A Internet do Dinheiro

COLETÂNEA DE PALESTRAS POR

Andreas M. Antonopoulos

VOLUME UM

"Sempre me perguntei o que teria acontecido se tivéssemos feito pagamentos com um clique no navegador desde o início. Com o bitcoin, finalmente conseguimos essa 'Internet do Dinheiro'. Mas este livro não é apenas uma ode ao bitcoin - é uma ode a protocolos abertos, o que acontece quando você conecta pessoas on-line com o poder da inovação na internet. "

Marc Andreessen , co-fundador da Netscape e Andreessen Horowitz

"Com Mastering Bitcoin, Andreas Antonopoulos escreveu um dos melhores livros técnicos sobre moeda digital. Com A Internet do Dinheiro, ele compara esse feito ao compilar suas palestras em um dos melhores livros sobre Bitcoin para um público amplo. Altamente recomendado."

Balaji Srinivasan , CEO 21.co

"Nos últimos três anos, a conscientização do potencial abrangente e transformador do bitcoin e sua tecnologia subjacente, o blockchain, cresceu exponencialmente. Isso exigiu que as pessoas compreendessem não apenas como essa tecnologia não ortodoxa funcionava, mas também sua profunda promessa para a sociedade. Ninguém fez mais que Andreas Antonopoulos para ajudar a todos nessa jornada. Leia ele. Isso fará você mais sábio."

Michael J. Casey , co-autor de A Era das Criptomoedas

Andreas M. Antonopoulos é um tecnólogo e empreendedor em série que se tornou uma das figuras mais conhecidas e respeitadas do bitcoin. Ele é o autor de “Mastering Bitcoin”, publicado pela O’Reilly Media e considerado por muitos como o melhor guia técnico para o bitcoin. Como um palestrante, professor e escritor envolvente, Andreas torna assuntos complexos acessíveis e fáceis de entender. Como consultor, ele ajuda as startups a reconhecer, avaliar e navegar pelos riscos de segurança e de negócios. Andreas foi um dos primeiros a usar a frase “A Internet do Dinheiro” para descrever o bitcoin e seus possíveis impactos sobre a humanidade.

A Internet do Dinheiro

Palestras de Andreas M. Antonopoulos
https://antonopoulos.com/
@aantonop

Submissões de erratas, pedidos de licença e informações gerais
errata@merklebloom.com

Primeira impressão (em português) 2018
Título original: The Internet of Money

Tradução Colaborativa

Este livro foi traduzido numa experiência colaborativa coordenada pela Editora EmRede, com a participação de mais de 20 pessoas.

Revisão geral

EmRede Editora
Langway

Revisão técnica

O trabalho de revisão técnica final foi realizado pela profissional especialista em criptomoedas e blockchain Rosine Kadamani, fundadora da Blockchain Academy, um projeto educacional na área.

Capa (adaptação do design original), projeto gráfico e diagramação

Tábata Araujo

Dados Internacionais de Catalogação na Publicação (CIP)

A627i

Antonopoulos, Andreas M.,
A internet do Dinheiro / Andreas M. Antonopoulos; tradução coletiva - São Paulo: EmRede Editora, 2018.

Título original: The Internet of Money
124p.

ISBN 978-85-85265-00-7

1. Tecnologia 2. Ciência da Computação 3. Economia

CDD 600
CDU 336

Dedicado à comunidade bitcoin

Ressalvas

Este é um livro de comentários e opiniões editadas. Grande parte do conteúdo é baseado em experiência pessoal e acontecimentos curiosos. Pretende-se promover considerações reflexivas de novas ideias, estimular o debate filosófico e inspirar pesquisas independentes. Não são conselhos de investimentos; não use este material para tomar decisões relacionadas a isso. Não é um aconselhamento jurídico; consulte um advogado em sua jurisdição para questões legais. Pode conter erros e dados incompletos, apesar dos nossos melhores esforços. Andreas M. Antonopoulos, Merkle Bloom LLC, editores, responsáveis editoriais, transcritores e *designers* não se responsabilizam por erros ou omissões. As coisas mudam rapidamente na indústria do *bitcoin* e *blockchain*. Use este livro como uma referência, mas não sua única referência.

Referências para obras com marcas registradas ou com direitos autorais são apenas para críticas e comentários. Qualquer termo de marca registrada é propriedade de seus respectivos proprietários. As referências a indivíduos, empresas, produtos e serviços estão incluídos apenas para fins ilustrativos e não devem ser considerados como endossos.

SUMÁRIO

INTRODUÇÃO

*Por **Andreas M. Antonopoulos***

Quando comecei minha jornada com o *bitcoin,* nunca achei que iria levar a isso. Este livro é como um diário abreviado das minhas descobertas sobre o *bitcoin* e foi produzido a partir de uma série de palestras que realizei entre 2013 e 2016.

Nos últimos três anos, realizei mais de 150 palestras públicas em todo o mundo. Gravei mais de 200 episódios de *podcast* e respondi algumas centenas de perguntas. Dei também mais de 150 entrevistas para a rádio, imprensa escrita e TV. Apareci em oito documentários e escrevi um livro técnico, com o título: *Mastering Bitcoin.* Quase todo esse material está disponível gratuitamente por meio de licenciamento de código aberto, *on-line*. As palestras incluídas neste livro são apenas uma pequena amostra do meu trabalho, selecionado pela equipe editorial, para fornecer uma visão inicial sobre *bitcoin*, seus usos e seu impacto sobre o futuro.

Cada uma das palestras foi realizada ao vivo, sem slides ou qualquer ajuda visual, e na maioria das vezes improvisada. Embora eu tenha sempre um tema em mente antes de cada palestra, muito da minha inspiração vem da energia e interação com cada público. De palestra para palestra, os temas evoluem à medida que experimento novas ideias, vejo a reação das pessoas e desenvolvo essas ideias ainda mais. No fim das contas, algumas ideias que começam como uma única frase evoluem ao longo de várias palestras, tornando-se um tópico inteiro.

Este processo de descobertas não é perfeito, claro. Por isso, minhas palestras gravadas contêm pequenos erros factuais. Eu menciono datas, eventos, números e detalhes técnicos com base na minha memória, e frequentemente cometo erros. Neste livro, os erros ocorridos durante esses improvisos e os meus tiques de linguagem foram corrigidos pelos editores. O que permanece é a essência de cada apresentação, como eu gostaria de tê-las apresentado, ao invés de uma transcrição literal de minhas palestras. Mas, por causa dessa edição existe um preço a ser pago. Perdeu-se a atmosfera dos encontros. A energia do público, o tom das minhas frases e minhas risadas espontâneas junto com as pessoas na sala. Por essas e por outras, você deve assistir aos vídeos. Os links estão descritos no livro.

Este livro e o meu trabalho nos últimos três anos é sobre mais do que o

bitcoin. Essas palestras refletem minha visão de mundo, minhas ideias políticas e esperanças, bem como meu fascínio técnico e minha nerdice escancarada. Elas resumem meu entusiasmo por essa tecnologia e o futuro surpreendente que eu imagino. Essa nova visão de mundo começou com o *bitcoin*. Um experimento excêntrico de *cypherpunk* que desencadeou uma onda de inovação, criando A internet do dinheiro e radicalmente transformando a sociedade.

Nota dos editores

Quase toda a comunidade *bitcoin* conhece a contribuição de Andreas. Além do seu trabalho escrito e em áudio, ele é um orador altamente solicitado. Um palestrante elogiado por entregar consistentemente conteúdos inovadores, estimulantes e engajantes. Este livro representa apenas uma pequena amostra do trabalho de Andreas na indústria de *bitcoin* e *blockchain* nos últimos três anos. Com tanto conteúdo, simplesmente decidir que palestras enxugar ou incluir foi uma tarefa árdua. Nós selecionamos essas palestras específicas porque elas se encaixam nos critérios do livro; nós poderíamos facilmente ter incluído dezenas mais.

Este livro é o volume 1, e esperamos publicar, em breve, o volume 2.

Começamos este projeto de livro com um objetivo: fornecer uma perspectiva geral, contando uma história fácil de ler, sobre por que o *bitcoin* importa e por que tantos entre nós estamos entusiasmados com isso. Nós queríamos algo que pudéssemos compartilhar com familiares, amigos e colegas de trabalho e que eles realmente pudessem compreender: um compêndio que eles pudessem explorar por cinco minutos sem compromisso ou até por algumas horas. Precisava ser algo envolvente, com analogias do mundo real, para tornar a tecnologia compreensível. Precisava ser inspirador, com uma visão de como essas coisas poderiam impactar positivamente a humanidade. Precisava ser honesto, ao reconhecer e identificar as deficiências de nossos sistemas atuais e da própria tecnologia.

Apesar dos nossos melhores esforços, temos certeza de que podemos melhorar e mudar as coisas, esta é uma primeira edição. Nós editamos pesadamente em alguns lugares para facilitar a leitura, enquanto procurávamos simultaneamente preservar a essência da palestra. Nós acreditamos que conseguimos um bom equilíbrio e estamos satisfeitos com o livro, como um todo. Esperamos que você também fique satisfeito. Se tiver algum comentário sobre esta edição, conteúdo ou sugestões de como podemos melhorar o livro, envie-nos um *e-mail* para emredeeditora@gmail.com.

Dica para tornar sua experiência de leitura ainda melhor:

Cada conversa pretende ser autônoma. Não há necessidade de começar no início - embora, se você não estiver familiarizado com *bitcoin*, você possa querer começar pela primeira conversa, "O que é *bitcoin*", para obter uma visão geral do tópico. Você notará alguns temas e analogias repetidas, como a Lei de Bandeira Vermelha ou a conversa pai-e-filho sobre dinheiro. Enquanto os exemplos ocasionalmente se repetem, eles são utilizados para ilustrar um ponto diferente em cada conversa.

Edição Brasileira

É com enorme alegria que trazemos a versão em Português desse livro tão importante para a comunidade Bitcoin mundial. A intenção de traduzir e distribuir o livro Bitcoin, a Internet do Dinheiro, é de trazer um guia simples e direto para a comunidade brasileira de usuários de criptomoedas que cresce dia após dia.

Toda a construção do livro foi feita incorporando princípios da rede Bitcoin. Fizemos uma tradução colaborativa com a participação de 34 pessoas, em um processo inclusivo aonde qualquer pessoa podia se conectar, traduzir e revisar. O trabalho foi remunerado por palavra traduzida/revisada, com o token da comunidade Prospera, o Prosper.

Esse livro foi uma vivência com a nossa capacidade de inovar, cocriar e colaborar. Quanto mais conseguimos expandir esse horizonte, maior é o grau de liberdade que alcançamos. O Bitcoin cria esse ambiente com uma estrutura tecnológica que propicia a mesma vivência com o dinheiro, numa escala nunca antes vista pela humanidade.

O espírito de inclusão radical no sistema financeiro trazido pelo Bitcoin é a principal mensagem desta obra. É um livro com a linguagem do Bitcoin para pessoas comuns. Para famílias, comunidades, empreendedores, vendedores, profissionais autônomos e empresas. Para adolescentes e adultos, para quem nunca teve contato e também para os especialistas.

Trabalhamos da melhor forma possível nesse processo e estamos muito satisfeitos com o resultado. Esta é a nossa forma de contribuir com essa (r) evolução do dinheiro iniciada pelo Bitcoin. Esperamos que você também fique satisfeito. Se tiver algum comentário sobre esta edição, conteúdo ou sugestões de como podemos melhorar o livro, envie-nos um e-mail para emredeeditora@gmail.com.

O QUE É BITCOIN?

Disromper, Start-up, Escalar: Atenas, Grécia; Novembro 2013

Link do Vídeo: https://www.youtube.com/watch?v=LA9A1RyXv9s

Nota do editor: esta palestra foi dada no final de 2013. As transações em *bitcoin* não são mais gratuitas, mas as taxas continuam sendo baixas.

Boa tarde, Atenas! Obrigado por me receber hoje. Quer ser disruptivo? Eu tenho algo disruptivo. Tenho participado de uma verdadeira revolução. Hoje, vamos falar sobre a mais empolgante, mais interessante e provavelmente a mais importante invenção tecnológica na ciência da computação dos últimos 20 anos. Estou aqui para falar sobre o *bitcoin*.

