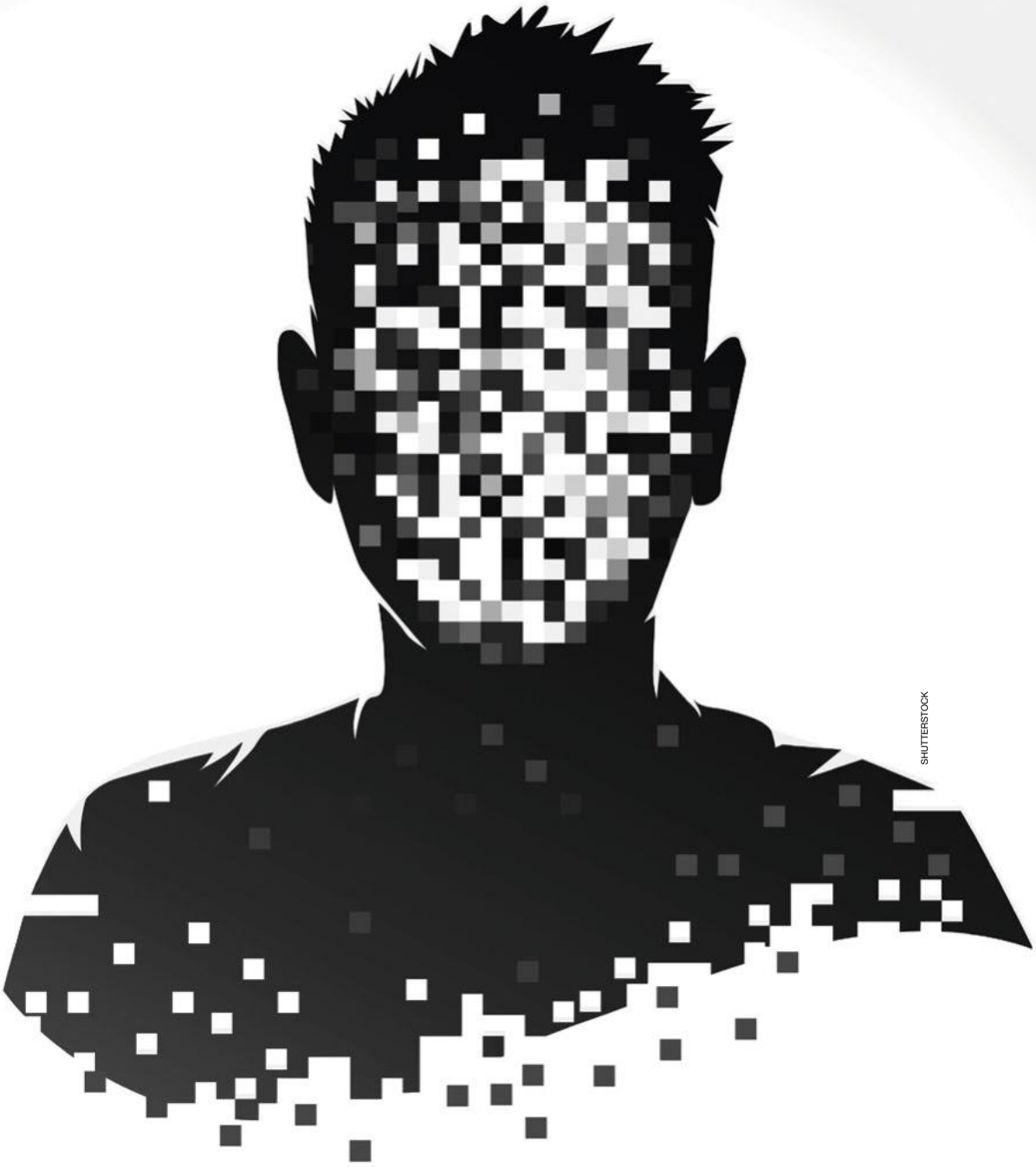
UM LONGO CAMINHO A PERCORRER

O movimento *cypherpunk* mantinha uma relação ambivalente com David Chaum. O seu artigo de 1982 «Blind Signatures for Untraceable Payments», que lançou as bases informáticas do dinheiro digital, roçava o sagrado. Eric Hughes trabalhou na DigiCash durante algum tempo. Contudo, muitos *cypherpunks*

ENQUANTO OS NÚMEROS DE SÉRIE E OS BANQUEIROS TORNAVAM RASTREÁVEL O DINHEIRO ANTIGO, O DINHEIRO DO FUTURO SERIA ANÓNIMO

indignaram-se com a orientação comercial de Chaum, que não hesitou em fazer valer as suas patentes. E o dinheiro de Chaum, visto pela lente dos *cypherpunks*, apresentava um defeito fundamental: necessitava de uma entidade emissora para criar a moeda e evitar a dupla despesa mediante a validação das transações. Chaum convenceu o Mark Twain Bank, de St. Louis, Missouri, a prestar esse serviço nos Estados Unidos. Mas, para os *cypherpunks*, uma entidade emissora representava um terceiro de confiança, um ponto único de falha, um alvo vulnerável. O Governo poderia encerrá-la por receio de fuga aos impostos; criminosos poderiam fazer mal ao detentor das chaves de qualquer Fort Knox virtual. «Recordemos o desejo de Nero de que Roma tivesse um só pescoço que pudesse cortar — escreveu muito mais tarde um *cypherpunks* chamado James Donald —. Se lhes oferecermos esse pescoço, cortá-lo-ão». No final, revelou-se que o dinheiro digital era um sonho que os *cypherpunks* nunca alcançaram. No final dos anos 90, os primeiros começaram a abandonar o grupo. Alguns aborreceram-se. Outros ocuparam-se com os empregos e a família. Outros cansaram-se da avalanche de *spam* e do caos geral que inevitavelmente afligia uma lista de correio povoada por anarquistas que denunciavam o mais pequeno esforço de moderação como «censura». O grupo dispersou-se ainda mais depois de 11 de Setembro, quando as diferenças políticas internas, até então mascaradas por uma crença partilhada na privacidade possibilitada pela criptografia, se tornaram mais evidentes.

Os *cypherpunks* continuavam a reunir-se para celebrar a caducidade de patentes, como naquela tarde de sábado de julho de 2005, numa esplanada em Portola Valley, Califórnia, onde brindaram pelo fim da patente de dezassete anos que Chaum detinha sobre as «assinaturas cegas», um método criptográfico que permite verificar transações mantendo o anonimato. E nesse ano houve uma explosão gloriosa, ainda que efémera, de energia *cypherpunks* quando um grupo tentou criar um paraíso de dados extraterritorial numa plataforma antiaérea fustigada pelo vento no Mar do Norte. No entanto, do final dos anos 90 até 2008, viveu-se uma idade negra do dinheiro digital, causada em parte pela repressão ao dinheiro alternativo durante a guerra ao terrorismo após 11 de Setembro; o mais bem-sucedido desses sistemas, o e-gold, acabou a enfrentar apreensões de ativos, ações cíveis e acusações criminais. Alguns dos *cypherpunks* mais empenhados começaram a perder a esperança. «O Tim May sucumbiu a um mau humor terminal — escreveu James Donald na agora degradada lista de cypherpunks — ao descobrir que a transcendência criptográfica não chegará tão cedo». Outros, entre eles o próprio Donald, mantinham o otimismo: «Temos um longo caminho a percorrer, mas estamos a fazê-lo». Um pequeno núcleo de *cypherpunks* nunca abandonou o sonho do dinheiro eletrónico. E, à medida que aprofundava a história do movimento, continuava a ouvir os mesmos nomes. ■



SHUTTERSTOCK

Wei

Wei Dai era um criptógrafo aficionado que criara a Crypto++, uma biblioteca de ferramentas de software utilizada pelo bitcoin, e Dai ainda a mantinha; mas a principal razão por que algumas pessoas pensavam que poderia ser Nakamoto era um conceito sobre o qual Dai escrevera em 1998.

B-money, como lhe chamou, combinava várias ideias que viriam a surgir no bitcoin: entre elas, uma rede entre pares que mantinha coletivamente um registo comum de todas as transações; um mecanismo de criação de moeda baseado na resolução de problemas computacionais; e o uso de criptografia de chave pública para proteger as identidades dos utilizadores. E o b-money de Dai, tal como o Hashcash de Back, contava-se entre o punhado de referências que Nakamoto mencionou explicitamente no final do livro branco do bitcoin.

ASC

Wei Dai é um dos precursores mais diretos e influentes da criação do bitcoin.

UM CRIPTÓGRAFO PROFISSIONAL

Dai era também, à semelhança de Nakamoto, uma figura enigmática. Formara-se na Universidade de Washington no final da década de 1990, mas pouco mais se sabia sobre ele. Era impossível encontrar uma única fotografia sua na internet. Um perfil tão reservado exigia, sem dúvida, aproximar-se com a máxima cautela e delicadeza.

—É o Satoshi Nakamoto? —disparei-lhe por e-mail naquele verão de 2011.

—Eu não sou o Satoshi —respondeu Wei.

Muito antes de o bitcoin aparecer, Wei, após anos dedicados à criptografia, concluíra que esta não seria tão determinante para o futuro como imaginara inicialmente e virara-se mais para a filosofia, explicou-me. Agora dedicava grande parte do seu tempo a participar no LessWrong, um blogue com grande audiência entre os futuristas de Silicon Valley, centrado em «aperfeiçoar a arte da racionalidade humana».

«Não creio que seja alguém do meu círculo —prosseguiu Wei, referindo-se a Nakamoto—, já que, ao que parece, desenvolveu o bitcoin de forma independente e desconhecia o meu artigo sobre b-money até que Adam Back lho mencionou. Concordo com a teoria de Gwern de que provavelmente não é um criptógrafo profissional nem um académico. Pressinto que deverá ser um estudante ou um programador solitário. (Eu próprio era estudante quando comecei a trabalhar na Crypto++ e escrevi sobre o b-money)».

Wei facultou-me alguns e-mails que Nakamoto lhe enviara. No primeiro, de agosto de 2008, Nakamoto dizia que queria citar o b-money no livro branco e precisava de saber quando Wei o tinha publicado. O segundo, do início de 2009, continha uma ligação para o software do bitcoin que Nakamoto partilhou com Wei no dia seguinte ao seu lançamento. «Creio que cumpre quase todos os objetivos que te propuseste resolver no teu artigo sobre o b-money», escreveu Nakamoto. ■

Boom boom

Um dos desafios mais sérios que o bitcoin enfrenta é a chegada dos computadores quânticos, capazes de quebrar a criptografia de chave pública que protege todas as transações e *wallets*.

SHUTTERSTOCK

Outra pessoa de interesse recorrente entre os Bitcoin Talkers era Nick Szabo, e foi a ele que me dirigi de seguida. Szabo era apenas um pouco menos solitário do que Wei, com um historial profissional em grande medida invisível. Mais tarde diria que acreditava na «segurança através do anonimato».

Szabo sentiu-se naturalmente atraído pelos *cypherpunks*, com o seu compromisso com a ação no mundo real. A criptografia permitiu-lhe aquilo a que chamou «realpolitik libertária: engenharia prática em vez de masturbação intelectual». Em abril de 1993, quando vivia no Oregon (onde trabalhara para o fabricante de computadores Sequent), escreveu um folheto sobre «como proteger a tua privacidade eletrónica» e distribuiu-o numa reunião de libertários em Portland. Também participou num fórum televisivo na área da Baía de São Francisco para discutir o seu plano de abandonar a AT&T em favor de outro operador, como protesto contra o apoio do gigante das telecomunicações ao Clipper Chip, e ofereceu 200 dólares adiantados a quem fosse o primeiro a produzir autocolantes de alta qualidade com a mensagem «Big Brother dentro». Propôs estratégias para contrariar a tecnologia emergente de reconhecimento facial através da «encriptação» da própria imagem, recomendando evitar disfarces demasiado evidentes (balaclavas, óculos de sol à noite) e preferir chapéus, penteados e técnicas de maquilhagem.

A LUA É UMA AMANTE CRUEL

Alto, com corpo algo flácido e um evidente desinteresse pela moda, Szabo crescera no estado de Washington e herdara do pai, Julius, um profundo repúdio pelo socialismo. Os pais de Julius, naturais da Hungria, tinham visto os comunistas confiscar-lhes a quinta. Durante os seus anos universitários nesse país, Julius participou na insurreição de 1956 contra o governo fantoche dos soviéticos e, mais tarde, fugiu para os Estados Unidos, onde desenvolveu carreira como cientista especializado em botânica. A mãe de Nick, Mary, também tinha uma inclinação natural para a matemática: trabalhava como contabilista e costumava levar para casa um Apple II do escritório para que os filhos pudessem usá-lo.

Quando Szabo era adolescente, o seu romance de ficção científica favorito era ***A Lua é uma amante cruel***, de Robert Heinlein, que fundia as suas duas grandes paixões: a filosofia libertária e o espaço. Enquanto estudava Informática na Universidade de Washington, uma década antes de Wei, conseguiu um estágio no Laboratório de Propulsão a Jato, em Pasadena, onde trabalhou na Rede do Espaço Profundo, programando comunicações para projetos como a ***Voyager***, a ***Galileo*** e a *Magellan*. Essa experiência transformou a sua vida. Ao observar a dinâmica dos projetos mais modestos que se desenvolviam ali e no vizinho Caltech — do *Mars Rover* às redes neuronais —, desiludiu-se com o programa espacial norte-ameri-

SZABO CRESCERA NO ESTADO DE WASHINGTON E HERDARA UM PROFUNDO REPÚDIO PELO SOCIALISMO

cano, que não estava orientado para a colonização do espaço a longo prazo, mas focado em erguer estações e vaivéns espaciais em busca de títulos de jornal. Passou a encarar esses «sacramentos do culto dos astronautas» como uma afronta de curto prazo: espetáculos mediáticos impostos aos contribuintes por uma burocracia inchada da NASA, repleta de «artistas das apresentações». Szabo conseguia intelectualizar ao ponto de encarar as suas próprias sensações corporais como se fossem dados recolhidos por instrumentos científicos externos. Até a sua excitação sexual se tornou uma métrica. Das mais de cem mulheres a quem tinha pedido para sair: «Em mais de metade das ocasiões, tive uma ereção». A canção *Dust in the Wind*, dos Kansas, deprimia-o: «Alguns estilos musicais podem ter um impacto muito forte nas minhas emoções, na minha experiência».

Talvez os infortúnios da juventude (no secundário fora alvo de bullying até começar a ripostar) o tivessem tornado combativo. Não se coibia de atacar quem esgrimisse argumentos que não respeitava, dizendo a um: «Obrigado pelas memórias, avô»; a outro: «Presumia que eras medianamente inteligente»; e a um terceiro: «Aqui tens uma proposta de reforma: "Acorda de uma vez para o mundo real lá fora"». Os seus antagonistas sugeriam, de várias formas, que precisava de lítio ou que estava «desesperadamente sozinho», ou perguntavam: «Alguém abusou sexualmente de ti quando eras criança?».

Pouco depois de se inscrever na lista dos *cypherpunks*, Szabo mudou-se do Oregon para a área da Baía de São Francisco, para estar perto das reuniões presenciais do grupo. Embora as interações online lhe fossem pelo menos tão estimulantes quanto as presenciais, deleitava-se com a sua nova vida embriagante. Numa noite de agosto, já depois da meia-noite, conduziu para sul de Los Gatos, afastando-se do brilho urbano, até aos sopés das montanhas de Santa Cruz, onde montou uma

JACK AND DEBORAH J. WARNER/ SMITHSONIAN INSTITUTION

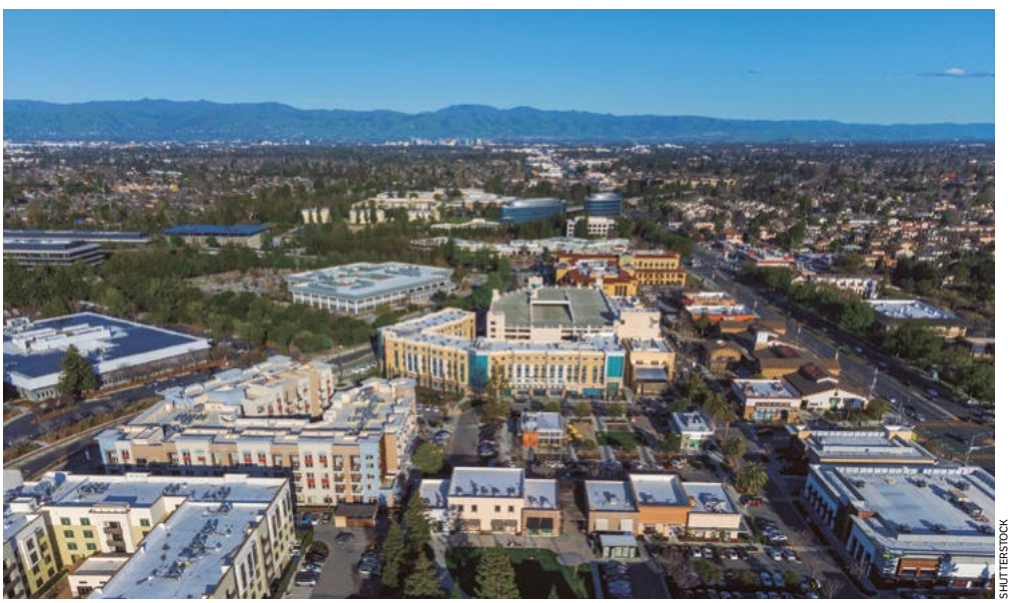
O Apple II colocou capacidades de processamento nas mãos de entusiastas, *hackers* e visionários, que o usariam para experimentar com criptografia, redes *peer-to-peer* e sistemas descentralizados.

espreguiçadeira, se cobriu com mantas e camisolas e ficou a contemplar o límpido céu noturno. Nas duas horas seguintes, fantasiou com a extração de recursos em cometas, colónias espaciais e «cérebros do tamanho de Júpiter», enquanto observava dezenas de meteoros deslumbrantes a sulcar o firmamento, incluindo «uma bola de fogo espetacular que explodiu no firmamento». Dois dias depois, assistiu a uma reunião de *cypherpunks* com todas as figuras de proa: John Gilmore, Eric Hughes, Tim May, Whit Diffie (co-inventor da criptografia de chave pública). No encontro, Romana Machado, programadora de *software* para o dispositivo portátil Newton, da Apple, e «modelo de glamour» conhecida como Cypherella (Playboy, novembro de 1985), apresentou o Stego, um *software* livre que criara para ocultar mensagens dentro de imagens.

ÊXTASE DO FUTURO

Machado era também membro de um grupo chamado os extropianos, com o qual Szabo viria a envolver-se profundamente. Dedicavam-se ao transumanismo, ou seja, à extensão extrema da vida, e abrangiam desde as smart drugs à inteligência artificial e à Singularidade, o momento futuro em que as consciências humanas poderiam ser transferidas para o domínio digital. Szabo chamava-lhe «êxtase futuro».

O extropianismo defendia a expansão em todos os sentidos. A T-shirt extropiana ostentava o lema: «Em frente, Para cima, Para fora» e vários membros do grupo adotaram alcunhas otimistas e tecnológicas como Jay Prime Positive, Tom Morrow, Max More e David Victor de Transcend. Tim May, como ele lhe chamava, era Klaus! von Future Prime, e Szabo por vezes assinava como Boom Boom ou Boom Boom von Past Primeval.



SHUTTERSTOCK

Vista aérea de Cupertino e da baía de São Francisco. Foi o epicentro onde convergiram todos os elementos que tornaram possível o bitcoin.

OS EXTROPIANOS DEDICAVAM-SE AO TRANSUMANISMO E À EXTENSÃO EXTREMA DA VIDA

Os extropianos fundiam a positividade do futuro com uma alergia libertária à restrição, fosse ela imposta pelo Estado, pela gravidade ou pelo envelhecimento. Um extropiano típico lera montanhas de ficção científica e era um ateu que fizera da tecnologia a sua religião. Embora o grupo partilhasse muitos membros com os *cypherpunks*, os extropianos eram mais hedonistas. Para quê viver mais tempo se não for para desfrutar? «Tinham drogas melhores, sem dúvida — recordava Doug Barnes, que pertencia a ambos os grupos —, e além disso eram mais bonitos e estavam em melhor forma». A oportunidade de os geeks saírem com mulheres bonitas «fazia parte da nossa marca», corrobora Tom «Morrow» Bell, um dos cofundadores do grupo.

UNIVERSIDAD DE OXFORD

Nick Bostrom, filósofo sueco e diretor do Future of Humanity Institute, em Oxford.

MEMBROS NOTÁVEIS

A lista de interesses do grupo era um programa de estudos para os futuros líderes de Silicon Valley do século XXI: extensão da vida, colonização espacial, ensino doméstico, *biohacking*, upload de consciência, IA, autossoberania, cidades marítimas flutuantes, dinheiro digital, oposição ao Estado, transumanismo, pluralismo jurídico, mercados de previsão, nómadas digitais (o seu termo era tecno-nómadas) e memética, entre outras coisas.

Um número notável de membros foi — ou viria a ser — influente. Nick Bostrom tornou-se o filósofo de Oxford da chamada hipótese da simulação, a crença, improvavelmente difundida entre Elon Musk e os seus pares, de que todos vivemos num videojogo. Robin Hanson foi pioneiro dos mercados de previsão modernos. K. Eric Drexler foi o principal defensor da nanotecnologia. Hans Moravec, especialista em robótica, foi o visionário da ideia de transferir a consciência humana para sistemas digitais. Bart Kosko foi um destacado divulgador da lógica difusa. Eliezer Yudkowsky tornar-se-ia o mais famoso pessimista da IA, bem como o líder do movimento racionalista, obcecado com estatística e teoria dos jogos.

À MEDIDA QUE SZABO MERGULHAVA NOS CÍRCULOS EXTROPIANOS E *CYPHERPUNKS*, O SEU CARÁTER PARECIA TRANSFORMAR-SE

Quando Szabo descobriu os extropianos, encontrou pessoas que discutiam a sério, como engenheiros a analisar projetos futuros viáveis, conceitos que ele anteriormente descartara como fantasias saídas das histórias de ficção científica de que tanto gostava. Criónica. Digitalização da consciência. Nanotecnologia. Nos dias em que não tinha de acordar cedo para ir trabalhar, gostava de ficar na cama, nesse estado entre o sono e a vigília, a fantasiar e a desenvolver as suas múltiplas ideias.

ADVERSÁRIOS DA MORTE

A visão do programador informático do corpo como um sistema suscetível de otimização fascinava-o. Inscreveu-se na Life Extension Foundation, seguiu um regime para perder peso, analisava a urina para controlar os níveis de cetonas, reduziu o consumo de gorduras a favor de alimentos cozidos ou crus, manteve-se fiel à Coca-Cola light e tomava suplementos vitamínicos e minerais, um nootrópico para a clareza mental chamado Deep Thought e o supressor de apetite Acutrim. Duas vezes por semana nadava um quilómetro e meio. Em seis meses, reduziu o peso de 108 para 82 quilos e, a partir de então, manteve uma dieta assente principalmente em saladas.

Era um homem jovem e solteiro, com muita vontade de conhecer mulheres, e parte desse regime extremo devia-se seguramente à vaidade. Mas também era partidário da aposta de Pascal. A versão original, concebida pelo filósofo francês do século XVII Blaise Pascal, colocava uma aposta religiosa: perante a possibilidade de que Deus existisse, fazia mais sentido viver como se a sua existência fosse certa, maximizando assim as probabilidades de alcançar a salvação eterna. O equivalente extropiano sustentava: deves esforçar-te por viver o máximo de tempo possível e da forma mais saudável possível para aumentares as probabilidades de que a reanimação criogénica ou a transferência mental estejam disponíveis antes de morreres.

Szabo também se entusiasmou com as visões mais ambiciosas dos extropianos. Interessou-se pela nanotecnologia e pelas definições da morte (os extropianos por vezes autodenominavam-se adversários da morte). Atraía-o a ideia de que, uma vez sendo possível a transferência de consciência e deixando o impulso sexual de ser necessário para a propagação da espécie, se pudesse redesenhar a sua finalidade: «Se experimentasse um orgasmo no dia de pagamento, em vez de receber apenas uma folha aborrecida com números abstratos, provavelmente estaria mais motivado para ganhar dinheiro».

Mudou-se para uma casa de tom acastanhado e pé-direito alto em Cupertino, residência de uma comunidade intencional chamada Nexus-Lite. Entre os seus quatro companheiros de casa estava Romana Machado, e por vezes organizavam festas, como um jantar partilhado, num sábado de março de 1994, a que chamaram Extropaganza. Alguns convidados, à chegada, cumprimentavam-se com o

aperto de mão extropiano idealizado pelo cofundador do grupo, Max More: depois de entrelaçar os dedos, lançavam-nos para cima. Szabo tinha uma personalidade erudita e os seus companheiros de casa partilhavam ideias políticas semelhantes: Machado circulava pela festa com um traje de dominatrix, vestida como «o Estado» e a segurar pela trela o namorado, Geoff Dale, que ia vestido como «o Contribuinte». A *play list* extropiana ia desde a certeira *Forever Young*, dos Alphaville, à música eletrónica futurista dos The Orb.

CONTRATOS INTELIGENTES

À medida que Szabo mergulhava nos círculos extropianos e *cypherpunks*, o seu caráter parecia transformar-se. Ficavam para trás os desvarios furiosos do ativista espacial combativo. Tornou-se mais cortês e empático. Embora mantivesse uma disposição tranquila e reservada, com pouco contacto visual, os extropianos que coabitavam com ele descreviam-no como «agradável» e «afável», além de reconhecerem que irradiava inteligência. O domínio de uma gama tão surpreendente de temas levou alguns extropianos que não o tinham conhecido pessoalmente a especularem que o seu nome era, na verdade, o pseudónimo de um coletivo.

Apesar do seu libertarismo, Szabo evitava o egoísmo de Ayn Rand e considerava-se um «comunitarista», alguém a quem não importava fazer voluntariado por um bem maior, em contraste com o próprio irmão, a quem chamava «um aproveitador: absorto nos seus próprios desejos e ambições». Em 1993, Szabo afastara-se da política do Partido Libertário e inclinara-se para a ação individualista, «a

MATT GREEN/ PRINCETON UNIVERSITY

Reunião de alguns dos pioneiros do bitcoin, onde surge Nick Szabo (assinalado com um X), cuja presença alimentou as especulações sobre a sua possível identidade como Nakamoto.

construir a minha própria liberdade num mundo não livre». Por essa altura, Szabo interessou-se especialmente pelos «contratos inteligentes», como lhes chamava, baseados em criptografia: um código informático autoexecutável que podia, à semelhança de uma máquina de venda automática que entrega uma barra de chocolate a troco de uma moeda, funcionar sem interferência humana. O seu outro grande interesse era o dinheiro digital e a sua capacidade de apoiar os mercados online. Durante um breve período, trabalhou, tal como Eric Hughes, para a DigiCash de Chaum, nos Países Baixos.

RESOLUÇÃO DE UM QUEBRA-CABEÇAS COMPUTACIONAL

Foi na lib-tech, uma lista de correio privada criada por Szabo para se focar em tecnologias que promovem a liberdade, que Wei Dai escreveu pela primeira vez sobre o b-money, em 1998. Foi também ali, nesse mesmo ano, que Szabo apresentou a sua própria ideia do bit gold, que descreveu como «dinheiro digital sem necessidade de confiança». Tal como o b-money, o bit gold antecipava o bitcoin: era motivado pelo desejo de eliminar o chamado terceiro de confiança e replicar no ciberespaço a «escassez infalsificável» dos metais preciosos. À semelhança dos bitcoins, o bit gold seria cunhado mediante a resolução de um quebra-cabeças computacional, a solução seria confirmada por uma rede de computadores e cada solução estaria ligada criptograficamente tanto ao seu predecessor como ao seu sucessor. Tal como os bitcoins, o bit gold teria «mineiros».

Após o anúncio do bitcoin por parte de Nakamoto, em outubro de 2008, Szabo mostrou uma cautela subtil ao estabelecer a ligação, republicando, em dezembro, uma entrada de blogue de 2005 sobre o bit gold, sem mencionar o recente aparecimento dessa proposta tão semelhante. A primeira vez que Szabo se referiu ao bitcoin pelo nome, em maio do ano seguinte, observou que funcionava «de maneira muito semelhante» ao bit gold. Mais tarde viria a descrever o bitcoin como «uma implementação da ideia de bit gold».

É O SENHOR SATOSHI NAKAMOTO?

Quando Gwern Branwen sugeriu que não havia nada tecnologicamente novo no bitcoin, Szabo saiu em sua defesa, afirmando que «não [é] uma mera lista de características criptográficas, mas um sistema extremamente complexo de matemática e protocolos interativos que perseguia um objetivo muito impopular. Sem dúvida, o principal obstáculo a que algo como o bitcoin tivesse surgido antes era o porquê: praticamente todos os que ouviram falar do conceito geral consideraram-no uma ideia péssima. Os únicos que nos entusiasmámos com a ideia fomos eu, o Wei Dai e o Hal Finney [outro *cypherpunk*], pelo menos o suficiente (ou, no caso do Dai, com o seu conceito relacionado) para a desenvolver até ao aparecimento do Nakamoto

TAL COMO OS BITCOINS, O BIT GOLD SERIA CUNHADO MEDIANTE A RESOLUÇÃO DE UM QUEBRA-CABEÇAS COMPUTACIONAL

DAVID CHAUM

A equipa técnica original da DigiCash (1994) posa com os computadores em que implementou o primeiro sistema funcional de dinheiro digital com privacidade criptográfica.

(pressupondo que o Nakamoto não fosse na realidade o Finney ou o Dai). O grupo onde confluem peritos em criptografia e libertários capazes de se entusiasmar com uma proposta tão ao estilo febre do ouro é, por si só, extremamente reduzido».

No verão de 2011, quando lhe perguntei sobre a sua experiência com o bitcoin, Nick respondeu: «Não o usei. Não há nada à venda que eu queira comprar, um problema comum quando se arranca com uma moeda. Li o documento, algumas descrições online e parte do código-fonte».

Tal como com Wei, experimentei a abordagem direta com Nick. Ainda não excluía a possibilidade de que Nakamoto estivesse frustrado por ninguém se ter dado ao trabalho de simplesmente lhe perguntar.

— É o senhor Satoshi Nakamoto?

— Não — respondeu Nick.

Quando lhe perguntei sobre o seu comentário «pressupondo que o Nakamoto não seja na realidade o Finney ou o Dai», respondeu:

— São apenas possibilidades lógicas.

Acrescentou que sempre achara a descrição do b-money, feita por Wei, «irremediavelmente vaga».

Mencionei-lhe outros candidatos a ser Nakamoto.

— Não vou continuar a especular sobre isso — respondeu Nick.

Creio que fez uma grande contribuição para o mundo e, em contrapartida, quero respeitar a sua privacidade.

No entanto, Nick mencionou Finney. Era «muito incapacitado, como Stephen Hawking», advertiu Nick, mas achou que eu devia tentar entrevistá-lo. Nick não foi a primeira pessoa a sugerir que eu contactasse Finney. Mike Hearn dissera que seria bom para «conhecimentos profundos». E Nick descreveu-me Finney como «a primeira pessoa a implementar este tipo de plano». ■

Uma noite de convívio sob pseudónimo

Na primeira conferência mundial de Bitcoin, a noite de convívio sob pseudónimo reuniu alguns pioneiros de todo o mundo em torno de um dinheiro invisível que mal começava a despertar curiosidade e ceticismo.

SHUTTERSTOCK

Não estava mais perto de encontrar uma resposta quando, semanas após a minha correspondência com Nick, assisti à primeira conferência mundial de bitcoin. Só conseguir uma entrada revelou-se complicado.

Custava 26 dólares e tinha de ser paga em bitcoin. Decidi comprar 200 dólares em bitcoin. Parecia-me uma loucura desembolsar catorze dólares por unidade por algo intangível, invisível e inútil para qualquer necessidade real.

Decidido a não repetir o erro do pobre Stefan Thomas, criei primeiro uma conta na Mt. Gox, a plataforma de câmbio de bitcoin, sediada em Tóquio, que todos consideravam a mais fiável. Depois, registei-me na Dwolla, um processador de pagamentos do Iowa que tinha de verificar a minha conta bancária antes de aceitar o meu dinheiro. Esse processo levou quatro dias. Depois transferi dinheiro do meu banco para a Dwolla, operação que demorou mais um dia a concluir-se. Subsequentemente, tive de mover o dinheiro da Dwolla para a Tradehill, uma casa de câmbio em São Francisco, para converter os meus dólares em catorze bitcoins. Por fim, retirei quatro deles da Tradehill para um endereço controlado pelo meu computador e enviei cerca de dois terços ao organizador da conferência (o preço de um bitcoin já tinha caído para menos de 11 dólares nessa altura). O restante transferi-o da Tradehill para a Mt. Gox, para custódia.

ASC

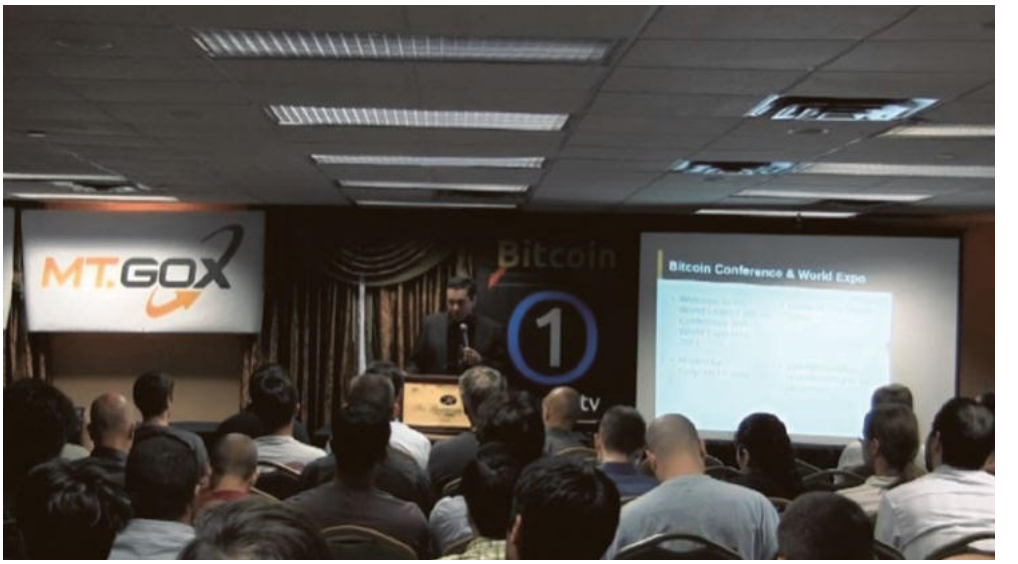
Bruce Wagner, apresentador de *The Bitcoin Show* em 2011-2012, foi dos primeiros a tentar levar o bitcoin ao grande público.