O *bitcoin* é uma moeda digital, mas é muito mais do que isso. Dizer que *bitcoin* é apenas uma moeda digital é como dizer que a internet é um telefone chique. É como dizer que a internet se resume a mandar *e-mail*. Dinheiro é apenas a primeira aplicação. O *bitcoin* é uma tecnologia, é uma moeda e uma rede internacional de pagamentos e trocas que é completamente descentralizada. Não depende dos bancos. Não depende de governos.

> *"Dizer que bitcoin é apenas uma moeda digital é como dizer que a internet é um telefone chique."*

Nós nunca fizemos isso antes na história da humanidade. Esta invenção é verdadeiramente revolucionária. Quando olhamos para trás, veremos que este é um momento histórico na evolução da ciência da computação, mas também é uma revolução social e política em construção. Então, vamos começar.

Bitcoin, a invenção

Bitcoin é dinheiro digital. É dinheiro assim como euros ou dólares, só que não é de propriedade de um governo. Você pode enviá-lo de qualquer ponto do mundo a qualquer outro ponto do mundo instantaneamente, de forma segura, com taxas mínimas ou sem taxas. Há dois dias, vimos uma das maiores transações já registradas na rede *bitcoin*, onde alguém transferiu $ 150 milhões entre duas contas *bitcoin*, em um segundo, com taxa zero. Só isso permite que você perceba o quão disruptiva esta tecnologia será em termos de sistemas de pagamento internacionais. Mas isso é só o começo.

Bitcoin é uma moeda digital que surgiu em 2008 como a invenção de uma

pessoa chamada Satoshi Nakamoto. Ele publicou um artigo no qual afirmou que encontrou o caminho para criar uma rede descentralizada, que poderia alcançar consenso e adesão sem qualquer autoridade central de controle. Agora, se você estudou ciência da computação ou sistemas distribuídos, isso é conhecido como "Problema dos generais bizantinos". Foi descrito pela primeira vez em 1982. Até 2008, era um problema sem solução. Então, Satoshi Nakamoto disse: "Eu resolvi o problema". Adivinha o que aconteceu depois? Todos riram, ignoraram-no e rejeitaram-no. Ele publicou seu artigo e, três meses depois, publicou o *software* que permitiu que as pessoas começassem a construir a rede *bitcoin*.

Bitcoin não é uma empresa. Não é uma organização. É um padrão ou um protocolo como o TCP/IP ou a internet. Não pertence a ninguém. Ele opera por simples regras matemáticas com as quais todos os que participam da rede concordam. Através deste mecanismo simples, criado por Satoshi Nakamoto, o *bitcoin* é capaz de permitir que uma rede de computadores completamente descentralizada entre em acordo sobre as transações ocorridas em uma rede, essencialmente concordando sobre quem tem atualmente o dinheiro.

Assim, quando eu envio dinheiro da minha conta para a conta de outra pessoa, nesta rede ponto a ponto (*peer to peer*), completamente descentralizada, é como se estivesse enviando um *e-mail*. Não existe ninguém no meio do caminho. A cada dez minutos toda a rede entra em acordo sobre as transações realizadas, sem qualquer autoridade centralizada, por uma simples eleição que ocorre eletronicamente.

Esta solução particular, esta invenção, é muito mais importante do que a moeda. A moeda é apenas a primeira aplicação que é possível se construir em um sistema distribuído de consenso. Outras aplicações incluem votação justa e distribuída, propriedade de ações, registo de ativo, autenticação e muitas outras aplicações em que nunca pensamos antes.

> *"Esta solução particular, esta invenção, é muito mais importante do que a moeda. Mas a moeda é apenas a primeira aplicação."*

Eu descobri o *bitcoin* em 2011 e, depois do advento da internet, eu nunca havia me sentido tão impressionado pelas possibilidades que vi. Eu estava lá no despertar da internet em 1991, quando era pré-comercial. Eu podia ver que isso mudaria o mundo, mas ninguém acreditava em mim. Eu tenho a mesma sensação sobre o *bitcoin*.

Agora, alguns de vocês devem ter ouvido falar que o *bitcoin*, enquanto moeda, tem um preço extremamente elevado num dia e muito baixo no dia seguinte. Estou aqui para dizer-lhe que ignore o preço, ignore o *bitcoin* enquanto di-nheiro e compreenda o *bitcoin* como tecnologia, como invenção e a rede que ele cria. Se essa moeda der errado, nós apenas reiniciaremos

outra. A invenção do *bitcoin*, a tecnologia que o torna possível, não pode ser desfeita. Ela cria as possibilidades de organização descentralizada em uma escala nunca antes vista neste planeta.

> *"A invenção do bitcoin, a tecnologia que o torna possível, não pode ser desfeita. Ela cria as possibilidades de organização descentralizada em uma escala nunca antes vista neste planeta."*

O dinheiro do povo

Aqui estão os motivos pelos quais o *bitcoin* é importante para mim.

Aproximadamente 1 bilhão de pessoas atualmente têm acesso a serviços bancários, de crédito e de financiamento internacional - principalmente as classes mais altas, as nações ocidentais. Seis bilhões e meio de pessoas neste planeta não têm conexão com o mundo do dinheiro. Elas operam em sociedades baseadas em dinheiro vivo com pouquíssimo acesso a recursos internacionais. Elas não precisam de bancos. Dois bilhões dessas pessoas já estão na internet. Com um simples *download* de aplicativos, elas podem se tornar imediatamente participantes de uma economia internacional, usando uma moeda internacional que pode ser transmitida para qualquer lugar sem taxas e nenhum controle do governo. Elas podem se conectar a um mundo de finanças internacionais que é completamente ponto a ponto. *Bitcoin* é o dinheiro do povo. No seu centro estão regras matemáticas simples com as quais todos concordam e que ninguém controla. A possibilidade de conectar essas 6 1/2 bilhões de pessoas ao resto do mundo é verdadeiramente revolucionária.

> *"Bitcoin é o dinheiro do povo."*

Os processadores de pagamento serão afetados. Essas enormes empresas cobram taxas mais elevadas para enviar dinheiro para países destinatários mais pobres, situação que é exploratória e corrupta. Estas organizações obtêm enormes ganhos por uma função que pode ser feita com *bitcoin* quase de graça. Como diz o provérbio que se criou na internet, "acabei de substituir toda a sua indústria por 100 linhas de código Python", é exatamente o que estamos fazendo com *bitcoin*.

Moedas, negócios e pagamentos internacionais

Como você pode usar o *bitcoin* hoje? Falando de modo simples, o *bitcoin* pode operar como uma moeda. Você pode considerar isso uma compra de moeda estrangeira: você pode conectar-se a uma corretora (*exchange*) na internet, transferir alguns euros e usar esses euros para comprar *bitcoins* pela taxa de câmbio praticada na ocasião. No entanto, essa não é a melhor maneira de fazê-lo. Somos empreendedores, certo? Queremos ser disruptivos.

A melhor maneira de fazer isso é encontrar um produto ou serviço que você possa oferecer a alguém que queira comprar com *bitcoin* e começar a ganhar *bitcoin*.

- **Solucionando problemas de pagamento**

Se você pensa em começar um negócio em um ambiente internacional, existem duas barreiras primárias para que o negócio se torne global. A primeira barreira é que é difícil transportar produtos e serviços através das fronteiras. Com a internet, nós resolvemos isso. Nós podemos agora criar produtos e serviços que são virtuais, que podemos vender em qualquer lugar do mundo. Então, podemos entregar o produto, mas ainda temos um grande problema: como seremos pagos? *Bitcoin* resolve essa parte. Permite-nos receber pagamentos de qualquer lugar do mundo, instantaneamente. A rede *bitcoin* permite que qualquer pessoa envie um montante tão pequeno quanto 100 milionésimos de *bitcoin*, que atualmente é uma quantidade muito pequena de dinheiro.

Você não pode fazer isso com o dinheiro e com os sistemas de pagamento de hoje. Os cartões de crédito foram feitos na década de 1950, e eles certamente não foram feitos para uma era na internet. *Bitcoin* é feito para a era da internet.

> *"Os cartões de crédito foram feitos na década de 1950, e eles certamente não foram feitos para uma era na internet. Bitcoin é feito para a era da internet."*

Então, se de repente você pode enviar pagamentos que são um centésimo de euro, ou um milésimo de euro, você pode vender conteúdo. Você pode fazer microtransações.

Você pode coletar pagamentos de milhões de pessoas em pequenas quantidades e fazê-los, de modo agregado, valer alguma coisa. Na mesma rede através da qual você pode enviar um milésimo de euro ou um milionésimo de euro, você pode enviar bilhões de euros ou trilhões de euros. A taxa será exatamente a mesma, porque as taxas dependem do tamanho da transação em *kilobytes*, não da quantidade ou do conteúdo.

Neutralidade, criminosos e bitcoin

Vamos olhar para trás, para a internet, e ver quais lições podemos aprender sobre por que o *bitcoin* é importante. Um dos princípios mais importantes da internet é a neutralidade. A internet não faz distinção entre uma organização de grande porte e uma pequena organização. Não sabe a diferença entre a CNN e um blogueiro egípcio. Ela permite que o blogueiro egípcio fale com o mundo com o mesmo poder de voz que a CNN tem.

Bitcoin é neutra para o remetente, para o destinatário e para o valor da transação. Isso significa que dá a cada cidadão, a cada usuário de *bitcoin*, a habilidade de inovar em termos de instrumentos financeiros, sistemas de pagamento e operações bancárias. Você pode operar no mesmo nível do Citibank. Isso é verdadeiramente revolucionário.

> *"Bitcoin é neutra para o remetente, para o destinatário e para o valor da transação. Isso significa que dá a cada cidadão, a cada usuário de bitcoin, a habilidade de inovar em termos de instrumentos financeiros, sistemas de pagamento e operações bancárias."*

Ele pega um sistema hierárquico de finanças internacionais e o vira do avesso. Até agora, a segurança desse sistema hierárquico foi alcançada através da limitação do acesso, porque esse é o método principal de confiança em nossos sistemas de pagamento - você não pode entrar, a menos que seja aprovado. *Bitcoin* cria uma rede completamente horizontal e descentralizada, onde cada nó é igual, onde o protocolo é neutro para as transações e força as inovações até o limite da rede, permitindo exatamente o mesmo fenômeno que vimos na internet: inovação sem permissão. Você não precisa perguntar a ninguém se sua aplicação pode ser publicada na internet. Você não precisa pedir a ninguém para subverter completamente uma nova indústria com sua tecnologia da informação. Com *bitcoin*, você não precisa pedir a ninguém para inventar um novo instrumento financeiro, um novo sistema de pagamentos, um novo serviço. Você pode simplesmente fazê-lo. Você pode simplesmente escrever o código e fazer parte de uma rede financeira internacional que pode executar esse código e colocar você em contato com milhões de consumidores.

> *"Com bitcoin, você não precisa pedir a ninguém para inventar um novo instrumento financeiro, um novo sistema de pagamentos, um novo serviço. Você pode simplesmente fazê-lo."*

Agora, estamos ainda no começo. Ainda não temos as interfaces lapidadas. É difícil de usar. É usado por criminosos. Ele é usado por diversas organizações ao redor do mundo, e não é fácil ver exatamente quem está usando o *bitcoin*. Já ouvi tudo isso antes. Quando eu estava na internet em 1991, ela era um antro de ladrões, pornógrafos, piratas e criminosos. Mas não importava naquela época e não importa agora. Não importa porque a mesma tecnologia poderosa que pode ser usada por um criminoso para promover suas atividades criminosas também pode ser usada por todos nós para fazer o bem, para fazer coisas incríveis em todo o mundo. E existem mais de nós do que deles.

O *bitcoin* cria um ambiente propício para a inovação, porque não é apenas uma moeda: é uma tecnologia, uma rede e uma moeda.

Posso te dizer hoje que estou muito feliz que o preço de *bitcoin* está subindo muito, porque eu possuo um pouco de *bitcoin* e isso me traz uma sensação

agradável. Mas não me importa o preço. Se o *bitcoin* colapsasse amanhã de manhã, a tecnologia continua sendo revolucionária. Tal como se um *site* falhar na internet, ou um aplicativo falhar na internet, a internet não desaparece.

> *"O bitcoin cria um ambiente propício para a inovação, porque não é apenas uma moeda, é uma tecnologia, uma rede e uma moeda."*

O bitcoin como um mecanismo de entrada e saída

Se você entende que *bitcoin* é uma tecnologia e não apenas uma moeda, você pode realmente entender a importância que ele tem. Novamente, não é sobre nós. É sobre os outros 6 1/2 bilhões. É sobre a habilidade de trazer ao mundo um nível de integração financeira nunca antes visto. Da nossa perspectiva no mundo privilegiado, é uma grande tecnologia. Podemos fazer alguma inovação disruptiva. Podemos construir alguns serviços interessantes. Mas se você é um agricultor queniano que está tentando arrecadar dinheiro para comprar semente, agora você pode fazer empréstimos de ponta a ponta e alcançar credores de todo o mundo, isso não é apenas uma tecnologia - isso realmente transforma vidas.

> *"Bitcoin é sobre a habilidade de trazer ao mundo um nível de integração financeira nunca antes visto."*

A vasta maioria do mundo vive sob regimes repressivos e corruptos com bancos centrais que impõem hiperinflação de 30% ao mês. É muito mais importante ver como o *bitcoin* pode afetar todas essas pessoas. Existem 2 bilhões de pessoas na internet e apenas 1 bilhão delas têm contas bancárias. Nós podemos mudar isso. Não vai ser fácil, não se enganem. Quando você lança uma tecnologia disruptiva no meio das organizações mais poderosas do planeta, elas não gostam disso. Neste momento, ainda estamos nos estágios iniciais. Para usar a expressão trivial: "Primeiro eles nos ignoram, então eles riem de nós, depois eles lutam contra nós e depois nós vencemos." Nós ainda estamos na fase em que eles riem de nós. Está tudo bem, porque quando eles começarem a lutar contra nós, eles já terão perdido. Esta tecnologia passou a ser global com a injeção de mais de US$ 2,5 bilhões de dólares de investidores chineses que descobriram um contrapeso à dominação mundial do dólar norte-americano enquanto moeda de reserva global.

• Altcoins: moedas para todos

Existem quase 200 moedas no mundo, mas apenas uma moeda internacional. Existem quase 200 moedas controladas por bancos centrais e governos, mas apenas uma moeda matemática hoje, e é o *bitcoin*.

> *"As moedas criptográficas serão o alicerce do nosso futuro financeiro. Você não pode desinventar esta tecnologia. Você não pode transformar este omelete em ovos novamente."*

Vamos construir mais delas. As moedas criptográficas serão o alicerce do nosso futuro financeiro. Elas farão parte do futuro deste planeta, porque elas foram inventadas. É simples assim. Você não pode desinventar esta tecnologia. Você não pode transformar este omelete em ovos novamente. Já temos mais de 100 moedas concorrentes no espaço, o que mostra a rapidez com que a inovação explodiu, mesmo além do *bitcoin* como moeda. Existem muitas outras moedas alternativas, *altcoins*, como são conhecidas — que usam a mesma tecnologia básica de um registro de ativos descentralizado usando o consenso na rede com o algoritmo do Satoshi. Algumas dessas moedas são inflacionárias, algumas deflacionárias, algumas utilizam penalidade por sobrestadia ou taxas de juros negativas, algumas são beneficentes e redistribuem uma proporção da renda para as organizações filantrópicas.

Podemos inventar dinheiro sem parar e criar novas formas de dinheiro e instrumentos financeiros.

> *"No final do dia, o bitcoin é dinheiro programável. Quando você tem dinheiro programável, as possibilidades são verdadeiramente infinitas."*

Dinheiro programável para todos nós

No final do dia, o *bitcoin* é dinheiro programável. Quando você tem dinheiro programável, as possibilidades são verdadeiramente infinitas. Podemos pegar muitos dos conceitos básicos do sistema atual que dependem de contratos legais e podemos convertê-los em contratos algorítmicos, em transações matemáticas que podem ser aplicadas na rede *bitcoin*. Como eu disse, não há terceiros, não há contraparte. Se eu optar por enviar o valor de uma parte da rede para outra, é de ponto a ponto com ninguém no meio. Se eu inventar uma nova forma de dinheiro, eu posso implementá-la em todo o mundo e convidar outras pessoas para virem se juntar a mim.

> *"Bitcoin é a internet do dinheiro. Moeda é apenas a primeira aplicação. bitcoin é uma tecnologia revolucionária que mudará o mundo para sempre."*

Bitcoin não é apenas dinheiro para a internet. É dinheiro perfeito para a internet. É instantâneo, é seguro, é de graça. Sim, é dinheiro para a internet, mas é muito mais. *Bitcoin* é a internet do dinheiro. A moeda é apenas a primeira aplicação. Se você entender isso, você poderá olhar para além do preço, para além da volatilidade, para além do modismo. Na sua essência, *bitcoin* é uma tecnologia revolucionária que mudará o mundo para sempre.

Junte-se a mim na revolução.

Obrigado.

DINHEIRO PONTO A PONTO

Reinventar dinheiro na Universidade Erasmus; Roterdão, Países Baixos; Setembro 2015

Link de vídeo: https://www.youtube.com/watch?v=n-EpKQ6xIJs

Muita gente me pede para falar sobre as últimas novidades no *bitcoin*, mas o que eu realmente quero falar é sobre a História Antiga. Quero fornecer um contexto histórico para o dinheiro e falar sobre por que o *bitcoin* é importante no contexto histórico.

Qual a idade do dinheiro?

Primeiro, um pequeno quiz para o público: se você pensa em dinheiro como tecnologia, como um sistema tecnológico que a civilização humana inventou, qual a idade desta tecnologia? Alguma ideia? (Audiência se manifesta com respostas variadas).

Muitas respostas diferentes aqui. É sempre surpreendente para mim que as pessoas digam que tem 400 anos, 1000 anos, 2000 anos de idade. Na verdade, nós realmente não sabemos a idade do dinheiro. Parte da razão pela qual não sabemos sua idade, é porque ainda não descobrimos uma civilização tão antiga que não tivesse dinheiro. Sabemos que o dinheiro é tão antigo quanto a civilização.

> *"O dinheiro é tão antigo quanto a civilização."*

Uma coisa que surpreende as pessoas é que o dinheiro é mais antigo que a escrita. Nós sabemos disto, porque quando olhamos para as descobertas arqueológicas da escrita, encontramos hieróglifos e encontramos cuneiformes. Quando olhamos para essas antigas formas de escrita, adivinhem sobre o que estavam escrevendo. Dinheiro. Eles escreviam livros contábeis. Toda a escrita antiga que encontramos, as primeiras formas de escrita, são livros contábeis. Eles escreviam sobre dinheiro. Porque o dinheiro é mais velho do que a escrita.

O dinheiro é mais antigo do que a roda? Não sei, mas sabemos que as rodas já foram usadas como dinheiro. Talvez a primeira roda tenha sido vendida por dinheiro ou tenha sido usada como uma forma de dinheiro em si. Os sítios arqueológicos que retornam à Idade da Pedra revelaram a presença de dinheiro sob a forma de conchas, penas e contas.

Na realidade, podemos ensinar aos primatas como usar o dinheiro. Há vários estudos nos quais os chimpanzés são ensinados como usar dinheiro. Eles são ensinados que um tipo específico de pedra pode ser trocado por bananas. Pesquisadores então observam os macacos para ver o que eles farão com essa nova informação. Então, eles rapidamente inventam o assalto à mão armada. Eles descobrem que, ao bater em outro macaco e pegar suas pedras, podem trocá-las por bananas. Surpreendentemente, uma segunda coisa que eles inventam é a prostituição. Descobrem que os favores sexuais podem ser trocados por pedras, que então podem ser trocadas por bananas. O que isso nos diz sobre a natureza do dinheiro?

Acho que o *insight* importante acerca da natureza do dinheiro é que ele é uma forma de comunicação. Em seu nível mais básico, o dinheiro não é valor. O dinheiro representa uma abstração do valor; é uma maneira de comunicar valor. É uma linguagem. O dinheiro é tão antigo quanto a língua, porque a habilidade de comunicar o valor é tão antiga quanto a linguagem e o dinheiro. Em muitos aspectos, tem características que o tornam uma construção linguística. É uma forma de comunicação.

> *"Usamos o dinheiro para comunicar valor um para o outro, para expressar um ao outro como valorizamos um produto, um serviço, um gesto."*

"Usamos o dinheiro para comunicar valor um para o outro, para expressar um ao outro como valorizamos um produto, um serviço, um gesto". Utilizamos-no como base da interação social porque, ao comunicar o valor de um para o outro, criamos laços sociais. Então, o dinheiro também é uma construção social muito importante. Esta é uma tecnologia verdadeiramente antiga. No entanto, ironicamente, é uma das tecnologias menos estudadas sob uma perspectiva histórica e tecnológica. Olhamos para *bitcoin* hoje e isso representa uma invenção, uma nova forma de dinheiro. Vamos pensar sobre isso por um momento.

Evolução tecnológica do dinheiro

Com que freqüência a tecnologia do dinheiro foi transformada por uma invenção? Quantas formas diferentes de dinheiro já existiram? Em um nível muito básico, uma forma de comunicar valor é trocando coisas que consideramos de igual valor. "Aqui está uma cabra. Eu aceito 20 bananas pela cabra. "Isso não é realmente dinheiro porque é uma transação de escambo, mas é a primeira forma de comunicação sobre o valor.

• Escambo para metais preciosos

Então, começamos a ver formas abstratas de dinheiro. A primeira grande evolução tecnológica foi começar a trocar algo que você não podia comer

- uma pena, uma pérola, uma corda com nós, alguma coisa colorida que pudesse ser usada para fins estéticos. Foi quando dinheiro assumiu uma forma abstrata. O primeiro grande momento de transformação tecnológica para o dinheiro foi quando o dinheiro deixou de ser usado para o consumo tangível de valor intrínseco, tornando-se algo que se referia ao valor, como uma abstração.

> *"O primeiro grande momento de transformação tecnológica para o dinheiro foi quando o dinheiro deixou de ser usado para o consumo tangível de valor intrínseco, tornando-se algo que se referia ao valor, como uma abstração. Uma das formas mais populares dessas abstrações foi usar metais preciosos para expressar o valor."*

Uma das formas mais populares dessa abstração foi usar metais preciosos para expressar o valor. Metais preciosos combinam algumas das características mais importantes do dinheiro: difícil de encontrar (escasso); facilmente transportáveis (pelo menos quando comparado a uma pedra gigante ou um barril inteiro de plumas); fácil de dividir (você pode cortar uma moeda de ouro em pedaços e subdividir as peças); e universalmente ser valorizado para fins estéticos. Essa é a segunda grande transformação na tecnologia do dinheiro. Foram necessários centenas de milhares de anos antes de vermos a introdução de metais preciosos. Historicamente, começamos a ver metais preciosos no início das civilizações agrárias na região do Crescente Fértil no Oriente Médio. Os babilônios, os egípcios e os gregos desenvolveram esses metais preciosos.

• Dos metais preciosos para o papel

Duas grandes evoluções tecnológicas e depois nada por alguns milhares de anos. Então, alguém apresentou uma ideia brilhante: se eu depositar ouro com alguém confiável, eles podem me dar um pedaço de papel que diz que eu tenho ouro neste cofre confiável. Então eu poderia trocar o papel ao invés do ouro. É mais fácil de transportar. Enquanto eu puder confiar que meu dinheiro está no cofre, então eu tenho uma nova forma de dinheiro.

Com cada evolução tecnológica do dinheiro, há ceticismo. Mas acho que este pode ser o momento de maior ceticismo na civilização humana. Para muitas pessoas, essa nova invenção do dinheiro como papel era algo controverso. Você acha que as pessoas estão enlouquecendo com o *bitcoin*? Imagine o quanto elas se assustaram quando lhes disseram que, agora, em vez de negociar ouro, elas trocariam pedaços de papel. Para muita gente, isso era impensável. Quero dizer, afinal de contas, claramente que para muitos, este papel não tinha qualquer valor real. Demorou cerca de 400 anos para que o papel, como dinheiro, fosse aceito amplamente. Foi uma grande aberração.