Era este o dinheiro do futuro?

«I AM SATOSHI»

A inscrição fez-se nos escritórios da OnlyOneTV, propriedade de Bruce Wagner, que produzia *The Bitcoin Show* no YouTube, num troço funcional da Quinta Avenida, no centro de Manhattan. Estávamos no final de agosto e os participantes —quase todos homens— tinham viajado de paragens remotas para falar de um dinheiro invisível, sem qualquer lastro, que quase ninguém compreendia, mas que se cotava a quinze dólares a unidade, face a menos de um dólar apenas seis meses antes. Gavin Andresen viera de Massachusetts. Jeff Garzik viera da Carolina do Norte. Stefan Thomas voara da Suíça e Roger Ver, um

A MT. GOX ERA A PLATAFORMA DE CÂMBIO DE BITCOIN, SEDIADA EM TÓQUIO, CONSIDERADA MAIS FIÁVEL



ASC/HENRY HOLLIGON

Fotografia da primeira conferência sobre o bitcoin no Hotel Roosevelt, na cidade de Nova Iorque, a 20 de agosto de 2011.

entusiasta promotor conhecido como «Bitcoin Jesus», do Japão. À minha frente, enquanto esperávamos para levantar as credenciais, distingui Jed McCaleb, futuro fundador da Ripple, que originalmente criara a Mt. Gox como uma plataforma para trocar cartas do seu jogo preferido (a sigla significava Magic: The Gathering Online eXchange) e posteriormente a vendera. Embora fôssemos pouco mais de 65 participantes, Bruce batizara o evento como «Bitcoin Conference & World Expo 2011 NYC».

Mais tarde, reunimo-nos num restaurante de Hell's Kitchen chamado Hudson Eatery, um dos poucos estabelecimentos que Bruce conseguira convencer a aceitar bitcoin como forma de pagamento, para «uma noite de convívio sob pseudónimo». No dia seguinte, nas conferências principais no Hotel Roosevelt, na East 45th Street, Gavin imaginou o dia em que o bitcoin seria algo banal e «aborrecido»; Jeff falou da necessidade de o bitcoin melhorar a sua estratégia de relações públicas, dada a facilidade com que podia ser mal interpretado; e Stefan apresentou as aplicações de programação para o bitcoin, então muito necessárias.

Não parecia propriamente uma revolução. Numa das noites da conferência, Stefan achou tão complicado pagar em bitcoin nos restaurantes que supostamente o aceitavam que acabou por saldar a conta em dólares. Ainda assim, sentia-se uma energia caótica no evento. Entre reflexões etéreas sobre um futuro dominado pelo bitcoin e o *networking* de empreendedores com *startups* ligadas à criptomoeda, os participantes trocavam teorias sobre Nakamoto (que nunca respondeu ao meu e-mail). Os matizes religiosos já se tinham começado a infiltrar na linguagem dos bitcoiners. O primeiro bloco minado por Nakamoto era, afinal, conhecido como o bloco Génesis. O *merchandising* do evento resumia-se a uma T-shirt com a legenda: «I am Satoshi». A pergunta pairava no ar: «Poderia estar aqui entre nós?».

«Não, se fosse alguém incapaz de fazer a viagem», pensei. ■

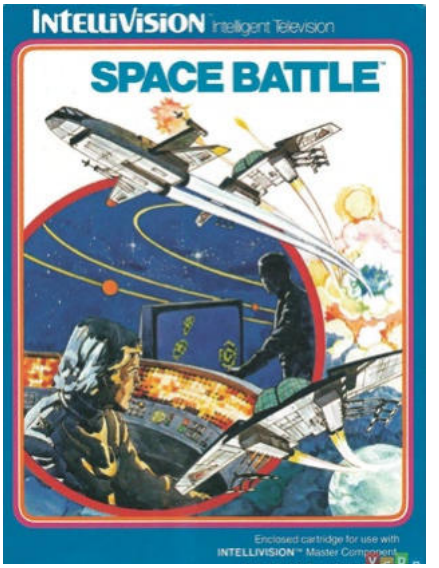

85

Sr. Rogers

Hal Finney personificou a vitalidade e a energia de quem foi, provavelmente, a figura mais importante da história inicial do bitcoin depois de Satoshi Nakamoto. Finney foi o primeiro destinatário de uma transação em bitcoin.

ASC

Hal Finney, o entusiasta do dinheiro digital de que Nick Szabo me falara, exibia um sorriso radiante e, durante algum tempo, um bigode recortado de tal exuberante amplitude e perfeição geométrica que parecia saído de *O Repórter: A Lenda de Ron Burgundy*. Nerd por excelência, Finney publicou certa vez um anúncio num jornal gratuito oferecendo-se para responder a qualquer pergunta científica ou técnica por um dólar e enfrentava os desafios intelectuais com um entusiasmo incansável. Quando trabalhava na nascente indústria dos videojogos no final dos anos 1970, a programar *Space Battle*, da Intellivision, e *Adventures of Tron*, da Atari, decidiu criar efeitos sonoros para Major League Baseball, da Intellivision.



SHUTTERSTOCK

Capa de *Space Battle*, Hal Finney trabalhou como programador de videojogos.

ACREDITAVA NO FUTURO

O *hardware* da Intellivision incluía um chip de som programável e David Rolfe, colega de casa e de trabalho na altura, recorda Finney a «mergulhar nos padrões de onda» para enfrentar o desafio de recriar os sons do estádio: «Se vivesses numa era em que os computadores nunca tivessem emitido sons e te dessem esta ferramenta, como reproduzirias um som de multidão? Como soa, afinal, uma multidão? Nessa altura estreou um filme desportivo, *O Céu Pode Esperar*, e Hal prestou particular atenção às cenas no estádio, quando a multidão vibrava, para depois recriar meticulosamente o clamor, os assobios e os efeitos de buzina. Chegou mesmo a recriar um "Estás fora!" que imitava de forma razoavelmente fiel a fala humana».

Finney sempre apreciara quebra-cabeças. Mesmo em criança, numa família que se mudou da Califórnia para Louisiana e depois para o Texas, acompanhando o trabalho do pai como engenheiro do petróleo, anotava em cadernos os seus próprios códigos secretos de letras e números. Era uma criança imaginativa, com gosto pela ficção científica. Ia buscar à biblioteca pública livros sobre avistamentos de OVNIs e lia-os na cama à noite, sentindo «uma deliciosa e aterradora emoção ao imaginar extraterrestres escondidos nas sombras». Perguntava-se muitas vezes: «Porque nasci aqui e agora, em vez de nalgum outro momento ao longo de toda a história?».

FINNEY PUBLICOU UM ANÚNCIO EM QUE SE OFERECIA PARA RESPONDER A QUALQUER PERGUNTA CIENTÍFICA OU TÉCNICA POR UM DÓLAR

De regresso à Califórnia para o liceu, aprendeu a programar em FORTRAN e ajudou os administradores do Arcadia High a processar os dados dos alunos, armazenando-os em cartões perfurados. Formou-se em 1974 como o melhor da sua turma e ingressou no Instituto de Tecnologia da Califórnia, onde, mesmo ali, era considerado excecionalmente brilhante — alguém capaz de percorrer um manual pela primeira vez na véspera de um exame importante e passar. Mais raro ainda, para alguém com o seu quociente de inteligência, era ser igualmente conhecido pela personalidade afável e otimista. Um colega de fraternidade recordaria que «levava toda a gente ao Tommy's às três da manhã para comer hambúrgueres, tantos quantos coubessem no seu Volkswagen».

Finney abraçou a ciência e a tecnologia e, juntamente com a mulher, a Fran, que fora sua namorada na universidade, deu aos filhos e aos animais de estimação nomes de objetos astronómicos: Arky, o nome do seu ridgeback rodesiano, vem de uma estrela da constelação do Boieiro. Depois de conhecer os extropianos, Finney tornou-se colaborador assíduo da respetiva lista de correio eletrónico. Evitava o álcool, porque sofrera convulsões na universidade e havia historial de alcoolismo na família, e começava agora a experimentar diferentes abordagens para se manter saudável: foi vegetariano durante menos de um ano, tentou uma dieta cetogénica, tomou suplementos vitamínicos antioxidantes e aderiu ao Weight Watchers, entre outras coisas.

Deu também um passo mais extremo, popular entre os extropianos. Em outubro de 1992, ele e a Fran conduziram de Santa Bárbara, para onde se tinham mudado recentemente, até Riverside, a sudeste de Los Angeles, para assinar a documentação necessária para se inscreverem na Alcor, uma organização de serviços criogénicos. A Alcor oferecia um pacote «neuro», mais barato, apenas para a cabeça, e um pacote mais caro, para o corpo inteiro, que foi o que os Finney escolheram. Quando morressem, os seus corpos seriam congelados, na esperança de que a tecnologia pudesse um dia reanimá-los. A Alcor entregou-lhes uma placa de identifi-

ASC

Hal Finney numa fotografia ao lado da futura esposa, Fran (1972). Décadas mais tarde tornar-se-ia uma das figuras mais admiradas do ecossistema bitcoin.

cação de emergência, que podia ser usada ao pescoço ou numa pulseira de elos. Hal passou a usar a placa de aço, profusamente gravada, desde então. Nela constavam um número de telefone disponível 24 horas por dia; a menção de uma recompensa por quem contactasse; instruções do «protocolo de bioestase»; e a ordem legal «Sem embalsamamento/sem autópsia». Isto alertaria os serviços de emergência, no caso da sua «desanimação», de que era um paciente criogénico com as quotas em dia e indicaria quem contactar para que a sua criopreservação pudesse iniciar-se sem interferências nem atrasos. «Não acreditava em Deus — explicou mais tarde a Fran. — Acreditava no futuro».

UMA AMEAÇA À SEGURANÇA NACIONAL

Através dos extropianos, Hal Finney tomou também contacto com o projeto que se tornaria a obra da sua vida. Quando leu que um tipo chamado Phil Zimmermann inventara o primeiro programa de criptografia DIY do mundo — um *software* que qualquer pessoa podia correr no seu computador pessoal para enviar e receber mensagens de correio eletrónico ilegíveis para intrusos — e que o Governo o considerava uma ameaça à segurança nacional, Finney descarregou-o, experimentou e ficou impressionado. Isto levou-o à biblioteca para aprofundar a investigação, onde encontrou os artigos de David Chaum que demonstravam, conceptual e matematicamente, como a nova criptografia podia ser usada para garantir a privacidade pessoal online. «Fiquei pasmado», recordaria mais tarde Finney.

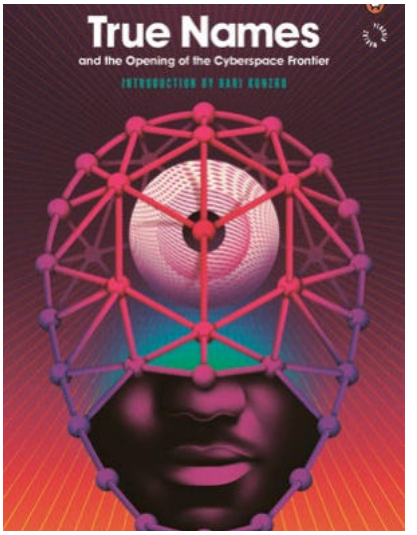
Cativaram-no «o mistério e o paradoxo» da criptografia. «O que sempre me fascinou num desafio intelectual é que, quando o dominas, ele dá-nos competências práticas». Sempre que se deparava com algo desse género, reconhecia a sua tendência para desenvolver um interesse obsessivo. «Apodera-se de mim um impulso completamente incontrolável».

HELEN DAVIS / DENVER POST

Phil Zimmermann inventara o primeiro programa de criptografia DIY do mundo, Pretty Good Privacy (PGP), um *software* de encriptação.

SEMPRE QUE SE DEPARAVA COM ALGUM DESAFIO, RECONHECIA A SUA TENDÊNCIA PARA DESENVOLVER UM INTERESSE OBSESSIVO

A criptografia era mágica para ele. Tal como Tim May, Finney inspirara-se em *True Names* e nas suas «identidades impossíveis de rastrear». Ao ler a novela, deu por si a apontar falhas nos aspetos técnicos da fantasia de Vinge. Como May, Finney vislumbrou de imediato como a criptografia, a versão adulta da sua fascinação juvenil, poderia ser o instrumento para materializar o futuro imaginado em *True Names*. Tomemos como exemplo os *nyms*: qualquer pessoa poderia usar o nome «Esquilo Secreto», assinalou Finney, mas só uma poderia provar a posse de uma chave privada vinculada a uma chave pública. «Pareceu-me tão evidente. Aqui deparamo-nos com problemas de perda de privacidade, informatização progressiva, bases de dados massivas, maior centralização, e Chaum propõe uma direção completamente diferente — uma que coloca o poder nas mãos das pessoas, em vez dos Governos e das corporações. O computador pode ser usado como ferramenta para libertar e proteger os indivíduos, em vez de os controlar».



PENGUIN RANDOM HOUSE COMPANY

Capa de *True Names*, de Vernor Vinge, uma das obras visionárias que antecipou conceitos do bitcoin.

AO NÍVEL DE STEPHEN HAWKING

Voluntariou-se para ajudar Phil Zimmermann e, ao longo dos anos seguintes, trabalhava a tempo inteiro, regressava a casa e consagrava as noites a trabalho voluntário intenso — ainda que no encantador cenário da costa central da Califórnia —, escrevendo linhas de código para o PGP. Mais tarde, depois de o PGP ter ultrapassado os seus problemas legais e se ter transformado numa empresa com fins lucrativos, Finney integrou a equipa como um dos seus dois primeiros empregados. Era o trabalho ideal para si, pois combinava a paixão pelos quebra-cabeças com o fervor pela privacidade.

Num meio que tendia para a paranóia e o autismo, Finney destacava-se pela afável normalidade. Will Price, que trabalhou com Finney no PGP, compara-o com outro criptógrafo, um «génio ao nível de Stephen Hawking», que também trabalhou para o PGP na década de 1990. Este criptógrafo evitava tomar banho, só escrevia código que oferecia e recusava receber dinheiro pelo trabalho porque não tinha conta bancária. «Tivemos de o pagar com computadores. Não quero usar a palavra psicopata. Ninguém o vê desde 2000. Julgo que vive nalguma floresta».

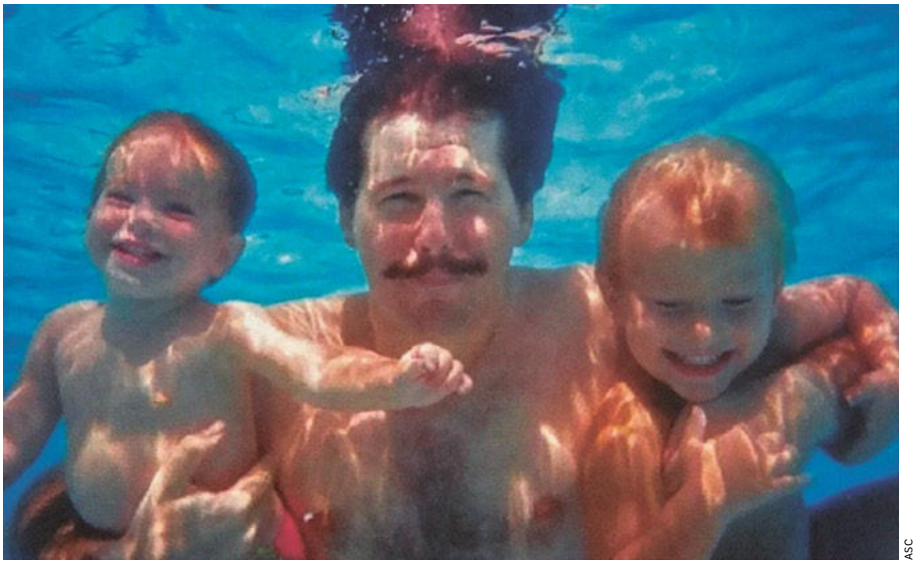
FINNEY ESCREVIA CÓDIGO QUE OFERECIA E RECUSAVA ACEITAR DINHEIRO PELO SEU TRABALHO PORQUE NÃO TINHA CONTA BANCÁRIA

Finney era mais convencional na aparência. Gostava de passar tempo com a família. Era «uma pessoa muito centrada», disse-me Will, que descreveu Finney como «sereno» e «nunca irritado». «Por vezes, as pessoas superinteligentes pagam um preço por isso — ecoou Phil Zimmermann. — Há algo na sua personalidade que não funciona exatamente bem. O Hal nunca pagou esse preço. Conservou a humanidade, a amabilidade e a graça. Vi Tom Hanks num filme sobre o Sr. Rogers. É desse tipo de alma que estou a falar».

NUNCA SE É DEMASIADO CAUTELOSO

Finney era, em muitos aspetos, um *cypherpunk* por excelência. Escrevia mesmo código. Mas, embora tivesse convicções fortes sobre a liberdade, era mais pró-social do que alguns companheiros de viagem. Falava sobre como a criptografia poderia ter ajudado os abolicionistas que operavam no Underground Railroad a facilitar a fuga de escravos. «Os Libertários, com L maiúsculo, tendem a ser menos compassivos — assinalou o Phil — e creio que o Hal era uma pessoa compassiva».

Finney concluiu que o anonimato e o uso de pseudónimos, apesar dos seus inconvenientes, proporcionariam «benefícios reais a todos os membros da sociedade». Citou *The Federalist Papers*, «publicados anonimamente por receio de re-

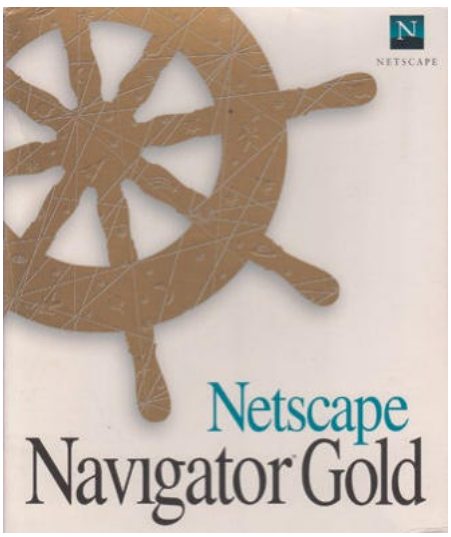


ASC

Hal gostava de passar tempo com a família; era uma pessoa muito centrada, serena e nunca se irritava. Hal Finney com os dois filhos (na imagem).

presálias políticas». E que dizer dos denunciantes e dissidentes? Ele próprio usara múltiplos pseudónimos na Internet. «Para mim, a criptoanarquia representa uma forma de oposição às bases de dados de informação pessoal em constante expansão, uma maneira de os indivíduos recuperarem o controlo sobre a informação das suas próprias vidas». Referia-se a *True Names*, onde «descobrirem a tua verdadeira identidade constituía o pior desastre imaginável, pois tornava-te vulnerável a numerosos tipos de ataque, quer de outros *hackers* quer do Governo».

Para Finney, não era uma abstração académica. Emocionava-se ao pensar em como mensagens de correio eletrónico não anónimas poderiam levar o seu chefe, Phil Zimmermann, à prisão. Já gastara mil dólares do próprio bolso para contratar um advogado que o aconselhasse sobre o risco de ser processado pelo trabalho voluntário que fizera para o PGP e advertiu outros *cypherpunks* de que, se o Governo os declarasse culpados de violar a Lei de Controlo de Exportação de Armas, poderiam ser multados em até um milhão de dólares e condenados a dez anos de prisão. «É repugnante, mas hoje em dia nunca se é demasiado cauteloso. Compreende-se perfeitamente a posição do Pr0duct Cypher e dos nossos outros participantes anónimos».



ASC

O Navigator Gold 2.01 democratizou o acesso à Internet e tornou possível a coordenação descentralizada necessária ao bitcoin.

DESAFIO AOS *CYPHERPUNKS*

Depois de um serviço de reencaminhamento alojado no computador de um homem na Finlândia ter sido alvo de rusga a pedido da Igreja da Cientologia, que procurava um denunciante anónimo de documentos internos, Finney desenvolveu e pôs em funcionamento um dos primeiros sistemas de reencaminhamento anónimo e encriptado: fazia as mensagens saltarem por múltiplos servidores, sem que nenhum conhecesse mais do que o ponto anterior e o seguinte na rota do envio. Quando o Governo dos Estados Unidos começou a exigir que as versões de exportação de programas populares empregassem uma criptografia mais fraca do que as versões nacionais, Finney — para evidenciar o absurdo dessa política e as suas desvantagens comerciais — lançou um desafio aos seus companheiros *cypherpunks* para que decifrassem a nova versão de exportação do navegador Netscape. Depois de uma equipa o ter conseguido decifrar em um mês, Finney publicou um segundo desafio e, desta vez, os *cypherpunks* quebraram a segurança em menos de trinta e duas horas.

Os sistemas de reencaminhamento de correio eram apenas os alicerces do mundo respeitador da privacidade que Finney queria ajudar a construir. O que realmente o apaixonava era o nível seguinte: o dinheiro digital. Esse sonho ficara re-

legado durante as batalhas pelo direito público a uma criptografia robusta, mas, uma vez assegurado esse direito, Finney concentrou cada vez mais a atenção no dinheiro eletrónico. Apontava razões práticas — os cartões de crédito não conseguiam gerir micropagamentos, nem toda a gente tinha acesso a eles e ofereciam pouca privacidade — e uma de ordem mais ideológica, aludindo aos banqueiros que imprimiam dinheiro e geravam inflação.

E Finney fez o trabalho árduo de pensar nos detalhes necessários para materializar o dinheiro digital. Que posição adotaria o Governo perante isto ou perante qualquer moeda alternativa em geral? Finney investigou a história das notas privadas e descobriu que tinham estado sujeitas a um imposto pesado por força de uma lei da época da Guerra Civil que ainda se mantinha em vigor. Soube que o fisco norte-americano (IRS) tinha tributado o intercâmbio e a troca de bens. Estudou alternativas às patentes de Chaum. Antecipou que, mesmo num sistema que iludisse o Governo, a conversão de moeda física em dinheiro digital constituiria um «ponto de estrangulamento» onde o Governo poderia exercer controlo.

A curto prazo, Finney considerou que uma forma de contornar o labirinto legal poderia ser criar «um jogo educativo» e sugeriu que «quem se proponha implementar um jogo deste tipo deverá ponderar lançá-lo anonimamente (na verdade, sob pseudónimo). Deste modo, não existirá um alvo concreto para quem deseje punir os utilizadores do jogo».

DINHEIRO MÁGICO

Com alguns *cypherpunks* de afinidades semelhantes, Finney equacionou possíveis nomes para a nova moeda: cryps, crydets, emoney, ecash ou, sugeriu com ironia, chaums. Assim seria menos provável que nos processasse por violação da sua patente. Depois de outra chuva de ideias, propôs CRASH, acrónimo de CRypto cASH.

Sempre que este ou aquele *cypherpunk* propunha um novo sistema de dinheiro digital, Finney respondia oferecendo apoio ou assinalando uma vulnerabilidade. Considerava que a ideia de Chaum de utilizar *hardware* criptográfico inviolável, instalado no computador de cada um para evitar o duplo gasto, era «o caminho errado», mas apressou-se igualmente a testar o produto de dinheiro eletrónico de Chaum. Depois de o Pr0duct Cypher ter publicado um *software* que escrevera para um sistema de «dinheiro mágico», Finney deu-lhe uma palmada nas costas: «Uau! Que bom!». Dois dias depois, Finney informou-o de que o dinheiro mágico podia ter uma falha de segurança.

Refletiu também sobre a estética da moeda digital. Ao ler um velho livro sobre o papel-moeda norte-americano, descobriu que algumas das notas arcaicas reproduzidas eram «surpreendentemente belas». Questionou-se, numa resposta a Pr0duct Cypher, se seria possível criar dinheiro digital que fosse belo e raro. Ima-

QUANDO NAKAMOTO LANÇOU O *SOFTWARE*, O COMPUTADOR DE FINNEY TORNOU-SE O SEGUNDO NÓ DA REDE

INSIDEBITCOINS

Nick Szabo continua a ser o candidato mais plausível, mas, após décadas de especulação e investigação, não existe prova definitiva da identidade de Satoshi.

ginou quantidades discretas dessa moeda com marcas temporais para demonstrar a sua antiguidade. O dinheiro digital seriam bits à deriva no éter, mas Finney sugeriu formas de tornar visíveis determinadas unidades da moeda, como «padrões apelativos, de aspeto fractal, para muitas notas. Com um pouco mais de reflexão, espero criar um visualizador para o seu Magic Money que destaque a sua beleza natural e raridade. Será indispensável para todos os colecionadores sérios de dinheiro digital».

Durante a crise do dinheiro eletrónico do início dos anos 2000, Finney foi um dos poucos que se manteve focado em resolver o problema. Estava suficientemente obcecado para lhe dedicar grande parte do tempo livre. Em 2004, lançou a sua própria implementação do bit gold de Nick Szabo. O RPOW (Reusable Proofs of Work) usava o mesmo método de quebra-cabeças computacionais proposto para o bit gold, empregava criptografia para assegurar o sistema e garantir a escassez, e pretendia ser descentralizado, substituindo um terceiro de confiança por *hardware* especializado que os computadores participantes teriam.

O RPOW nunca teve grande sucesso, mas, quando Nakamoto anunciou o bitcoin quatro anos mais tarde, Finney foi a primeira pessoa em Metzdowd a elogiá-lo. Deu a sua opinião a Nakamoto sobre o código-fonte e, quando este lançou o *software* em 9 de janeiro de 2009, o computador de Finney tornou-se o segundo nó da rede. «Executando o bitcoin», tuitou Finney.

Isto serviu também como piscadela à sua nova paixão. Dada a natureza sedentária do trabalho de Finney, na meia-idade o seu peso passara de 77 para cerca de 113 e, depois de o médico lhe ter dito que era obeso, começou a fazer dieta e a competir em meias-maratonas. Com o tempo, desceu para 73. No início de 2009, Finney estava na sua melhor forma física e a treinar para a primeira maratona completa. ■

Vê sempre o lado positivo

Finney manteve até à morte os dez bitcoins que Satoshi lhe enviou na primeira transação — apesar de valerem centenas de milhares de dólares e de a família enfrentar custos médicos astronómicos. ISTOCK

Um mês depois de ter escrito no Twitter sobre o bitcoin, Finney notou que os seus tempos de corrida já não melhoravam. Cansava-se mais depressa e tinha cãibras com mais frequência. Fran reparou que, quando corriam juntos, ele já não conseguia falar e correr ao mesmo tempo, como antes. Quando ela mencionou isso, ele respondeu com uma impaciência invulgar: «Ninguém consegue falar e correr ao mesmo tempo».

Finney começou a notar que a fala, por vezes, se lhe entrecortava, quase como se tivesse estado a beber. A mão direita começou a tremer. Fran, fisioterapeuta, sabia que algo não estava bem. «Não parava de lhe dizer: "Hal, tens de fazer exames, tens de ir ao médico". Não queria ter razão». Em maio, quando o Hal correu a Maratona de Los Angeles, as cãibras e os espasmos na perna direita tornaram-se tão intensos que parou no Sunset Strip, por volta da milha 13.

Em cada aniversário desde o casamento, em 1979, ele e Fran saíam para um passeio de bicicleta, uma milha por cada ano de matrimónio. Nesse ano celebravam trinta anos e, a partir de uma pousada em San Luis Obispo, partiram numa bicicleta tandem para um percurso de trinta milhas. Pela primeira vez, o Hal estava demasiado cansado para terminar. Uma semana depois, diagnosticaram-lhe ELA, a doença neurodegenerativa também conhecida como doença de Lou Gehrig.

HAL NÃO TINHA OS MESMOS PLANOS

A voz tornou-se mais ténue. Prendia-se com mais frequência. As mãos enfraqueceram. «É incómodo e preocupante que os meus sintomas iniciais se estejam a manifestar na voz e nas mãos, as duas vias de saída mais utilizadas e com maior largura de banda de que disponho», escreveu aos amigos no *LessWrong*, em termos que a comunidade de tecnólogos apreciaria.

ASC

Hal e Fran Finney numa maratona solidária para angariar fundos contra a ELA.

Surpreendeu-o saber que mais de 90% das pessoas com ELA optavam por morrer quando já não conseguiam respirar por si próprias. O Hal não tinha esses planos. Tencionava continuar com ventilação mecânica. Um serviço gratuito de banco de voz do Laboratório de Investigação da Fala da Universidade de Delaware estava a modelar a sua voz, que depois poderia ser reproduzida através de um sintetizador. Lera que Stephen Hawking, que brevivera quarenta anos com ELA, conseguia escrever dez palavras por minuto contraindo um músculo da face. «Talvez até consiga escrever código — comentou Hal aos leitores do *LessWrong* —, e o meu sonho é contribuir para projetos de *software* de código aberto mesmo a partir de um corpo imóvel. Essa será uma vida que valerá bem a pena viver».

ASC

Hal Finney ao lado da esposa, Fran, nos últimos anos de vida, completamente paralisado pela ELA, dependente de ventilação assistida para respirar.

Nesse dezembro, a angariar fundos para o combate à ELA como parte de uma equipa de estafetas na Maratona Internacional de Santa Bárbara, Fran levou o chip de cronometragem até Hal, e caminharam juntos o último troço de três quilómetros, com Hal a apoiar-se numa bengala. Cresceu a esquiar e tornou-se exímio nas pistas, enfrentando pistas «double black diamond» e fazendo acrobacias, mas, em dezembro, esquiou pela última vez, limitando-se às pistas para principiantes e lutando para subir e descer do teleférico.

SEMPRE QUE HAL CONSEGUIA ALGO, FICAVA RADIANTE

Hal enfrentou o destino com um otimismo tal que Phil Zimmermann o comparou a *Always Look on the Bright Side of Life*, dos Monty Python. Quando Phil visitou Hal em casa, já com a doença muito avançada, este disse-lhe: «Bem, agora tenho mais tempo para ler».

«Todos os que têm ELA falam do quão terrível é, de todas as coisas que já não podes fazer — escreveu Hal no *LessWrong*. Mas ninguém parece aperceber-se de que há muitas coisas que podes fazer e que nunca tinhas feito. Nunca usei uma cadeira de rodas elétrica. Nunca controlei um computador com os olhos. Nunca tive um sintetizador de voz treinado para imitar a minha voz natural. Se dissesse às pessoas dos fóruns de ELA que estou ansioso por experimentar algumas destas coisas, iam achar que estou louco. Talvez as pessoas daqui percebam».

LERA QUE STEPHEN HAWKING CONSEGUIA ESCREVER DEZ PALAVRAS POR MINUTO CONTRAINDO UM MÚSCULO DA FACE

SHUTTERSTOCK

Hal mantinha a esperança de que o bitcoin encontraria o seu lugar num mundo cada vez mais interligado, embora o seu destino dependesse da capacidade humana para o aperfeiçoar.

ESPERAVA QUE O SISTEMA MONETÁRIO SE TORNASSE MAIS COMPLEXO, COM O BITCOIN A DESEMPENHAR UM PAPEL RELEVANTE

Já não se conseguia levantar da cadeira? Pois bem, nada que uma cadeira elevatória e um poste por perto não resolvessem. Sempre fora rápido ao teclado; quando a mão direita deixou de funcionar, aprendeu a escrever depressa só com a esquerda. Quando essa mão enfraqueceu, imobilizou os dedos com talas para poder continuar a escrever com dois dedos. Quando lhe restou apenas um dedo útil, escrevia com esse dedo. Quando perdeu por completo o uso das mãos, passou para um rastreador ocular. Quando os músculos oculares começaram a falhar, mudou para ecrãs em que tinha apenas quatro letras à escolha de cada vez. Quando a cadeira de rodas começou a provocar-lhe dolorosas úlceras de pressão, obrigando outras pessoas a ajustar-lhe constantemente a posição, montou um sistema que lhe permitia controlar a cadeira com *software* de rastreio ocular. «Ficou encantado por conseguir fazê-lo — disse Fran mais tarde —. Isso dava-lhe uma felicidade suprema. Sempre que Hal alcançava algo que o entusiasmava, ficava exultante».

HONRAR O DESEJO DE SATOSHI

Quando o contactei em agosto de 2011, Hal apenas conseguia comunicar através do rastreador ocular. Ainda assim, respondeu amavelmente às minhas perguntas por correio eletrónico. Escreveu que antecipava melhorias no bitcoin e que isso «poderia conduzir à fragmentação e à concorrência entre diferentes versões». Esperava que o sistema monetário internacional se tornasse muito mais complexo, com o bitcoin a desempenhar um papel relevante. Previu a questão de saber se, uma vez esgotadas as moedas por extrair e alterados os incentivos à preservação da integridade do bitcoin, o sistema continuaria estável. Preocupavam-no os problemas que continuariam a afetar o bitcoin e os seus derivados, afastando a maioria dos utilizadores, e comentou-me que «a experiência com o bitcoin demonstrou, de forma eloquente, o lamentável estado da segurança informática atual. Proteger moedas digitais contra o roubo revelou-se inesperadamente difícil».

Perguntei a Hal se era o Satoshi Nakamoto.

— Não, não sou — respondeu —. Quem me dera ter criado algo tão potencialmente revolucionário como o bitcoin. Nas minhas circunstâncias atuais, com uma esperança de vida limitada, teria pouco a perder em abdicar do anonimato. Mas não fui eu.

— Achava que o Wei Dai poderia ser o Nakamoto?

— Conheço o Wei há muitos anos — respondeu-me. É brilhante e, sem dúvida, seria capaz de criar algo tão imaginativo como o bitcoin. No entanto, a minha impressão quanto ao estilo de escrita do Satoshi é que é diferente.

Hal contornou com delicadeza as restantes perguntas sobre o tema:

— Não queria desencorajar a tua investigação, mas sinto algum desconforto em participar tão ativamente neste exercício de especulação. Satoshi valoriza evidentemente a sua privacidade e talvez a melhor forma de lhe mostrarmos respeito e gratidão pela sua criação seja precisamente honrar esse desejo. ■

O alfinete, não a bolha

O bitcoin tem sido dado como «morto» mais de 470 vezes pelos meios financeiros tradicionais desde 2010. Sofreu quebras de 80-90% em múltiplas ocasiões (2011, 2014, 2018, 2022) e, de cada vez, os críticos proclamam que, finalmente, a bolha rebentou. No entanto, recupera e atinge novos máximos históricos.

SHUTTERSTOCK


BITCOIN • DIGITAL • DECENTRALIZED • PEER TO PEER

SHUTTERSTOCK

Desde 2021, Miami emergiu como o *hub* mais *cripto-friendly* dos Estados Unidos, atraindo empresas de *blockchain* e eventos de grande escala como a Bitcoin Conference...

Onze anos depois, em Miami, numa noite em que caminhava pela Collins Avenue a caminho do hotel, um homem ruivo, com inquietantes entradas, passava a passo apressado na direção contrária; cruzou-se comigo e fiquei estupefacto. Usava óculos, calções, uma camisa de manga curta abotoada e ténis Converse pretos de cano alto com meias. Virei-me para observar a sua figura encolhida.

—Não era aquele...?

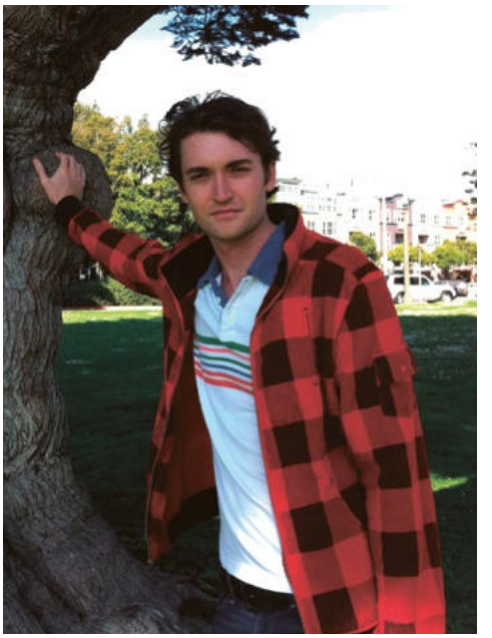
—Era o Adam Back —disse um tipo que vinha atrás de mim no passeio—. Tive a mesma reação.

—Tem uma ilha privada em Malta, não é? —comentou um homem que caminhava na direção oposta com três amigos.

Era uma quinta-feira de abril, durante a conferência Bitcoin 2022. Miami tinha-se apresentado recentemente como a cidade dos Estados Unidos mais favorável às criptomoedas e estimava-se a presença de vinte e seis mil pessoas. Back, que em 2011 fora um obscuro consultor de criptografia, dirigia agora a Blockstream, uma empresa de infraestrutura de *blockchain* avaliada em três mil milhões de dólares, de que era cofundador. No dia seguinte, após Back fazer uma apresentação em palco, vi a imprensa especializada em cripto e os fãs a rodeá-lo, à procura de respostas e de selfies. Figuras que uma década antes tinham sido obscuros especialistas técnicos eram agora superestrelas do setor. O bitcoin demorara a escapar aos estreitos círculos dos informáticos. Quando isso aconteceu, a atenção inicial não foi favorável.

PARA ALÉM DA SILK ROAD

Num episódio de 2012 de *The Good Wife*, o Governo dos Estados Unidos perseguia o criador do bitcoin pela sua «moeda ilegal online». Em *Os Simpson*, Krusty, o Palhaço, faliu depois de investir em bitcoin, entre outras coisas. No final de 2013, a Silk Road, o mercado da web obscura onde o bitcoin era a moeda preferida, foi encerrado e o seu criador, Ross Ulbricht, detido. Em 2014, a Mt. Gox, a plataforma segura e fiável onde guardara os meus sete bitcoins restantes, declarou falência depois de desaparecerem 850 000 bitcoins, e o seu proprietário, Mark Karpelès, foi detido; foi absolvido de furto, mas acabou por receber uma pena suspensa por «manipulação de registos eletrónicos». A volatilidade do bitcoin tornava-o excitante para os especuladores e aterradora para a maioria. Um ciclo de euforia e queda em 2011, de 1 para 32 e daí para 2 dólares, foi apenas o primeiro de muitos episódios semelhantes. Nos primeiros meses de 2013, o bitcoin subiu de 13 para 260 dólares antes de desabar, em menos de uma semana, até aos 50 dólares. Na segunda metade desse ano, passou de menos de 100 dólares para mais de 1100, para depois perder metade do seu valor em apenas um par de semanas, em dezembro. Ainda assim, apesar das flutuações extremas e de inúmeros ataques e burlas, o valor do bitcoin continuava a crescer, embora de forma errática.



ASC

Ross Ulbricht criou a Silk Road, sob o alias «Dread Pirate Roberts», o primeiro mercado *darknet* em grande escala.

Começaram a surgir sinais intermitentes de que estava a alargar a sua atratividade. Em 2014, o Senado norte-americano realizou uma audição surpreendentemente otimista sobre o bitcoin, intitulada «Para além da Silk Road: riscos potenciais, ameaças e promessas das moedas virtuais». Richard Branson anunciou que a sua empresa de viagens espaciais, a Virgin Galactic, passaria a aceitar bitcoins, pois, segundo ele, estava a «impulsionar uma revolução». Bill Gates considerou o bitcoin «entusiasmante, melhor do que a moeda e um *tour de force* tecnológico». Um ano depois, Marc Andreessen, pioneiro do navegador web antes de se tornar investidor de capital de risco, afirmou: «Es-

MIAMI PROCLAMARA-SE COMO A CIDADE MAIS FAVORÁVEL ÀS CRIPTOMOEDAS DOS ESTADOS UNIDOS

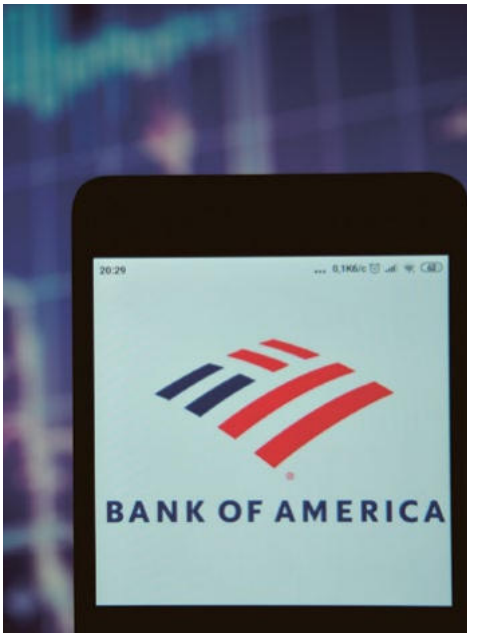
SHUTTERSTOCK

Acima, Richard Branson em frente à *SpaceShipTwo*, no Spaceport America, Novo México, em 2011. O empresário foi um dos empreendedores visionários do bitcoin.
Em baixo, Bill Gates representa a postura cética da elite tecnológica tradicional face ao bitcoin e tem mantido uma perspetiva crítica ao longo dos anos.

SHUTTERSTOCK

tamos bastante convencidos de que, quando nos sentarmos aqui dentro de vinte anos, falaremos do bitcoin como hoje falamos da internet.» E quanto mais tempo passava, quanto mais tempo o bitcoin passava sem ser comprometido com sucesso, mais sólido parecia.

E agora, anos após a sua criação, um único bitcoin valia mais de 65 000 dólares e representava apenas uma fração de uma indústria muito mais ampla. Cripto, termo que historicamente fora a abreviatura de criptografia, designava agora, para consternação dos criptógrafos, o universo das criptomoedas. Existiam, roçando o inverosímil, mais de dezasseis mil criptomoedas distintas, todas variações do único modelo que existia em 2011. Em conjunto, tinham ultrapassado recentemente a assombrosa marca de três biliões de dólares em capitalização. 86% dos estadunidenses tinham ouvido falar das criptomoedas. 16% tinham-nas utilizado, negociado ou incluído nos seus investimentos.



SHUTTERSTOCK

A banca tradicional convive hoje com um ecossistema cripto que evolui a grande velocidade.

«LIBERTEM ROSS!»

No entanto, isso não significava que fossem compreendidas. Eu próprio não tinha a certeza de as entender, apesar de as estudar há onze anos. As pessoas perguntavam: «O que é o bitcoin?», uma questão que estava longe de ter uma resposta simples.

—Porque é que o bitcoin vale alguma coisa? —perguntou um dia o meu sogro. —Porque é que o ouro vale alguma coisa? —retorqui.

O meu sogro olhou-me, impaciente.

—Porque é que todos a quem faço esta pergunta me respondem com outra?

Durante o voo para a Florida, sentei-me entre um executivo que geria ativos digitais no Bank of America e um financeiro dedicado a conceder empréstimos a mineiros de bitcoin. Ambos classificaram o veterano e imperturbável bitcoin de «aborrecido», em comparação com a efervescência e o dinamismo dos novos projetos de criptomoedas. As experiências com DeFi (finanças descentralizadas), NFT (tokens não fungíveis) e DAO (organizações autónomas descentrali-

A AUTODETERMINAÇÃO REPRESENTAVA A EXPRESSÃO MÁXIMA DO ESPÍRITO LIBERTÁRIO DO BITCOIN

zadas) decorriam sobretudo noutras cadeias de blocos, em especial a Ethereum. Ainda assim, era precisamente essa previsibilidade que tornara o bitcoin a criptomoeda com maiores hipóteses de adoção em massa. Em Miami, a senadora do Wyoming Cynthia Lummis tinha agendada uma «conversa informal» sobre legislação relacionada com o bitcoin, enquanto Tucker Carlson se apresentaria no centro de congressos com uma equipa da Fox para entrevistar Michael Saylor, cuja empresa, a MicroStrategy, detinha mais de 5000 milhões de dólares em bitcoins. Na fila para levantar as credenciais, conversei com dois indivíduos que afirmaram residir no Panamá e operavam uma instalação de mineração de bitcoin, alimentada por energia hidroelétrica, numa zona remota do Paraguai. Vi um casal vestido integralmente de laranja, a cor emblemática do logótipo do bitcoin.

A multidão que percorria o edifício era apenas um pouco menos masculina do que o grupo da conferência a que assistira uma década antes, mas estes homens pareciam mais contestatários. Apontei os lemas estampados nas T-shirts e nas sweatshirts com capuz que observei:

SHUTTERSTOCK

A MicroStrategy consolidou-se como um dos maiores detentores institucionais de bitcoin, simbolizando a convergência entre a estratégia empresarial e as criptomoedas.

— «Defensor absoluto da liberdade de expressão».
— «Bitcoin contra o mundo».
— «Clube social anti-fiat».
— «O bitcoin é o alfinete, não a bolha».
— «Introvertido mas disposto a falar de cripto».
— «Nascemos demasiado tarde para explorar os mares; demasiado cedo para explorar as estrelas; mesmo a tempo de consertar o dinheiro».
— «Eu sou o Satoshi Nakamoto».

Num longo corredor do segundo piso, agachei-me para examinar o que parecia lixo na alcatifa. Era uma nota de cinco dólares, ou o que restava dela. Alguém a rasgara em pedaços num acesso de ressentimento contra o dólar ou como uma espécie de instalação artística improvisada. Um grande cartaz, «Libertem Ross!», procurava um milhão de assinaturas para lançar uma petição pela libertação de Ross Ulbricht, o criador encarcerado da Silk Road que operara como o Temível Pirata Roberts, a personagem de *A Princesa Prometida* que, tal como a conceção que algumas pessoas têm de Satoshi Nakamoto, não era um indivíduo, mas uma identidade que passava de pessoa em pessoa. Ter-se-ia generalizado o uso do bitcoin? Num debate intitulado «Tornar-se um indivíduo soberano» participaram um cripto-influencer cabeludo chamado Robert Breedlove, que tinha o símbolo da criptomoeda tatuado no bíceps; o então *quarterback* dos Buffalo Bills, Matt Barkley, e Pascal Gauthier, diretor-geral do fabricante de carteiras de *hardware* Ledger, que trazia anéis em seis dedos. A autodeterminação representava a expressão máxima do espírito libertário do bitcoin. Enquanto ouvia os oradores, refleti sobre como a ideologia provavelmente fora indispensável para impulsionar o bitcoin nos primórdios, mas a sua persistente hegemonia na cultura do bitcoin constituía agora um obstáculo. O bitcoin despertava tantos receios como admiração. O libertarismo radical soava antipático ao cidadão comum. Havia algo profundamente desalentador nessa desconfiança tão enraizada nas pessoas que levava a depositar toda a fé numa rede de máquinas. A maioria preferia confiar em bancos, forças de segurança e serviços públicos. Não aspiravam a criar os filhos numa plataforma petrolífera apátrida que teriam de defender com armas semiautomáticas.

ASC/LEDGER

Pascal Gauthier, CEO da Ledger, lidera uma das empresas-chave na custódia de bitcoins e criptomoedas.

A VIOLÊNCIA TORNOU-SE INEVITÁVEL

Era difícil sustentar que as criptomoedas eram uma alternativa melhor quando continuavam a desfazer-se nas mãos das pessoas. Como Hal Finney já receava, muitos dos problemas que afetaram o bitcoin nos primeiros anos — da volatilidade de preços ao azar e ao crime — tinham-se intensificado. Agora que o bitcoin valia significativamente mais, também cresciam os riscos. Um homem no País de Gales, que deitara acidentalmente fora um disco rígido que continha as chaves de 8000 bitcoins, avaliados em 320 milhões de dólares à data da conferência, dedicara os últimos nove anos a tentar escavar um aterro para recuperar a fortuna perdida.

Quando o único que protegia os bitcoins era uma sequência de letras e números, a violência tornou-se inevitável. Nos Países Baixos, um comerciante de bitcoins de trinta e oito anos foi atacado em casa por ladrões que usavam balaclavas, coletes à prova de bala e casacos militares. Torturaram-no diante da filha de quatro anos, durante mais de uma hora, segundo declarou à polícia, atando-lhe as mãos atrás das costas, dando-lhe pontapés, apontando-lhe uma pistola à cabeça, sufocando--o com a mangueira do duche, usando uma ferramenta elétrica para lhe perfurar sete buracos na perna e no pé e pendurando-o pelo pescoço.

Os seguidores mais fanáticos do bitcoin, por vezes chamados maximalistas ou maxis do bitcoin, pareciam indiferentes a como estes riscos afetavam as pessoas comuns, mesmo que essa atitude os condenasse a permanecer na marginalidade.

—Sim!

O som veio da minha direita. Um homem sentado ali inclinou-se para a frente, absorto. Do outro lado do corredor, outro homem usava um capacete de mota ao estilo Daft Punk, com a viseira escura descida. O anonimato transbordava para o espaço físico.

Gauthier, da Ledger, dizia que 70% do mundo não vive em democracia.

—Uau! —exclamou o tipo ao meu lado—. Uau!

Depois, na rua, passei junto de um homem que erguia um cartaz com os nomes de ícones do economista libertário: Ludwig von Mises, Murray Rothbard, Friedrich Hayek. Ali perto, uma reunião paralela, programada para coincidir com a conferência, acolhia entusiastas de armas. Vi um raro graffiti dissidente: «Que se lixe a cripto, é um esquema em pirâmide, e não do tipo divertido».

O BITCOIN ERA UM AVISO

Depois do almoço, estava programada a intervenção de Peter Thiel, fundador da PayPal tornado capitalista de risco. Apesar de se dizer que o bitcoin não tinha líder, Satoshi Nakamoto estava, na sua ausência, em todo o lado. O palco Nakamoto, onde tiveram lugar as conferências magnas e as principais intervenções, estava ladeado por ecrãs iluminados que exibiam uma sequência rotativa de excertos dos

NOS PAÍSES BAIXOS, UM COMERCIANTE DE BITCOINS FOI ATACADO EM CASA POR LADRÕES QUE USAVAM BALACLAVAS

seus escritos. Tinham a qualidade, semelhante à de Dianética, de serem banais para os de fora e profundas para os iniciados.

«Imagina que o ouro se tornava chumbo quando o roubavam».

«Escrever uma descrição disto para o público em geral é diabolicamente difícil. Não há nada com que o relacionar».

«Estou certo de que dentro de vinte anos haverá um volume de transações de bitcoin muito grande... ou nenhum volume».

«A rede é robusta na sua simplicidade não estruturada».

Antes de Thiel subir ao palco, um vídeo de 1999 mostrava uma versão mais jovem e mais magra dele, entusiasmado com o futuro do dinheiro online. Quando todos os membros da classe média tivessem um telemóvel com ligação à internet, algo que ele previa acontecer nos cinco anos seguintes, países como a China ou a Índia teriam de fechar as redes de telecomunicações ou abdicar da sua soberania monetária.

Thiel surgiu então pelo lado direito do palco, vestido com um pólo branco. Atirou um maço de notas de cem dólares às primeiras filas: «É uma loucura isto ainda funcionar, sabem?». Porque —perguntou à multidão— é que o bitcoin, que agora valia 813 000 milhões de dólares, não tinha substituído o ouro, que valia 12 biliões de dólares? O bitcoin era um aviso, disse, de que o sistema fiduciário tinha terminado.

SHUTTERSTOCK

Se o bitcoin quer ser usado por milhões, tem de integrar-se em plataformas acessíveis. O PayPal, com mais de 400 milhões de utilizadores ativos, é uma porta de entrada.

WARREN BUFFETT, O INIMIGO N.º 1...

Mostrou um slide que dizia «BTC vs. ETH». Ether era a segunda criptomoeda mais valiosa. Por cima de «BTC» havia uma fotografia de um homem a apontar uma metralhadora à câmara, enquanto por cima de «ETH» havia uma foto do fundador da Ethereum, Vitalik Buterin, na sua versão mais desengonçada e com calças roxas. Por muito inovador e tecnicamente superior que fosse o bitcoin, disse Thiel, era um movimento político, e o que se interpunha no seu caminho eram «os inimigos deste movimento».

«E por isso quero concluir com uma lista de inimigos — afirmou —, pessoas que, creio, estão a travar o bitcoin». Desejava «expô-los». Mostrou um slide de um adversário a que denominou «Inimigo n.º 1». Era Warren Buffett. Eu sabia que Buffett era célebre pela sua prudente estratégia de investimento, que sentia paixão pelo *bridge* e que se comprometera a doar integralmente a sua fortuna. Porém, segundo Thiel, Buffett ocultava um lado negro. Chamou-lhe «o avô psicopata de Omaha». (O crime de Buffett fora classificar o bitcoin como «veneno para ratos»). O inimigo n.º 2 era o diretor executivo do JP Morgan Chase, Jamie Dimon, que exemplificava o que Thiel denominava «o enviesamento do banqueiro nova-iorquino». (Dimon cometera o erro de desprezar o bitcoin, chamando-o «sem valor»). O inimigo n.º 3 era o diretor executivo da BlackRock, Larry Fink. (O seu crime contra o bitcoin não ficou imediatamente claro). Em conjunto, estes homens representavam aquilo a que Thiel, então com 54 anos, chamava «a gerontocracia». Thiel contrapôs estes veteranos a uma imagem da vibrante Miami e a este «movimento juvenil revolucionário. Temos de sair desta conferência e conquistar o mundo!». O público presente no cavernoso espaço

SHUTTERSTOCK

Embora o bitcoin tenha sido o pioneiro em criar dinheiro digital descentralizado, a Ethereum foi mais longe: introduziu os contratos inteligentes, permitiu que as transações fossem programáveis...

NAKAMOTO ERA O MAIOR DETENTOR DE A MOEDA E ALGUÉM QUE PODIA INFLUENCIAR SIGNIFICATIVAMENTE O SEU PREÇO

ASC/ROOTSTOCK

Sergio Demian Lerner defende que o desaparecimento de Satoshi foi crucial para que o bitcoin se tornasse um sistema descentralizado.

irrompeu em vivas. Mais tarde, soube-se que, na altura deste discurso, a empresa de investimento de Thiel se desfizera de uma grande posição em bitcoins que mantivera durante oito anos. Em Miami, Thiel concluiu o seu discurso dizendo à multidão que os «inimigos» que nomeara eram «extensões do Estado». O bitcoin, pelo contrário, não era uma empresa e não tinha conselho de administração. «Não sabemos quem é Satoshi», acrescentou Thiel para enfatizar».

Saí de lá com o meu amigo Andy, também ele investidor de capital de risco.

—Que loucura —disse o Andy, abanando a cabeça.

Não sabemos quem é Satoshi. Em 2011, fora o programador anónimo de uma moeda experimental que interessava sobretudo a uma comunidade marginal. Dez anos depois, era o mítico fundador de um projeto com uma capitalização de mercado de um bilião de dólares, o que o tornava o nono ativo mais valioso do mundo, logo abaixo da Tesla e acima da Meta (Facebook). O sucesso de Nakamoto em permanecer anónimo, apesar dessa mudança, tornara-se um dos seus maiores feitos. E era incrivelmente rico.

Um informático chamado Sergio Demian Lerner, através de uma engenhosa análise da primeira *blockchain*, estimou que quase 1,1 milhões de bitcoins tinham sido extraídos pelas mesmas máquinas, presumivelmente as de Nakamoto. O valor dessas moedas, nesse momento, era de 40 mil milhões de dólares. Nakamoto era, de longe, o maior detentor da moeda e alguém que podia influenciar significativamente o seu preço.

ASCENSÃO E QUEDA DO BITCOIN

Quando a plataforma de negociação de criptomoedas Coinbase foi para bolsa na primavera de 2021, o que lhe deu um valor de mercado instantâneo de 86 mil milhões de dólares, um dos fatores de risco enumerados no prospeto que a empresa

ISTOCK

Desde a sua criação, o bitcoin tem sido comparado ao ouro pela sua escassez, resistência à censura e o seu papel como reserva de valor.

apresentou à Comissão de Valores Mobiliários dos Estados Unidos (SEC) era a identificação pública de Nakamoto ou a transferência do seu tesouro de bitcoins. Não era difícil imaginar cenários em que a identidade de Nakamoto — quais eram os seus motivos e intenções — pudesse ser relevante. O próprio Thiel especulara que Nakamoto estaria entre os seus companheiros participantes numa conferência de criptografia financeira na ilha de Anguila, no ano 2000. Falando com o meu amigo Andy à porta do centro de congressos, onde se acotovelavam miúdos desorientados, a pele salpicada de borbulhas alaranjadas, a embebedarem-se da curiosa mistura de fervor revolucionário, hedonismo de Miami e contabilidade, mencionei a minha recente busca por Nakamoto. Andy perguntou-me por que falava tão baixo. No universo do bitcoin, expliquei, sem levantar a voz, o mistério de Nakamoto era considerado necessário, uma caraterística mais do que um defeito. Para ser verdadeiramente descentralizado, o bitcoin precisava de um nascimento virginal. Privá-lo de uma figura humana, um indivíduo imperfeito com uma identidade particular que poderia ser aceitável para este grupo mas não para aquele, dava-lhe a melhor hipótese de ser recebido nos seus próprios termos e adotado em massa.

E assim, entre os bitcoiners, o alias Nakamoto tornara-se sagrado, e desencorajavam-se investigações sobre ele. Enquanto algumas pessoas conjeturavam que o criador do bitcoin se escondera principalmente para sua proteção, para não ser processado por evasão fiscal ou atacado fisicamente pelo seu pecúlio de moedas, a opinião comum era a de que agira de forma altruísta. Os bitcoiners mais fervorosos

OS BITCOINERS MAIS FERVOROSOS TRATAVAM A NAKAMOTOLOGIA COMO UMA ESPÉCIE DE BLASFÉMIA: NAKAMOTO ERA SAGRADO

tratavam a Nakamotologia como uma espécie de blasfémia, semelhante a perguntar a cientologistas por Xenu.

Existia também um historial caótico de jornalistas que tinham tentado desvendar o mistério. Alguns repórteres ficaram em evidência por excesso de confiança ou credulidade. Um escritor envolveu-se numa ação judicial que lhe custou mais de 100 000 dólares. Pelo menos um repórter recebeu «ameaças de morte». A vida de um cidadão comum foi destruída por um linchamento mediático. Prevalecia, então, uma antipatia generalizada para com os jornalistas que tentavam lançar luz sobre este segredo. A isto somava-se um desprezo alargado pela cobertura das criptomoedas nos meios tradicionais. Um site chamado Bitcoin Obituaries catalogava mais de 440 artigos que tinham anunciado prematuramente a iminente desaparecimento do bitcoin. Um deles era o meu artigo de 2011 na *Wired*, intitulado «Ascensão e queda do bitcoin».

«POR FAVOR, NÃO TENTE APROXIMAR-SE DE MIM NA CONFERÊNCIA»

Ainda assim, a principal razão por que viera a Miami era para assistir a uma palestra de Nick Szabo nesse mesmo dia. A meio da tarde, Nick subiu ao palco Nakamoto, vestido com uma camisa por fora das calças, um microfone sem fios preso à cabeça e o cabelo, agora grisalho, bastante curto. Ao vivo, Nick parecia evitar a interação social presencial. A rara exceção era alguma apresentação ocasional em palco, com abundantes diapositivos e sem período de perguntas: uma entrada de blogue ao vivo. Um ano antes, quando um repórter da *Harper's* mencionou que planeava assistir a uma das suas palestras, Nick respondeu: «Por favor, não tente aproximar-se de mim na conferência».

«Hoje vou falar — começou Nick — de alguns dos sonhos e ideias que, creio, influenciaram o bitcoin». As pessoas por detrás destes conceitos e ideias foram «pioneiros da era pré-bitcoin» que ajudaram a materializar «sonhos libertários», elementos como «despolitizar o dinheiro» e «fazer cumprir contratos de forma não violenta». Nick prestou homenagem a vários informáticos cujo trabalho preparara o terreno para o bitcoin. Era uma versão descentralizada da história da origem da moeda.

Apesar dos esforços dos organizadores para embelezar estas palestras — meteoros rasgavam uma paisagem lunar no ecrã situado atrás de Nick —, a sua apresentação resumia-se a uma lista sóbria de nomes e tópicos que mal insinuavam a rica história que encerravam. Nick só se animou quando falou dos *cypherpunks* e dos extropianos e dos seus velhos amigos Tim May e Hal Finney. O que mais me interessava ouvir era como é que ele próprio se colocaria nessa linhagem, porque estava convencido de que Nick era Satoshi Nakamoto. ■

Estudos sobre Satoshi

Satoshi Nakamoto, cuja identidade real nunca foi confirmada, desapareceu em 2011 sem revelar quem era na realidade, embora existam múltiplas teorias sobre quem poderia ser: Nick Szabo, Hal Finney, Dorian Nakamoto ou mesmo um grupo de pessoas.

SHUTTERSTOCK

Quando a minha reportagem saiu na *Wired*, no final de 2011, dois jornalistas já tinham proposto candidatos a Satoshi Nakamoto. Joshua Davis, que fazia cobertura para a *The New Yorker*, defendia a tese de que Nakamoto era um criptógrafo experiente e apresentou-se na Crypto, a conferência anual do setor, em Santa Bárbara. Ali, identificou um participante irlandês de vinte e três anos, de cabelo comprido, chamado Michael Clear. Clear preenchia vários dos requisitos de Nakamoto: era pós-graduando em Criptografia, usava ortografia britânica, era reservado (a sua página de perfil no Trinity College, ao contrário das dos colegas, não exibia fotografias nem números de telefone), estudava redes entre pares e tinha um brilho invulgar (em licenciatura fora o melhor da sua turma em Informática), além de ter trabalhado em *software* de negociação de câmbios.

«MESMO QUE FOSSE, NÃO TO DIRIA»

Nas escadas em frente ao edifício onde decorriam as aulas, Davis conseguiu trazer ao de cima um dado relevante: Clear sabia programar em C++, a linguagem em que o bitcoin foi programado, mas, quando Davis lhe perguntou diretamente se era Nakamoto, Clear sorriu e não respondeu; ofereceu-se, sim, para «rever» o desenho do bitcoin para ele. Uma semana depois, Clear enviou um e-mail a Davis informando-o de que cria poder identificar Nakamoto. Ao que parece, a curiosidade sobre a identidade de Satoshi ficara-lhe a roer, mas mostrava-se ambivalente e explicou a Davis que «seria injusto publicar uma identidade quando a pessoa ou pessoas tomaram medidas importantes para permanecer no anonimato», ao mesmo tempo que adiantava o nome de «um indivíduo que corresponde ao perfil do autor em muitos níveis».

Essa pessoa, um investigador finlandês de moeda virtual chamado Vili Lehdonvirta, também se riu quando Davis lhe perguntou se era Nakamoto, respondendo que não tinha os conhecimentos necessários de C++ nem experiência em criptografia. Davis achou a negativa convincente e voltou a Clear, sugerindo que talvez Clear fosse Nakamoto, afinal. Desta vez, Clear disse: «Não sou o Satoshi, mas, ainda que fosse, não to diria.» E sublinhou o que se estava a tornar o refrão na moda entre os bitcoiners: a identidade de Nakamoto não deveria importar. Essa era a essência de uma moeda descentralizada. O anonimato era o seu maior atributo. Após a publicação do artigo de Davis, Clear negou veementemente ser Nakamoto. Tinha falado «a brincar» quando se mostrou evasivo com Davis. «Nunca me poderia ser atribuído, ainda que remotamente, o engenho e o trabalho árduo de outra pessoa.»

Entretanto, um repórter da *Fast Company* chamado Adam Penenberg, que anteriormente desmascarara as fraudes jornalísticas de Stephen Glass, deparou-

PENENBERG HAVIA FICADO CATIVADO PELO MISTÉRIO DE NAKAMOTO E PROCUROU NO GOOGLE FRASES DISTINTIVAS DOS SEUS ESCRITOS

NIALL CARSON

Michael Clear, durante a sua intervenção na Web Summit realizada no RDS, em Dublim, partilha a sua análise e perspetivas sobre a evolução do bitcoin.

-se com uma coincidência surpreendente. Também ele se deixara cativar pelo mistério de Nakamoto e procurou no Google frases distintivas dos escritos de Nakamoto. Ao pesquisar uma delas, «computacionalmente impossível de reverter», obteve um resultado intrigante: um pedido de patente para um método de comunicações seguras que continha essa mesma frase fora submetido a 15 de agosto de 2008, três dias antes de Nakamoto registar o *bitcoin.org*. «Que coincidência», escreveu Penenberg. A patente incluía três inventores: Neal King e Charles Bry, que viviam em Munique, e Vladimir Oksman, residente em Nova Jérsia. Penenberg encontrou outras coincidências: Bry visitara a Finlândia seis meses antes de o *bitcoin.org* ser registado através de uma empresa finlandesa de internet. A página de Facebook de King estava repleta de mensagens contra Wall Street, e as críticas na Amazon que King escrevera lembravam, na opinião de Penenberg, as publicações de Nakamoto no fórum.

Embora King não usasse ortografia britânica, Penenberg já acreditava que Nakamoto utilizara anglicismos como «pistas falsas, colocadas ali para despistar os perseguidores».

Quando Penenberg contactou Bry, o informático respondeu: «Espero não te dececionar demasiado ao dizer-te que não sou o Satoshi» e podia afirmar «com absoluta certeza» que nenhum dos seus co-inventores o era. King disse a Penenberg que o enfoque da patente era muito diferente do do bitcoin, que nunca ouvira falar do bitcoin «até surgir esta questão» e que, agora que lera sobre o assunto, lhe parecia «uma solução à procura de um problema».

Penenberg considerou os argumentos de King pouco convincentes. Sem pretender ter identificado Nakamoto, acreditava que as suas provas circunstanciais eram «muito mais convincentes» do que as de Davis. Tive de concordar com ele e arrependi-me de não ter pensado em usar o seu método de procurar frases únicas no Google.

AMERICAN PROGRAM BUREAU, INC.

Adam L. Penenberg, professor de jornalismo na Universidade de Nova Iorque e editor da *PandoDaily*, publicação *online* de notícias tecnológicas.

Nos dois anos seguintes, não se passou grande coisa no incipiente campo dos estudos sobre Satoshi. Então, a 1 de dezembro de 2013, alguém que usava o pseudónimo Skye Grey publicou um argumento, num blogue recém-criado chamado *Like in a Mirror*, intitulado «Satoshi Nakamoto é (provavelmente) Nick Szabo».

Grey, tal como Penenberg, examinara o livro branco em busca de frases invulgares e seguiu-lhes o rasto na web. Entre elas figuravam termos como servidor de carimbo de tempo e terceiro de confiança, que o conduziram a uma série de artigos de Nick sobre bit gold. Grey reconheceu que Nakamoto provavelmente assimilara o trabalho de Nick e poderia exprimir-se de forma semelhante, pelo que também analisou o que chamou «expressões de conteúdo neutro».

QUEM ESCREVEU O LIVRO BRANCO?

Também neste caso a coincidência foi notável. Ao comparar algumas «expressões do livro branco» que também surgiam nos artigos de Nick Szabo com a sua presença na literatura académica sobre criptografia, Grey destacou «o uso repetido de portanto sem vírgulas de separação, contra a convenção; a expressão pode caraterizar-se, frequente no blogue do Nick (encontrada em 1% dos documentos de criptografia), e o uso de para os nossos propósitos ao descrever hipóteses (presente em 1,5% dos documentos de criptografia)».

«Ou o Nick escreveu o livro branco ou foi escrito por alguém a imitar o estilo de escrita de Nick», argumentou Grey. Reconheceu também que a grafia *favour*, utilizada por Nakamoto, não era usada por Nick. Isso levou Grey a concluir que «é muito provável que o documento tenha tido vários autores» ou, como acreditava Penenberg, que as expressões britânicas tinham sido incluídas como distração deliberada.

Grey considerou que outras provas também apontavam para Nick. Porque é que o livro branco citava Adam Back e Wei Dai, mas não Nick, cujo trabalho era claramente uma inspiração direta? Porque é que Nick, um dos mais persistentes defensores do dinheiro digital descentralizado, esperara meses após o lançamento do bitcoin para o mencionar, de passagem, numa frase no final de um extenso ensaio? Grey observou que, em abril de 2008, seis meses antes de o livro branco ser publicado, Nick escrevera no seu blogue que o bit gold «beneficiaria enormemente de uma demonstração, um mercado experimental (com, por exemplo, um terceiro de confiança a substituir a complexa segurança que seria necessária num sistema real). Alguém quer ajudar-me a programar um?». E assinalou que, depois do lançamento do bitcoin, o projeto bit gold, no qual Nick estivera ativamente interessado apenas meses antes, «caiu no silêncio».