> *"Você acha que as pessoas estão enlouquecendo com o bitcoin? Imagine o quanto elas se assustaram quando lhes disseram que, agora, em vez de negociar ouro, elas trocariam*

pedaços de papel."

• Do papel para o plástico

Então, cerca de 60 anos atrás, vimos uma nova forma de dinheiro na forma de cartões de plástico. Na verdade, os primeiros cartões eram de papel ainda. Nos Estados Unidos, o Diners Club foi o primeiro a criar um cartão de crédito, que era uma forma de cheque de viagem. Então, as pessoas tornaram a dizer: "Isto não é dinheiro. Por que você não me dá o bom e velho papel que eu conheço?". Essa foi outra grande transformação do dinheiro.

• Do plástico para o bitcoin

Agora, temos o *bitcoin*. *Bitcoin* é, na minha mente, uma transformação muito radical. É tão radical como uma mudança de metais preciosos para o papel-moeda. Talvez ainda mais radical. Então o que é *bitcoin*? A questão fundamental na descrição do *bitcoin* é que se você usar como referências a nossa experiência existente, essa experiência é baseada em milhares de anos de compreensão do dinheiro em uma forma física. Agora, estamos tentando explicar uma forma de dinheiro que é completamente abstrata. "É um *token* que representa a aceitação em uma rede, uma forma de dinheiro centrado na rede". Mas isso nem sequer começa a descrever o que é o *bitcoin*.

Um dos equívocos mais comuns, quando eu tento descrever o *bitcoin*, é que as pessoas pensam que é simplesmente um sistema de pagamento, que o *bitcoin* é simplesmente uma forma de digitalização de dinheiro. É dinheiro digital. Ótimo. Bem, isso é meio inútil porque nós já temos dinheiro digital. Todos vocês usam dinheiro digital todos os dias, muito antes do *bitcoin* aparecer. Você tem contas bancárias. Essas contas bancárias possuem livros-razão digitais. Você usa essas contas bancárias para enviar pagamentos eletronicamente. Isso é dinheiro digital.

"Bitcoin é uma transformação fundamental da tecnologia do dinheiro"

Bitcoin não é só dinheiro digital. "*Bitcoin* é uma transformação fundamental da tecnologia do dinheiro". É difícil de entender porque é muito diferente de tudo que conhecíamos antes. Então, vou usar uma abordagem diferente para falar sobre ele. Quero dar uma olhada na arquitetura de rede por um segundo.

Mudando para uma era centrada em rede e baseada em protocolo

Bitcoin não está acontecendo no vácuo. Está acontecendo em um momento da história quando vemos uma transformação de muitas instituições sociais

fundamentais. Essa transformação é uma grande "era" centrada em redes.

Durante séculos, as instituições sociais são organizadas em torno de organizações hierárquicas: instituições, democracia, sistema bancário, educação. Todas as nossas interações sociais foram organizadas apoiando-se em autoridades nessas hierarquias, essas burocracias de pessoas. Mas algo aconteceu com a invenção da internet. Começamos a ver cada vez mais essas instituições sociais modificando-se de sistemas que eram fechados, opacos, complexos hierárquicos inexplicáveis com suas próprias regras, para plataformas. Começamos a ver uma introdução de sistemas que possuem interfaces, APIs que podemos acessar, onde a informação pode fluir para dentro e para fora da organização. Então, passamos de instituições para plataformas.

Começamos a ver uma transformação ainda mais importante, quando passamos de plataformas para protocolos. A coisa interessante sobre a mudança entre uma plataforma e um protocolo é que, quando você possui um protocolo, não existe um polo central para recursos. TCP/IP não funciona em referência a um provedor de serviço. TCP/IP funciona sem contexto em todo o mundo. Você não precisa se inscrever em nenhuma conta para usar TCP/IP; você só precisa usar a linguagem. Quando você move uma plataforma para uma linguagem, abrem-se todas essas possibilidades.

> *"Bitcoin é a primeira forma de dinheiro centrada em rede, baseada em protocolo. Isso significa que existe sem referência a um contexto institucional ou plataforma."*

O *Bitcoin* é a primeira forma de dinheiro centrada em rede e baseada em protocolo. Isso significa que existe sem referência a um contexto institucional ou plataforma. Eu voltarei a isso em um segundo, esse é um ponto realmente importante.

• Arquitetura p2p

Nós dizemos que o *bitcoin* é um dinheiro ponto a ponto. O que isso significa? Refere-se a uma arquitetura usada em termos de ciência da computação ou rede ou sistemas distribuídos, usados para descrever uma relação entre os participantes em um sistema. A arquitetura do *bitcoin* é ponto a ponto porque cada participante na rede usa o protocolo *bitcoin* em um nível igual. Não há nenhum nó *bitcoin* especial; todos os nós são iguais.

Ponto a ponto significa que quando você envia uma transação para a rede, cada ponto a trata da mesma maneira. Não existe um contexto dentro de um sistema de ponto a ponto além do que é recebido da rede. Uma questão interessante em sistemas distribuídos é essa questão de contexto e estado. Se você logar no Facebook e tiver uma conta do Facebook, você não está usando um protocolo. Todo o estado é controlado pelo Facebook. Você tem uma

sessão de *login* e todos os dados são mantidos por eles. Nós chamamos isso de arquitetura cliente-servidor. *Bitcoin* é diferente por que é ponto a ponto, como *e-mail* ou TCP/IP.

• Arquitetura cliente-servidor

Nós somos relutantes quanto a discutir sobre dinheiro. De fato, é chocante saber que em muitos países, dinheiro não faz parte do sistema de educação. Crianças de 5 anos fazem grandes perguntas sobre dinheiro. A maioria dos pais acha quase impossível responder a essas perguntas. "O que é dinheiro, mamãe? Como funciona o dinheiro? Por que não temos mais dele? Por que todos não podem ter mais dele?". Você não fala pra ela: "Suzy, vá pro seu quarto estudar inflação, como uma boa garota, e não saia de lá até saber responder a todas essas questões!".

Nós não discutimos sobre dinheiro. É interessante, usamos essa tecnologia como fundamento em quase todos os aspectos de interação social e ainda é um assunto totalmente tabu. Nós todos fingimos que não estamos particularmente preocupados com dinheiro, pelo menos não intrinsecamente. Nós temos metas e aspirações maiores. Nós usamos o dinheiro nas experiências cotidianas, mas não falamos sobre ele. É um assunto sujo.

Eu acho que a arquitetura tem algo a ver com isso. Antes do *bitcoin*, nas primeiras versões do dinheiro -- quando começou a ser emitido a troco de metais preciosos guardados em um cofre --, o que ele representava era uma forma de débito. Esse é um conceito importante para compreender, pois dá cores à nossa discussão.

> *"Antes do bitcoin, nas primeiras versões do dinheiro -- quando começou a ser emitido a troco de metais preciosos guardados em um cofre --, o que ele representava era uma forma de débito."*

Quantos de vocês têm dinheiro no banco? Nenhum de vocês tem dinheiro no banco. Vocês depositaram dinheiro físico em um caixa forte? Se sim, talvez possam dizer que têm dinheiro no banco. O resto de vocês tomou empréstimo junto a um o banco. Pelo privilégio de emprestar seu dinheiro a um banco, você é pago com a maravilhosa taxa de juros de 0,00001 por cento ao ano. Seu banco pega esse dinheiro, vira para o lado e o empresta a alguém próximo a você a juros de 24,99 por cento ao ano.

> *"Esta é uma relação de cliente-servidor. Porque o dinheiro apenas existe como um débito em um livro de registro que você não controla. Um livro de registro que é guardado por um servidor e você é apenas um cliente. De fato, você não tem absolutamente nenhum controle sobre ele."*

Esta é uma relação de cliente-servidor. Porque o dinheiro apenas existe como um débito em um livro de registro que você não controla. Um livro de registro que é guardado por um servidor e você é apenas um cliente. De fato, você não

tem absolutamente nenhum controle sobre ele. Você não tem nem qualquer interação básica com esse dinheiro, a menos que seja mediada pelo servidor. É o que faz uma arquitetura cliente-servidor.

- **Arquitetura mestre-escravo**

Temos outro termo em sistemas distribuídos que descreve uma forma específica de arquitetura cliente-servidor, onde a entidade secundária tem apenas uma cópia parcial que não é realmente significativa. Chamamos a isso de uma arquitetura de mestre-escravo. Se você pensa no uso anterior do dinheiro como uma arquitetura de mestre-escravo, você tem que fazer uma pergunta desconfortável: quem é o escravo? Porque em um sistema de dívida, uma das duas partes é sempre o escravo.

> *"... em um sistema de dívida, uma das duas partes é sempre o escravo."*

Você é o cliente. Você não é o servidor. O servidor não serve realmente a você; eles servem a si próprios porque eles são o mestre. Esta é a arquitetura de dinheiro em que vivemos. Essa é a arquitetura do dinheiro que usamos em nossa civilização: uma arquitetura de dinheiro em que não temos qualquer controle; uma arquitetura de dinheiro em que cada interação é mediada por um terceiro que tem controle absoluto sobre esse dinheiro.

Hoje, se você vai para um caixa eletrônico e insere o seu cartão, o banco pode decidir se lhe dará o seu dinheiro. Um dia — como o povo de Chipre, Grécia, Venezuela, Argentina, Bolívia, Brasil e uma lista de centenas de países ao longo das últimas décadas e mesmo séculos descobriram —, você vai ao banco e o banco não quer dar-lhe o dinheiro, porque não são obrigados. Essa é a essência de uma relação mestre-escravo.

> *"Bitcoin é fundamentalmente diferente porque, em bitcoin, você não deve nada a ninguém e ninguém deve nada a você. Não é um sistema baseado em dívida."*

Bitcoin é fundamentalmente diferente porque em *bitcoin*, você não deve nada a ninguém e ninguém deve nada a você. Não é um sistema baseado em dívida. É um sistema baseado na propriedade desse *token* abstrato. Propriedade absoluta. Temos uma expressão nos Estados Unidos, que é "se você tem a posse, isso é nove décimos da lei." No *bitcoin*, posse é dez décimos da lei. Se você controlar as chaves do *bitcoin*, o *bitcoin* é seu. Se você não controlar as chaves do *bitcoin*, o *bitcoin* não é seu. Você está de volta para a relação mestre-escravo.

> *"No bitcoin, propriedade é dez décimos da lei. Se você controlar as chaves do bitcoin, o bitcoin é seu. Se você não controlar as chaves do bitcoin, o bitcoin não é seu."*

Bitcoin, uma transformação fundamental de dinheiro

Bitcoin representa uma transformação fundamental de dinheiro. Uma invenção que muda a tecnologia mais antiga que temos na civilização. Alterando-o radicalmente e disruptivamente ao mudar a arquitetura fundamental para uma onde cada participante é igual. Onde as transações não têm nenhum estado ou contexto, a não ser obediência das regras de consenso da rede que ninguém controla. Onde seu dinheiro é seu. Você o controla absolutamente através do uso de assinaturas digitais e ninguém pode censurá-lo, ninguém pode capturá-lo, ninguém pode congelá-lo. Ninguém pode lhe dizer o que fazer ou não fazer com seu dinheiro.

É um sistema de dinheiro que é simultaneamente absolutamente transnacional e sem fronteira. Nunca tivemos um sistema de dinheiro assim. É um sistema de dinheiro transmitido na velocidade da luz, que qualquer pessoa no mundo pode participar com um dispositivo tão simples quanto um telefone de mensagens de texto.

Isso representa uma inovação tecnológica que é aterrorizante para muitas pessoas, porque é uma transformação fundamental no dinheiro. O que eles vão lhe dizer é que eles estão preocupados. Eles estão muito preocupados. Eles estão preocupados que os criminosos venham a usar *bitcoin*. Mas a verdade é que eles estão muito mais aterrorizados que o resto de nós venha a usá-lo.

Obrigado.

PRIVACIDADE, IDENTIDADE, VIGILÂNCIA E DINHEIRO

Barcelona, Bitcoin Reunião no FabLab; Barcelona, Espanha; Março 2016

Link para o vídeo: https://www.youtube.com/watch?v=Vcv15piG1Yg

Hoje, eu vou falar sobre os conceitos de neutralidade, descentralização, privacidade e o que torna o *bitcoin* tão especial. Você já ouviu falar muito sobre *bitcoin*. Quando eu uso a palavra "*bitcoin*", eu não estou falando sobre a moeda. Estou falando de um conceito mais amplo: o conceito de redes horizontais e totalmente descentralizadas para fornecer aplicações confiáveis. Se você tiver uma rede horizontal, completamente descentralizada, e que forneça aplicações confiáveis, a primeira aplicação mais lógica é a moeda. Mas a moeda é apenas a primeira aplicação.