JAN3

Skye Grey publicou num blogue: «Satoshi Nakamoto é (provavelmente) Nick Szabo (na imagem)».

PACIÊNCIA E PREVISÃO

Grey postulou que, no mínimo, Nick era o autor principal do livro branco. Talvez o bitcoin tenha sido programado por outra pessoa. «Parece muito mais provável que alguém com o perfil de Satoshi, que inventasse o bitcoin, contactasse primeiro o "pai" original do projeto, em vez de começar por dedicar todos os seus recursos a lançar aquilo que, em grande medida, era a ideia preferida de outrem.»

Grey explicou mais tarde que o motivara «a simples curiosidade. Gosto de mistérios». E defendeu a sua investigação, que reconheceu «não ter sido bem recebida»: «Quando alguém começa a ter um grande impacto no mundo, perde o direito ao anonimato.» Justificou a publicação das suas conclusões «para responder à preocupação de que alguém mal-intencionado pudesse ter criado o bitcoin».

Outros investigadores chegaram a conclusões semelhantes. Dominic Frisby, um comediante e escritor financeiro inglês, centrou-se na combinação de conhecimentos que Nakamoto teria de ter: «programação informática, matemática, bases de dados, contabilidade, sistemas entre pares, propriedade digital,

DEPOIS DO LANÇAMENTO DO BITCOIN, O BIT GOLD, EM QUE NICK SZABO TRABALHARA, «CAIU NO SILÊNCIO»

direito, contratos inteligentes, criptografia e história monetária». Acreditava que a forma como o bitcoin fora lançado sugeria «experiência em empresas emergentes de tecnologia de código aberto». As defesas impenetráveis do *software* revelavam um *hacker* perito em segurança; a prosa de Nakamoto, a de um escritor; e o seu pseudónimo, alguém familiarizado com o sigilo. Nakamoto revelou paciência, previsão, humildade, integridade e uma acuidade quanto à psicologia humana. Apenas um libertário ou um *cypherpunk* teriam a motivação e o instinto necessários para apresentar a sua criação. Frisby centrou-se na data de nascimento que Nakamoto registou no site da Fundação P2P: 5 de abril de 1975. A 5 de abril foi quando, em 1933, o presidente Franklin D. Roosevelt declarou ilegal a posse de ouro por cidadãos norte-americanos, e 1975 foi o ano em que lhes foi novamente permitido possuir esse metal. Frisby assinalou que, em 2007, Nick, que acabara de se licenciar em Direito aos 42 anos, dispunha de tempo para abraçar outro grande projeto.

Embora Frisby tenha construído um caso circunstancial convincente, quando o apresentou a Nick, este respondeu: «Receio que te tenhas enganado ao fazer-me *doxxing* como Satoshi, mas já estou habituado.» O *doxxing*, que anteriormente significara revelar dados pessoais como a morada ou o número da Segurança Social de alguém, perdera claramente o seu significado para algumas pessoas.

Nem as conclusões de Grey nem as de Frisby pareciam sustentar-se. Ambos tinham sublinhado a decisão de Nakamoto de lançar o bitcoin através de um artigo de cunho académico e a sua atividade de publicação, que parecia intensificar-se durante o verão. Grey escreveu que «Nick é um professor com um

SHUTTERSTOCK

Em 1933, Roosevelt declarou ilegal a posse de ouro por cidadãos norte-americanos. Só em 1975 lhes voltou a ser permitido possuir este metal.

NICK CONSEGUIA ATRAIR GRANDES AUDIÊNCIAS APESAR DO SEU ESTILO POUCO ANIMADO E DE TEMAS RECORRENTES

historial de publicações significativo». Mas Nick não era nem nunca fora professor. E, embora tivesse escrito extensamente no seu blogue, e com erudição, nunca publicara academicamente. Alguns dos termos que Grey interpretara como provas irrefutáveis, como assinaturas digitais e provas criptográficas, eram correntes em criptografia.

IMPOSSÍVEL EXCLUÍ-LO COMO CANDIDATO

No ano seguinte, Nathaniel Popper, repórter do *New York Times*, confrontou Nick num encontro do setor, em casa de um gestor de *hedge funds* em Lake Tahoe. Popper fora convidado por cobrir a criptomoeda e Nick comparecera como funcionário de uma nova empresa emergente ligada ao bitcoin chamada Vaurum. Nos cocktails antes do jantar, quando surgiu o tema Nakamoto, Nick disse a um pequeno grupo: «Bem, direi isto, na esperança de esclarecer as coisas: não sou o Satoshi e não sou professor universitário.» A certa altura, Popper interpelou Nick na cozinha e este reconheceu: «Existem todos esses paralelismos e eu acho graça, tal como muita outra gente.» Mais tarde, Nick enviou um e-mail a Popper com uma negação definitiva: «Como disse muitas vezes, toda esta especulação é lisonjeira, mas errada: eu não sou o Satoshi.» Pouco depois, Popper noticiou que Nick abandonara a Vaurum «depois de ficar nervoso com a exposição pública».

Grey, Frisby e Popper assinalaram que Nick republicara os seus antigos ensaios sobre bit gold depois de outubro de 2008 e sugeriram que o fizera para que parecesse tê-los escrito após o bitcoin, a fim de desviar de si as suspeitas. Contudo, mesmo depois de o *New York Times* apontar Nick como a pessoa que os peritos de Silicon Valley consideravam ser Nakamoto, a ausência de provas contundentes manteve esta teoria numa zona cinzenta que não chegaria a esclarecer-se.

Na primavera de 2022, onze anos depois de eu ter perguntado a Nick se era Satoshi Nakamoto, e apesar das suas negativas então e em inúmeras ocasiões posteriores, continuava a ser impossível excluí-lo como candidato. O mundo, por vezes, tratava-o como se fosse Nakamoto, mas de maneiras peculiares. A Universidad Francisco Marroquín, na Guatemala, destacando a sua «investigação em contratos digitais e moeda digital», concedeu-lhe um doutoramento *honoris causa* e uma cátedra. O *podcaster* Tim Ferriss entrevistou-o durante duas horas e meia, apresentando-o como «o mestre silencioso das criptomoedas», sem mencionar nem perguntar uma única vez pelo evidente pano de fundo da presença de Nick no programa. Nick conseguia atrair grandes audiências nas suas apresentações, apesar do seu estilo pouco animado e de temas recorrentes.

Havia mais indícios que apontavam para Nick, mas esse facto diluíra-se, de algum modo, no ruído de outras conjeturas sobre Nakamoto. Em todo o caso, havia agora razões adicionais para voltar a centrar atenções nele. ■

Anónimo

Mark Felt e Satoshi Nakamoto têm sido vistos como heróis por uns e como figuras problemáticas por outros, dependendo da perspetiva política e filosófica

UNITED STATES CONGRESS

A primeira coisa que notei nas minhas novas reflexões sobre «Nick como Nakamoto» foi que já não atribuía grande peso aos seus desmentidos. A minha aceitação anterior desses desmentidos fora ingénua. Não tinha que ver com a sua honestidade, ou com a falta dela. Simplesmente, familiarizara-me com outros casos em que alguém que usava um pseudónimo tinha sido desmascarado.

Em 1996, um professor de Inglês chamado Donald Foster identificou o jornalista Joe Klein como o autor anónimo de um romance de grande sucesso sobre a campanha presidencial de Clinton em 1992, intitulado *Cores primárias*, com base em semelhanças de estilo. Klein negou ser o autor. «Pelo amor de Deus, não fui eu que o escrevi», exclamou a um repórter do *New York Times*. Deixou uma mensagem de voz negando a autoria, negou-o na CBS News, onde era comentador, e negou-o perante os seus próprios colegas na *Newsweek*, chegando mesmo a permitir que a revista publicasse especulações que apontavam outros suspeitos anónimos. Por fim, Klein admitiu que, efetivamente, era o autor do livro.

MARSHA MILLER

Joe Klein, jornalista e autor de *Cores primárias* (1996), sátira à campanha presidencial de Bill Clinton.

«GARGANTA FUNDA»

Mark Felt, antigo diretor-adjunto interino do FBI, afirmou, repetida e explicitamente, que não era «Garganta Funda», a fonte secreta cuja ajuda permitiu aos repórteres do *Washington Post* Bob Woodward e Carl Bernstein desvendar o Watergate. Felt depôs perante um grande júri, sob pena de perjúrio, que não era «Garganta Funda» (antes de retirar precipitadamente o depoimento). Ao *The Wall Street Journal* sugeriu a teoria de que «Garganta Funda» poderia ser «um compósito» de várias pessoas. Nas suas próprias memórias, Felt sublinhou que «nunca fiz fugas de informação, nem a Woodward nem a Bernstein nem a mais ninguém!». Anos mais tarde, quando um amigo do filho de Bernstein, Jacob, num campo de férias, disse ao *The Hartford Courant* que Jacob identificara Felt como «Garganta Funda», Felt declarou ao jornal: «Não, não sou eu. Teria feito melhor. Teria sido mais eficaz». Finalmente, Felt admitiu que era, de facto, «Garganta Funda».

EM 1996, DONALD FOSTER IDENTIFICOU JOE KLEIN COMO O AUTOR ANÓNIMO DO ROMANCE *CORES PRIMÁRIAS*

Estas pessoas negaram-no sempre. As negações de Felt, refletiu Woodward mais tarde, «apenas consolidaram a minha triste compreensão» de que qualquer pessoa que esteja em apuros, ou julgue estar, dirá o que for preciso para se proteger e sair do aperto. Com o tempo, todos acabamos por nos vincular a uma versão da história das nossas vidas. A simplificação e a repetição solidificam o relato e tendemos a manter-nos nessa identidade». (Woodward sabia do que falava, depois de mentir ao seu colega do *Washington Post*, Richard Cohen, que se preparava para escrever uma coluna identificando Felt como «Garganta Funda», até que Woodward o desmentiu). Quando alguém já se comprometera com o anonimato e aceitara os incómodos de manter uma identidade encoberta, acrescentar uma mentira explícita era apenas mais um passo.

O problema foi ilustrado por Ralph Merkle, co-inventor da criptografia de chave pública, cujo trabalho foi um dos oito artigos citados no livro branco do Bitcoin, e que inventara uma estrutura de dados — as árvores de Merkle — em que o *software* do Bitcoin assenta para construir os blocos na *blockchain*. Inevitavelmente, figurava na longa lista de possíveis candidatos a ser Nakamoto.

Quando lhe perguntaram sobre o assunto numa entrevista, disse:

—Nego ser o Satoshi.

—Então posso riscar o seu nome da lista também?

—Claro. Mas esperas mesmo que Satoshi diga: «Sim, sou o Satoshi»?

—Se fosses o Satoshi, dir-me-ias que és o Satoshi?

—Valha-me Deus, não! ■

ASC

Ralph C. Merkle é um cientista informático e inventor norte-americano, pioneiro fundamental da criptografia; sem as suas inovações, o Bitcoin tal como o conhecemos não existiria.

Uma espetacular demonstração de retrospetiva

Nick Szabo colecionava notas da época da banca livre, estudava contas de concha, admirava moedas sem rostos de políticos. Depois, concebeu uma moeda sem governo, sem bancos, sem rostos. Apenas matemática pura.

ISTOCK

Muitas outras pistas apontavam para Nick Szabo. O nível de segurança operacional de Nakamoto indicava tratar-se de alguém que tinha refletido profundamente e praticado a arte de evitar todas as formas como a internet pode associar dados pessoais. «A sua capacidade para não deixar rasto é praticamente inigualável — explicou-me Ray Dillinger, um criptógrafo que, juntamente com Hal Finney, tinha revisto o código de Nakamoto antes do lançamento do bitcoin —. Nunca conheci ninguém que realmente conseguisse manter o anonimato na internet quando assim o desejava».

«SE NÃO O ENTENDES, NÃO POSSO AJUDAR-TE MAIS»

Nick refletira sobre estas questões durante quinze anos antes de surgir o bitcoin. «Na minha limitada experiência a criar pseudónimos na internet, a necessidade constante de evitar deixar pistas do meu verdadeiro nome distraiu-me bastante», comentou Nick aos seus companheiros *cypherpunks* em 1993. Tudo, desde os ficheiros partilhados aos hábitos ortográficos, podia denunciar-te. «Os perigos espreitam por todo o lado. Com as nossas ferramentas atuais é praticamente impossível manter um pseudónimo ativo durante um período prolongado perante um adversário suficientemente determinado, e é bastante complicado manter sequer um mínimo de segurança aceitável».

As negativas de Nick, quando lhe perguntaram se era o Nakamoto, tinham sido lacónicas. O facto de o livro branco do bitcoin não reconhecer a influência evidente de Nick, além de um comentário posterior no *BitcoinTalk* em que Nakamoto escreveu que «O Bitcoin é uma implementação da proposta b-money de Wei Dai… nos *cypherpunks*… em 1998 e da proposta de bitgold de Nick Szabo», continuava sem explicação. A dívida para com o trabalho de Nick era tão óbvia que o *cypherpunk* James Donald, a primeira pessoa a responder a Nakamoto no *Metzdowd* no final de 2008, se referiu aos bitcoins como «moedas bitgold». Enquanto comentava que a melhor forma de dissipar as dúvidas sobre o bitcoin seria publicar o seu código-fonte, Hal Finney respondeu: «Descobri que existe um projeto no SourceForge criado para o bitgold, embora ainda não contenha código».

Porque é que Nick nunca se tinha mostrado ofendido com a omissão do seu trabalho nas citações do livro branco? Se estivesse a ser modesto, porque não teria ao menos falado em nome do Hal e dito: «Sim, é estranho que o RPOW do Hal não tenha sido citado no livro branco»? Nunca dissera: «Quem me dera poder reclamar o mérito, mas os meus conhecimentos de C++ não chegam nem de longe aos de Satoshi». Também não disse: «Compreendo porque é que todos pensam que sou o Satoshi, mas vamos desfazer este rumor: este é o chefe para quem

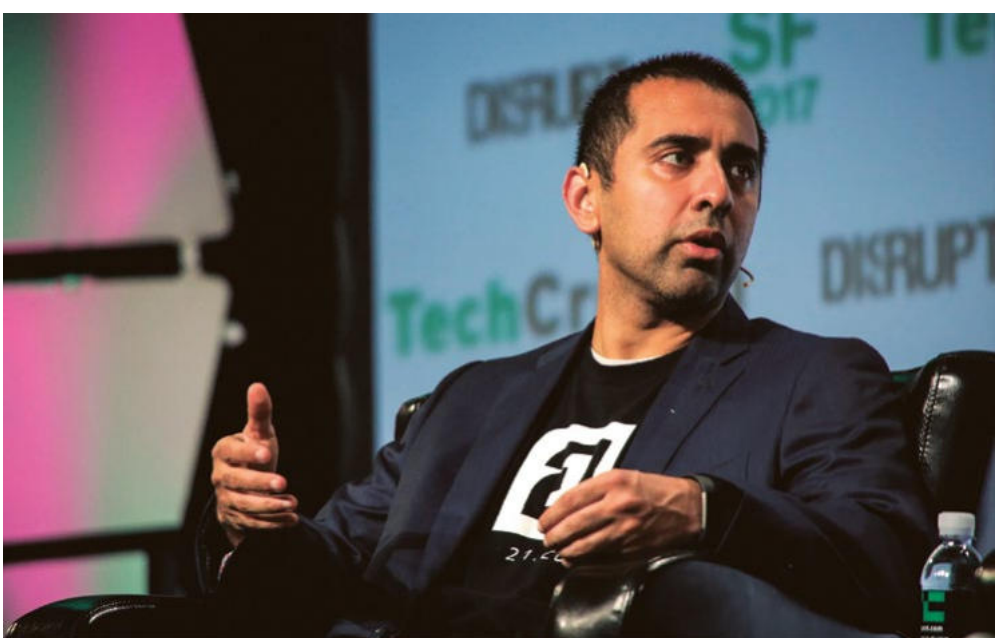
PORQUE É QUE O NICK NUNCA SE TINHA MOSTRADO OFENDIDO COM A OMISSÃO DO SEU TRABALHO NAS CITAÇÕES DO LIVRO BRANCO?

trabalhava em 2008 e 2009, e esta é a pessoa com quem mantinha uma relação. Ambos podem confirmar que eu trabalhava doze horas por dia noutro projeto e que, quando o Nakamoto conseguiu fazer o que eu andara a tentar durante anos, fiquei paralisado de inveja».

Nick não devia explicações a ninguém, mas as suspeitas perseguiam-no precisamente porque raramente reconhecia as numerosas razões para pensar que poderia ser o Nakamoto. Isso levava as pessoas a crer que ou era o próprio Nakamoto, ou não lhe importava que o pensassem.

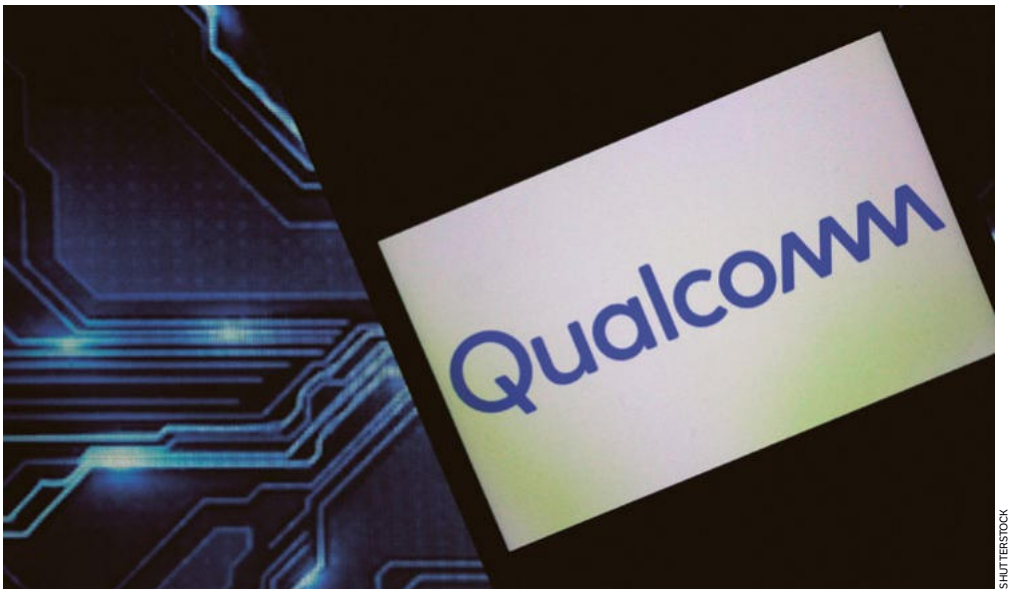
Quase tão significativas como o silêncio de Nick foram as raras exceções a esse silêncio. Depois de Gwern Branwen argumentar que o bitcoin não era assim tão inovador, Nick escreveu uma longa réplica em que qualificou o argumento de Branwen como «uma espetacular demonstração de retrospetiva». Quando um investidor de Silicon Valley chamado Balaji Srinivasan exerceu os seus poderes de moderação num canal do Telegram que ostenta o nome do fundador do bitcoin, Nick troçou de Srinivasan pelas suas «patéticas regras corporativas», que pareciam tratar o nome de Nakamoto como sua propriedade e censurar pessoas sob a sua égide. E Nick via-se claramente como o pai das criptomoedas quando escrevia: «O conhecimento da longa história do dinheiro não governamental foi uma das inspirações para a invenção original da criptomoeda com confiança minimizada».

Quando, em 2022, me mergulhei nos volumosos escritos de Nick na internet, foi fácil ouvir ecos do fundador do bitcoin. Nakamoto escreveu uma vez: «Se não acreditas em mim ou não o entendes, não tenho tempo para tentar convencer-te, lamento». Nick escreveu uma vez: «Se não o entendes, não posso ajudar-te mais». Voltei a olhar para um longo correio eletrónico que Nick me enviara em 2011 e vi que, tal como Nakamoto, usava dois espaços após um ponto e jargão da



ASC

Balaji S. Srinivasan é um empresário, investidor e tecnólogo norte-americano, figura muito influente no mundo das criptomoedas e da tecnologia *blockchain*.



SHUTTERSTOCK

Nick Szabo, pioneiro dos contratos inteligentes, investiu a maior parte das suas poupanças na Qualcomm quando ninguém acreditava na telefonia móvel digital.

internet, incluindo BTW. Nick sentia-se à vontade com os mesmos vocabulários e referências que Nakamoto, desde a obra do economista austríaco Carl Menger até ao conceito de equilíbrio do pioneiro da teoria dos jogos, John Nash.

«O design admite uma enorme variedade de tipos de transações possíveis que concebi há anos — escrevera Nakamoto —. Transações de custódia, contratos de caução, arbitragem por terceiros, assinaturas de múltiplas partes, etc.». Nick, em 1994, escreveu: «Estou particularmente interessado na arte de redigir contratos e de desenhar transações para serviços de dados online», e fez um desvio de três anos, já na meia-idade, para frequentar a Faculdade de Direito.

«O REALISMO NÃO DESTRÓI OS SONHOS»

Muitos tinham falado do dinheiro do futuro, mas o bitcoin foi o primeiro sistema de dinheiro digital descentralizado que funcionou. Nick sempre ancorara os seus sonhos num rigor teimoso, desdenhando os utópicos frágeis como «gente da Hello Kitty». Filtrava cada discussão através de uma lente pragmática, fazendo contas ao que era exequível no imediato. Acreditava que os projetos espaciais deviam ser impulsionados pelo mercado: «Primeiro temos de satisfazer as necessidades das pessoas, e depois eles virão», e não «um caso de assistência social». No início da década de 1990, arriscou o seu próprio dinheiro, investindo a maior parte das poupanças em empresas na vanguarda da tecnologia espacial, como a Qualcomm e a Orbital Sciences. Quando as pessoas usavam o termo contabilístico, ele ofendia-se e fazia uma análise de fluxos de caixa numa folha de cálculo, por exemplo, sobre como deslocar asteroides para terraformar Vénus. Não queria apenas saber o que era cientificamente possível, mas também o que era economicamente provável. «O realismo não destrói os sonhos — escreveu —. Dá-nos uma forma de os tornar realidade».

FALAVA-SE DO DINHEIRO DO FUTURO, MAS O BITCOIN FOI O PRIMEIRO DINHEIRO DIGITAL DESCENTRALIZADO QUE FUNCIONOU

Nick também fizera um estudo aprofundado sobre as origens do dinheiro. Com a intuição de um arqueólogo no que toca à moeda física, deleitava-se com a variedade de objetos que, historicamente, tinham servido de dinheiro, desde contas de conchas de caracol a cascas de ovo de avestruz e marfim de mamute. Fascinavam-no expressões como «desgranar» que derivavam das contas de concha de amêijoa conhecidas como *wampum*. Colecionava notas da era da banca livre do século XIX, emitidas por corporações como o Boone County Bank Indiana e a Great Western Railroad Company, que lhe pareciam belíssimas e «notavelmente isentas de rostos de políticos».

TODD WHITE

Tim Ferriss é um empresário, autor, podcaster e investidor norte-americano, conhecido pelo seu livro *The 4-Hour Workweek*.

Um argumento recorrente contra Nick, sempre que alguém sugeria que poderia ser o Nakamoto, era o de que não era conhecido como programador. No entanto, o Nick especializou-se em Informática na universidade e, após se licenciar, desempenhou vários cargos na área do *software*. Vasculhando os vestígios dos primórdios da internet, descobri que, no início dos anos 1990, promovera a sua experiência em «arquitetura e engenharia de *software*», as suas «amplas habilidades de hacking» e o seu conhecimento de C/C++ e Windows/DOS. Referiu que tinha nada menos do que seis livros de C/C++ em cima da secretária. Noutra ocasião, escreveu: «Teço um código malvado».

Também estudara japonês e sentia fascínio pela cultura japonesa. As iniciais de Nakamoto, SN, eram o inverso das de Nick, o que batia certo com a convenção tanto japonesa como húngara de antepor o apelido ao nome: na Hungria, o nome de Nick seria Szabo Nikolas e, no Japão, seria, digamos, Szaboshi Nickamoto.

Depois, Nick apareceu no podcast de Tim Ferriss em 2017. A dada altura da entrevista, enganou-se: «Desenhei o bitcoi-gold com duas camadas». Quando vi o Nick falar em Miami, voltou a cometer um deslize: «Na minha implementação, ou no meu design, do bit gold…».

Pensava: «Como é possível que o Nick não seja o Nakamoto?». ■

A lista de verificação de Satoshi

A pergunta errada é «Quem é Satoshi?». A pergunta certa é «Porque é que nunca tirou a máscara?». A máscara dos Anonymous lembra-nos que algumas revoluções só resultam se o revolucionário desaparecer.

SHUTTERSTOCK

DUQUESNE UNIVERSITY

O professor Patrick Juola é docente de Ciências da Computação na Universidade Duquesne, especializado em análise forense linguística e estilometria computacional.

No verão de 2022, depois da minha visita a Patrick Juola — o perito que identificou J. K. Rowling — no seu laboratório de Pittsburgh, colei num quadro cinzento na parede do meu gabinete uma folha de cálculo com mais de uma centena de candidatos propostos para Satoshi Nakamoto. Lá estavam os suspeitos do costume, na sua maioria *cypherpunks*. Havia nomes menos conhecidos oriundos de áreas afins, como a matemática, a criptografia e a economia. Alguns eram programadores envolvidos no projeto de *software* do bitcoin. Outros, criadores de criptomoedas mais recentes. Muitos eram simplesmente pessoas famosas e brilhantes: Bill Gates, Steve Jobs, John Nash (o matemático imortalizado em *Uma Mente Brilhante*). Para cada candidato enumerei argumentos a favor e contra. Estava no âmago do jornalismo de investigação: desvendar verdades que alguém se empenhava em silenciar. «Um bom quebra-cabeças é algo justo — disse em tempos Ernő Rubik (o criador do famoso cubo) —. Ninguém mente, tudo é muito claro, o problema depende apenas de ti.» Não tinha a certeza de que o enigma de Nakamoto obedecesse a esses requisitos, mas era reconfortante mergulhar por completo no projeto.

«PODEMOS GANHAR UM NOVO TERRITÓRIO DE LIBERDADE»

Por cima da folha de cálculo, colei uma lista de verificação, uma coluna de critérios que qualquer candidato plausível a ser Nakamoto teria de cumprir:

—Ferramentas de *software*
—Peculiaridades do código
—Idade
—Geografia

—Horário
—Uso do inglês
—Nacionalidade
—Estilo narrativo
—Política
—Circunstâncias de vida (Como é que Nakamoto arranjou tempo para lançar o bitcoin? Porque é que abandonou o projeto naquela altura?)
—Currículum (Não sou advogado)
—Perfil emocional (humilde, confiante, irritável, agradecido)
—Motivação para criar o bitcoin
—Raciocínio, previsão e capacidade para criar um pseudónimo à prova de bala (Quem se daria ao trabalho de limpar uma cena de crime antes de ser uma cena de crime? Quem era tão bom em privacidade em 2008?)
—Capacidade monástica para renunciar a uma fortuna

A lista de verificação partia do princípio de que Nakamoto, embora reservado, não tinha construído uma persona ficcional complexa. Mas alguns traços eram mais discutíveis do que outros. Os conhecimentos de programação em C++ eram inegáveis. Já os indícios de inglês britânico eram muito mais fáceis de fingir, os horários podiam ser manipulados e as inclinações políticas podiam ser encenadas. Embora Nakamoto tivesse usado uma vez a frase claramente libertária: «Podemos ganhar um novo território de liberdade», noutra referiu-se a como o bitcoin seria «muito apelativo do ponto de vista libertário», o que soava mais a observação distanciada do que a convicção pessoal.

Na outra parede fiz uma *colagem*. A maioria das histórias que investigara trazia vivacidade ou intimidade incorporadas. Na baía de Guantánamo, pude concentrar-me nos modestos pertences de um detido menor: ténis de corrida sem atacadores, desodorizante Mennen Speed Stick. No apartamento de um palhaço em São Francisco, pude observá-lo, de pé, diante do espelho da casa de banho em cuecas, a aplicar rouge. Na Polónia, passei uma semana com um ferroviário que despertara de um coma quinze anos depois, tendo perdido o fim do comunismo e a morte da sua devota esposa.

«BITCOIN RENAISSANCE»

A intangibilidade do bitcoin tornava-o difícil de apreender. As tentativas de representar as criptomoedas recorriam frequentemente a números rabiscados ao estilo de *Uma Mente Brilhante*. Em Miami, percorri uma sala de exposições onde um cartaz anunciava «a maior galeria de arte do bitcoin da história». Ali decorria uma exposição intitulada «Bitcoin Renaissance»: «Em 1494, a invenção da contabilidade de partida dobrada marcou o início de uma nova era de prosperidade humana

ESTAVA NO ÂMAGO DO JORNALISMO DE INVESTIGAÇÃO: DESVENDAR VERDADES QUE ALGUÉM SE EMPENHAVA EM SILENCIAR

e, pouco depois, de uma idade de ouro da expressão artística. Desde 2008, a invenção do bitcoin inaugurou o mais recente capítulo do florescimento humano».

Não era arte que exigisse franzir o sobrolho para interpretá-la. Havia representações criativas do símbolo do bitcoin, endereços de chave pública, o livro branco, slogans populares como «JUST HODL IT» (*hodling*, no jargão do bitcoin, significa «reter» ou comprar bitcoins para o longo prazo), celebridades do bitcoin como o presidente de El Salvador, Nayib Bukele, e olhos laser, um meme popular entre os bitcoiners para exibir a sua lealdade tribal. Alguém reinterpretara *A Noite Estrelada*, de Vincent van Gogh, com o símbolo do bitcoin no lugar das estrelas. Alguém publicara um livro ilustrado para crianças: *Bitcoin em rima.* Muitas das imagens, em consonância com o ressentimento tribal dos bitcoiners, eram combativas: a cara de Jamie Dimon a derreter-se, um bitcoin a travar um duelo de espadas com um dólar, um grupo de velhos brancos em redor de um Monopoly apoiado sobre as costas de escravos multirraciais («Falsos lucros»), uma soqueira com o símbolo do bitcoin ao centro e as palavras «Fiat Facelifter», uma tabela classificativa de «moedas fiduciárias falhadas» (o bolívar, o papel-moeda) ao lado de uma tabela de «alternativas de dinheiro sólido» (bitcoin, ouro, prata).

UM DEUS NÃO INTERVENCIONISTA

Tinha curiosidade em ver como seria representado Nakamoto, o líder sem rosto da utopia descentralizada do bitcoin. A esta altura, os contornos religiosos da cultura do bitcoin mal se disfarçavam. O livro branco era a escritura sagrada. Os bitcoiners evangelizadores eram os eleitos; todos os demais, os condenados. Satoshi, o desprendido detentor de uma fortuna obscena, era o seu Deus não intervencionista.

SHUTTERSTOCK

Em 2021, El Salvador tornou-se o primeiro país a adotar o bitcoin como moeda oficial. Nayib Bukele, presidente de El Salvador, sai da Casa Branca após reunião presidencial.

TINHA CURIOSIDADE EM VER COMO SE INTERPRETARIA VISUALMENTE NAKAMOTO, O LÍDER SEM ROSTO DA UTOPIA

As representações que dele se faziam, como um peluche vendido na Amazon em 2016, tinham traços asiáticos. Em Miami, alguns artistas recorreram a uma figura encapuçada e sem rosto; outros, a máscaras de Guy Fawkes. O rosto de Dorian Nakamoto estava por todo o lado: numa pintura pontilhista, no lugar de um presidente numa «nota de bitcoin» em forma de dólar, numa carta colecionável numa capa rígida transparente (outra das cartas mostrava Hal Finney). Alguns anos após a reportagem mal concebida da *Newsweek*, Dorian começara a frequentar conferências sobre bitcoin, onde era acolhido como figura de culto. A mesma comunidade que atacara ferozmente Leah Goodman por o ter apontado como Satoshi Nakamoto agora deleitava-se alegremente em usar a sua imagem como substituto.

ASC

Leah McGrath Goodman é uma jornalista de investigação norte-americana que trabalhou para a *Newsweek*.

O SANTO FUNDADOR

Percebi porque é que a arte do bitcoin era tão literal. Partilhava o impulso de tornar material o etéreo. A compulsão de pendurar fotografias de parafernália do bitcoin parecia-me semelhante ao impulso de corroborar Nakamoto, identificando-o.

O meu painel de inspiração no gabinete era feito de caras com carência de vitamina D, dispositivos de aspeto estranho e gestos desconcertantes. Quando queria, podia rodar a cadeira e olhar para as imagens para manter os pés assentes no chão por um momento. Havia moedas Casascius, fichas metálicas que incrustavam uma chave privada e um endereço bitcoin e estavam protegidas por um autocolante holográfico à prova de adulterações. Uma plataforma de mineração. Uma carteira de *hardware*. O aterro galês com o disco rígido de 8000 bitcoins algures. Homens com capacetes dos Daft Punk. Outros homens com máscaras nas quais eram projetados avatares digitais. Um gráfico montanhoso do historial sísmico de preços do bitcoin.

Da primeira vez que a minha mulher viu tudo aquilo (a folha de cálculo, a lista de verificação, a *colagem*), sorriu. Na verdade, foi um sorriso trocista.

—Vais acrescentar algum fio vermelho? — perguntou.

ASC

Zooko Wilcox-O'Hearn é criptógrafo, empresário e figura fundamental do movimento *cypherpunk*, criador da criptomoeda Zcash.

Quando tentei voltar a contactar fontes antigas e potenciais, deparei-me com uma resistência inesperada. Em parte, devia-se à polarização que invadira a internet desde a primeira vez que escrevi sobre o bitcoin. Quando enviei uma mensagem a Robert Hettinga, um verboso *cypherpunk* de Anguila, há muito interessado em dinheiro digital, bloqueou-me no Twitter e gabou-se perante os seus 942 seguidores de que, dez anos antes, «teria dado o testículo esquerdo» para falar com um jornalista, mas agora se punha «a resfolegar como um ultra-MAGA» contra um escritor de «programas de merda liberticidas».

Grande parte do atrito tinha que ver com o tabu em torno de Satoshi Nakamoto. Sempre houve uma fação hostil a investigar a sua identidade. («Fez uma contribuição valiosa, pelo que os seus desejos devem ser respeitados. O que importa não é a pessoa, mas a ideia, o código.») À medida que se foi criando uma lenda em torno de Nakamoto, «o santo fundador» desta tecnologia que mudará o mundo, nas palavras de Gavin Andresen, simples perguntas sobre quem poderia ser passaram a ser gatilhos para os bitcoiners. E a revelação da identidade de Dorian Nakamoto arruinou todo o projeto. O *doxxing*, se vivias na bolha do bitcoin, aplicava-se agora até ao nome de uma pessoa de interesse jornalístico. Os editores da *Reason* («Mentes livres e mercados livres»), desgostosos com «o som indecoroso dos escribas de olhos muito abertos» que andavam a investigar a autoria do bitcoin, publicaram um artigo intitulado: «Deixem o Satoshi em paz!». Quando tentei falar com Peter McCormack, um *podcaster* centrado no bitcoin, em Inglaterra, que no LinkedIn se descrevia como «jornalista a tempo inteiro», resfolegou: «Não me interessam as reportagens que vasculham as origens à procura da identidade de Satoshi; ele escolheu manter-se anónimo e acho que devemos respeitar essa decisão».

O cordão de proteção pareceu-me absurdo. Nakamoto colocara o seu engenho na praça pública. Era legítimo perguntar quem o tinha colocado ali e porquê. Identifiquei-me com um utilizador do Reddit que, respondendo aos fanáticos da privacidade quando Skye Grey expôs a sua teoria sobre Nick Szabo, escreveu: «A toda

PONDEREI EM QUE CIRCUNSTÂNCIAS ME ABSTERIA DE REVELAR A IDENTIDADE DE SATOSHI NAKAMOTO

a gente que diz que não lhe importa quem é Satoshi e que não quer saber: admiro o orgulho que sentem por não terem curiosidade, mas não vos percebo de todo. É um dos últimos grandes mistérios que restam na internet, e é fascinante. Ensinem-me os vossos poderes zen de indiferença, quero aplicá-los ao meu amor por bolachas e bolos».

«QUEM ME DERA QUE O SATOSHI AINDA ESTIVESSE VIVO»

Quando falei com Bill Dodd, um desalinhado diretor de *software* de Mobile, no Alabama, que treinara uma rede neuronal com o arquivo do *Metzdowd* e aplicara aprendizagem automática à sua própria busca de Nakamoto, perguntou-me:

—O que pensas do dilema ético de revelar a identidade de alguém que, claramente, quer que o deixem em paz?

Vislumbrei uma reprimenda no horizonte, mas o Bill revelou-se um tipo encantador, com uma mistura muito humana de curiosidade e empatia.

—Dependeria de quem viesse a ser Nakamoto — respondi.

—Sim, eu também. Comecei por simples curiosidade, e não lhe dediquei muito tempo... Só queria saber, porque foi algo importante na minha formação e, como recém-chegado, pareceu-me fascinante que, dez anos depois, este mistério ainda persistisse — disse Bill e, depois de confessar que, ao princípio, se mostrara cético quanto à ideia do bitcoin, acrescentou —: Acho que ao mistério às vezes é difícil de resistir. Também vou oscilando. Por um lado, tens algo que se tornou uma parte tão importante do espírito do tempo que quase parece uma história incompleta cujo nome não é conhecido pelas pessoas. E, por outro lado, não gostaria que aparecessem as carrinhas da CNN quando eu tiver cinquenta ou sessenta anos e estiver reformado na minha residência em Londres, ou onde quer que seja. Por isso, percebo, percebo os dois lados.

A sensibilidade, assim como uma certa fadiga do tema entre os bitcoiners após anos de tentativas falhadas de desmascarar Nakamoto, moldou a minha forma de abordar as pessoas. Consoante a pessoa, comecei por vezes a substituir o altissonante «origens do bitcoin», quando descrevia pela primeira vez o tema da minha investigação, pelo mais potencialmente provocador «identidade de Satoshi».

Ponderei em que circunstâncias me absteria de revelar a identidade de Nakamoto. Talvez a resposta fosse dececionante. Afinal, que importância teria descobrir que se tratava desta pessoa anónima e não daquela outra, igualmente desconhecida? Em 2017, Zooko Wilcox — um *cypherpunk* que trabalhara na DigiCash, mais tarde criador da Zcash (uma criptomoeda com maior privacidade) e incluído nas listas de possíveis candidatos a ser Nakamoto — escreveu: «Quem me dera que o Satoshi ainda estivesse vivo, para podermos verificar que é tão ignorante, inadequado e banal como todos nós». ■

Um ser humano imperfeito

Cinco meses depois de Craig Wright ter sido — e depois não ter sido — identificado como Satoshi Nakamoto, na segunda-feira, 2 de maio de 2016, o australiano voltou a surgir no meu feed de notícias. Agora parecia que, de facto, era Nakamoto.

ADORAMOS CRIAR HERÓIS

Desta vez, a notícia chegou em bombardeamento mediático às oito da manhã, com exclusivos sobre as alegações de Wright no *The Economist* e na BBC, que anunciavam: «O Sr. Wright forneceu provas técnicas para sustentar a sua alegação, utilizando moedas que se sabe pertencerem ao criador do bitcoin. Membros destacados da comunidade do bitcoin e das suas principais equipas de desenvolvimento dizem ter confirmado as suas afirmações». Um deles foi Jon Matonis, cofundador da Bitcoin Foundation, uma organização sem fins lucrativos criada para promover o crescimento da criptomoeda, que escreveu no seu blogue «Como conheci Satoshi», declarou à BBC estar «absolutamente convencido» de que Wright era Nakamoto e acrescentou que a invenção do bitcoin estava «ao nível da imprensa de Gutenberg». Mas quem deu maior credibilidade às alegações de Wright foi Gavin Andresen, antigo programador principal do bitcoin, que escreveu no seu blogue: «Creio que Craig Steven Wright é a pessoa que inventou o bitcoin: adoramos criar heróis, mas também parece que adoramos odiá-los se não corresponderem a algum ideal inatingível. Seria melhor que Satoshi Nakamoto fosse o nome de código de um projeto da NSA ou uma inteligência artificial enviada do futuro para aperfeiçoar o nosso dinheiro primitivo. Não é: é um ser humano imperfeito, como todos nós. Espero que consiga ignorar, em grande medida, a tempestade que o seu anúncio irá provocar e continue a fazer aquilo de que gosta: aprender, investigar e inovar».

Gavin contou também como, um mês antes, chegara a convencer-se desta verdade. ■

SHUTTERSTOCK

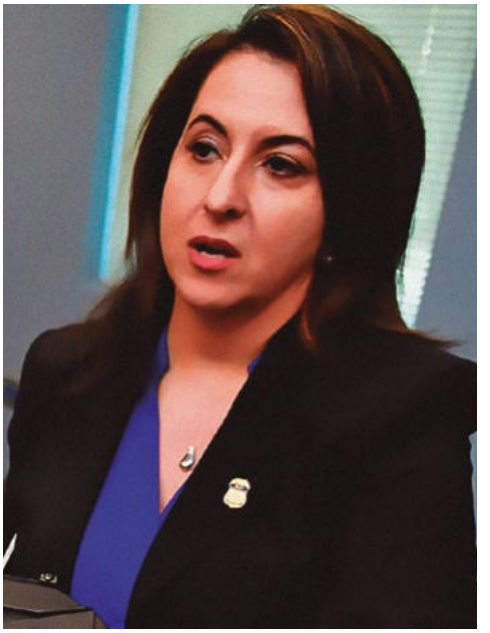
O informático e empresário australiano Craig Wright afirma ter participado na criação do bitcoin, embora não haja consenso nem provas verificáveis que o confirmem.

Liberdade de informação

Satoshi Nakamoto era um engenheiro meticuloso que trabalhava abertamente em fóruns, respondia com rigor técnico, publicava código auditável. Não atacava sistemas; construía um novo.

SHUTTERSTOCK

Em 2022 encontrei outra pista promissora. Na primavera de 2019, Rana Saoud, agente assistente a cargo da divisão de Imigração e Controlo Aduaneiro do Departamento de Segurança Interna, falara na Conferência OffshoreAlert, em Miami, no âmbito de um colóquio intitulado «Regulação de criptomoedas e ICO: valor mobiliário, mercadoria ou moeda?». Durante a apresentação, recordou a investigação de um colega sobre a Black Market Reloaded, um dos mercados da web obscura que sucederam à Silk Road: «É um agente extremamente inteligente e visionário. Disse-me: "Quero entrevistar o Satoshi Nakamoto". Na altura pensávamos: "Pode ser uma personagem fictícia, talvez exista, talvez não". Por isso, raciocinámos: "Se um agente quer falar com essa pessoa e temos orçamento, porque não tentar? Vamos perceber como tudo isto funciona". E foi isso que aconteceu: os agentes voaram para a Califórnia e descobriram que Nakamoto não tinha criado o bitcoin sozinho, mas que havia outras três pessoas envolvidas. Reuniram-se com todos para entender realmente como funcionava o sistema e qual era o seu propósito».



GLADSTONE TAYLOR

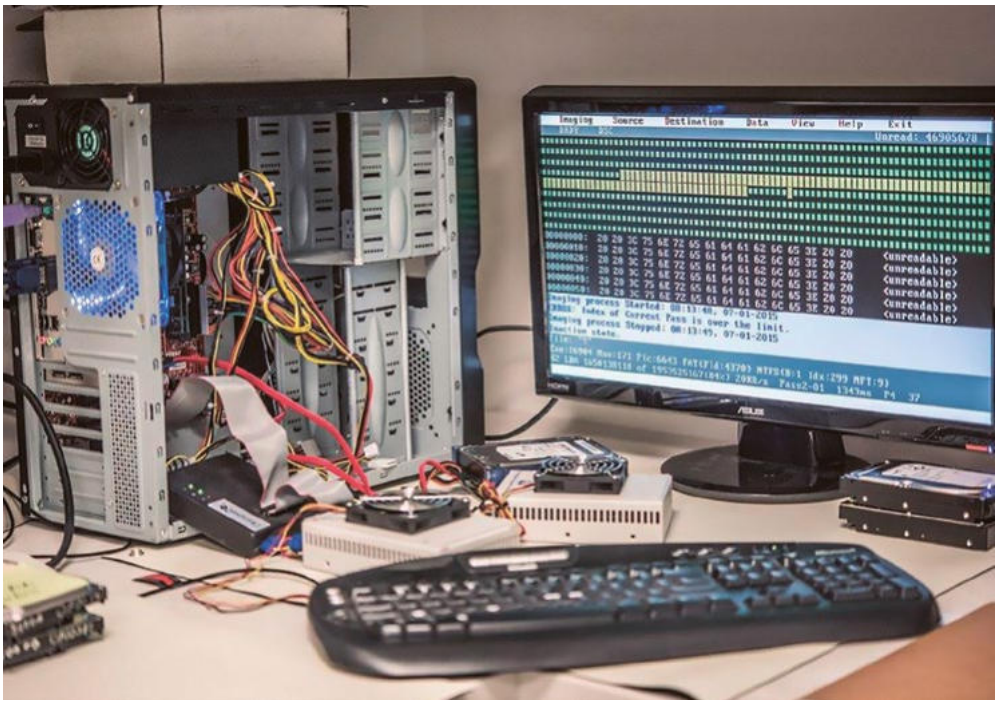
Rana Saoud, agente assistente a cargo da ICE/HSI (Divisão de Imigração e Controlo Aduaneiro).

O QUE TINHA DESCOBERTO?

Este episódio causou um breve rebuliço no Reddit, mas depois caiu no esquecimento. Quando ouvi pela primeira vez o áudio das declarações de Saoud, mantive o cepticismo. Por que razão alguém precisaria de falar com Nakamoto para saber como funcionava o bitcoin? E a forma tão despreocupada como largou a bomba («Sim, o Satoshi são quatro pessoas na Califórnia») sugeria que não compreendia a magnitude do que estaria a revelar se fosse verdade: seria o primeiro encontro presencial documentado com Nakamoto, a primeira prova de que o Governo conhecia a sua identidade e a primeira confirmação de que Nakamoto não era uma só pessoa, mas um grupo. Isto levou-me a suspeitar que, de algum modo, tinha interpretado mal o colega.

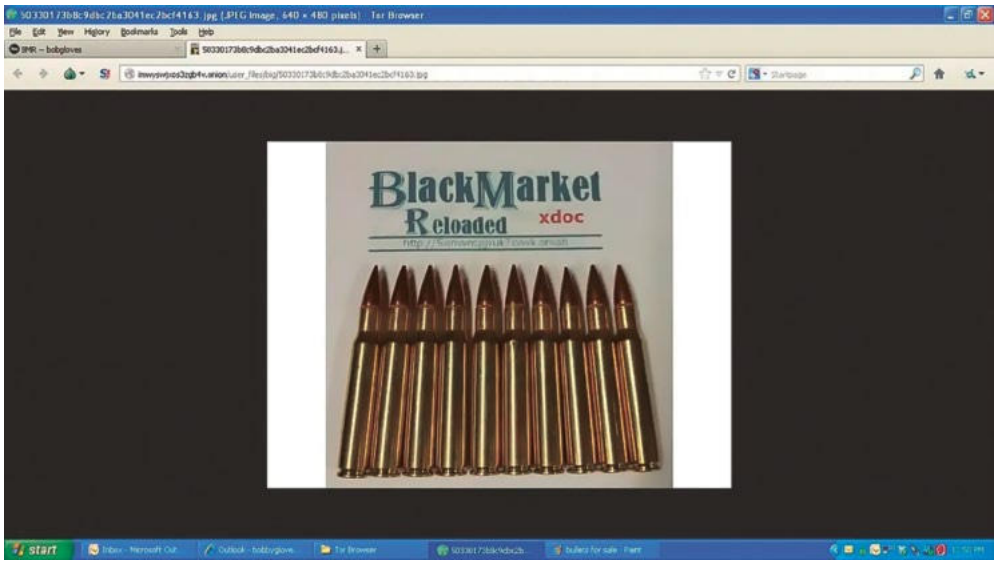
Ainda assim, não era descabido pensar que Nakamoto pudesse ser uma equipa de pessoas que desejassem manter o anonimato perante as multidões da internet e os media, mas que, em última análise, fossem cidadãos cumpridores da lei que não se furtariam a falar com investigadores federais. Talvez fossem até pessoas preocupadas com a associação do seu invento a mercados negros e desejosas de esclarecer mal-entendidos. Surgiam-me inúmeras perguntas. Como é que o agente contactara Nakamoto? Que garantias lhes oferecera? Durante

NAKAMOTO NÃO TINHA CRIADO O BITCOIN SOZINHO; HAVIA OUTRAS TRÊS PESSOAS ENVOLVIDAS



U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT/ ICE

Acima, ecrãs do HSI (Homeland Security Investigations) mostram análises de mercados da web obscura que vendiam droga e armas, onde aceitavam bitcoins.
Em baixo, munições de calibre .223 à venda por bitcoins.



GLOBALNEWS/ GIL SHOCHAT

quanto tempo haviam conversado? Que descobrira? Telefonei à agente Saoud. Respondeu-me que precisava de consultar os advogados e os «especialistas em ética» da sua divisão. Isto desembocou numa busca infrutífera, que incluiu vários pedidos complexos ao abrigo da Lei da Liberdade de Informação, todos sem sucesso.

ADEUS À TEORIA DOS GRUPOS

Acabei por conseguir falar diretamente com o agente a que Saoud se referira. Ryan Landers dirigira a investigação sobre a Black Market Reloaded, que culminou em várias detenções, incluindo a de um indivíduo que vendia ricina e outras toxinas a nível internacional. Quando falei por telefone com Ryan, explicou-me que tinham procurado Nakamoto porque, na altura, queriam perceber se o bitcoin tinha alguma vulnerabilidade desconhecida que os investigadores pudessem explorar para rastrear transações ilícitas.

— Falámos com o irmão e a mulher dele — disse-me Ryan.

— Como? Então o Satoshi era uma única pessoa e não quatro — inquiri.

— Sim — confirmou Ryan.

SHUTTERSSTOCK

Dorian Nakamoto conversa com vários participantes durante a primeira conferência de bitcoin em São Francisco, Califórnia, a 25 de junho de 2019.

RYAN LANDERS LIDEROU A INVESTIGAÇÃO SOBRE O BLACK MARKET RELOADED QUE CULMINOU EM VÁRIAS DETENÇÕES

Adeus à teoria dos grupos, mas, enfim, Ryan parecia saber quem era Nakamoto.

— Então, de quem eram o irmão e a mulher com quem falaram? — perguntei-lhe, esperando que Ryan não escolhesse aquele momento para se calar.

— Dorian Nakamoto — disparou.

— Espera, o quê?

— Achamos que é o Dorian — disse.

A revelação deixou-me estupefacto. Poderia ser que Leah Goodman tivesse acertado desde o início e todos a tivéssemos desacreditado injustamente? Pedi a Ryan que me desse mais detalhes, ansioso por saber que provas tinham ficado de fora da reportagem da *Newsweek*.

ASC

Fran Finney, esposa de Hal, escreveu mensagens para a comunidade, incluindo um emotivo *post* na Bitcoin Foundation.

Segundo Ryan, a ex-mulher de Dorian, uma enfermeira com cerca de sessenta anos, descrevera-o como uma pessoa com traços autistas, obcecada com comboios em miniatura e «permanentemente frustrada» pelas complicações bancárias e pelos problemas cambiais quando encomendava modelos a partir de Inglaterra.

— Quando se ouvia a descrição que ela fazia do Dorian — recordou Ryan —, percebia-se como a sua personalidade e motivações encaixavam na perfeição no que estava exposto no livro branco.

— E?

— Foi tudo.

Essa era toda a prova. Não era mais convincente do que a apresentada por Goodman. Ryan precisou mais tarde: «Não estou certo de ter acreditado que houvesse apenas um inventor, mas suspeitei que o Dorian Nakamoto estava envolvido e que talvez fosse o autor do documento técnico».

Ele e um segundo agente também visitaram Hal Finney. Fran Finney «foi incrivelmente hospitaleira... e fez tudo o que podia para nos ajudar», mas Hal já nem sequer conseguia utilizar o *software* de seguimento ocular nessa altura e viria a falecer poucas semanas depois. ■

Eat/ sleep/ hodl/ repeat

Eat/Sleep/HODL/Repeat («*Comer*/Dormir/ Manter/Repetir») nasceu de um erro tipográfico em 2013 e evoluiu para o acrónimo «*Hold On for Dear Life*» (HODL, «agarra-te à tua querida vida»), que se tornou uma filosofia de investimento para a comunidade.

ISTOCK

A sala 250 do Palácio da Justiça do Distrito de Oslo era um espaço luminoso, de madeiras claras, divisórias de vidro e linhas suaves, ocupado por advogados de toga preta. Na parede atrás do estrado da juíza Helen Engebrigtsen brilhava um escudo heráldico vermelho com um leão rampante coroado a ouro.

Era uma manhã de segunda-feira de setembro. Craig Wright entrou com ar presunçoso e peito inchado, vestido com um fato de três peças e um vistoso anel no dedo mínimo. Seguia-o a sua sombra, Michel, um guarda-costas moreno, sorridente, com um impecável fato por medida que ostentava o tridente dourado distintivo dos veteranos das forças especiais anfíbias suecas. Era a primeira vez que via Wright em pessoa. Nos sete anos decorridos desde que veio a público, o cabelo apresentava um tom mais louro salpicado de brancas, a constituição tornara-se mais flácida e a papada mais proeminente. A boca desenhava um constante esgar de desdém.

O MANTO DO ANONIMATO

Magnus Granath, um homem de quarenta e cinco anos, com cabelo e barba grisalhos, óculos discretos, um camisolão cinzento e um anoraque azul, sentou-se do lado oposto da sala e tirou da sua mala a tiracolo um livro de bolso e um portátil coberto de autocolantes.

O contraste era evidente. Granath sentou-se ao lado dos seus dois advogados. Wright estava rodeado por nove, embora tivessem deixado um lugar vago de cada lado do cliente. A imagem era paradoxal. Wright apresentava-se como vítima de assédio digital.

Com os participantes estrangeiros a seguirem o processo através de auscultadores com tradução simultânea do norueguês, a juíza Engebrigtsen começou por esclarecer que não estava em causa, para além de qualquer dúvida razoável, determinar se Wright era Satoshi Nakamoto. No entanto, reconheceu que essa questão era fundamental para decidir se Granath difamara ou não Wright.

Nos dias seguintes, o julgamento ganhou dinâmica própria. Uma equipa da *CoinGeek* ocupou a galeria de imprensa do lado de Wright, juntamente com a sua esposa, Ramona, e o filho, Ben. Uma equipa de quatro pessoas da *Bitcoin Magazine*, que estava a filmar o julgamento, instalou-se na galeria de imprensa do lado de Granath, perto da mãe e da namorada dele. Antes de o processo começar, Granath, consciente de que estava prestes a perder o anonimato e preferindo fazê-lo nos seus próprios termos, concedera uma entrevista a um jornal norueguês usando o seu nome verdadeiro e permitindo ser fotografado. Ainda assim, durante todo o julgamento, a *Bitcoin Magazine* referir-se-ia a Granath apenas como «Hodlonaut» e desfocaria o seu rosto nas imagens de vídeo. Quando o tradutor da revista tweetou #WeAreAllHodlonaut, alguém respondeu: «Quem precisa de ob-

GRANATH TINHA CONCEDIDO UMA ENTREVISTA USANDO O SEU NOME VERDADEIRO E PERMITINDO SER FOTOGRAFADO

PETTER BERNTSEN/DAGENS NÆRINGSLIV

Magnus Granath, conhecido como «Hodlonaut», a depor num tribunal norueguês durante a sua batalha legal contra Craig Wright.

jetividade?». Um seguidor de «Hodlonaut» chamado Norbert fez a cobertura do julgamento em direto no Twitter, escrevendo freneticamente num portátil com o autocolante «eat/sleep/hodl/repeat». Eu alternava entre ambos os lados, receoso de parecer alinhado com um grupo em particular e que o outro deixasse de falar comigo.

Alguns pontos tangenciavam a fronteira entre os comentários no Twitter e a difamação punível. Não tinha Wright respondido na mesma moeda? Assim o sustentaram os advogados de Granath, apontando tweets de Wright em que chamava Julian Assange de «violador» e onde afirmava: «Mal posso esperar para ver esmagados todos esses maricas beta». Qualquer estranho que entrasse casualmente na sala veria o advogado principal de Wright, Halvor Manshaus, eminência do foro de Oslo, a debitar um jorro de norueguês ininteligível, pontuado por termos como *scamtard, bitchboy* e *leet speakers*. Seguiu-se depois uma troca em que um dos advogados de Granath teve de explicar à desconcertada juíza expressões como *cuck, Low T* e *massive Tassy*, que todos interpretámos como algum obscuro insulto australiano que, ao que parecia, fazia referência à forma triangular de um púbis do tamanho da Tasmânia. Os representantes legais de Wright, por seu turno, tinham passado em revista cerca de trinta e sete mil tweets de Granath e detetaram entre eles alguns algo inquietantes: «É difícil verificar quantos Hitler matou, dado que questionar a versão oficial da história é ilegal na maior parte da Europa», «A história oficial do 11 de Setembro é tão credível como o CSW ser o Satoshi» e «Os promotores das vacinas são extremistas perigosos. Chega».

Por vezes, parecia que eram os próprios valores do bitcoin a estarem em julgamento. «É difícil responsabilizar alguém quando permanece anónimo», argumentou Manshaus. Evocou o anel de Giges, um episódio de *A República* de Platão, que Wright mencionava ocasionalmente para ilustrar como as pessoas se comportam indevidamente quando vestem o «manto do anonimato».

GEORGIA RESEARCH ALLIANCE

Ami Klin, psicólogo especializado em autismo, fundador da EarliTecDX e diretor do Marcus Autism Center da Universidade de Emory.

«WRIGHT MERECIA EMPATIA, NÃO DESPREZO»

Grande parte da defesa de Granath assentou em provas apresentadas inicialmente em Miami. Para além de todos os golpes prévios na credibilidade de Wright, a equipa de Granath apresentou um novo relatório forense de 227 páginas elaborado pela KPMG5, que concluía que 71 documentos juntos por Wright neste caso pareciam ter sido manipulados, falsificados ou deliberadamente antedatados.

Manshaus procurou contornar os problemas de personalidade e credibilidade de Wright, vinculando-os entre si. Segundo ele, era o peculiar estilo comunicacional de Wright que levara cinco juízes de quatro tribunais diferentes a questionar a sua veracidade. «Wright merecia empatia, não desprezo», afirmou Ami Klin, diretor do Marcus Autism Center da Universidade de Emory. Quando o advogado principal de Granath, Ørjan Salvesen Haukaas, interrogou Klin, perguntou-lhe se os sintomas do transtorno do espetro do autismo e do transtorno narcisista da personalidade «poderiam ser semelhantes».

— À superfície, pode argumentar-se que essas manifestações parecem semelhantes. Mas, do ponto de vista clínico, não têm absolutamente nada em comum — respondeu Klin.

Wright adotou uma posição inédita e decididamente pouco *cypherpunk* sobre como provar a identidade. Para além de Gavin Andresen e Jon Matonis, havia «entre oitenta e cem» pessoas que conheciam «todos os detalhes sobre a minha criação do bitcoin», afirmou em tribunal.

— Na minha opinião, as pessoas é que são a prova. A identidade não está ligada às chaves — argumentou Wright.

Um pequeno grupo de familiares e antigos colegas australianos depôs a seu favor, embora a maioria pouco adiantasse quanto à sua afirmação de ser Nakamoto.

O ESTILO COMUNICACIONAL DE WRIGHT ERA O QUE TINHA LEVADO VÁRIOS JUÍZES A QUESTIONAR A SUA VERACIDADE

Wright afirmara também ter encontrado recentemente alguns documentos supostamente perdidos há muito, entre eles um rascunho manuscrito de cerca de oitenta páginas do livro branco que disse ter começado em agosto de 2007, e uma nova versão datilografada, também de 2007, embora, neste último documento, tivesse surgido misteriosamente um tipo de letra que não existia antes de 2012. E Wright contou uma história completamente nova sobre a razão por que não podia aceder às chaves privadas de Nakamoto: em 2016, depois da sua tentativa de suicídio, teria «calcado o disco rígido» e esmigalhado com um martelo uma unidade USB que continha os fragmentos de chaves, para que nunca pudesse ser obrigado a provar o seu valor através da criptografia, o que daria aos seus inimigos «a saída fácil».

PETTER BERNTSEN/ DAGENS NÆRINGSLIV

Craig Wright, empresário e informático australiano, afirma desde 2016 ser Satoshi Nakamoto, o criador do Bitcoin.

Na quarta-feira, o terceiro dia do julgamento, a sala do tribunal estava mais concorrida do que o habitual quando Granath, vestido com uma camisa Oxford azul por baixo de um fino camisola de gola em V, subiu ao estrado e descreveu o seu percurso até ao bitcoin.

NÃO SE TORNAR UM ALVO

Recebera o seu primeiro computador quando tinha oito ou nove anos, um Commodore 64, e guardava ficheiros em cassetes. Em criança, reparou como, ano após ano, o preço dos gelados Krone-is de que tanto gostava não parava de subir. Foi o seu primeiro encontro com a inflação, algo que o desiludiu profundamente.

Falou do seu fascínio pela oferta monetária limitada do bitcoin e pela ideia de que possuir um token significava deter uma fatia desse bolo. Explicou o milagre da escassez digital: ao contrário de qualquer outra coisa na internet, o bitcoin era impossível de duplicar.

Granath comentou que, inicialmente, criara a sua conta de Twitter com um pseudónimo para não se tornar um alvo caso o bitcoin viesse a atingir grande valor. Depois de ter transacionado anteriormente «altcoins ou shitcoins», àquela altura já se considerava «o que a maioria chamaria um maximalista do bitcoin», acumulando bitcoins e depreciando todas as outras criptomoedas. «O que tornava

SERIA ESTRANHO QUE ALGUÉM COMO SATOSHI NAKAMOTO FOSSE TÃO DESCUIDADO AO PONTO DE SER REVELADO DESTA MANEIRA

o bitcoin especial era a sua ausência de liderança», afirmou. O pequeno tamanho de bloco do bitcoin permitia que qualquer pessoa executasse um nó da rede. Uma criptomoeda mais centralizada era simplesmente «um projeto de base de dados, suscetível de ser alterado por quem a controla».

— Disseste que um aspeto fundamental do bitcoin para ti era não ter líder nenhum, mas depois temos a figura de Satoshi Nakamoto. Poderias partilhar a tua opinião sobre esta pessoa ou pessoas? — assinalou Haukaas, o advogado de Granath.

— Eu, pessoalmente, nunca idolatrei Satoshi, mas sinto um imenso respeito por quem está por detrás do bitcoin e do nome Satoshi Nakamoto. Pareceu-me que a pessoa, ou pessoas, por trás desse nome era alguém humilde e afável, profundamente empenhado neste projeto — respondeu Granath.

— Conheces mais alguém, além de Craig Wright, que tenha afirmado ser Satoshi Nakamoto?

— Bem, Craig Wright é provavelmente quem o proclamou de forma mais aberta. Muita gente sente curiosidade quanto a isto, e alguns têm especulado com diversos nomes. Por exemplo, muitos acreditam que Hal Finney teve algo a ver. Também se tem mencionado Nick Szabo. Na verdade, isso não tem assim tanta importância, e nunca me dediquei a investigá-lo. Mas alguns fizeram essa afirmação.

Ainda recebo mensagens no Twitter de pessoas que garantem ser o Satoshi. Também me contactaram para «ajudar» — disse, fazendo aspas com os dedos — nessa investigação, mas não lhes respondo nem acredito neles — concluiu.

Quando Granath ouviu falar pela primeira vez de Craig Wright, após os artigos da *Wired* e da *Gizmodo*, achou que «seria estranho que uma pessoa ou pessoas como Satoshi Nakamoto fossem descuidadas o suficiente para serem reveladas desta maneira». Teorizou que Wright se declarara primeiro Nakamoto para se livrar do seu problema fiscal na Austrália e que, mais tarde, se tornara lucrativo ser Nakamoto, quando Wright lançou uma moeda chamada Bitcoin Satoshi Vision.

— Podem imaginar o quão revoltante é para quem, acima de tudo, admira Satoshi e é contra a fraude. Depois aparece alguém que afirma ser Satoshi e, para cúmulo, pretende processar toda a gente que diga que não é Satoshi — testemunhou Granath.

AJUDA PARA FINANCIAR A DEFESA LEGAL

Granath sentiu-se encorajado pela forma como a comunidade do bitcoin se uniu para o apoiar. Uma organização sem fins lucrativos chamada OpenSats angariou 15 milhões de coroas norueguesas, cerca de 1,4 milhões de dólares, de mais de 2600 contribuintes, incluindo algumas das maiores empresas de bitcoin, para financiar a sua defesa legal. Até o detetive que o contactara inicialmente em nome dos advo-

gados de Wright lhe enviou mais tarde uma mensagem a dizer que se arrependia de ter aceite o trabalho e que considerava Wright um *nisse*, um tipo de duende nórdico. Granath soava comovido quando falava do apoio dos bitcoiners. Disse que sentia estar ali a representá-los a eles e ao bitcoin.

Depois de Granath terminar o seu depoimento, a juíza Engebrigtsen perguntou-lhe se queria acrescentar algo sobre os tweets incendiários que Manshaus lera.

— Poderia, mas não sinto uma necessidade imperiosa de o fazer — respondeu Granath.

Engebrigtsen insistiu, assinalando que ele não tivera oportunidade de os comentar.

— O tweet que me pareceu pior fora de contexto foi o dos vendedores de vacinas — assinalou Granath —, embora mantenha todas as minhas opiniões… Lembrem-se, não tenho assim tantos seguidores noruegueses.

Acrescentou que tinha amigos noutros países a quem «tinham sido retiradas certas liberdades por se recusarem a vacinar-se».

— Creio que o ponto alto foi quando vi o primeiro-ministro canadiano, Justin Trudeau, a falar com crianças pequenas, instando-as a convencer os pais a vacinar-se. Pareceu-me uma pressão completamente deslocada — acrescentou.

Wright não dava entrevistas à imprensa durante o julgamento, mas, depois de o tribunal suspender a sessão no dia seguinte, jantei com Kurt Wuckert, Jr., correspondente da *CoinGeek* e o mais fervoroso defensor de Wright. Kurt fazia apenas uma refeição por dia, por isso comemos um guisado de porco a meio da tarde. Mais tarde, iria a um ginásio de MMA treinar.

ISTOCK

A OpenSats angariou 15 milhões de coroas norueguesas, cerca de 1,4 milhões de dólares, de mais de 2600 pessoas para financiar a defesa legal do Hodlonaut.

«O BITCOIN MUDA-TE»

Kurt não estava a ver o mesmo julgamento que eu. Enquanto eu achava que Wright estava a ser completamente desacreditado, Kurt andara a transmitir em direto com uma leitura muito diferente. Segundo ele, a linguagem corporal de Granath denotava nervosismo. Enquanto Manshaus se mostrava «sereno», Kurt assinalava que Granath mal conseguia conter um sorriso trocista quando se liam os seus tweets mais polémicos. Os advogados de Granath, a seu ver, pareciam inquietos. «Sou bastante otimista, francamente», confessou-me. E acrescentou que a situação estava «claramente do lado do Craig».

Kurt tomou à letra as desculpas extravagantes de Wright. Inclinara-se para Wright e para o BSV, disse, porque a resistência do bitcoin a tornar-se uma moeda útil «deixava-me maluco». Sentia que Wright falava do bitcoin como o fizera Nakamoto. Disse conhecer os argumentos contra Wright e afirmou:

— A verdade é que nunca esperei que a história de Satoshi fosse limpa. É uma figura anónima da web obscura. Satoshi é uma personagem fundamentalmente desonesta. É um narrador pouco fiável. Esse é o Satoshi Nakamoto. Essa é a questão, não é? Por isso, quando as pessoas dizem «isto não faz sentido», não sei, eu gosto de literatura. Gosto de ler histórias. Gosto das grandiloquentes tontarias, das narrativas e dessas coisas. Sempre supus que Satoshi seria essencialmente dececionante, certo? Porque a lenda na tua própria cabeça vai ser sempre genial. É como nos filmes de terror. Há vinte ou trinta anos, quando os efeitos não eram tão bons, não se mostrava o monstro até à última cena, mas ele era assustador na tua

KURTWUCKERTJR.COM

Kurt Wuckert Jr., «Chief Bitcoin Historian» da CoinGeek, uma publicação de média que promove Craig Wright como Satoshi Nakamoto e defende o Bitcoin SV (BSV).