Bancos: de liberador a limitador

Estamos reestruturando a sociedade através da reconstrução de instituições. Tradicionalmente, nossas instituições têm um *design* estrutural hierárquico. Essa foi uma invenção da industrialização. Um conceito do século XVIII, para permitir que as pessoas se organizem e se comuniquem em uma escala maior. Foi muito eficaz na quebra dos monopólios dos reis e sistemas feudais. Agora este sistema já correu seu curso.

Às vezes, as pessoas me perguntam quais são minhas posições políticas e é muito difícil de explicar, mas uma palavra captura a minha ideia, eu acho: eu sou um disrupcionista. O que isso significa é que a cada 30 ou 40 anos pelo menos, as coisas que se estabeleceram precisam ser disruptadas.

Porque uma vez que elas se estabelecem, o poder se acumula, elas se tornam centralizadas e, com poder centralizado, a corrupção ocorre. Esse não é um conceito novo. Meus antepassados - venho da Grécia - descobriram que a corrupção ocorre em sistemas de poder. E o poder absoluto produz corrupção absoluta. Não há mais poder absoluto do que o poder sobre o dinheiro.

> *"A cada 30 ou 40 anos pelo menos, as coisas que se estabeleceram precisam ser disruptadas. Porque uma vez que elas se estabelecem, o poder se acumula, elas se tornam centralizadas e, com poder centralizado, a corrupção ocorre. Não há poder mais absoluto do que o poder sobre o dinheiro. "*

Vivemos em um mundo onde o banco foi inventado como um grande libertador. Foi uma invenção que transferiu as finanças dos reinos dos reis, para o domínio das pessoas comuns.

Esse sistema libertou bilhões de pessoas. E então se tornou concentrado, adquiriu poder e o poder levou à corrupção. O que nos resta hoje não é um sistema libertador, e é hora de disruptá-lo. *Bitcoin* é uma das coisas que irá atrapalhar a centralização do poder. Por que isso?

Resultados negativos por design, não intenção

Uma das coisas que me interessa como cientista da computação e que trabalha com sistemas distribuídos é a arquitetura de sistemas. A arquitetura é um tema excelente para esta cidade. A arquitetura de sistemas é o que finalmente produz os resultados.

Trabalhei com muitos banqueiros. São pessoas legais. Eles tentam alimentar a família, pagar sua hipoteca, manter seu emprego estável. Entre eles, existem alguns sociopatas que inevitavelmente se elevam às mais altas posições de poder, porque a sociopatia é uma vantagem em sistemas hierárquicos. Mas a maioria dos problemas com a concentração tradicional de poder no dinheiro não tem nada a ver com as pessoas serem malignas. Isso tem a ver com o fato, de que essas instituições, através de sua forma, através de sua arquitetura, produzem resultados que não são bons. Eles produzem resultados que não são igualitários. Eles produzem resultados que são restritivos. Eles começam a expressar o nativismo, o nacionalismo, o tribalismo, a estrutura de classes e todas essas coisas fazem do mundo um lugar menor.

Comunicações expandem enquanto o acesso às operações bancárias declina

Na verdade, nos últimos 15 anos, vimos a internet se tornar um enorme poder para a descentralização das comunicações. Tem sido uma força muito libertadora. Mas se você olhar para a inclusão econômica e como funciona a operação bancária, não expandimos as oportunidades. Não ampliamos o acesso. Na verdade, agora estamos regredindo. A inclusão econômica está diminuindo.

A razão pela qual está diminuindo é que essas estruturas isoladas de finanças, em sua própria arquitetura, levantam paredes: fronteiras nacionais, estruturas de classes e diferenças em como seu dinheiro e seu comércio são tratados. Vivemos em um mundo cada vez mais global e interligado. Existe até uma cultura global emergente através da internet. E, ainda assim, nossos sistemas financeiros são paroquiais, insulares e separados.

"Vivemos em um mundo cada vez mais global e interligado, e ainda assim, nossos sistemas financeiros são paroquiais, insulares e separados."

Se você está olhando para uma perspectiva de rede, existem sistemas de dinheiro para transmissão de pequenas quantidades e sistemas de dinheiro para transmissão de grandes quantidades. Sistemas de dinheiro para pagamentos de consumidores, sistemas de dinheiro para pagamentos de empresa a empresa. Todos eles são separados geograficamente com base em fronteiras, jurisdições legais, estados-nação. O que essa estrutura produz é uma separação. Isso significa que, como pessoas, somos cada vez menos livres para negociar com o resto do mundo. A geopolítica está afetando as finanças de uma forma séria porque a combinação de estado e dinheiro produz resultados tóxicos.

E estamos prestes a disromper tudo isso.

Nova arquitetura, novo acesso

O que a arquitetura do *bitcoin* nos dá é uma nova maneira de organizar o mundo, exatamente da mesma forma que a internet horizontalizou o acesso à comunicação e criou todos os sistemas que se conectem a ela igualmente. Se eu tiver um endereço IP, meus pacotes não são tratados de forma diferente dos pacotes de qualquer outra pessoa na rede. Na maior parte, isso dá voz a todos. Isso dá a todos o poder da impressora em escala global. *Bitcoin* fará o mesmo, dando a todos o poder do banco em uma escala global.

"O que a arquitetura do bitcoin nos dá é uma nova maneira de organizar o mundo, exatamente da mesma forma que a internet horizontalizou o acesso à comunicação e criou todos os sistemas que se conectem a ela igualmente."

Pense nisso como um banco por computador. Da mesma forma que a impressão pelo computador, as publicações por computador, e os *websites* mudaram a comunicação, o banco por computador - bancos controlados individualmente com todo o poder do maior banco do mundo - criará disrupção.

Imagine um mundo onde cada pessoa tem uma habilidade não apenas para executar transações, mas também para criar instrumentos e sistemas financeiros complexos sem pedir permissão a ninguém. Simplesmente conectando-se à rede, qualquer um pode iniciar uma nova aplicação. Sistemas centralizados não podem fazer isso.

Em um sistema centralizado, quanto mais longe do centro você estiver, menos controle você tem. Quanto mais perto você chegar do sistema, e quanto mais longe você chegar na hierarquia, mais controlado e mais limitado é o acesso. Mas não com o *bitcoin*. Com sistemas como o *bitcoin*, cada nó na rede tem acesso igual para todos os serviços financeiros. Em um sistema cen-

tralizado, você pode criar um novo aplicativo, mas você deve primeiro pedir permissão. E então, a permissão só é concedida se o seu uso puder aplicar-se a uma população muito grande e ser lucrativa.

Na internet ou no *bitcoin*, tudo o que é necessário para iniciar uma aplicação são dois nós, duas pessoas, dois sistemas. Eles podem começar a se comunicar, construir seus próprios protocolos, seus próprios sistemas, e esse aplicativo, com apenas duas pessoas que o utilizam é tão válido quanto qualquer outro aplicativo na rede.

Neutralidade da rede e não-discriminação

Quando você olha para a internet, o mal-entendido fundamental é que as pessoas pensam que o poder da internet vem da habilidade de transmitir informações rapidamente. Mas o verdadeiro poder da internet vem da neutralidade da rede. A neutralidade da rede é o conceito de que a internet não discrimina com base na fonte, destino ou conteúdo.

"Bitcoin é a primeira rede financeira que apresenta neutralidade"

"*Bitcoin* é uma primeira rede financeira que apresenta neutralidade". Em uma transação de *bitcoin*, a rede não se preocupa com a fonte, o destino, a quantidade ou o tipo de aplicativo financeiro que ela está apoiando. A única questão relevante é, você pagou uma taxa suficiente para usar os recursos da rede? E se você fez, sua aplicação é válida.

• Não há transações de spam no bitcoin

Temos uma conversa interessante acontecendo no *bitcoin* agora. Talvez alguns de vocês tenham ouvido o termo "transações de spam". O que é uma transação de spam? O que é preciso para uma transação ser "spam"? Eu acho que esse termo não faz sentido porque, para decidir quais transações são spam e quais não são, você está aplicando um julgamento de cima para baixo. Você está impondo, na arquitetura, escolhas de quais aplicações são legítimas. Então a pergunta é, legítimo a quem? O usuário final? Não existe tal coisa como uma transação de spam simplesmente porque, se uma transação carregou a taxa suficiente, isso significa que o remetente dessa transação a considerou valiosa o bastante para transmitir - e, portanto, é uma transação legítima. Isso substitui os conceitos de controle e conteúdo por tomada de decisões sobre o que é bom, o que é ruim, o que é legítimo, o que é ilegítimo, o que é uma aplicação válida, o que não é uma aplicação válida, com um mecanismo simples de mercado. Se você paga essencialmente uma pequena taxa para sua transação, então, devido à democratização do financiamento, sua transação é válida e não é spam.

Dinheiro centrado em rede

A partir da década de 1970, vimos o mundo começar a adotar moedas digitais. Quando as pessoas chamam o *bitcoin* de uma "moeda digital", eles estão perdendo o ponto. O euro é uma moeda digital, o dólar é uma moeda digital. Menos de 8% dessas moedas existem em forma física; o resto é *bits* e registros em livros contábeis. Mas a diferença fundamental é que esses livros são controlados pelas organizações centralizadas, enquanto no *bitcoin*, não são. *Bitcoin* possui uma rede descentralizada, uma rede aberta.

"Bitcoin não é uma moeda digital. É uma criptomoeda. É um dinheiro centrado em rede."

Bitcoin não é uma moeda digital. É uma criptomoeda. É um dinheiro centrado em rede. Eu realmente gosto da ideia de um dinheiro centrado na rede. Uma rede que permite substituir a confiança nas instituições, a confiança nas hierarquias, pela confiança na rede. A rede age como um árbitro maciçamente difuso da verdade, resolvendo qualquer discordância sobre transações e segurança de uma forma onde ninguém tem controle.

Sonhando com controle totalitário sobre todas as transações financeiras

A partir da década de 1970, nossas moedas começaram a ser digitais, mas não é o mesmo sentido "digital" que tem o *bitcoin*. Isso começou a se tornar um sonho para os governos. O sonho de poder um dia controlar cada transação financeira de todo ser humano no planeta, de modo que tudo fosse visível para as estruturas de poder. Onde a privacidade morre. Onde a capacidade de fazer uma transação imediatamente coloca você sob a lente dos sistemas que o monitoram. Nós criamos um sistema de vigilância financeira global, um sistema de vigilância totalitária em todo o mundo.

"Isso começou a se tornar um sonho para os governos, o sonho de poder um dia controlar todas as transações financeiras de todo ser humano no planeta, de modo que tudo fosse visível para as estruturas de poder. Onde a privacidade morre."

Esse sistema, que exige verificação de identidade e de crédito e limitação de acesso, é responsável pelo fato de que a inclusão econômica está regredindo. Isso é responsável pelo fato de 2,5 bilhões de pessoas, não terem qualquer acesso a serviços bancários. Isso diz respeito apenas aos chefes de família, sem contar suas famílias. E sem contar as pessoas que têm acesso limitado a bancos em uma moeda única, dentro de uma única fronteira. Se você contar todos eles, são bilhões e bilhões.

- **Censura de transações financeiras**

Como membro da elite privilegiada do mundo desenvolvido, tenho a habilidade de abrir uma conta de corretagem em 24 horas, eletronicamente. E dentro de 24 horas, posso negociar em ienes no mercado de ações de Tóquio. Eu posso enviar e receber dinheiro em qualquer lugar do mundo sem realmente nenhum limite. Tudo o que tenho a fazer é sacrificar minha privacidade e minha liberdade.