MAGNUS GRANATH MAL CONSEGUIA CONTER UM SORRISO TROCISTA QUANDO SE LIAM OS SEUS TWEETS MAIS POLÉMICOS

mente, porque a história era boa. Depois vês o monstro e é uma marioneta de borracha, mas não faz mal, porque já te assustaste a ti mesmo durante todo o filme. Tu próprio preenches esses espaços em branco. E com o Satoshi era muito mais suculento. Quando conheces o Craig, é como, está bem, o Nakamoto é este australiano autista e barulhento que é um grande chato, mas de que é que precisávamos que fosse? Precisávamos que fosse o que foi durante aquele período de tempo, mas não há problema se ele for a marioneta de borracha no fim do filme.

— Kurt mente como um velhaco o tempo todo — dizia Magnus Granath.

Era o dia seguinte do julgamento, eu estava sentado com o Magnus e a namorada, a Katia, que era da Ucrânia e se fazia chamar Katoshi na internet. Estávamos numa mesa da cave de um café perto do tribunal e, enquanto o Magnus comia uma tosta de gambas e a Katia uma fatia de bolo de chocolate, falámos da *Citadel*, uma revista de cultura bitcoin que tinham fundado para destacar as «vozes de base».

Os últimos anos tinham sido extenuantes. Desde que começou a ação, o Magnus perdera o pai e a Katia, o dela. Depois, a Rússia invadiu a Ucrânia e a mãe de Katia foi viver com eles para Oslo. O processo foi demolidor. Durante o julgamento, uma equipa de documentaristas de cinco pessoas com duas câmaras, contratada por uma empresa de relações públicas propriedade de Calvin Ayre, seguiu o Magnus quando este saía do tribunal.

Magnus era o oposto de um criptoespeculador que joga com as flutuações de preços.

— «O bitcoin muda-te», disseram muitas pessoas. Outros acrescentaram: «Não te muda, expõe o teu caráter». Creio que ambas as afirmações são igualmente verdadeiras.

— E tu?

— Não creio que tenha mudado assim tanto — confessou-me Magnus —. Talvez o bitcoin me tenha tornado ainda mais decidido a dizer a verdade. Algumas pessoas dizem que o bitcoin é uma seita. Outras, uma religião. Acho que é uma perspetiva fascinante para refletir. Porque é, de facto, algo especial. Pela primeira vez na história, temos uma verdade inegociável. Toda a gente concorda que a *blockchain* do bitcoin é partilhada por toda a parte, não está sujeita a discussão.

Refleti sobre a profunda desconfiança que impregnava o mundo do bitcoin. O estilo de vida de um verdadeiro *hodler* já abrangia tudo: desde o peso morto, a comer fígado e «apanhar sol, nu», tudo com o objetivo de «escapar à Matrix». A cidadela no título da revista aludia a um meme do bitcoin sobre um futuro anárquico em que os fiéis da criptomoeda se refugiariam em fortalezas no alto das colinas, completamente autossuficientes, enquanto o resto do mundo malvivia em ermos apocalípticos.

O Magnus real era franco, humilde e capaz de rir. Apesar dos seus tweets conspiracionistas, acabei por lhe ganhar afeição. As suas publicações pareciam antes

uma extensão desafiadora da desconfiança endémica entre quem é cético quanto à «fiat», aos «terceiros de confiança» e à «narrativa oficial» sobre praticamente qualquer tema.

Perguntei-lhe pelo livro de que não parava de se socorrer durante o julgamento.

— São as *Meditações* de Marco Aurélio — disse-me Magnus.

Tornara-se adepto do estoicismo depois de ler o romance de Tom Wolfe *Um Homem em Cheio* vinte anos antes, muito antes de se tornar a filosofia de eleição dos irmãos de fraternidade.

— Aprendi que não era boa ideia investir demasiado significado ou energia em coisas fora do meu controlo e concentrar-me apenas no que posso gerir.

Obviamente, isso era crucial neste julgamento. Antes de depor, repetiu para si mesmo: «Não compliques, Magnus. Entra e diz a verdade». Propôs-se a não se preparar em demasia para que as suas respostas não soassem ensaiadas.

— Se me tivesse limitado a pensar apenas no desfecho, no que diriam ou no que me perguntariam, provavelmente teria enlouquecido. Isto foi, provavelmente, o mais stressante que experimentei: o doxing, a recompensa, a preparação para o julgamento. Sou pai, tenho um filho, tenho uma vida para além disto tudo, e este processo roubou-me tempo demais. Mas, por outro lado, suponho que sou teimoso ou tenho princípios, escolhe o que preferires. De forma alguma iria aos tribunais dizer que o Craig Wright é Satoshi.

VOLTAR A SER UM CIDADÃO QUALQUER

Magnus estava particularmente desiludido com Gavin Andresen, cujo apoio original Wright continuava a usar como principal esteio. Desde 2016, Gavin matizara a sua posição. Na declaração do caso de Miami, afirmou que foi uma surpresa para ele saber que Calvin Ayre estava por detrás de Wright. Apelidou o momento decisivo na cave do hotel em Londres de «suposta cerimónia de prova». Deixou claro que Wright podia ser desonesto por vezes e que fora «enganado» pela sua «verborreia sem sentido».

Mas Gavin ainda parecia acreditar que Wright era Nakamoto, tentando explicar o seu comportamento com a hipótese de uma possível «paranoia» clínica e especulando que a razão por que Wright não devolvera os 0,11 BTC de Gavin seria evitar revelar que reteve indevidamente chaves privadas que se supunha estarem bloqueadas num trust. Quando o advogado de Wright, Manshaus, perguntou a Magnus por Gavin, este respondeu com contundência: «Serei o mais direto possível: na minha avaliação absoluta do que aconteceu a Andresen… enganaram-no. É uma situação dolorosa e difícil de engolir. Matonis e Andresen são a prova disso. Pergunto-me por que não estão aqui para o contar eles mesmos». Em 2020, explicou Magnus, perguntou a Jon Matonis no Twitter se ainda apoiava

PERGUNTAVA-ME POR QUE RAZÃO SATOSHI NAKAMOTO NÃO DERA UM PASSO EM FRENTE PARA DESACREDITAR WRIGHT

SMART SPEAKERS

Jon Matonis foi diretor fundador da Fundação Bitcoin e economista-chefe da Cypherpunk Holdings, Inc., empresa de investimento em protocolos de privacidade.

Wright, preocupado com o impacto noutras pessoas, uma vez que o seu apoio estava a ser usado como prova. Matonis bloqueou-o. «Os bitcoiners gostam da verdade e querem verificar», sentenciou Magnus. O que não toleram é «um apelo à autoridade».

Agora, no café, interrogava-me sobre por que razão Satoshi Nakamoto não dera um passo em frente para desacreditar Wright.

— Ficaria desapontado — disse Magnus —. Estou completamente certo de que não o fará. Não faço ideia se ele, eles ou ela ainda estão vivos, mas, se assim for, espero que não façam nada. Mesmo que Satoshi aparecesse agora, não conseguiria controlar o bitcoin. O bitcoin já é algo autónomo. Poderia fazê-lo, claro. Mas não seria bom para a pessoa ou pessoas, e também não o seria para o projeto.

Não poderia Nakamoto, pelo menos, publicar uma mensagem assinada digitalmente a dizer: «Não sou o Craig Wright»?

— Não é que não me parecesse ótimo — expressou Magnus —. Se, de repente, acordar amanhã e, veja-se, assinou «Hodlonaut livre» ou algo do género, claro que seria incrível, mas não gostaria que essas pessoas se expusessem. Tenho plena consciência do quão insignificante é o meu caso, do quão pouco isto importa, em comparação com... Vejo o bitcoin como uma revolução descomunal, com consequências monumentais para a liberdade humana no futuro. Por isso, é muito surreal estar envolvido nisto agora.

Esperava, quando tudo terminasse, voltar a ser um cidadão qualquer.

— Creio que continuarei a ser o Hodlonaut, mas talvez prefira ter outra conta para poder falar com mais liberdade. Veremos para onde o mundo se move.

A juíza Engebrigtsen só anunciaria a decisão um mês depois. ■

Número um

O que é afinal o bitcoin? É dinheiro digital descentralizado, como prometeu Satoshi? Um ativo especulativo volátil? Ouro digital como reserva de valor? Uma tecnologia revolucionária ou uma bolha elaborada? A resposta depende de quem se pergunta: os maximalistas do bitcoin veem-no como a única moeda verdadeiramente descentralizada; os economistas tradicionais consideram-no especulação sem valor intrínseco.

ISTOCK

Ainda não tinha conseguido descartar o candidato mais convincente. Meses antes, dera de caras com outra pista. Era um eco de um eco na internet: uma menção fugaz a uma publicação no Facebook de alguém chamado Will Price, que trabalhara com Hal Finney e comentara aos amigos que acreditava que Hal era Satoshi Nakamoto. Uma captura de ecrã mostrava as primeiras linhas da publicação, que fora rapidamente apagada.

Hal continuava a ser um suspeito recorrente nas especulações sobre Nakamoto. Era muito mais hábil no segredo tático do que Nick Szabo, pois escrevera código para PGP, esteganografia e remailers. As primeiras avaliações estilométricas da Juola & Associates, embora limitadas a um conjunto restrito de candidatos, tinham identificado Hal como a correspondência mais próxima de Nakamoto. E havia aspetos em que a vida e a morte de Hal se ajustavam ao perfil de Nakamoto. Hal publicara a sua primeira mensagem no BitcoinTalk em novembro de 2010, apenas um mês antes de Nakamoto publicar a sua última mensagem ali. O agravamento da saúde de Hal explicaria o momento da saída de Nakamoto do projeto. A morte de Hal poderia explicar as moedas intocadas e a preservação imaculada do pseudónimo nos anos posteriores.

O ANONIMATO ASSENTAVA NA MODÉSTIA DE HAL

O seu compromisso com o ideal da descentralização era profundo. Após o seu falecimento, antigos colegas começaram a falar mais abertamente sobre o seu papel no PGP, que criara o primeiro *software* de encriptação de chave pública disponível ao grande público. Um problema persistente com a criptografia de chave pública era como garantir que uma chave pública pertencia realmente à pessoa a quem se supunha pertencer. Quando Phil Zimmermann lançou a segunda versão do *software*, em 1992, apresentava uma «rede de confiança», em que as pessoas assinavam criptograficamente as chaves de quem conheciam. Isto eliminava a necessidade de uma autoridade central que atribuísse chaves a identidades do mundo real. A fiabilidade de uma chave podia avaliar-se pelo número e pela qualidade das ligações que tinha. Uma das atividades principais nas reuniões mensais dos *cypherpunks* era uma sessão de assinaturas em que todos certificavam as chaves PGP uns dos outros. Hal fora em grande parte responsável por implementar e programar a rede de confiança.

Havia outro argumento a favor de que Nakamoto fosse alguém que trabalhara no PGP. Emin Gün Sirer, cofundador da *blockchain* Avalanche, analisou o código-fonte do bitcoin e concluiu que Nakamoto era autodidata e provavelmente uma única pessoa, mas, sobretudo, que se esforçara «por pensar de forma contraintuitiva». Nakamoto estava tão paranoico perante a possibilidade de as agências de

HAVIA ASPETOS EM QUE A VIDA E A MORTE DE HAL SE AJUSTAVAM AO PERFIL DE SATOSHI NAKAMOTO

ASC

Emin Gün Sirer, professor em Cornell e fundador da Avalanche, representa a categoria de críticos do bitcoin que, em vez de assinalarem problemas, construíram *blockchains* alternativas.

informação terem introduzido portas traseiras nos algoritmos criptográficos mais usados que tomou a precaução de empregar dois diferentes, de origens distintas (uma norte-americana e outra europeia), para gerar novos endereços de bitcoin, utilizando, no essencial, um codificador duplo.

—Isto não é algo que uma pessoa normal faria —argumentava Sirer—. Tem de ter sido alguém que passou muito tempo a preocupar-se com o que os atores estatais são capazes de fazer. Tem de ter sido alguém com experiência a escrever código para cenários de uso adverso, o que realmente reduz quem poderia ser Satoshi.

Alguém que tivesse trabalhado no PGP, segundo Sirer, era exatamente esse tipo de pessoa.

—Por isso, Hal é, na minha opinião, um excelente candidato a Satoshi. Achei que Sirer podia ter razão.

—Inculquei uma atitude generalizada em todas as pessoas que trabalharam no PGP de que estamos em confronto com os principais governos —explicou-me Phil Zimmermann.

Uma das razões por que o papel de Hal na rede de confiança só se tornou conhecido anos depois de a ter construído foi o facto de, durante o período em que Phil esteve sob ameaça de acusação, se ter precavido para nunca mencionar Hal aos investigadores. Fê-lo, com o consentimento de Hal, para o proteger.

—Sentia-me culpado por não mencionar o nome dele mais vezes —recordava Phil—. Merecia o reconhecimento.

Mas o anonimato assentava tanto na modéstia de Hal como no à vontade com que trabalhava na sombra.

Apesar de tudo isto, eu fora cético quanto a Hal como candidato desde que me deu o que me pareceu uma negação sincera, em 2011. Tinha até apresentado docu-

mentação em 2014, quando forneceu à *Forbes* cópias das suas trocas privadas de e-mails com Nakamoto. O bitcoin possuía uma elegância de que o RPOW de Hal carecia. Se Hal lançara o RPOW em seu próprio nome, porque não faria o mesmo com o bitcoin? «Não quero parecer um socialista, não me importa que a riqueza esteja concentrada», algo que Nakamoto escreveu uma vez, pareceu-me invulgarmente insensível vindo de Hal. Por isso, quando contactei Will Price, ex-colega de Hal e autor da publicação no Facebook que afirmava que Hal era Nakamoto, não tinha grandes expetativas.

PRIVACIDADE. SEGURANÇA. ANONIMATO

Will nasceu numa família proeminente de Hollywood. O pai, Frank, foi um lendário executivo de estúdios que dirigiu, em diferentes períodos, a Columbia Pictures e a Universal Studios. Frank nascera na pobreza e tornou-se um leitor voraz e, quando Will, um de quatro irmãos, cresceu em Beverly Hills, a história, o grego, o latim e a literatura eram venerados em casa dos Price. Will acabaria por se especializar em Estudos Clássicos na universidade, disciplina que o apaixonava.

Mas a sua verdadeira obsessão eram os computadores. A partir dos catorze anos, utilizando um modem ligado à rede móvel que instalou no quarto da residência de estudantes da Phillips Academy, em Andover, Massachusetts, ganhou centenas de dólares vendendo um *software* que desenvolvera e que permitia publicar mensagens num antigo serviço de quadro de anúncios na internet. Acabado de fazer vinte anos, quis encriptar os ficheiros do seu disco rígido, pelo que aprendeu criptografia por conta própria e criou e lançou um software chamado CryptDisk.

Isto chamou a atenção de Phil Zimmermann, que nessa altura receava ser processado pelo Governo e supervisionava um pequeno círculo de voluntários que

SHUTTERSTOCK

A Phillips Academy, em Andover, Massachusetts, uma das escolas mais prestigiadas dos Estados Unidos, onde se formaram alguns atores-chave no ecossistema bitcoin.

«NÃO QUERO PARECER UM SOCIALISTA, NÃO ME IMPORTA QUE A RIQUEZA ESTEJA CONCENTRADA», ESCREVEU NAKAMOTO

trabalhavam para expandir o PGP. Enquanto Hal trabalhava no PGP 2.0, Phil queria que Will programasse o PGP Phone, um *software* que permitiria efetuar chamadas encriptadas através da internet. Will estava a falar com Phil em 11 de janeiro de 1996, quando este o pôs em espera para atender outra chamada. Quando Phil voltou à linha, disse: «Will, vão arquivar a investigação. Acabou».

Depois disso, o PGP entrou numa nova fase, constituindo-se como empresa e procurando capital de risco. Will e Hal foram os dois primeiros empregados de Phil. Doze meses após a transformação em entidade com fins lucrativos, conta Will, a PGP tinha sete milhões de dólares de financiamento e gastava-os de forma desmedida. Para uma feira comercial em Manhattan, a empresa gastou dois milhões de dólares a servir sushi com a marca PGP, montar um espetáculo de luzes laser com a marca PGP e adornar o seu stand com três colunas romanas, cada uma entalhada com uma palavra: «Privacidade. Segurança. Anonimato». Esse diretor-executivo não durou muito.

UWE ARANAS

Phil Zimmermann numa conferência na HAL2001 (Hackers at Large), na Universidade de Twente, Países Baixos.

CRIPTÓGRAFOS EXCÊNTRICOS

Will foi o superior hierárquico direto de Hal durante muitos anos e, por essa razão, estava quase certo de que Hal era Nakamoto. Will fora testemunha em primeira mão de como Hal trabalhava na sombra de Phil. Vira o quão confortável Hal se sentia sem receber reconhecimento público. Além disso, Hal, como empregado a tempo inteiro de uma empresa, tinha motivos para recear que esta pudesse reclamar como seu tudo o que criasse.

—Garanto-lhe —afirmou Will— que, algures nesses contratos, há uma cláusula a dizer: se escrever código, é nosso.

Em 2008, Will, Hal e outros que tinham começado como idealistas ao lado de Phil estavam «fartos» da propriedade corporativa do PGP pós-Phil, que trabalhava para o Barclays Bank e, suspeitavam, para a CIA.

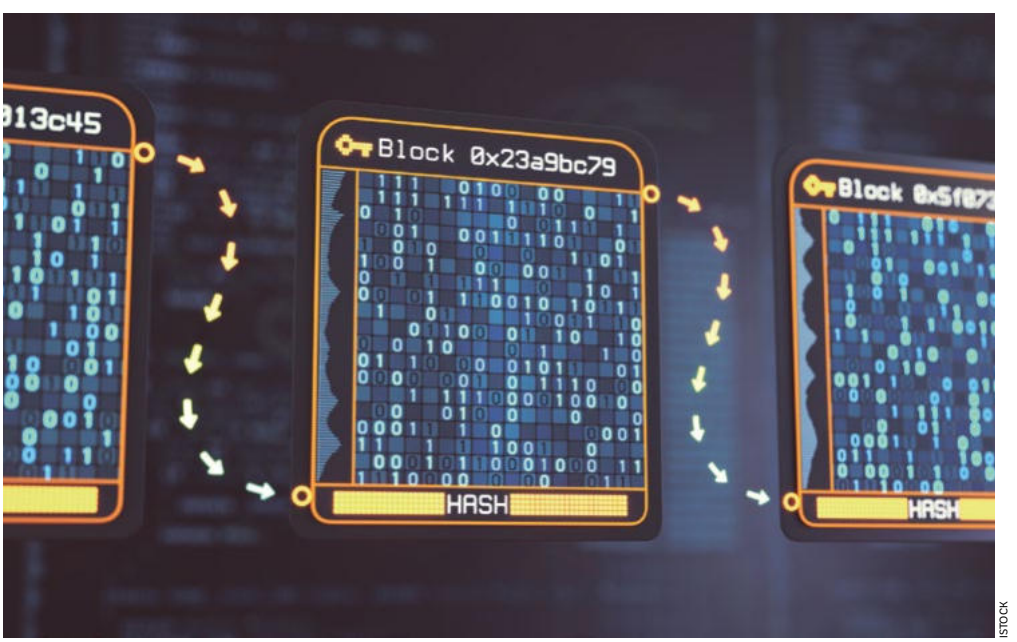
A NATUREZA METICULOSA DO CÓDIGO-FONTE ORIGINAL DO BITCOIN ERA TÍPICA DE HAL FINNEY

Will também conhecia intimamente o estilo de programação de Hal.

—Passei vinte anos a ler o código do Hal —disse-me Will—. Ninguém examinou o código do Hal mais do que eu.

Will considerava que a natureza meticulosa do código-fonte original do bitcoin era típica de Hal. Embora fosse mais conhecido como programador de C, usara tanto C como C++ no PGP. E Will concordava com Sirer quanto ao uso que Nakamoto fez de dois algoritmos criptográficos diferentes.

—Estas coisas são o pão nosso de cada dia —explicou-me Will—. Parte disto roça a bruxaria... Se queres que algo perdure centenas de anos, tens de assumir que algum algoritmo acabará por ser quebrado. O meu trabalho de 1996 a 2009 —prosseguiu— foi contratar, encontrar e dirigir criptógrafos excêntricos, de entre os quais o Hal era, de longe, o número um em termos de capacidade e conhecimento. Enquanto a maioria dos criptógrafos se destacava num ou noutro aspeto, o Hal era «um todo-o-terreno». Podia debater de igual para igual com Diffie e Hellman num almoço... E, ao mesmo tempo, podia escrever código para nós e convertê-lo em código de qualidade profissional. O meu trabalho consistia em conhecer toda essa gente, e a realidade é que o número de pessoas capazes de criar o bitcoin naquela época caberia numa pequena sala de jantar.



ISTOCK

Blockchain: blocos individuais que contêm dados (representados por código binário) ligados sequencialmente por funções *hash* criptográficas (as setas douradas).

Contudo, o que mais convenceu Will foi que conhecia a agenda de Hal. Sabia em que projetos Hal trabalhava e quando.

—Há anos que vínhamos a desenvolver uma certa aversão à empresa, por isso não era como se disséssemos: «Vamos enriquecer a companhia». Durante muitos anos [incluindo, segundo Will, o período imediatamente anterior ao aparecimento do bitcoin], mal lhe atribuí trabalho. Assim, tinha anos de emprego totalmente remunerado para desenvolver isto. Era um membro distinto, irrepreensível, com muito tempo livre. Nunca ninguém esteve numa posição tão privilegiada para fazer exatamente isto.

TEMOS A PROVA DE QUE ELE NÃO O FEZ

Em agosto de 2009, Hal anunciou aos colegas do PGP que tinha ELA. Houve uma cerimónia nessa altura, mas só se retiraria oficialmente da empresa no início de 2011, o que também coincidiu com a retirada de Nakamoto do projeto bitcoin.

—Como explicas então as anomalias: os horários de publicação, os espaços duplos, os giros britânicos? —perguntei.

Na sua opinião, eram triviais.

—Com um pseudónimo, estabeleces regras: este tipo acorda às dez, usa espaços duplos, vive em Inglaterra. Essa é a ideia. Crias a personagem, crias vários endereços de e-mail para essa pessoa. O que for necessário. O Hal não era parvo. Sabia que é preciso criar todos estes elementos.

—Mas e o e-mail de Nakamoto para o Hal, onde Nakamoto escreveu: «Isso significa muito vindo de ti, Hal»? A sério que o Hal se escreveria isso a si próprio?

—Eu inverteria essa frase —respondeu Will—. Não é isso que tu farias? Não queres evidências de que comunicaram, de que eras destinatário? Tem de haver provas por e-mail. Subestimam muito o Hal se acham que estas coisas são [difíceis]. Se vais criar um pseudónimo credível, tens de o tornar real.

A Will parecia-lhe ridículo que as pessoas falassem do «computador» do Hal, como se só tivesse um.

—Vimos o computador, o computador tinha estas transações, e agora temos provas de que ele não o fez. E a realidade é, claro, que o homem tinha pelo menos seis computadores.

Quanto a outras questões, como a forma como Hal pôde morrer sem deixar uma fortuna, Will só podia especular. Talvez tenha perdido as chaves. Talvez as tenha escondido. Will disse que tinha apagado a sua publicação no Facebook a pedido da família de Hal, mas agora sentia que a nomeação de Hal como Nakamoto já chegava demasiado tarde.

—Entristece-me que a história não se tenha divulgado —lamentou—. Estou totalmente em desacordo com esses tolos: «Não será melhor nunca o sabermos?». Não, já morreu há oito anos. Acho que deveria receber o reconhecimento. Há quem se ofenda com a ideia de expor o Satoshi… Nunca alinhei nessa corrente. Para mim, foi o Hal que o criou.

Sabia também que havia uma possível explicação, além de Hal simplesmente não ser Nakamoto, para as suas negações tardias e a publicação dos e-mails privados. Ocorreram uma série de acontecimentos que o teriam motivado a redobrar o anonimato, talvez até sem o comunicar à própria família, e que levaram os

UM HOMEM AFIRMOU QUE TINHA ASSASSINADO A ESPOSA E O FILHO E IA SUICIDAR-SE. DEU A MORADA. ERA A DE HAL FINNEY

ASC

Hal e Fran Finney numa fotografia dos anos setenta, décadas antes de Hal se tornar um pioneiro do bitcoin e de enfrentar a devastação da ELA.

Finney a preocuparem-se, compreensivelmente, com que Hal fosse identificado como Nakamoto.

«ESTÁ ALGUÉM A SER ATACADO EM SUA CASA?»

Como que a antecipar possíveis ameaças, na sua mensagem de despedida à comunidade bitcoin, em março de 2013, Hal escreveu: «Os meus bitcoins estão guardados na nossa caixa de segurança…». As especulações públicas sobre Hal como Nakamoto já tinham provocado ameaças, e alguém que se fazia chamar Bitcoin Troll ameaçou os Finney com a publicação de informação pessoal sobre a família na internet se não pagassem um resgate de mil bitcoins. Era mais do que os Finney possuíam, e a ELA é uma doença muito cara, com muitos tratamentos não cobertos pelo seguro. Os Finney precisavam do seu dinheiro para manter Hal confortável, não para pagar a extorsionários.

Na manhã de 29 de maio de 2014, pouco depois da perseguição a Dorian Nakamoto e do artigo da revista *Forbes* onde Hal voltava a negar ser Satoshi, o departamento do *shériff* de Santa Bárbara recebeu uma chamada na sua linha interna. Um homem do outro lado da linha afirmou que tinha assassinado a sua esposa e o seu filho. Agora, disse, ia suicidar-se e queimar a sua casa. Deu a morada. Era a casa de Hal Finney.

A polícia de Santa Bárbara já estava em alerta máximo. Dias antes, um homem chamado Elliot Rodger semeara o terror na Universidade da Califórnia em Santa Bárbara, numa vaga de esfaqueamentos e tiroteios que deixou seis mortos e catorze feridos. Agora a polícia mobilizou-se rapidamente. Várias escolas locais entraram em confinamento. Os vizinhos dos Finney foram evacuados e foi ordenado a outros residentes do quarteirão que se refugiassem em casa. Quando tocou o telefone na casa dos Finney, uma moradia unifamiliar numa rua sem saída, Hal estava a meio de um banho que Fran e uma enfermeira lhe estavam a dar num duche adaptado. Fran demorou um momento a atender. Era um operador do 911, cujas primeiras perguntas foram: «Está bem? Está alguém a ser atacado em sua casa?». O operador prosseguiu: «Devo informá-la de que uma equipa SWAT está prestes a chegar a sua casa e pedir-lhe-á que saiam».

Fran Finney espreitou pelo visor da porta. A casa estava rodeada de polícias com equipamento tático e espingardas de assalto. Um helicóptero sobrevoava a zona. A polícia gritou a Fran que pousasse o telefone e saísse. Jason Finney e a enfermeira de Hal levaram-no para fora; como estava a meio do duche, tinham-lhe desligado o suporte de vida. Durante a meia hora seguinte, enquanto a polícia revistava meticulosamente a casa e o jardim, teve de esperar no relvado, a tremer. Não conseguia engolir e Fran estava constantemente preocupada de que se engasgasse com a própria saliva. «Estava aterrada de que precisasse de sucção ou algo do género —confessou mais tarde à *Wired*—. Não levava nada consigo, exceto o ventilador».

A polícia não encontrou nada. O número de telefone do comunicante não era local. Tinha sido um *swatting*, uma perigosa partida viral na altura. Nem sequer foi a única que os Finney sofreram nesse período, mas foi a que causou mais dano. Ficou também claro que o responsável era o Bitcoin Troll, que há quase um ano acossava os Finney.

AS MEIAS BITCOIN

E não parou. Nos dois meses seguintes ao ataque, telefonou para casa dos Finney nove vezes, ameaçando agredir membros da família e publicar a sua informação pessoal. Nunca foi apanhado.

Fran Finney deixou de falar publicamente sobre Hal e, anos depois, continuava indignada. O incidente não só prejudicou a saúde de Hal e encurtou-lhe a vida, como «lhe roubou parte da paz que poderia ter tido durante os seus últimos meses. Isso consumia-lhe imensa energia emocional».

Atualmente, Fran dedica o seu tempo a combater a ELA. Em 2021, inaugurou uma meia maratona anual, o Running Bitcoin Challenge, para angariar fundos destinados a encontrar uma cura para a doença que lhe tirou a vida ao marido.

Achei bem possível que Will Price, como um caçador de tesouros obcecado nas Montanhas Rochosas ou um pai irresponsável que abandonara o seu bem remunerado trabalho jornalístico para procurar um inventor anónimo e provavelmente impossível de localizar, estivesse a sofrer de apofenia. Mas depois falei com Jon Callas, o especialista em segurança informática que fora diretor científico do PGP e ocupara altos cargos na Apple e na Electronic Frontier Foundation. Jon exibía um bigode farto e tinha um sentido de humor absurdo; certa vez proferiu um discurso de quase três minutos e meio que consistiu simplesmente em repetir a palavra *blockchain* mais de duzentas vezes.

—Em retrospetiva —disse-me Jon—, há conversas que mantive com Hal em que, basicamente, não sabia que ele estava a deixar de trabalhar em bitcoin. Hal falava muito sobre a prova de trabalho, por exemplo. Eu era muito crítico da prova de trabalho. Lembro-me de Hal me dizer: «Tens toda a razão, mas não vejo outra forma de o fazer». Muitos dos que conhecíamos o Hal perguntávamo-nos: «Quem mais poderia ser Satoshi?».

Jon achava que a coincidência geográfica de Hal com Dorian Nakamoto em Temple City não podia ser casual. Não que acreditasse que o Nakamoto da *Newsweek* tivesse algo a ver com a invenção do bitcoin. Simplesmente considerava provável que, quando Hal estava a decidir um pseudónimo, se tivesse inspirado nesse nome. Talvez ao folhear uma lista telefónica local. Talvez, sugeriu um terceiro ex-colega do PGP chamado Gene Hoffman, o conhecesse de alguma das suas viagens.

Da última vez que Jon visitou Hal na sua casa de Santa Bárbara, este já utilizava cadeira de rodas. Mostrou um televisor de ecrã plano e meias de caxemira, conhecidas em casa como «as meias bitcoin», que comprara para a família usando bitcoins. Perguntei diretamente a Hal e ele negou-mo de uma maneira que não consegui saber se era um piscar de olho cúmplice.

Jon também perguntou a Fran e Jason «e ambos o desmentiram». Phil Zimmermann, mentor e chefe de Hal durante muito tempo, também o visitou e perguntou-lhe se era Nakamoto.

A COINCIDÊNCIA GEOGRÁFICA DE HAL COM DORIAN NAKAMOTO EM TEMPLE CITY NÃO PODIA SER CASUAL

THEREGISTER.COM

Gene Hoffman, cofundador da PrivNet em 1996, quando era estudante na UNC Chapel Hill, criou o Internet Fast Forward, o primeiro *software* comercial de bloqueio de publicidade na internet.

—E disse que não. Quero dizer, negou-o rotundamente. Eu também perguntei à esposa. Ela também me disse que não.

Jon era dos que acreditavam que Nakamoto perdera as suas chaves privadas. Talvez começasse a minar na segunda-feira e perdesse as chaves na quinta. Ia começar de novo e desfazer meia semana de trabalho?

O JARDINEIRO INVISÍVEL

Mas Jon não acreditava que a solução para o mistério de Nakamoto fosse tão simples como Satoshi = Hal. Havia um registo público de Hal a correr uma prova de dez milhas em Santa Bárbara na manhã de 18 de abril de 2009, numa altura em que Satoshi Nakamoto estava a enviar um e-mail a outro desenvolvedor do bitcoin.

—É como explicar uma fotografia do Super-Homem e de Clark Kent juntos — assinalou Jon—. Havia também o facto de C, e não C++, ser a principal linguagem de Hal. Portanto, é preciso dizer que este tipo programou em C toda a vida, mas a sua obra-prima não seguiu esse padrão. Fascina-me que, quanto mais se investiga sobre a identidade de Satoshi, mais surgem pequenas anomalias que exigem explicação se se sustentar que Hal e Satoshi são a mesma pessoa, em vez de aparecerem indícios que reforcem essa teoria. Conhece o filósofo Antony Flew? —perguntou-me Jon.

De seguida, Jon explicou-me a parábola do jardineiro invisível de Flew:

—Chegas a um prado no meio da floresta, é belo e parece um jardim, e perguntas: «Quem cuida deste jardim?». E alguém responde: «Vem um jardineiro, mas ninguém o viu». Então propões uma série de coisas: «Porque não pomos campainhas

A 18 DE ABRIL DE 2009, HAL PARTICIPOU NUMA CORRIDA; NESSE MOMENTO, NAKAMOTO ESTAVA A ENVIAR UM E-MAIL

nos arbustos para tentar detetar o jardineiro?». Como as campainhas não tocam, alguém responde: «O jardineiro deve ser muito cuidadoso». E depois as desculpas multiplicam-se em cascata, no que se chama «morte por mil nuances». Podes argumentar: «Talvez o Hal estivesse numa maratona e tivesse pedido ao Jason que o fizesse». Mas então estás a complicar desnecessariamente a tua teoria, a ser demasiado engenhoso. Já não é simplesmente o Hal ser Satoshi, mas o Hal juntamente com o Jason. A explicação perde coerência com o tempo.

Em suma, Jon acreditava que Hal não atuara sozinho.

Eu, há bastante tempo, estava convencido de que Nakamoto não era um grupo. Ao que parecia, Jon precisava que lhe esclarecessem algumas coisas.

—O que disse Ben Franklin? Duas pessoas podem guardar um segredo se uma delas estiver morta? —inquiri.

Esperei pacientemente que surgisse o lampejo de compreensão nos olhos de Jon quando a lâmpada se acendesse no seu adorável e ingénuo cérebro.

—Três pessoas podem guardar um segredo se duas delas estiverem mortas —corrigiu-me Jon.

Era uma expressão que utilizava frequentemente nas suas conferências. Afinal, era um destacado engenheiro de segurança.

SIMON LAW

Len Sassaman, especialista em criptografia e defensor da privacidade, trabalhou no PGP, em *remailers* anónimos e em projetos de privacidade digital antes de se suicidar em 2011.

—Bem, neste caso, uma das pessoas está morta —disse Jon—. Acho que eram duas pessoas. Acho que eram Hal e mais alguém. Talvez até uma terceira. Vi todas as teorias sobre quem poderia ser Satoshi. Penso que há rastos por todo o lado a sugerir que várias pessoas trabalharam juntas.

Perguntei em voz alta se Hal poderia ter-se associado a Len Sassaman. Depois de falar com Evan Hatch, que foi o primeiro a avançar a teoria de Sassaman, contactei Bram Cohen, que partilhara casa com Sassaman em São Francisco e escrevera o artigo «Pynchon Gate» com ele e outra pessoa. Bram disse que não considerava impossível que Sassaman tivesse sido Nakamoto.

—Sassaman sempre mostrara um grande interesse pelo anonimato —comentou-me Bram, enquanto uma roda gigante para gatos girava lentamente atrás de si—. Tenho uma vaga memória, sobretudo porque Len me contou e eu não prestei muita atenção, de um pseudónimo chamado Product Cypher que publicava anonimamente na lista *cypherpunks* e depois desapareceu. A insinuação parecia ser que era Hal ou Len ou alguma combinação de ambos.

PROCURAR ENTRE OS EXTROPIANOS

Sassaman insistira com Bram para que publicasse o BitTorrent de forma anónima «para demonstrar que era algo razoável», embora este tivesse ignorado o conselho.

—Não creio que Len tivesse os conhecimentos técnicos para o desenvolver por si só —prosseguiu Bram—, mas quase tudo nos escritos de Satoshi coincide com o seu perfil. Em particular, as publicações públicas. Essa falsa identidade britânica. A Europa. O seu *modus operandi*. A lista de *cypherpunk* estava a desaparecer nessa altura. Parece-me bastante plausível que Hal e Len tenham unido forças. Ambos estavam muito interessados neste conceito de dinheiro na internet. Len falava com entusiasmo sobre isto.

Mas Jon Callas, que trabalhara com Sassaman no PGP, duvidava que ele tivesse feito parte de alguma colaboração com Nakamoto.

—Sassaman era mais uma pessoa de controlo de qualidade do que um programador, isto é, alguém que testa o código em vez de o escrever.

E, tal como Ben Laurie, Jon não acreditava que Sassaman tivesse sido capaz de manter um segredo assim.

—Len também era um amigo meu muito próximo. Não creio que estivesse envolvido —afirmou.

Jon pensava que o melhor lugar para procurar um possível colaborador de Hal seria entre os extropianos, o grupo a que pertenciam Hal, Wei Dai e Nick Szabo.

—São pessoas extraordinariamente inteligentes, eruditos autodidatas. E alguém com conhecimentos básicos de criptografia que fizesse as perguntas certas e discretas seria um bom candidato para trabalhar com Hal.

Refleti sobre os intermitentes giros britânicos. As mudanças de tom entre o ideológico («um novo território de liberdade») e o distante («o ponto de vista libertário»). A presença tanto do estilo caraterístico de Donald como de evidências de uma personalidade mais equilibrada («coitadinha»). Um criador coletivo explicaria várias destas inconsistências. ■

A navalha de Ockham

SHUTTERSTOCK

A navalha de Ockham sugere que a explicação mais simples é que Satoshi foi um indivíduo brilhante a trabalhar sozinho ou com colaboração mínima, e não uma equipa corporativa secreta.

Pouco depois das minhas conversas com Will e Jon, almocei com o meu amigo Andrew e contei-lhe a minha revelação. — Não é um grupo — afirmou, categórico. Era evidente que não fazia ideia do que eu estava a falar, mas acompanhei-o:

— Por que é que estás tão seguro?

— A navalha de Ockham — respondeu —. Duas pessoas não conseguem guardar um segredo…

— Três pessoas — corrigi-o, com alguma petulância —. Sim, eu também sempre me inclinei para essa opinião, mas…

Então repeti-lhe alguns dos argumentos do Jon Callas, como o de que um grupo explicaria porque é que cada candidato individual plausível apresentava anomalias. Esforcei-me por recordar conspirações bem-sucedidas. Não havia muitas.

— A NSA guarda segredos constantemente — observei.

Aliás, continuei, ainda antes de três criptógrafos californianos inventarem a criptografia assimétrica nos anos 1970, um trio em Inglaterra alcançara, de forma independente, o mesmo avanço. Mas, ao contrário dos norte-americanos, os três britânicos trabalhavam para o GCHQ, a agência de informações de sinais do Reino Unido, e a descoberta permaneceu oculta até ser finalmente desclassificada em 1997, passados vinte e cinco anos.

ASC

O assalto em Media, na Pensilvânia, que expôs o COINTELPRO demonstra que pequenos grupos conseguem manter segredos.

O PRECEDENTE HISTÓRICO

Andrew acompanhou-me por instantes, mencionando o COINTELPRO. Em 1971, um grupo de oito ativistas, que se autodenominavam Comissão Cidadã para Investigar o FBI, arrombara uma fechadura e abrira outra com uma alavanca para aceder a um escritório local perto de Filadélfia. Levaram malas repletas de documentos e enviaram-nos a jornais, revelando o programa do FBI de vigilância nacional e assédio a grupos políticos dissidentes, com o nome de código COINTELPRO. O FBI investigou o assalto até 1976, quando o crime prescreveu. Os autores tinham jurado manter em segredo as suas ações e nunca mais voltaram a reunir-se como grupo. Apenas 43 anos após o assalto, três dos oito confessaram a sua participação.

Portanto, sim, acontecia muito raramente.

Percebi que o Andrew continuava cético.

Mas, depois de anos a pensar que era improvável que Nakamoto fosse um grupo, agora acreditava no contrário. ■

Vincent Adult man

Vincent Adultman é uma personagem da série de animação *BoJack Horseman*, onde três crianças se escondem debaixo de um sobretudo fingindo ser um adulto. A metáfora de Vincent Adultman aplicada a Satoshi Nakamoto é a ideia de que várias pessoas se revezavam a escrever código, o que explicaria as inconsistências estilísticas.

NETFLIX

Não houve qualquer teste de paternidade para o bitcoin. Não existiu nenhum baú do tesouro que confirmasse que as pistas tinham sido interpretadas corretamente. Não havia forma de provar quem era Nakamoto a menos que ele se apresentasse e demonstrasse possuir as chaves privadas pertinentes, ou pelo menos documentos contemporâneos autênticos que sustentassem a sua história. O mais perto que alguém poderia chegar, em teoria, seria se Nakamoto tivesse cometido um erro ou confiado em alguém. Mas, com o passar dos anos, o rasto, se é que existia, tornava-se cada vez mais ténue. Talvez Nakamoto tivesse tornado impossível, mesmo para si, provar a sua identidade, ao desfazer-se das suas máquinas, das suas chaves privadas e das palavras-passe de e-mail, sem jamais revelar o seu segredo a ninguém.

DOC SEARLS

Ben Laurie é um informático britânico conhecido pelo seu trabalho em segurança informática e criptografia.

NÃO EXCLUIR NINGUÉM

Ben Laurie argumentara que, a menos que a rede bitcoin representasse pelo menos 50 % da capacidade computacional total do mundo, estaria sempre vulnerável a um ataque de uma rede maior. Com Nakamoto passava-se algo semelhante: a menos que se dispusesse de uma amostra de escrita de cada falante de inglês vivo em 2008 e de uma amostra de código de cada programador de C ou C++, nunca se poderia ter a certeza de que alguém identificado pela estilometria como a aproximação mais próxima fosse realmente Nakamoto.

Mesmo que todos, ou quase todos, os escritos de Nakamoto pudessem ser atribuídos a uma só pessoa, outros poderiam ter concebido, desenhado e programado o bitcoin. Continuava a achar que um Nakamoto coletivo explicaria muitos aspetos, incluindo o uso que ele fez de três contas de e-mail e a notável segurança do código original do bitcoin, algo difícil de alcançar para um programador solitário.

Pensei em várias combinações. Quando se ouvem cascos, pensa-se em cavalos, não em zebras: parecia-me esmagadoramente óbvio que Nick Szabo estivera envolvido de algum modo; que, mesmo não sendo Nakamoto, pelo menos sabia mais do que

UM NAKAMOTO COLETIVO EXPLICARIA O USO POR PARTE DELE DE TRÊS CONTAS DE E-MAIL

deixava transparecer. Talvez tivesse ficado nos bastidores, e alguém se encarregara da programação e das interações com a comunidade. Quanto a Hal Finney, embora não tivesse sido o mais próximo segundo a estilometria textual ou de código, estava suficientemente perto para que nenhuma dessas análises o tivesse descartado.

Considerei diferentes equipas. Nick Szabo e Hal Finney. Nick Szabo, Hal Finney, Ray Dillinger e Travis Hassloch. Três destes quatro, mais Ben Laurie ou Bram Cohen ou Zooko Wilcox ou James Donald. Gwern Branwen especulara sobre Elaine Ou, uma desenvolvedora de *blockchain* mais jovem, cronista ocasional na *Bloomberg*, experiente programadora de C++, e esposa de Nick Szabo. Era de Los Angeles. Em fevereiro de 2009, tuitou: «A trabalhar em algo fantástico». Havia certa harmonia temática na ideia de Nakamoto como grupo. O bitcoin era descentralizado. O seu criador também. «Recordemos o desejo de Nero de que Roma tivesse um só pescoço que pudesse cortar. Se lhes fornecermos esse pescoço, cortá-lo-ão». Uma identidade distribuída permitiria a qualquer membro negar, sinceramente, ser o Satoshi.

ASC

Elaine Ou é engenheira na Global Financial Access, em São Francisco, e cronista da *Bloomberg Opinion* sobre criptomoedas.

Imaginava Nakamoto como Vincent Adultman, a personagem de BoJack Horseman, que são três miúdos com um sobretudo a fazer-se passar por um adulto. Talvez os membros de Nakamoto se revezassem. Quando Nakamoto escreveu «não sou advogado» e «dou-me melhor com códigos do que com palavras», Nick Szabo estava fora de serviço. Quando Nakamoto escreveu «non-fencible», James Donald estava aos comandos.

PODERIA SER UMA EQUIPA DA NSA...

A minha compreensão de Nakamoto também era descentralizada, uma nuvem de influências e possibilidades. Talvez fosse uma das pessoas já suspeitas. Talvez fossem várias delas. Ou talvez estivéssemos todos bêbedos debaixo de um candeeiro, a procurar onde havia luz, enquanto Nakamoto permanecia oculto nos arbustos. Afinal, podia ser uma zebra. Podia ser uma mulher. Podia ser uma equipa da NSA.

Se Nakamoto ainda estivesse vivo, perguntava-me o que pensaria da sua criação. Embora o bitcoin se tivesse tornado extremamente valioso e quase convencional, não se podia afirmar, em 2024, que tivesse cumprido a visão do seu criador. Ainda não funcionava como um sistema de dinheiro. Poder-se-ia argumentar que continuava muito centralizado, com quatro grupos de mineração a controlarem mais

RAY DILLINGER CONSIDERARA O BITCOIN «UM FRACASSO E UM DESASTRE» E VENDEU TODAS AS SUAS MOEDAS

de 75 % da rede, e apenas dois a controlarem mais de 53 %. A sua privacidade, tão elogiada inicialmente, revelou-se largamente sobrestimada. Nunca se libertara da dependência das plataformas de troca como pontes a partir do sistema de moeda fiduciária, um número surpreendente dessas plataformas mostrara-se pouco fiável, e esses estrangulamentos eram cada vez mais suscetíveis de ser regulados. O bitcoin continuava a ter dificuldades em escalar.

O fosso entre as origens do bitcoin e o seu uso principalmente como ativo especulativo ou reserva de valor desanimara pessoas que, de outro modo, poderiam tê-lo apreciado. «Eu diria que o Satoshi está, no mínimo, a dar palmadas na cara por isto ou a resmungar: "Para isso não o construímos"», comentou Jon Callas. Leslie Lamport, que fundou a teoria da computação distribuída, base tanto da internet como dos computadores multiprocessador, e foi um dos primeiros a definir o problema de coordenação de rede que o bitcoin tentou resolver, disse-me: «Vejo muito pouco uso real para isto, além de criar uma criptomoeda para criminosos». O herói *cypherpunk* Phil Zimmermann, cujo portátil agora ostentava um autocolante com um rosnado («crypto significa criptografia»), classificou o bitcoin como «uma vergonha» e «um gueto de criminalidade e fraude». Mike Hearn, um dos primeiros programadores principais que se sentira frustrado com a resistência à escalabilidade, vendera as suas moedas, abandonara o projeto e declarara que fora «uma experiência que falhou». Ray Dillinger, do mesmo modo, considerara o bitcoin «um fracasso e um desastre» e vendeu todas as suas moedas.

SHUTTERSTOCK

Ray Dillinger é criptógrafo e programador que participou em fóruns de criptografia e na comunidade *cypherpunk*.

—Estou realmente desgostoso com o que aconteceu com a especulação da *blockchain* —confidenciou-me—. Tenho esta ideia antiquada de que os negócios devem deixar tanto o vendedor como o cliente em melhor posição, e quando fazes especulação, que é basicamente no que o bitcoin se tornou, por cada vencedor tens sempre um perdedor equivalente.

Quanto a Nakamoto, Ray acrescentou:

—Acho que o Satoshi ficaria aborrecido com o que aconteceu. Ele imaginou aquilo a que eu chamaria usos respeitáveis do bitcoin, mesmo depois de ter ficado fora do alcance das pessoas comuns.

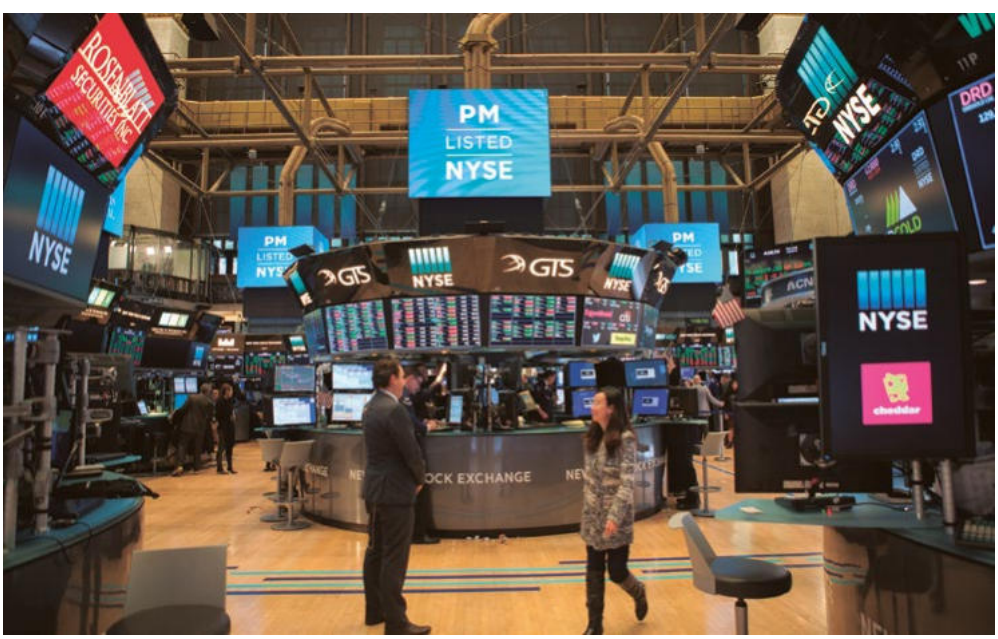
PROVAS DE CONHECIMENTO ZERO

Ray referia-se ao facto de Nakamoto sempre ter esperado que o bitcoin evoluísse de algo com que os indivíduos interagiam para uma infraestrutura de fundo para um novo sistema financeiro construído sobre ele.

—Ele não esperava que as pessoas fossem aldrabar outras com toda esta publicidade excessiva. Por isso, sim, a sua partida pode ter sido como levantar as mãos e dizer: «Já chega».

Até Tim May escrevera, antes de morrer: «Acho que Satoshi estaria enojado», embora, no seu caso, a queixa fosse sobre o quão obediente à lei se tornara a indústria das criptomoedas.

Mas, apesar de todas as fraudes descaradas, dos falsos utópicos e dos executivos de Wall Street que papagueiam o jargão *cypherpunk*, alguns dos *cypherpunk* mais clarividentes — e candidatos a Nakamoto — conseguiram ver para lá do crime, da especulação, da política e da estridência das criptomoedas. O bitcoin cumprira a sua missão. Fora uma experiência necessária, uma prova de conceito que, ao derrubar barreiras conceptuais e técnicas antes consideradas intransponíveis, abrira novas perspetivas de possibilidade e invenção. Estes mais otimistas mantinham os olhos postos num futuro que ainda consideravam inevitável. Zooko Wilcox, desde os seus dias como um jovem de dezanove anos que abandonou a universidade e



SHUTTERSTOCK

Desde a irrupção do bitcoin e das criptomoedas, Wall Street convive com um novo modelo de mercado digital descentralizado que redefine o valor do dinheiro.

SE HAL ERA NAKAMOTO, ENCONTRARA A MANEIRA DE CRIAR UM ABISMO INTRANSPONÍVEL ENTRE A SUSPEITA E A PROVA

se tornou programador júnior na DigiCash em meados dos anos 1990, focara-se na importância de preservar a privacidade. Quando surgiu o bitcoin, admirava o que este tentava fazer, e chegou a «adorar» Nakamoto, mas «compreendi imediatamente que a sua falta de privacidade era um defeito fatal e que, em última instância, o destruiria». Também observara como o bitcoin «se ia ossificando». Depois de outros informáticos descobrirem, em 2013, uma forma de utilizar uma criptografia de vanguarda que prioriza a privacidade, chamada provas de conhecimento zero, para criar um bitcoin melhorado, Zooko dedicou-se a desenvolver uma criptomoeda chamada Zcash utilizando o novo método.

OURO DIGITAL PARA OS PRÓXIMOS MILÉNIOS

James Donald, por seu turno, mantinha uma visão equilibrada e ampla, lamentando a falta de anonimato e a relativa centralização do bitcoin, mas elogiando a sua rapidez e conveniência para o «branqueamento de capitais» e vendo como promissoras as recentes inovações de *software* que melhoravam a privacidade e permitiam transações mais rápidas na rede. Nick Szabo tornara-se brevemente defensor do ethereum, apenas para o denunciar mais tarde como «uma shit-

SHUTTERSTOCK

Zooko Wilcox-O'Hearn propôs-se criar uma versão melhorada do bitcoin. Desse trabalho nasceu a Zcash, uma criptomoeda centrada na privacidade e na segurança dos utilizadores.

coin» que «se transformara num culto centralizado». Parecia desdenhar a normalização das criptomoedas, escrevendo: «Multidões e charlatães entraram nos espaços das criptomoedas e dos contratos inteligentes que não só carecem dos valores *cypherpunk*, como odeiam os valores *cypherpunk*, incluindo a minimização da confiança que confere às criptomoedas como o bitcoin os seus valores de mercado». Ainda assim, isso não o impedira de acrescentar ao seu avatar do Twitter uns olhos laser «maxi» de bitcoin. E Adam Back, cujo avatar também tinha olhos laser, apostou na criptomoeda original, adotando com entusiasmo o meme *hodler*, chamando ao bitcoin «ouro digital para os próximos milénios», celebrando cada subida de preço, enaltecendo simultaneamente os valores *cypherpunk* e as notícias sobre a adoção institucional, e dirigindo uma das maiores empresas privadas do setor.

Eu continuava apenas com teorias, umas mais interessantes do que outras. Havia muitas razões para pensar que Hal Finney fora Nakamoto — e para o desejar. Mas, sempre que me sentia tentado a aceitar essa resposta satisfatoriamente simples, as inconsistências inquietavam-me. O facto de tanto a estilometria textual como a de código terem encontrado outras pessoas (Hassloch, Dillinger, Laurie) como coincidências mais próximas. As trocas de e-mails que pareciam naturais entre Hal e Nakamoto, tanto em público como em privado. Estes elementos eram lacunas que eu não podia ignorar. Se Hal era Nakamoto, encontrara a maneira de criar um abismo intransponível entre a suspeita e a prova.

A MINHA ÚLTIMA PISTA SÓLIDA

Ficava sempre uma ponta solta. Alguns dos *cypherpunk* mais interessados em dinheiro digital, incluindo Finney e Szabo, nunca tinham negado conhecer a identidade de Nakamoto, mas também não tinham afirmado sabê-la. Houve uma exceção. «Sei quem era Nakamoto», escrevera James Donald, num comentário a outro comentário numa entrada do Jim's Blog, «e quais eram os seus objetivos políticos e sociais». Isto fez de James o único *cypherpunk* original que declarara publicamente algo tão categórico sobre a identidade de Nakamoto. Talvez, fiel à sua persona online, estivesse a fanfarronar e, quando afirmou sabê-lo, na realidade apenas sugerisse ter um candidato preferido. Mas era alguém que podia realmente sabê-lo com certeza, o que o tornava a única pessoa a possuir esse conhecimento de modo inequívoco. Era a minha última pista sólida, ou o que realmente parecia sê-lo, e decidi que, afinal, devia ir procurá-lo.

Ao examinar os registos de avaliação imobiliária das diversas propriedades de James nos Estados Unidos, descobri que, durante um par de anos na década de 2000, uma casa que possuía em Austin constava em nome de James com um endereço postal na costa nordeste da Austrália. Em avaliações mais recentes, as propriedades norte-americanas estavam registadas em seu nome na mesma cidade australiana, embora agora surgisse apenas um apartado de correio. Claramente, James era ou fora proprietário de uma habitação ali. Mas desenvolvera a maior parte da sua carreira na Califórnia, e eu não percebia como encaixava a propriedade australiana na sua constelação de residências. Residia ali permanentemente? Só parte do ano? Funcionava principalmente como endereço de correspondência? O apartado indicava que já não vivia naquele endereço postal?

Sabia que a sua esposa falecera em 2016 e, utilizando o site Find a Grave, encontrei uma fotografia do cemitério da cidade australiana com uma placa em sua memória. Assim, James provavelmente vivera ali pelo menos até então. Cinco anos depois, publicou no seu blogue uma pequena foto do que parecia ser a vista da sua varanda: em primeiro plano, um pequeno copo e uma jarra de um licor que descreveu como caseiro. Ao longe, via-se um mar azul intenso, com o horizonte interrompido por um par de pequenas ilhas. Comparei essa vista com outras imagens da paisagem marítima tiradas a partir da mesma cidade, e pareciam coincidir. Portanto, ele permanecia ali pelo menos até 2021. Mas podiam ter acontecido muitas coisas nos três anos seguintes. Não ia dar a volta ao mundo sem confirmar que continuava ali. Já começara a procurar voos, e nenhum era simples. Um dos mais rápidos incluía três escalas e passava pelas Fiji.

Procurei na internet detetives privados em Queensland e encontrei um, Daniel Quinn, que vivia a uma distância razoável de carro da cidade costeira onde suspeitava que James morava. Enviei a Daniel o endereço da casa e uma foto de James de há vinte anos que encontrara num blogue universitário abandonado de um dos seus filhos.

Uns dias depois, Daniel remeteu-me um relatório das suas primeiras horas de vigilância. «O jardim está muito descuidado, com a relva muito alta e arbustos e árvores demasiado frondosos, definitivamente não é um amante das plantas». Anexou uma foto da casa de James e do caminho de entrada, esburacado, que partilhava com outras duas habitações. Havia uma palmeira solitária junto ao passeio e, subindo a colina, um bangaló sobre estacas, no meio do mato, com uma varanda virada ao Mar do Coral.

EM ALGUM MOMENTO PRECISAVA DE PARAR

Daniel não viu James nesse dia, mas, num sábado de manhã, várias semanas depois, acordei com uma mensagem: Daniel conseguira fotografar um homem de pé à porta da casa. Era evidentemente vinte anos mais velho do que o homem da foto que eu enviara. Mantinha a mesma barba cerrada, embora agora branca. Usava óculos grandes de armação metálica semelhantes. Conservava o mesmo nariz carnudo. Três dias depois, seguia viagem para a Austrália.

Havia uma porta mosquiteira e não havia campainha, por isso bati na ombreira da porta de James. Deixara o carro no sopé da colina e estava sem fôlego depois de subir pelo íngreme caminho de entrada, desviando-me por entre bananeiras e tomando a vereda de gravilha até à sua casa. Tinha a boca seca de nervos. Estava convencido de que James não era Nakamoto, mas não excluía que pudesse ter feito parte do projeto, e era a única pessoa que eu conhecia que poderia ter a resposta que procurava.

Comecei, porém, a refletir sobre como James encararia a minha visita. Muita gente pode ver um repórter à porta como algo intrusivo e incómodo, mas não mais do que uma Testemunha de Jeová ou um avaliador imobiliário não convidado. James, no entanto, esforçara-se por se tornar impossível de localizar. Vivia no fim de um caminho privado subindo uma colina escarpada. Aquele era o seu refúgio secreto.

Chegara à cidade no dia anterior, depois de voar para São Francisco, depois para

UMA VIAGEM DE 37 HORAS PARA UM ENCONTRO DE TRÊS MINUTOS. NINGUÉM DEDICARA TANTO TEMPO A RESOLVER ESTE ENIGMA

Melbourne, depois para Brisbane e, finalmente, para uma pequena localidade em Queensland, onde alugara um carro e conduzira quarenta minutos até à costa. Antes de sair dos Estados Unidos, escrevera a James mais uma vez, que deixara de me responder no outono anterior depois de eu lhe perguntar sobre os paralelos entre ele e Nakamoto. Agora, mencionava-lhe que ia estar na Austrália e perguntava-lhe se podíamos encontrar-nos. Queria pelo menos avisá-lo de que sabia em que continente se encontrava e tentar uma abordagem mais cortês.

Não respondera, por isso agora optava por algo mais direto. Ao atravessar o alpendre rumo à porta principal, pude ver James através de uma janela de vidro, sentado em frente a um computador na sala de estar, com os auscultadores postos. A sua última entrada no blogue, publicada apenas umas horas antes, era uma divagação sobre como os georgianos (do país Geórgia) não querem que «as suas igrejas sejam destruídas ou transformadas em santuários de Gaia e sexo gay, que os seus velhos e belos edifícios sejam arrasados e substituídos por monstruosidades pós-modernas e demoníacas». As ONG ocidentais estavam a trabalhar para que «a Geórgia ficasse "maricas" e fosse atirada para a picadora de carne contra a Rússia».

SHUTTERSTOCK

Brisbane, na Austrália, tem surgido em investigações sobre as origens do bitcoin, já que vários programadores e empresários tiveram ligação a Queensland.

O alpendre tinha algumas plantas de interior e oferecia uma vista panorâmica do Pacífico. Passado um minuto, tentei bater diretamente à porta principal. Um momento depois, James abriu-a e saiu.

Era mais magro do que eu esperava e vestia umas ceroulas pretas e uma camisa de manga comprida com camuflado vermelho.

Comecei a falar. Tinha-lhe enviado um e-mail e…

—Oh, sou bastante esporádico a ler os meus e-mails —respondeu James.

Não recebera o meu. Recordei-lhe a nossa troca do ano anterior e o livro que eu estava a escrever.

—Ah, claro —disse James.

Exprimi algo sobre como me apresentar em sua casa teria sido imperdoável se não tivesse esgotado todas as possibilidades de falar com ele.

—Está bem —disse James—, bom, em resumo, não te posso dizer o que não te digo. —O tom era afável, perplexo.

Assinalei que era o único *cypherpunk* que insistira publicamente em que sabia quem era Nakamoto e quais eram os seus objetivos sociais e políticos.

—Podes dar mais detalhes?

—Não, lamento.

—Está bem. Sabes mesmo? Ou achas que tens uma ideia bastante clara de quem poderá ser?

—Tenho uma ideia muito clara de quem poderá ser, mas, na realidade, não, não.

—Achas que foi Hal Finney?

—Não posso responder a isso.

—É apenas por respeitares a sua privacidade?

—Não me é permitido dizer nada a ninguém, e não me é permitido dizer às pessoas o que já lhes disse.

—Posso convidar-te para uma cerveja enquanto estou na cidade?

—Ah! —exclamou James—. No álcool está a verdade. E eu estou obrigado a não dizer a verdade às pessoas.

—Tomamos o pequeno-almoço? —propus—, assim não há álcool a revelar a verdade.

James riu-se.

—Olhe —disse—, tenho tendência para falar demais, e tenho grande tendência para falar demais depois de uns copos, por isso lamento.

Procurei prolongar a conversa, deixando-lhe os meus contactos e outro livro que escrevera, que pensei que pudesse apreciar, mas as respostas dele tornaram-se monossilábicas. Fiquei com a sensação de que, depois do choque inicial, agora calculava como e porquê é que um estranho intrometido aparecera no seu alpendre.

—Bem, percebo porque vives aqui —disse, apontando a sua impressionante vista.

—Sim —disse James, olhando para o mar.

Agradeci-lhe e desci de novo a colina.

A HBO EM BREVE AMPLIARIA A LISTA DE CONJETURAS SOBRE NAKAMOTO COM O DOCUMENTÁRIO *MONEY ELECTRIC*

Tinha aprendido a programar, carregara com o meu portátil sobreaquecido e a minha preocupação obsessiva a minha paciente família, recrutara um perito em aprendizagem automática, um especialista em estilometria e um detetive privado, e havia feito uma viagem de 37 horas para um encontro de três minutos. Estava bastante certo de que ninguém dedicara tanto tempo como eu a tentar resolver isto. Tinha sido cuidadoso em não me fixar num único candidato ou teoria sem provas sólidas, mas começava a sentir afinidade com Sahil Gupta, que não se deixava demover da ideia de que Nakamoto era outra pessoa que não Elon Musk. A certa altura, precisava de parar.

ARGUMENTOS A FAVOR E CONTRA QUALQUER COLABORADOR

A HBO em breve ampliaria a lista de conjeturas sobre Nakamoto com um documentário *intitulado Money Electric* que nomeou Peter Todd, o antigo programador principal do bitcoin, como o seu criador. Todd era um suspeito relativamente invulgar e o cineasta, Cullen Hoback, reunira um punhado de coincidências intrigantes, incluindo uma das primeiras publicações de Todd no fórum do Bitcoin, cujo momento e conteúdo, argumentava Hoback, sugeriam ter sido uma sessão iniciada por engano por Nakamoto utilizando a conta de Todd. Achei a teoria interessante. Não estava convencido de que fosse correta, mas, pelo menos, parecia plausível. Todd negou, mas eu sabia que isso pouco valia.

A comunidade do bitcoin, em geral, opôs-se pelas razões habituais: o documentário colocou Todd sob os holofotes e era melhor para o bitcoin que Nakamoto continuasse desconhecido. Os bitcoiners mostraram-se também rotundamente céticos de que Hoback tivesse razão e algumas das suas críticas

HBO SCREENGRAB.

Peter Todd, o antigo programador principal do bitcoin, foi nomeado no documentário Money Electric, da HBO, como o criador do bitcoin.

específicas, embora meramente intuitivas, pareciam dignas de ser levadas a sério: Amir Taaki, o antigo programador principal do bitcoin, reiterou todas as razões pelas quais o código de Nakamoto parecia apontar para um autor mais velho. Jens Ducrée, o estudioso de Nakamoto, recordou numa nova atualização da sua obra de oitocentas páginas sobre a questão de Satoshi que Nakamoto falara de «tipos de transação que concebi há anos», incluindo «contratos de fiança» e «arbitragem multipartes», o que dificilmente parecia condizer com as palavras de um estudante de Artes de vinte e três anos em Toronto, que era o que Todd era na época. Adam Back perguntou-se se Satoshi Nakamoto, mestre de OPSEC e anónimo convicto, aceitaria ser entrevistado várias vezes perante câmaras para um documentário. «Não creio que Satoshi vá ser identificado neste momento —disse-me Back num e-mail—. Podem construir-se argumentos igualmente a favor e contra qualquer colaborador anterior ou investigador de dinheiro eletrónico».

Chamou-me especialmente a atenção que, embora Hoback se descrevesse como «muito, muito seguro» de ter encontrado Nakamoto, não tentara corroborar a sua afirmação utilizando a estilometria. Quando Gideon Lewis-Kraus, do *New Yorker*, lhe perguntou porquê, Hoback disse que estava satisfeito em «deixar esses detalhes como um exercício para o público».

Recolhi à pressa mais de vinte mil palavras de prosa escrita por Todd de várias fontes na internet e enviei-as a Florian Cafiero, o especialista em estilometria. Enquanto reunia o texto, reparei que Todd, ao contrário de Nakamoto, cometia muitos erros tipográficos. Enviei também vários programas que Todd escrevera em C e C++ antes do bitcoin, alguns da sua página pública no Github e outros que o próprio Peter me enviara a meu pedido, a Brian Timmerman, o perito em aprendizagem automática.

HBO SCREENGRAB.

Com um enfoque que combina história e investigação, Money Electric explora as origens do bitcoin e o mistério que envolve o seu criador, Satoshi Nakamoto.

A IA SERÁ CAPAZ DE O DIZER A QUALQUER MOMENTO

Brian respondeu que a maioria dos programas eram demasiado leves e repetitivos para fornecer muita informação, mas assinalou que os artefactos no código apontavam para terem sido criados no sistema operativo Linux, utilizando o editor de código Vim. Isto coincidia com o que eu sabia da história de Peter de programar principalmente para Linux e diferia das ferramentas que Nakamoto utilizara ao criar o bitcoin: o sistema operativo Windows e o editor de código VS. De facto, quando procurou criar uma versão para Linux do seu programa, Nakamoto pedira — e aparentemente precisara — da ajuda de outros programadores. Vi também que Peter, ao contrário de Nakamoto, não utilizara notação húngara no seu código.