Porque enquanto eu posso fazer todas essas coisas e elas são muito poderosas, existem algumas coisas que não posso fazer. Não estou falando sobre comprar drogas. Não é assim tão interessante. O que estou falando são coisas simples, por exemplo, doar para uma organização ativista como o WikiLeaks. Alguns anos atrás, o WikiLeaks foi completamente excluído do sistema financeiro mundial simplesmente pela pressão extrajudicial aplicada nos poucos e principais fornecedores de pagamento: a Visa, a MasterCard, o sistema de transferência bancária, o PayPal, etc. Sem qualquer processo legal, sem qualquer condenação e talvez, na minha opinião, sem qualquer crime, além de revelar a verdade do crime, WikiLeaks foi cortado do sistema financeiro do mundo. Isso está acontecendo agora não apenas nas associações ativistas; está acontecendo com países inteiros.

O sonho dos Estados-Nação, para criar um sistema financeiro totalitário, morreu em 3 de janeiro de 2009, com uma invenção do bitcoin e mineração do bloco Gênesis.

> *"O sonho dos Estados-Nação, para criar um sistema financeiro totalitário, morreu em 3 de janeiro de 2009, com uma invenção do bitcoin e mineração do bloco Gênesis."*

- **O dinheiro centrado na rede é resistente à censura**

Bitcoin é resistente à censura. Você pode já ter ouvido este termo. Você não pode controlar quando o dinheiro é transmitido em *bitcoin*. Não está atrelado a identidades ou geografia. No *bitcoin*, a vigilância de todos não é possível. No *bitcoin*, resistência à censura é um artefato criado pela neutralidade, a arquitetura de uma rede horizontal sem fronteiras. A arquitetura de neutralidade que não atribui qualquer interpretação sobre a origem, destino ou valor, é o que cria resistência à censura.

Sousveillance, not surveillance

Privacidade é muito importante, mas é um termo que muitas vezes tem um significado político muito profundo. Eu gosto de justapô-la a um outro termo: sigilo. Qual é a diferença entre privacidade e sigilo? Em última análise, e praticamente no vocabulário de hoje, a privacidade é o direito de bilhões de

indivíduos de não serem supervisionados. O sigilo é um poder de uma minoria, para escapar da prestação de contas e para fugir às responsabilidades, para não ter transparência.

Vivemos em um mundo onde cada transação individual que você faz através do sistema financeiro é catalogada, analisada e transmitida para serviços de inteligência em todo o mundo que colaboram, e ainda assim não temos ideia do que nossos governos fazem com o dinheiro. Os sistemas financeiros dos poderosos são completamente opacos. Nossas transações são totalmente visíveis através desse novo sistema de vigilância. Este mundo está de cabeça para baixo. *Bitcoin* dá esse direito.

A privacidade é um direito humano e o sigilo tem sido um privilégio do poder, e precisamos estar em um mundo onde temos uma privacidade completa, plena e forte para bilhões de pessoas. Porque isso é um direito humano, porque é um alicerce das liberdades de expressão, de associação, de discurso político e de todas as outras liberdades que estão muito ligadas à privacidade. Precisamos viver em um mundo onde o sigilo é inconstante e facilmente perfurado, onde o poder tem que enfrentar a prestação de contas, porque eles estão sob os holofotes da transparência. Precisamos inverter este sistema de cabeça para baixo.

> *"A privacidade é um direito humano. O sigilo é um privilégio do poder. Precisamos viver em um mundo onde o sigilo é inconstante e facilmente perfurado, onde o poder tem de enfrentar a prestação de contas, porque estão sob os holofotes da transparência."*

Uma das minhas palavras favoritas é uma palavra francesa: *Sousveillance*. É o oposto da vigilância (*Surveillance*). Vigilância significa olhar de cima, *Sousveillance* significa olhar de baixo. Em seu sonho de estados-nação controlando todos os nossos futuros financeiros, eles cometeram um erro de cálculo importante. É muito mais difícil para algumas centenas de pessoas observarem 7 bilhões e meio. Mas o que você acha que acontece quando 7 bilhões e meio de nós ganham o poder de olhar de volta? Quando o pan-óptico olhará de volta? Quando nossos sistemas financeiros, nossos sistemas de comunicação, são privados, e o sigilo é uma ilusão que não pode ser sustentada? Quando crimes cometidos em nomes de Estados e corporações poderosas são vulneráveis a *hackers*, denunciantes e vazadores de informação (*leakers*)? Quando tudo finalmente sai de baixo do tapete? Temos uma grande vantagem, porque o equilíbrio natural do sistema é aquele em que os indivíduos podem ter privacidade, mas os poderosos já não podem ter sigilo. *Bitcoin* é um dos primeiros passos para isso.

> *"Temos uma grande vantagem porque o equilíbrio natural do sistema é aquele em que os indivíduos podem ter privacidade, mas os poderosos não podem mais ter sigilo. Bitcoin é um dos primeiros passos para isso."*

Bancos para todos

A habilidade de transacionar através das fronteiras significa que nós agora seremos capazes de estender os serviços financeiros para bilhões de pessoas que não possuem acesso. Não necessariamente através de uma tecnologia complicada. Às vezes eu falo com vários bancos regionais, aqueles que não têm medo de *bitcoin*. Dizem-me coisas como 80% da nossa população está a quilômetros de distância de uma agência bancária e não podemos servi-los. Em um caso, eles disseram que eram quilômetros de canoa. Vou deixar você adivinhar em qual país. No entanto, mesmo nos lugares mais remotos na Terra, agora há uma torre de celular. Mesmo nos lugares mais pobres da Terra, muitas vezes vemos um pequeno painel solar em uma pequena cabana que alimenta um telefone Nokia 1000, o dispositivo mais produzido na história da fabricação, com bilhões deles espalhados. Podemos transformar cada um desses, não numa conta bancária, mas num banco.

"Não tenho uma conta bancária suíça no meu bolso. Tenho um banco suíço."

Duas semanas atrás, o presidente Obama no "South by Southwest" fez uma apresentação e falou sobre nossa privacidade. Ele disse: "Se não podemos desbloquear os telefones, isso significa que todos têm uma conta bancária suíça no bolso". Isso não é inteiramente exato. Não tenho uma conta bancária suíça no meu bolso. Eu tenho um banco suíço, com a capacidade de gerar 2 bilhões de endereços surgidos de uma única semente e posso usar um endereço diferente para cada transação. Esse banco está completamente criptografado, então, mesmo que você desbloqueie o telefone, eu ainda tenho acesso ao meu banco. Isso representa a dissonância cognitiva entre os poderes do sigilo centralizado e o poder da privacidade, como um direito humano que temos agora ao nosso alcance. Se você acha que isso vai ser fácil ou que vai ser sem luta, você está muito enganado.

Bitcoin, o zumbi de moedas

Se você ler algo sobre *bitcoin*, você verá as mesmas coisas que eles disseram sobre a internet no início dos anos 1990. É um paraíso para os pedófilos, terroristas, traficantes e criminosos. Quantos de vocês nesta sala têm *bitcoin*? Quantos de vocês nesta sala são terroristas, pedófilos, traficantes de drogas ou criminosos? *Risos na plateia*.

Você lê um pouco sobre *bitcoin*, enquanto eles empurram essa história e de vez em quando alguém, que nunca ouviu falar de *bitcoin*, percebe algo importante: ele ainda não está morto, o que é sempre surpreendente porque a cada dois ou três meses há um artigo que diz que ele morreu. Esse é um excelente *marketing*. Porque cada vez que alguém ouve "isso está morto" e, três meses depois, ouve que ainda não morreu, pensa: "Uai, essa coisa real-

mente tende a sobreviver". Eu chamo de *bitcoin* "a internet do dinheiro", mas talvez devêssemos chamá-lo de "o zumbi das moedas". É a moeda que é um morto-vivo.

> *"Eu chamo de bitcoin 'a internet dinheiro', mas talvez devêssemos chamá-lo 'o zumbi das moedas'. É uma moeda que é um morto-vivo."*

A questão aqui é que agora estamos criando um sistema que ameaça a maior indústria do mundo, a indústria financeira. Eles vão se opor. Eles vão tentar impedir o avanço, e eles vão usar a tática emocional mais comum e efetiva que existe, que é o medo. Eles vão tratá-lo de tal forma, como se você fosse um idiota e vão tentar convencê-lo de que é algo a ser temido. Quando as pessoas ouvem essa mensagem e, talvez, no dia seguinte, vêm a uma dessas reuniões aqui e conhecem um dentista que possui *bitcoin*, um arquiteto que possui *bitcoin* ou um motorista de táxi que usa *bitcoin* para enviar dinheiro para a família - pessoas normais que usam *bitcoin*, que lhes dá poder financeiro e liberdade financeira –, cada vez que uma mensagem é quebrada pela dissonância cognitiva, o *bitcoin* sai ganhando. Tudo o que o *bitcoin* realmente tem que fazer é sobreviver. Até agora, está indo muito bem.

Moedas evoluem

No novo mundo centrado em rede, moedas ocupam nichos evolutivos. Eles evoluem, como espécie, com base no estímulo que eles têm do seu ambiente. O *bitcoin* é um sistema dinâmico com desenvolvedores de *software*, que podem mudá-lo. A questão é, em qual direção o *bitcoin* evoluirá? Em qual nicho ambiental ele se encaixará? E como isso é afetado pelas ações dos poderosos? Se eles atacarem o *bitcoin*, ele evoluirá para se defender contra os predadores, assim como qualquer espécie.

Se eles atacarem o anonimato do *bitcoin*, ele evoluirá para se tornar mais anônimo. Se eles atacarem sua resiliência, ele evoluirá para se tornar mais descentralizado. No final, apesar de todas as mensagens de medo, o *bitcoin* é um ursinho fofinho das moedas e você não quer chutá-lo. Porque, como na evolução, se você pisotear a pequena lagartixa, ela evoluirá até que seja um dragão de Komodo e, então, você não poderá mais pisar nele.

Às vezes, as pessoas me perguntam: "Você acha que os governos vão proibir o *bitcoin*? Você acha que eles vão tentar fazer com que inexista através da regulação? Você acha que irão atacá-lo com negação de serviços? "A resposta é realmente simples porque, em sistemas centrados na rede - sistemas dinâmicos e adaptáveis, sistemas que exibem antifragilidade - ataques fazem com que o sistema se adapte, evolua e torne-se resistente. Pense nisso por apenas um segundo.

> *"Em sistemas centrados em rede, ataques fazem com que o sistema se adapte, evolua e torne-*

se mais resistente."

- **Ataques criam resistência**

Estou envolvido com a internet desde 1989. Nos primeiros dias, muitos artigos foram escritos sobre como a internet não era resiliente, não podia escalar para fazer envio de voz, não era segura. Lembro-me de momentos em que os ataques de negação de serviço derrubaram o Yahoo, o AltaVista e até o Google por horas, às vezes dias. O que aconteceu entre aquela época e agora? Quantas vezes você já viu o Google cair nos últimos cinco anos? Será que as pessoas pararam de atacar o Google? Muito pelo contrário. O Google pode sustentar agora *gigabits* de negação de serviços em todo o mundo e redirecionar dinamicamente. O mesmo se aplica para todas aplicações da internet. Os ataques não pararam. O sistema tornou-se imune porque, como um sistema imunológico humano, se você está exposto a um vírus e ele não o mata, você cria resistência e, na próxima vez que você estiver exposto ao vírus, isso não fará nada para você.

Os governos tentarão proibir o *bitcoin*? Regular o *bitcoin*? Atacarão o *bitcoin*? Eles já estão tentando. Eles o combatem desde o início, e o *bitcoin* está ficando cada vez mais forte. É um sistema que está sob um constante ataque de negação de serviço, que está na internet sendo atacada por *hackers*, por agentes e por vários sistemas, 24 horas por dia.

> *"Bitcoin está se tornando mais forte. É um sistema que está sob um constante ataque de negação de serviço, que está na internet sendo atacado por hackers, por agentes, por outros sistemas, 24 horas por dia."*

Em segurança, temos um termo muito engraçado, que é um *honeypot*. Um *honeypot* é um sistema que visa atrair os *hackers*. Qual *honeypot* maior você poderia ter que uma rede financeira com US$ 6 bilhões? Se você hackear o *bitcoin*, há uma recompensa de US$ 6 bilhões para você. Ninguém conseguiu essa recompensa ainda, e não é porque não estão tentando. Eles tentam sem parar. Mas sistemas como o *bitcoin* são resistentes.

Bem-vindo ao futuro do dinheiro

Lembre-se de que o que estamos fazendo aqui não é uma moeda. É a reformulação dos sistemas sociais de organização, que falharam conosco. Os sistemas de hierarquias do século XVIII que não se escalam em um mundo global e interligado estão sendo substituídos por arquiteturas horizontais centradas na rede - seja a internet, qualquer uma das aplicações que funcionam em cima dela ou o próprio *bitcoin*. Moeda é apenas a primeira aplicação. Quando você tem uma rede que pode fornecer confiança neutra, você pode construir miríades de aplicações em cima e sem ter que pedir permissão.

Bitcoin é muito mais do que uma moeda. Quando digo que o *bitcoin* é "a internet do dinheiro", a ênfase não está em "dinheiro", a ênfase está em "internet". Bem-vindo ao futuro do dinheiro.

Obrigado.

INOVADORES, DISRUPTORES, DESENCAIXADOS E BITCOIN

Maker Faire; Henry Ford Museum, Detroit Michigan; Julho de 2014

Link para o vídeo: https://www.youtube.com/watch?v=LeclUjKm408

Antes do início desta apresentação, os participantes visualizaram um vídeo apresentado pelo museu sobre a história do automóvel. Esse é o vídeo referenciado em toda essa conversa.

Bom dia! Nossa, que vídeo engraçado, não? Há cerca de um mês, eu vendi meu carro para comprar *bitcoin*. Foi uma experiência interessante, um novo mundo. Quantos aqui têm *bitcoin*? Daqueles que não têm, quais de vocês já ouviram falar de *bitcoin*? 95% do público já ouviu falar de *bitcoin*. Alguém nunca ouviu falar de *bitcoin*? Okey, ótimo, isso vai ser muito mais fácil do que pensei.

Reconhecendo a inovação

O *bitcoin* é o dinheiro digital da internet, mas é muito mais do que isso. Para este público em particular e para as pessoas que estão aqui no Maker Faire, quero falar sobre *bitcoin* na perspectiva dos desencaixados, dos esquisitos, dos anormais. As pessoas que se recusam a pensar da forma que todos os outros pensam. As pessoas que veem uma tecnologia elegante com metade do trabalho em andamento, e não veem o trabalho pela metade; elas veem o lado elegante. Elas reconhecem a inovação. E elas reconhecem inovação, não apenas alguns meses ou alguns anos antes dos outros, mas às vezes uma década antes. Esses são os tipos de pessoas que vêm para Maker Faire. E então é um ótimo lugar para começar a falar sobre *bitcoin*.

Bitcoin é inesperado. *Bitcoin* não é dinheiro, tal como conhecemos. *Bitcoin* não deveria ter acontecido. *Bitcoin* não tinha realmente nenhuma possibilidade de sucesso. Não é possível que funcione. É uma daquelas coisas que não funciona na teoria, mas que funciona na prática. Como a Wikipédia. Como o Linux. Como a internet. Ideias estranhas tidas por pessoas com rabo de cavalo e barba no pescoço. Esquisitos que ninguém realmente confia.

Bitcoin é bem-sucedida porque funciona. Como uma tecnologia, é elegante. Eu quero falar sobre esse espírito do desencaixado. Sobre dar uma volta na sala de reuniões de uma indústria dizendo "Quer saber? Estamos prestes a

mudar tudo", e ser zoado por todos na sala. Então, seguir em frente e continuar, até, de fato, mudar tudo. Isso acontece em tecnologia o tempo todo. Nós só esquecemos isso. Nós ignoramos. Nós reescrevemos a história em termos brilhantes.

Os perigos dos automóveis, eletricidade e bitcoin

Nós acabamos de ver um vídeo sobre o início do automobilismo. Você sabe o que a mídia disse sobre os primeiros automóveis? Eles ridicularizaram aqueles carros. Eles zombaram daqueles carros. Carros eram mais lentos que os cavalos. Carros quebravam o tempo todo. Carros precisavam de gasolina cara que você não poderia encontrar em qualquer lugar. Eles necessitavam de enormes infraestruturas para funcionar. Os meios de comunicação focaram na parte da história que vendia mais jornais: acidentes de carro, pedestres mutilados por carros. Por mais de duas décadas quando foram inventados os primeiros carros, os boatos eram sobre aquelas máquinas infernais, nojentas, sujas, barulhentas, que eram muito inferiores aos cavalos, que não podiam ir a lado nenhum, que somente esquisitos usariam e que, na maioria das vezes, matavam os ocupantes e todos que chegassem perto delas.

> *"Por mais de duas décadas, quando foram inventados os primeiros automóveis, os boatos eram sobre aquelas máquinas infernais, nojentas, sujas, barulhentas, que eram muito inferiores aos cavalos, que não podiam ir a lado nenhum, que somente esquisitos usariam e que, na maioria das vezes, matavam os ocupantes e todos que chegassem perto delas."*

Essa histeria ficou tão séria que, em 1865, no Reino Unido, aprovaram uma lei chamada a Lei da Bandeira Vermelha. A Lei da Bandeira Vermelha instituía que para operar um veículo seriam necessários três tripulantes na equipe: um motorista, um engenheiro e um sinalizador. O motorista iria conduzir o veículo, o engenheiro iria supervisionar essa operação (pense em ferrovias) e o sinalizador carregaria uma bandeira vermelha e andaria 100 metros à frente do carro para avisar os pedestres da chegada iminente de uma máquina mortífera infernal que iria cortá-los ao meio.

Adivinha o que aconteceu ao Reino Unido? Eles perderam a corrida industrial automobilística porque ao ver essa tecnologia, em vez de enxergar o seu potencial, deixaram o medo definir sua reação. Eles criaram um ambiente onde um carro não poderia fazer as coisas que um carro pode fazer. Se você fizer um carro ir tão lento como um pedestre correndo à frente com uma bandeira vermelha, você perde todas as vantagens de um carro. Se um carro requer uma equipe de três pessoas para operar, você perde as vantagens de um carro. Eles tentaram encaixar o carro na perspectiva de ferrovias e cavalos. Eles falharam. Eles perderam a corrida.

O que você não viu neste vídeo é que, até então, eles estavam vencendo. Os primeiros carros realmente funcionais foram construídos na Inglaterra.

Eles já haviam vencido a corrida na Revolução Industrial, com o motor a vapor. Naquela época, a Inglaterra era uma potência na inovação industrial. Estavam ganhando, até que eles decidiram que aquela máquina suja deveria ser confinada a um espaço muito limitado e cercada de regras. Eles mataram o ganso. Sem mais ovos de ouro para eles.

> *"Os primeiros carros realmente funcionais foram construídos na Inglaterra... Naquela época, a Inglaterra era uma potência na inovação industrial. Estavam ganhando, até que eles decidiram que aquela máquina suja deveria ser confinada a um espaço muito limitado e cercada de regras."*

Isto é instrutivo porque acontece frequentemente na tecnologia. No início, quando a eletricidade tornou-se doméstica e as pessoas começaram a eletrificar suas casas, você acha que a mídia anunciou "Isso é brilhante! Edison é um gênio! Isto vai mudar o mundo!"? Não. O que eles disseram era que aquela era uma tecnologia perigosa que iria queimar as casas das pessoas. Criaram muitas histórias sobre pessoas sendo eletrocutadas, sobre casas queimando.

> *"No início, quando a eletricidade tornou-se doméstica e as pessoas começaram a eletrificar suas casas, você acha que a mídia anunciou, 'Isso é brilhante! Edison é um gênio! Isto vai mudar o mundo!'? Não. O que eles disseram era que aquela era uma tecnologia perigosa que iria queimar as casas das pessoas."*

Claro, você realmente não poderia usar eletricidade porque seria necessária uma revisão completa de sua casa. Você teria que colocar fios em sua casa, que poderiam pegar fogo. Você teria que comprar dispositivos especiais para se conectar a esses fios, antes de sua casa pegar fogo. Só os ricos poderiam pagar. Claramente, essa tecnologia foi apenas uma moda entre ricos. Era só um brinquedo com nenhum valor prático.

O prefeito de Paris, durante a Exposição Mundial de 1900, disse: "Após este evento, esta moda de eletricidade será esquecida tão rapidamente como o apagar de uma luz." Famosas últimas palavras são muito comuns em tecnologia, palavras que, em retrospecto, soam ridículas. Como o chefe da IBM que disse: "Eu prevejo uma necessidade de não mais que cinco computadores em todo o mundo.", como as pessoas que disseram que o telefone nunca sucederia.

> *"Famosas últimas palavras são muito comuns em tecnologia, palavras que, em retrospecto, soam ridículas."*

Você pode adivinhar o que as pessoas estão dizendo sobre o *bitcoin*? Estão dizendo que é uma tecnologia estranha e complicada. Uma tecnologia que atende aos desencaixados, traficantes, degenerados, pornógrafos, terroristas, ladrões, vigaristas. Não vejo nenhuma dessas pessoas nesta sala..., mas é melhor tomarmos cuidado, no caso de elas aparecerem.

Claro, eles estão errados. *Bitcoin* não é nenhuma dessas coisas. *Bitcoin* é ape-

nas uma tecnologia. Muitas vezes, o primeiro uso que uma tecnologia encontra é nas mãos de criminosos. Os primeiros carros foram usados como veículos de fuga. Os primeiros telefones foram usados para tramar conspiração. Os primeiros telegramas foram usados para enviar postais de longa distância contendo esquemas de fraude e esquemas de Ponzi. As primeiras formas de eletricidade foram usadas para executar fraudes médicas e enganar as pessoas. Essas coisas sempre acontecem com uma nova tecnologia, e elas acontecem com *bitcoin* também.

> *"Bitcoin é apenas uma tecnologia. Muitas vezes, o primeiro uso que uma tecnologia encontra é nas mãos de criminosos. Os primeiros carros foram usados como veículos de fuga. Os criminosos utilizam a mais avançada tecnologia porque eles operam em um ambiente com margens de lucro muito altas e de muito alto risco."*

Por que acha que os criminosos usam a tecnologia dessa forma? Poderíamos ser moralistas e olhar para as razões reais. Os criminosos utilizam a mais avançada tecnologia porque eles operam em um ambiente com margens de lucro muito altas e de muito alto risco. Nesse ambiente, a concorrência é feroz. Usar uma tecnologia nova, se você já está correndo enormes riscos, não significa grande coisa. E se você ganhar, isso lhe dá uma vantagem enorme. Ao longo da história, as tecnologias mais incríveis foram adotadas por criminosos primeiro. Acho que não é necessariamente o que queremos dizer no plano de *marketing* do *bitcoin*, mas é interessante olhar para o que os criminosos fazem e como isso acaba sendo tecnologia *mainstream* uma década mais tarde. Há uma certa dinâmica aí.

Bitcoin já passou de sua fase inicial e já não é da alçada dos criminosos. De fato, indiscutivelmente não o foi em primeiro lugar, apesar do que a mídia disse. Agora, o *bitcoin* está atingindo o grande público e as coisas estão mudando muito rapidamente.

> *"Enquanto tecnologia, algo muito interessante está acontecendo com o bitcoin. Algo vai abalar nosso sistema financeiro e bancário como os carros fizeram com a indústria do cavalo, como o petróleo fez com a indústria baleeira, tanto quanto a eletricidade abalou a indústria de madeira e lenha."*

Hoje vou falar sobre o *bitcoin* enquanto tecnologia porque está acontecendo algo muito emocionante. Algo vai abalar nosso sistema financeiro e bancário como os carros fizeram com a indústria do cavalo, como o petróleo fez com a indústria baleeira, tanto quanto a eletricidade abalou a indústria de madeira e lenha. Bancos estão prestes a sofrer disrupção. Sem dúvida, isso já está acontecendo. Na verdade, quando eles descobrirem como esta destruição é séria, o jogo já terá acabado. Isso é geralmente o caso.

Reações dos detentores de poder à inovação

Quando indústrias estabelecidas e já consolidadas vêem uma nova tecnolo-

gia disruptiva, elas ignoram-na porque não pensam ser possível se tratar de uma ameaça. Na perspectiva dos detentores do poder, dos galhos mais altos de uma empresa monopolista estabelecida, essas ameaças parecem crianças brincando. Para o JPMorgan Chase, *bitcoin* é como uma barraca de limonada tentando quebrar a Walmart. Se a tecnologia continua a existir, então eles vão para a próxima fase, quando começam a zombar da tecnologia. De repente eles a veem por toda parte e eles começam a fazer piadas. Então, assim como com o automóvel, as primeiras pessoas que compraram carros foram ridicularizadas. Eles eram retratados sempre de joelhos com uma chave inglesa, tentando consertar sua máquina que tinha quebrado novamente. Era a imagem de um proprietário de automóvel nos primeiros anos.