Havia um programa que Peter me enviou, para um videojogo chamado Corporate Raiders que escrevera em 1999, que era suficientemente substancial para que Brian fizesse uma estilometria de código. Quando Brian executou os seus modelos de classificação no conjunto de candidatos que já avaliara, com Peter agora incluído, Ben Laurie continuava a ser a correspondência mais próxima para os dois ficheiros principais do bitcoin (main.cpp, node.cpp). Peter era o mais semelhante apenas para um ficheiro do bitcoin chamado node.h. Pedi a Brian que sintetizasse a importância das suas conclusões. «Eu diria que estas

EM 2013 ZOOKO WILCOX-'HEARN ESCREVEU QUE «SATOSHI SERÁ, OU JÁ FOI, DESANONIMIZADO»

NICK BRADSHAW

Jens Ducrée dedicou anos a compilar um manuscrito de 800 páginas tentando decifrar a identidade de Satoshi Nakamoto através de análises linguísticas, técnicas e contextuais.

TOBIAS KLENZE

Zooko Wilcox-O'Hearn durante a sua intervenção no 34.º Congresso do Caos da Comunicação (CCC), Leipzig. Zooko desenvolveu a criptomoeda Zcash.

AS MEMÓRIAS ESBATEM-SE. AS PESSOAS MORREM. O TEMPO ERA O INIMIGO DE UMA SOLUÇÃO

provas são indeterminadas e não apontam com força para ninguém no grupo de candidatos», respondeu. Quanto a Peter especificamente, «mesmo neste contexto de não haver afirmações sólidas, os resultados realmente não apontam na sua direção».

Florian e Jean-Baptiste Camps, depois de um fim de semana atribulado a voltar a executar os seus modelos com Peter incluído, não encontraram indícios de que ele fosse o autor de nenhum dos escritos de Nakamoto. «Não creio que seja o Todd», concluiu Florian.

Pensei que Hoback fizera uma contribuição valiosa para o cânone das teorias sobre Nakamoto, mas provavelmente estava errado. Ao apresentar uma afirmação muito discutível com tanta autoconfiança, tornara-se o mais recente caçador de Nakamoto a enredar-se imprudentemente na armadilha de quem é Satoshi. «É irónico —disse Peter Todd à CoinDesk— que um realizador também conhecido por um documentário sobre o QAnon tenha recorrido aqui ao pensamento conspirativo baseado em coincidências ao estilo do QAnon».

Havia quem achasse que uma resposta era inevitável. Zooko Wilcox, que em 2013 escrevera que «Satoshi será, ou já foi, desanonimizado» por estilometria, e que não há nada que eles nem ninguém possam fazer para o evitar, manteve esta crença mais de uma década depois. «Continuo a achar que tenho razão — disse-me—. Creio que sim, a IA será capaz de nos dizer a qualquer momento», a menos que quem estivesse por detrás de Nakamoto nunca mais publicasse nada na internet. Mas eu estava convencido de que talvez nunca soubéssemos, para além de qualquer dúvida razoável, quem era Nakamoto. As memórias esbatem-se. As pessoas morrem. O tempo era o inimigo de uma solução. Embora provavelmente tivesse descartado algumas possibilidades, não podia dizer que estivesse mais perto da resposta. Ele, ela ou eles bem poderiam estar nestas páginas. Mas, a menos que soubesse quem era Nakamoto, ainda poderia ser alguém de quem nunca ouvira falar. O último grande mistério por resolver podia continuar a sê-lo.

Senti certo alívio ao aceitá-lo. Continuava deslumbrado com o feito da invenção de Nakamoto, mas quase igualmente com a perfeição do seu desaparecimento. E, à medida que ensaiava mentalmente cada cenário, nenhum — e nenhum que me ocorresse — suplantava o mistério em si. Talvez algo que começara por razões quotidianas tivesse adquirido uma mística que não merecia. «O caso Watergate mudou a história —escreveu Bob Woodward uma vez sobre o papel de Mark Felt como "Garganta Funda"—, e existe certamente uma tendência, da minha parte e da de muitos outros, para associar um resultado épico a um motivo épico. Talvez seja um exagero desnecessário».

Ou talvez o bitcoin tenha surgido de um motivo mais épico do que eu imaginara. ■

Uma nova forma de vida

Ralph Merkle criou as Merkle Trees, estruturas de dados que permitem verificar eficientemente a integridade de grandes conjuntos de informação através de hashing hierárquico. STANFORD UNIVERSITY

ALCOR

Um técnico da Alcor Life Extension Foundation trabalha entre tanques criogénicos que contêm corpos preservados a -196 °C. Hal Finney está lá desde agosto de 2014

Depois de realizar o seu trabalho seminal em criptografia, Ralph Merkle, que mantém uma lista de previsões pessimistas que se revelaram erradas, começou à procura de outros problemas interessantes por resolver. Isso levou-o à extensão da vida.

—Um dia, estava a pensar nisso e disse para comigo: «Percebo isto de crescer e essas coisas, mas envelhecer é uma seca, e morrer… haverá alternativa? Talvez não morrer?». Não é que me oponha visceralmente à morte, mas haverá algo melhor que se possa fazer? —contou-me.

Ao princípio, a criónica desencorajou-o.

—Pensei que era uma ideia bastante má —recordou—, tendo em conta tudo o que implica arrefecer e reaquecer a máquina molecular enormemente complexa que é uma pessoa, de um modo minimamente destrutivo.

Ainda assim, pareceu-lhe um problema digno da sua atenção.

—Comecei a pensar no que é a vida e a morte.

OUTRO TIPO DE CRIPTOANÁLISE

Fê-lo durante os «seis a doze» meses seguintes e saiu desse período de reflexão com uma nova conceção do problema. Havia a morte clínica e a morte «teórica da informação». A morte clínica era desligar um computador. A morte teórica da informação era dissolver o computador em ácido. Se pensássemos nas pessoas como informação, uma matriz de moléculas, em vez de sacos de sangue e ossos, a criónica passava a ser um método de preservação da informação. Se alguém fosse cremado, não havia forma de o ajudar. Mas, se simplesmente experimentasse a morte clínica, podia preocupar-se menos com todas as formas como a maquinaria

molecular poderia desmoronar-se ou ser impossível de voltar a montar, e concentrar-se antes em saber se a informação que a compunha era recuperável. Merkle via o processo de recuperação de informação como outro tipo de criptoanálise, decifrando o texto cifrado de um corpo criopreservado, danificado mas intacto, para encontrar o texto em claro da pessoa original.

—Uma vez chegado a essa conclusão, tornou-se evidentemente óbvio que a criónica não era apenas uma opção razoável, mas uma opção muito razoável.

Merkle era então investigador no Xerox PARC e escreveu um artigo sobre como a microscopia eletrónica podia recuperar informação do cérebro, o que o convenceu de que era exequível. Convenceu-se ainda mais com o livro Engines of Creation, de K. Eric Drexler, que expunha como, em teoria, a nanotecnologia podia reparar células utilizando minúsculas máquinas reparadoras de células, os chamados ensambladores. Merkle tornou-se um membro ativo do conselho de administração da Alcor.

Numa tarde de abril, conduzi pela monótona planície desértica do norte de Scottsdale, no Arizona. As obras tinham cortado estradas, obrigando a desvios. O meu destino, quando surgiu à vista, era tão banal que poderia albergar o consultório de um dentista ou o serviço de distribuição de uma editora. Era um edifício baixo e quadrado, revestido de estuque cinzento-claro e com um ajardinamento ralo de flora regional. Havia alguns carros no parque de estacionamento e câmaras de vigilância esféricas pendiam das paredes do edifício. Um discreto letreiro em letras azuis dizia: ALCOR.

A organização de criónica mais ativa do mundo mudara-se para aqui, vinda da Califórnia, em 1994. Tinha havido problemas com o médico-legista e o Departamento de Saúde de Riverside, que não partilhavam plenamente o sonho da criónica. O Arizona oferecia calma geológica e meteorológica. Nem terramotos nem tufões perturbavam o deserto de Sonora. A política de não-interferência do Estado também se revelava favorável ao projeto.

Ali, a minha ignorância sobre a identidade de Satoshi Nakamoto parecia uma concessão trivial ao incognoscível. Não tínhamos todos conseguido viver com perguntas metafísicas muito mais transcendentes durante toda a nossa existência sem sucumbirmos à catatonia existencial? E, no entanto, ali estava um templo construído por e para um grupo de pessoas que, confrontadas com o maior de todos os mistérios, estavam certas de ter uma resposta.

A CALIFÓRNIA ERA O EPICENTRO DAS COISAS QUE LHE INTERESSAVAM

Quando entrei no edifício, via-se apenas um funcionário administrativo. O amplo átrio incluía uma mostra de números antigos da revista *Cryonics*. Um deles contava a história de um antigo executivo da Alcor cujo «primeiro ciclo de vida» durou de 1941, quando nasceu, até 1991, quando foi criopreservado.

A MORTE CLÍNICA ERA DESLIGAR UM COMPUTADOR; A MORTE TEÓRICA DA INFORMAÇÃO ERA DISSOLVÊ-LO EM ÁCIDO

Instantes depois, um homem chegou de motocicleta e entrou no edifício, envergando uma T-shirt preta justa que lhe moldava os bíceps, calças de fato de treino pretas e ténis pretos. Aos 58 anos, ainda restava algum louro avermelhado no cabelo em retrocesso. Tinha a pele clara e um princípio de barba.

—Max More —apresentou-se, estendendo a mão para cumprimentar.

Em criança, Max O'Connor, que cresceu em Bristol, Inglaterra, era um leitor insaciável de ficção científica. Os seus primeiros rabiscos eram de foguetões e botas voadoras. Quando tinha cinco anos, viu as alunagens de Apollo na televisão. Na adolescência, lia libertários como Murray Rothbard e David Friedman e os livros de Robert Anton Wilson, que escrevia sobre coisas como a IA e drogas para potenciar o cérebro. Através de Wilson, que criopreservou o cérebro da filha, Luna, depois de ela ter sido assassinada aos quinze anos, Max soube que a criónica era algo real. Aos dezassete anos, começou a apanhar o comboio para Londres uma vez por mês para assistir às reuniões de um grupo de extensão da vida e, já estudante universitário em Oxford, fundou a primeira organização criónica de Inglaterra e uma revista chamada Biostasis. Depois de receber seis semanas de formação na Alcor, na Califórnia, regressou ao seu quarto no St. Anne's College com uma caixa de fármacos criopreservantes e uma bomba de circulação extracorporal.

Max estava impaciente para se mudar para a Califórnia, que lhe parecia o epicentro de muitas das coisas que o interessavam. Quando foi fazer um doutoramento em Filosofia, fê-lo na UCLA. Nesse mesmo ano, saiu o livro de Drexler sobre nanotecnologia. De repente, a criónica tinha um roteiro.

—Porque antes era uma espécie de mistério —disse Max—. Como diabo se resolve, sabes, reparar biliões de células?

ASC

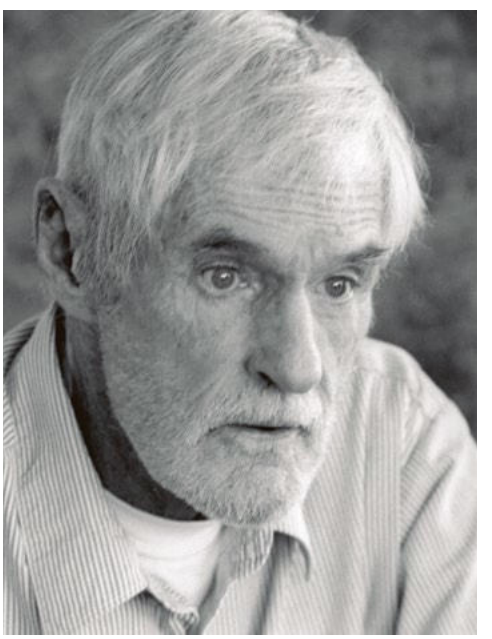
Max More, filósofo britânico e teórico do transumanismo, numa conferência em Stanford em 2006. More fundou o Extropy Institute e cunhou o termo «transumanismo».

QUANDO SE PUBLICOU O LIVRO DE DREXLER SOBRE NANOTECNOLOGIA, DE REPENTE, A CRIÓNICA PASSOU A TER UM ROTEIRO

Em 1986, quando tinha vinte e dois anos, Max inscreveu-se para se tornar o membro n.º 68 da Alcor. A criónica parecia-lhe lógica e queria ser um exemplo para os outros. Como a maioria dos membros, pagou o serviço comprando um seguro de vida e nomeando a Alcor como beneficiária.

TANTO RELIGIOSOS COMO ATEUS

Foi também então que mudou legalmente de nome para Max More e inventou a sua própria filosofia, o extropianismo. Juntamente com Tom Bell, alias Tom Morrow, cofundou o grupo extropiano e lançou a revista *Extropy: Vaccine for Future Shock*. Max conheceu a futura esposa, que nascera Nancie Clark e se tornaria Natasha VitaMore, numa festa em 1992 em casa de Timothy Leary, que nessa altura estava interessado na criónica.



SHUTTERSTOCK

Timothy Leary, psicólogo, defensor das drogas psicadélicas e ícone contracultural dos anos 60, escolheu a criogenização após a sua morte.

—Mudou de ideias —disse Max com tristeza—. Estava rodeado de gente que acreditava na reencarnação e esse tipo de coisas. Acho que também teve algumas experiências menos boas com um par de criónicos de trato difícil, talvez... Desistiu e acabou por enviar as cinzas para o espaço, creio. É uma pena, porque foi uma espécie de influência precoce, de certa forma. Tinha a fórmula SMI2LE, que sempre achei uma coisa protoextropiana: migração espacial, aumento da inteligência, extensão da vida.

Max fora diretor-geral da Alcor até dois anos antes da minha visita e continuava a ser embaixador da organização e da causa. No átrio, observámos fotografias de membros da Alcor criopreservados. Uma era uma mulher da China.

—É muito difícil tirar pessoas de lá —declarou Max—, por isso não creio que voltemos a fazê-lo.

A mais jovem dos membros era uma menina de dois anos com cancro cerebral, filha de médicos, que fora transportada de avião desde a Tailândia depois de várias operações falhadas. FM-2030, um transumanista irano-americano que nascera

SHUTTERSTOCK

Steve Aoki, DJ de música eletrónica, numa atuação em São Francisco. Aoki lançou NFTs (tokens não fungíveis) avaliados em milhões e aceitou bitcoins como pagamento por atuações.

Fereidoun M. Esfandiary em 1930, morrera de cancro do pâncreas, ou fora «desanimado», aos 69 anos.

—Um amigo meu —disse Max—. Não chegará a 2030, mas esperemos que volte.

Havia também fotos de Lyekka, uma gata, e de Nutmeg, um pastor-alemão. A Alcor preservara cerca de noventa animais de estimação até à data. O primeiro cão de Max, um *golden retriever* de quinze anos, estava entre eles.

—Eu não gostava muito de cães, mas a minha mulher insistiu. E era um cão tão bom que tivemos de o criopreservar.

Por agora, cerca de 1700 pessoas inscreveram-se no serviço da Alcor. Custa 220 000 dólares para o corpo inteiro e 80 000 dólares para a opção neuro. O DJ Steve Aoki declarou que é membro e foi noticiado que Peter Thiel também o é. Vários antigos amigos extropianos de Max também eram membros. Max disse que os informáticos ateus representavam o contingente mais numeroso.

—A mentalidade *hacker* vê basicamente um problema muito difícil e complexo e pensa: «Bem, se o decompomos em componentes, conseguimos resolvê-lo».

Mas a Alcor também tinha membros religiosos.

—Suponho que haja menos motivação se acreditas que vais para o céu, seja lá o que isso for, nunca tive uma resposta clara a isso, mas não vejo incompatibilidade,

NA ALCOR, O SERVIÇO CUSTA 220 000 DÓLARES PARA O CORPO INTEIRO E 80 000 PARA O NEURO. CERCA DE 1700 PESSOAS INSCREVERAM-SE

porque para mim é apenas uma extensão da medicina de emergência, não é? Primeiro tentas a dieta e o exercício, depois a medicina convencional e os fármacos, depois os cuidados intensivos; se estiveres mesmo em mau estado… poderias entrar num ensaio clínico; e, no fim, se isso não resultar, tens a criónica.

Um marco para o campo foi a publicação, em 1964, de The Prospect of Immortality, de Robert C. W. Ettinger, considerado agora o pai da criónica.

—Um título infeliz —disse Max—, porque não gostamos da palavra imortalidade.

As histórias sobre a Alcor costumavam usar a palavra, mas ela prometia demasiado. Quem sabia se o universo duraria para sempre? E uma pessoa podia estar com a sua adesão à Alcor em dia, mas ser assassinada ou morrer num acidente de viação, de tal maneira que o seu cérebro ficasse irremediavelmente danificado, ou ser eliminada por «asteroides a cair-lhe em cima da cabeça».

A «MELHOR» ALTERNATIVA

O mito da imortalidade estava carregado de um sombrio lastro literário. Havia «uma história horrível de Karel Čapek», disse Max, referindo-se a uma peça chamada *O Caso Makropulos*, com uma personagem incapaz de morrer. A deusa grega Eos pediu a Zeus que concedesse vida eterna ao marido, Títon, mas não especificou que permanecesse jovem, pelo que Títon viveu, murchando. *Zardoz*, um filme de John Boorman de 1974, «na realidade, bastante mau», apresentava os Eternos, uma «sociedade de imortais estagnados» que tinham inventado um deus, Zardoz, para controlar um grupo de selvagens chamados os Brutais. Sean Connery interpretava um Brutal chamado Zed.

—Todos imploram ao selvagem que os mate porque estão tão aborrecidos da vida.

Chegámos a uma sala separada de nós por uma parede de vidro de segurança do chão ao teto. Para lá dela, havia duas fiadas ordenadas de recipientes Dewar que continham os 234 membros preservados da Alcor. Uma plataforma elevatória estava pronta para descer a cápsula seguinte. Um par de técnicos trabalhava na substituição de um pé de um dos tanques gigantes. Alguns Dewars eram atarracados, outros mais altos. Um Dewar padrão podia acomodar quatro pacientes de corpo inteiro. Havia um novo modelo, um Super Dewar que Max chamava «Bigfoot», capaz de albergar doze pacientes de corpo inteiro e com uma parte superior cónica que abrandava a evaporação do azoto líquido. Cada um fora transportado por camião de um fabricante da Costa Leste e custava cerca de 25 000 dólares o padrão e 100 000 dólares o Super.

—Os pacientes neurológicos estão num separadamente —disse Max—. Temos uns dez pacientes neurológicos no mesmo Dewar.

Max e a mulher, como metade dos membros da Alcor, estavam inscritos na opção neuro.

—Tudo o resto é substituível, por isso prefiro focar-me no que importa.

Dentro das câmaras de aço à nossa frente estavam a cabeça e o corpo de Ted Williams, o jogador de basebol; Marvin Minsky, considerado o pai da IA, e Hal Finney, que podia ou não ter inventado o bitcoin. Perguntei em que Dewar estava o Hal. Max disse que não o sabia de memória.

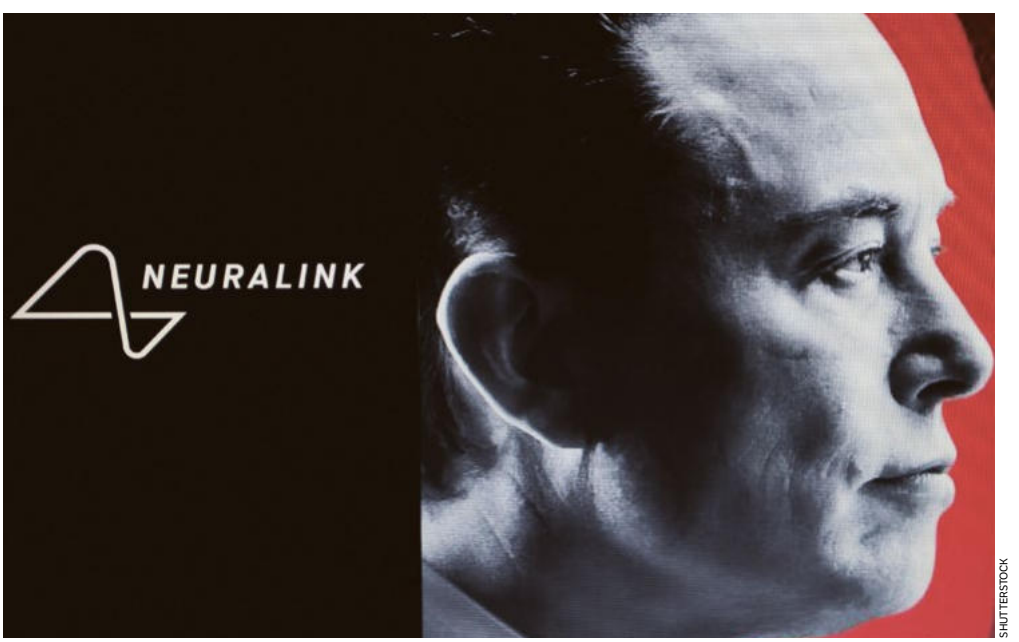
—Regra geral, não os identificamos por razões de segurança.

Muitas das visões dos extropianos tinham-se tornado realidade. Na internet, os memes dominavam o dia. Elon Musk era, entre outras coisas, o porta-estandarte

AS PESSOAS COM VISÃO DE FUTURO SENTIAM-SE ATRAÍDAS TANTO PELA CRIÓNICA COMO PELAS CRIPTOMOEDAS

de um impulso para colonizar as estrelas. A Neuralink de Musk era pioneira numa interface cérebro-computador, e pessoas não totalmente sérias debatiam se a melhor hipótese de sobrevivência da humanidade residia em oferecer-se como animais de estimação da inteligência artificial geral. O sonho tecno-libertário de *Exit* ardia eterno: a navegação marítima dera lugar aos «estados em rede» — sociedades intencionais habilitadas pela internet — e a projetos-piloto como Próspera (Honduras), Praxis (o Mediterrâneo) e Cabin (uma «cidade» «distribuída» e coordenada por blockchain de cabanas remotas em zonas florestais), destinados a levá-los ao mundo físico.

—É algo agradável —admitiu Max sobre a deriva extropiana da história recente—. Não estou muito otimista quanto a conseguirmos resolver o envelhecimento durante a minha vida. Estava, há trinta anos. Achava que era muito provável. Mas não obtivemos financiamento. Portanto, vai levar muito tempo. Não é como se tivéssemos um projeto *Apollo* que provavelmente pudesse fazer uma grande diferença. Por isso, não creio que lá chegue, mesmo que viva mais quarenta anos. Acho que vou ter de ser criopreservado, o que é um bocado lixado. Não quero estar ali. Mas é melhor do que a alternativa, na minha opinião.



SHUTTERSTOCK

Em julho de 2016, Elon Musk fundou a Neuralink, uma empresa de neurotecnologia especializada no desenvolvimento de interfaces cérebro-computador.

NAKAMOTO VIVERIA ETERNAMENTE

A criónica e as criptomoedas eram simbióticas. As pessoas com visão de futuro sentiam-se atraídas por ambas: Roger Ver, o primeiro bitcoiner, conhecido como Bitcoin Jesus (e mais tarde processado por Craig Wright), inscrevera-se na Alcor aos vinte anos. Vitalik Buterin doara criptomoedas a organizações de extensão da vida e, em 2018, um investidor chamado Brad Armstrong fez a maior doação até à data à Alcor, cinco milhões de dólares numa moeda chamada stellar, para criar um Fundo de Investigação de Criónica Hal Finney. Existia também uma ligação mais profunda. No início da década de 1990, um extropiano chamado Mark Plus cunhou o termo «aeonomics» para descrever «o estudo dos problemas económicos da existência imortal». A ideia de prolongar radicalmente a vida exigia repensar muitas coisas, entre elas o modo como os anos adicionais na Terra poderiam afetar o seu plano 401(k). A criónica acrescentava o desafio de garantir que o dinheiro que tinhas quando eras desanimado continuaria disponível quando fosses reanimado. Se os extropianos se iam congelar, precisariam de uma forma de enviar dinheiro para o futuro, pronto a ser reclamado ao despertar. Deste modo, o dinheiro digital seria uma bênção para a criónica.

Ralph Merkle tentou descrever uma vez por que motivo a gente técnica estava tão apaixonada pelo bitcoin, chamando-o «o primeiro exemplo de uma nova forma de vida». Vivia na internet, pagava às pessoas para o manter vivo e ninguém o podia alterar, corromper ou travar. Qualquer um podia executar o seu software. Qualquer um podia ver o que fazia e como funcionava. «Se uma guerra nuclear destruísse metade do nosso planeta, continuaria a viver, sem se corromper», escreveu Merkle. «Continuaria a oferecer os seus serviços. Continuaria a pagar às pessoas para o manterem vivo».

Andreas Antonopoulos, autor do livro *Mastering Bitcoin*, comparara-o a «uma ratazana de esgoto». Nick Szabo e Elaine Ou, nos últimos anos, tinham andado a trabalhar para inocular o bitcoin inclusive contra a morte da internet. Ou inspirou-se em 2016, quando a China ameaçava proibir as criptomoedas, e ela e Szabo começaram a experimentar a ampliação da rede bitcoin utilizando a rádio amadora.

A blockchain era eterna. Após a morte de Len Sassaman, uns amigos incrustaram numa transação de bitcoin um retrato ASCII do seu rosto barbudo, juntamente com a inscrição «Len rabbi Sassama (1980-2011). Len era nosso amigo. Uma mente brilhante, uma alma bondosa e um autêntico mistério». A transação passou a integrar o bloco 138725, o que significava que viveria na blockchain enquanto esta existisse, com cópias em todos os computadores que compunham a rede.

Como projeto utópico, o bitcoin nunca teve, tal como todos os projetos utópicos, grande hipótese. A magia e a loucura estavam a esvair-se. Mas, como nova classe de ativos, mostrara a sua resiliência. O seu preço voltou a subir, e atingiu um novo máximo histórico acima dos 73 000 dólares em março de 2024. A Fidelity aconselhava agora os clientes de retalho a alocar uma pequena parte das suas carteiras às criptomoedas. E a tecnologia blockchain parecia inevitável, o espaço criativo que abria continuava entusiasmante.

Satoshi Nakamoto representava algo que quem estivesse por detrás do pseudónimo jamais poderia encarnar. Era um nome e uma ideia que, livre das limitações de um corpo físico ou de uma história pessoal que o ancorasse, viveria eternamente. ■

BIBLIOGRAFIA

❏ Adrian Chen, *«The Underground Website Where You Can Buy Any Drug Imaginable»,* Gawker, 1 de junho de 2011.

❏ Álvaro D. María, *La filosofía del Bitcoin. La caída del Estado.* Editorial Deusto, 2024.

❏ Andrew O'Hagan, *«The Satoshi Affair»,* London Review of Books, 30 de junho de 2016.

❏ Benjamin Wallace, *«The Rise and Fall of Bitcoin»,* Wired, dezembro de 2011.

❏ Bob Woodward, *The Secret Man: The Story of Watergate's Deep Throat* (Nova Iorque: Simon and Schuster, 2005), 131-32.

❏ Bobby C. Lee, *La promesa del Bitcoin. El futuro del dinero y cómo puede funcionar a tu favor.* McGraw-Hill Interamericana de Espanha, 2022

❏ Brian Fung, *«Marc Andreessen: In 20 Years, We'll Talk About Bitcoin Like We Talk About the Internet Today», The Washington Post,* 21 de maio de 2014.

❏ Carlos Domingo, *Todo lo que querías saber sobre Bitcoin, criptomonedas y blockchain y no te atrevías a preguntar.* Ed. Martínez Roca, 2018.

❏ *Craig Wright Reveals Himself as Satoshi Nakamoto, The Economist,* 2 de maio de 2016.

❏ Jacqueline Lindenberg y Adam S. Levy, *«Kanye West Steps Out for a Solo Outing in Beverly Hills», Daily Mail Online,* 17 de outubro de 2022.

❏ James O'Shea, *«The Secret Irishman Likely Behind Bitcoin, the Internet Currency Code», IrishCentral,* 4 de outubro de 2011.

❏ Javier López Menacho, *La otra cara de las criptomonedas,* Holobionte, 2024.

❏ Jeff John Roberts, *Los reyes de las criptomonedas,* Empresa Activa, 2021.

❏ Jens Ducrée, *Satoshi Nakamoto and the Origins of Bitcoin: The Greatest Mystery in the Entire History of Science and Technology,* publicado por Ducrée, 17 de junho de 2023.

❏ Jim Epstein, *«Tim May, Father of "Crypto Anarchy", Is Dead at 66», Reason,* 16 de dezembro de 2018; *e Nathaniel Popper, «Timothy C. May, Early Advocate of Internet Privacy, Dies at 66», The New York Times,* 21 de dezembro de 2018.

❏ Jonathan Bier, *The Blocksize War: The Battle for Control Over Bitcoin's Protocol Rules* (publicação independente, 2021).

❏ Jon Matonis, *«Cómo conocí a Satoshi», Medium,* 2 de maio de 2016.

❏ Josep Busquet, *Bitcoin. La caza de Satoshi Nakamoto.* Editorial Dibbuks, 2014.

❏ Nathaniel Popper, *«Decoding the Enigma of Satoshi Nakamoto and the Birth of Bitcoin»,* The New York Times, 15 de maio de 2015.

❏ Nathaniel Popper, *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money* (Nova Iorque: Harper / HarperCollins, 2015).

❏ Nathaniel Popper, *«Lost Passwords Lock Millionaires Out of Their Bitcoin Fortunes», The New York Times,* 12 de janeiro de 2021.

❏ Nick Szabo, *«Re: sobre el anonimato, la identidad, la reputación y la suplantación de identidad»,* CP, 18 de outubro de 1993.

❏ Nik Bhatia, *Del oro al Bitcoin.* Deusto Ediciones, 2022.

❏ Nour Al Ali y Chris Kingdon, *«Musk: I Am Not Bitcoin's Satoshi Nakamoto», Bloomberg News,* 28 de novembro de 2017.

❏ Phil Champagne, *El libro de Satoshi. La colección de escritos del creador de Bitcoin Satoshi Nakamoto.* Blockchain Espanha, 2014.

❏ Phinnaeus Gage, *«Definitive Proof That Satoshi Nakamoto is James A. Donald»,* BF, 28 maio, 2014.

❏ Roger Ver y Steve Patterson, *El secuestro de Bitcoin. La historia oculta del BTC.* Ed. Eda, 2024.

❏ Saifedean Ammous, *El patrón Bitcoin. La alternativa descentralizada a los bancos centrales.* Deusto Ediciones, 2025.

❏ Sahil Gupta, *«Elon Musk Probably Invented Bitcoin»,* HackerNoon, 22 de novembro de 2017.

❏ Satoshi Nakamoto, *«Re: Quieren borrar el artículo de Wikipedia»,* BF, 20 de julho de 2010.

❏ Simon Singh, *The Code Book: The Evolution of Secrecy from Mary, Queen of Scots, to Quantum Cryptography* (Nova Iorque: Doubleday Anchor, 2000).

❏ Sophie Elmhirst, *«The Disastrous Voyage of Satoshi», The Guardian,* 7 de setembro de 2021.

❏ Stephen Katte, *«The Last Bitcoin: What Will Happen Once All BTC Are Mined?»,* Cointelegraph, 21 de julho de 2023.

❏ Tim May, *«El manifiesto criptoanarquista», en Peter Ludlow, Crypto Anarchy, Cyberstates, and Pirate Utopias* (Cambridge, MA: MIT Press, 2001), 61-63.

❏ Tom Simonite, *«The Man Who Really Built Bitcoin», MIT Technology Review,* 15 agosto, 2014.

❏ Will Feuer, *«Statue of Anonymous Bitcoin Creator Satoshi Nakamoto Unveiled in Hungary»,* New York Post, 17 de setembro de 2021.

❏ Will Stephenson, *«Cryptonomicon», Harper's,* março de 2022.

❏ *«Bits and Bob», The Economist,* 13 junho, 2011.

❏ Para os registos da lista de correio eletrónico dos *cypherpunks*: cypherpunks.venona.com, https://marc.info e https://cryptoanarchy.wiki.

❏ Repositórios da lista de correio eletrónico dos extropianos.
- Coleção dos resumos do grupo de 1992 a 1994 em https://diyhpl.us/~bryan/irc/extropians/raided-mailing-list-archives/archives/.
- Wei Dai aloja um duplicado da listagem que abrange 1996-2002 em extropians.weidai.com.
- As publicações a partir de 2003 podem ser encontradas em lists.extropy.org/piper mail/extropy-chat/.

❏ Os arquivos da revista Extropy estão em https://hpluspedia.org/wiki/Extropy_Magazines y fennetic.net/irc/extropy/.

❏ NakamotoInstitute.org alberga uma coleção inigualável de textos relevantes para Bitcoin, incluindo os escritos completos de Satoshi Nakamoto. O fórum Bitcoin em bitcointalk.org.

SUPER INTERESSANTE

REDAÇÃO
Direção: **Carmen Sabalete** (csabalete@zinetmedia.es)
Subdiretora: **Cristina Enríquez** (cenriquez@zinetmedia.es)
Coordenação de design: **Óscar Álvarez**
Muy Interesante Digital:

Autor dos textos: **Benjamin Wallace.**
Texto original: *Mr. Nakamoto. El enigmático creador de bitcoin (The Mysterious Mr. Nakamoto: The Fifteen-Year Quest to Unmask the Secret Genius Behind Crypto).*
© Editorial Pinolia S. L., 2025.
Colaboradores: **Javier Alvaredo** (edição e revisão), **Manuel Arrubarrena** (layout e documentação).

zinet MEDIA GLOBAL

REDAÇÃO EM MADRID
C/ Alcalá 79 1º A - 28009 Madrid; tel.: 810 58 34 12
Subscrições: suscripciones@zinetmedia.es
Consultora: **Marta Ariño**
Diretor Geral Financeiro: **Carlos Franco**
CRO (Diretor Comercial): **AlfonsoJuliá** (ajulia@zinetmedia.es)
Brand Manager: **Marta Espresate** (mespresate@zinetmedia.es)

DISTRIBUIÇÃO
VASP – Distribuição e Logística, S.A.
A Super Interessante é uma publicação registada na Entidade Reguladora para a Comunicação Social com o n.º 118 348.
Depósito legal: 122 152/98.

«O BITCOIN É UMA CONQUISTA CRIPTOGRÁFICA EXTRAORDINÁRIA. A CAPACIDADE DE CRIAR ALGO QUE NÃO POSSA SER DUPLICADO NO MUNDO DIGITAL TEM UM VALOR ENORME.»

Eric Schmidt (1955),
ex-CEO (2001-2011) e presidente do conselho de administração (2011-2015) da Google.

SUPER
INTERESSANTE