Enquanto eles zombam, *bitcoin* continua a crescer e melhorar. Depois de um tempo, você vê uma mudança. Primeiramente, alguns dos executivos na indústria dizem: "Ei, talvez precisemos experimentar isso. Talvez nós precisemos começar a olhar para isso." Então há uma debandada, pois de repente percebem que isso vai mudar nossa indústria para sempre.

A essa altura, é tarde demais. A essa altura, eles são Kodak: indo de número um do mundo para, no prazo de três anos, perder uma indústria de US$ 12 bilhões para uma empresa da qual nunca tinham ouvido falar antes. Uma empresa que nem mesmo fazia câmeras. Você sabe quem destruiu a Kodak? Uma pequena empresa finlandesa que nunca tinham ouvido falar chamada Nokia. Uma empresa que não fabrica câmeras — até que eles fizeram. Dentro de três anos, eles fizeram meio bilhão de câmeras e destruíram a Kodak. Tower Records dominaram a indústria da música. Dentro de quatro anos, desapareceram. Por que? Porque o MP3 deu escolha às pessoas.

IBM era a empresa mais inabalável no ramo de computadores. Eles garantiam qualidade. De fato, comprar qualquer coisa que não fosse IBM era um sinal de que você era um perdedor. Então aconteceu o Linux. Linux abalou a IBM no seu cerne, pois subverteu a ideia básica de que para entregar tecnologia de qualidade, para entregar o melhor computador possível para trabalhos sérios como bancos, engenharia e operações governamentais, você precisaria da IBM. Você precisaria de um sistema controlado, fechado e cuidadosamente organizado, construído por sérios engenheiros com PhD.

Lá em 1992, quando Linus Torvalds disse "Eu estou construindo um sistema operacional no meu dormitório porque não tenho dinheiro para comprar um", essa ideia pareceu completamente absurda. Sistemas operacionais eram como enormes edifícios de complexidade que necessitavam de engenheiros para serem construídos. Linus Torvalds começou simples. Ele começou construindo um sistema operacional. Seis anos depois, Linux começou a dominar a indústria da computação e a Sun Microsystems começou a sentir o estrago. Oito anos depois, a Sun Microsystems en-

cabeçou a lista de falidos, HP foi comprada, seu setor de computação foi fechado e a IBM deu o fora da indústria de computadores pessoais.

Agora, 80 por cento dos celulares no planeta rodam o sistema Android -- que a propósito é Linux. Os servidores se conectaram para rodar Linux. Os bancos que usamos rodam Linux. Os sistemas de entretenimento que usamos rodam linux. Os carros que dirigimos rodam Linux. Você poderá perceber se eles pararam de rodar Linux: a telinha azul que o cumprimenta dirá *"Blá. Desculpe. Falha. Escolha errada de sistema operacional"*. Imagine que você está num avião. O sistema de entretenimento que inicia roda Linux. Se você dissesse, 15 anos atrás, para um engenheiro da IBM "Vocês estão prestes a ser destruídos por um sistema operacional construído por um estudante finlandês em seu dormitório", ele provavelmente riria de você.

> *"Se você dissesse, 15 anos atrás, para um engenheiro da IBM "Vocês estão prestes a ser destruídos por um sistema operacional construído por um estudante finlandês em seu dormitório", ele provavelmente riria de você."*

Aqui estamos hoje, e o *bitcoin* está enfrentando o sistema bancário, a indústria mais poderosa do mundo. E adivinha? O *bitcoin* vai vencer. Vai vencer por uma razão simples. Não é só porque é melhor. Não é só porque o sistema bancário é usado por gângsters, criminosos e os executivos mais vazios. E também não é porque o sistema bancário passou os últimos 50 anos entregando somente duas inovações aos consumidores -- caixas eletrônicos e cartões de crédito -- e gastou o resto do tempo tentando descobrir como enrolar você. O *bitcoin* vai vencer porque é aberto. Em um mundo de pensadores, experimentadores e fazedores, o que é aberto vence. A razão para o sucesso é o fato de permitir que a inovação floresça.

> *"Bitcoin vai vencer porque é aberto. Em um mundo de pensadores, experimentadores e fazedores, o que é aberto vence. A razão para o sucesso é o fato de permitir que a inovação floresça.*

Livre inovação e sistemas optativos

Deixe-me explicar o que quero dizer com isso. Todo sistema financeiro do mundo tem um modelo de segurança e confiabilidade que requer exclusão de maus agentes. Não posso acessar e programar a rede da Visa, porque isso colocaria em risco a segurança de sua rede. Não posso conectar à rede mundial de transferências bancárias SWIFT, porque isso colocaria a segurança dessa rede em risco. Todas essas redes são desenhadas para serem fechadas, porque sua segurança primária depende do controle de acessos. Avaliando muito cuidadosamente qualquer pessoa que tenha acesso e tente tocar o código. Avaliando muito cuidadosamente qualquer aplicação que tente rodar nesse sistema, porque se eles permitirem um único sujeito pernicioso no cerne do sistema, a segurança já era. Esse sujeito pode tomar conta de tudo

e fazer o que quiser. Claro, em 2008 descobrimos que esses seres maliciosos na verdade comandavam os bancos. E eles assumiram o controle. Eles destruíram milhões de proprietários de imóveis, aposentados e poupadores pelo mundo com sua ganância.

> *"Bitcoin é diferente porque não depende de controle de acesso para permanecer seguro. Depende de uma simples fórmula matemática de incentivos e recompensas."*

Bitcoin é diferente. O motivo de ser diferente não é porque de repente encontramos as pessoas mais honestas do mundo. Ou porque não há obstáculos no *bitcoin*. Ou porque a rede não é atacada. A diferença é que há muitos trapaceiros usando *bitcoin* - a rede é atacada a todo momento - mas a rede não depende de controle de acesso para permanecer segura. Depende de uma simples fórmula matemática de incentivo e recompensa. Para participar da rede *bitcoin* e proteger a rede enquanto minerador, o que é uma função especial no *bitcoin,* você precisará utilizar bastante força computacional e gastar muita eletricidade. Se você vence essa competição, você ganha *bitcoins* como recompensa. Essa equação simples cria um sistema de incentivos onde é muito melhor jogar de acordo com as regras do que contra elas. É a teoria dos jogos. É como um jogo de Sudoku gigante.

Se você olhar para isso como um cientista da computação, ou até como um banqueiro, você diz: "Não é possível que isso funcione. Como assim isso é um jogo de Sudoku gigante e todos competem uns contra os outros? Essas não são as bases de um sistema de segurança. Isso iria trazer o caos." É um pensamento parecido com "Como assim uma enciclopédia que qualquer um pode editar? Isso vai virar um caos", disse a Enciclopédia Britânica. Se você tiver menos que 40 anos, você nunca ouviu falar dela.

Bitcoin é uma rede completamente aberta. Qualquer um pode se conectar a ela. Você pode criar uma aplicação agora mesmo, conectá-la à rede *bitcoin* e ensiná-la a fazer algo novo. Você pode criar um novo serviço financeiro. Você pode criar um novo instrumento financeiro. Quando você faz isso, você não precisa se identificar para a rede nem pedir permissão para ninguém. Você não precisa ser aprovado. Você não precisa receber garantias. A rede não teme você porque sua segurança não depende de manter agentes maliciosos fora. De fato, *bitcoin* funciona muito bem mesmo havendo muitos agentes maliciosos bem perto do seu núcleo, porque não existe núcleo, não existe centro. É um sistema completamente descentralizado. O que acontece se você cria uma rede onde o acesso livre a serviços financeiros é possível? Onde, pela primeira vez na história, qualquer um pode conectar e criar uma aplicação?

> *"Bitcoin é a internet de dinheiro e a moeda é apenas a primeira aplicação."*

Bitcoin não é moeda. Essa é uma coisa importante de se perceber. A moeda

é uma aplicação que roda na rede *bitcoin*. *Bitcoin* é a internet do dinheiro e moeda é apenas a primeira aplicação. Hoje, existem milhares de empresas criando a próxima aplicação. Essas empresas empregam dezenas de milhares de pessoas na mais vibrante indústria que nós temos visto nas duas últimas décadas. Em 2014, *startups* de *bitcoin* receberão mais de 250 milhões de dólares em investimentos. Isso é notável porque é um crescimento mais rápido que a taxa de investimentos na internet em 1995. Nós estamos à frente da curva. *Bitcoin* está crescendo mais rápido que o Twitter nos seus primeiros três anos. *Bitcoin* está crescendo mais rápido que o Facebook nos seus primeiros anos. A razão para isso é que cada um dos desajustados, estranhos, esquisitões ou programadores de qualquer lugar do mundo pode se conectar ao *bitcoin* sem pedir permissão a ninguém, levar a cabo sua ideia desajustada e criar um novo serviço financeiro. Uma nova aplicação bancária. Um novo aplicativo de compras. Um novo aplicativo para *escrow*. E isso é exatamente o que as pessoas estão fazendo. Elas estão construindo coisas inovadoras, novas, e brilhantes. Coisas que nunca vimos no mundo bancário antes. Coisas que nunca passariam nas reuniões de planejamento do seu banco, porque seriam derrubadas.

> *"Quando você tem estes dois ambientes funcionando lado a lado -- o ambiente bancário, onde tudo requer permissão e o mais certo é que não seja concedida, e um sistema que é completamente aberto, onde inovações acontecem nas periferias sem permissão --, adivinha qual vence. Adivinha onde todas as coisas interessantes acontecem."*

Quando você tem dois ambientes funcionando lado a lado -- o ambiente bancário, onde tudo requer permissão e o mais certo é que não seja concedida, e um sistema que é completamente aberto, onde inovações acontecem nas periferias sem permissão --, adivinha qual vence. Adivinha onde todas as coisas interessantes acontecem. Adivinha onde todas as inovações acontecem? Isso é inovação que serve aos consumidores.

> *"Bitcoin é um sistema optativo. Você escolhe usá-lo. Você escolhe os aplicativos que vai rodar. Você escolhe com que vai interagir. Você escolhe as regras do jogo pelo qual você vai interagir. É por isso que bitcoin vai vencer. Ele entrega as inovações que os consumidores querem e precisam."*

Ninguém está investigando *bitcoin* tentando encontrar uma forma de estar na frente rodando um algoritmo de negociação de alta frequência para poder espremer 3 microcents 4 microsegundos mais rápido que o outro banco gigante que trabalha com algoritmos. Ninguém está tentando achar uma maneira de ludibriar você para usar seu cheque especial, uma inovação que foi estreada por um dos grandes bancos, acho que em 2007. Eles perceberam que com cheque especial, em vez de fazer uma grande transação de empréstimo, eles podem inverter a ordem e rodar muitas transações menores. Você paga uma taxa de 25 dólares por transação para eles e eles podem maximizar seus lucros. Esse é o tipo de inovação em que eles estão focados.

Então, eles inovaram de muitas maneiras para enrolar seus clientes.

Em *bitcoin* ninguém está fazendo esse tipo de inovação. A razão por que esse tipo de inovação não é feita é que em *bitcoin* não se pode forçar alguém a usar uma aplicação. Se você é cliente de um grande banco, trata-se da rede deles, da política deles, você estará usando o cartão de débito deles, jogando as regras deles, e se você não gosta disso, você pode ir para outro banco e descobrirá que todos são iguais. *Bitcoin* é um sistema optativo. Você escolhe usá-lo. Você escolhe os aplicativos que vai rodar. Você escolhe com que vai interagir. Você escolhe as regras do jogo com o qual vai interagir. Se você não gosta de uma aplicação, não a usa. Se você ama uma aplicação, você faz *download* e fala a todos os seus amigos sobre ela. É por isso que *bitcoin* vai vencer. Pois entrega as inovações que os consumidores querem e precisam.

Incluindo 6,5 bilhões de pessoas em uma economia global

Há outra razão pela qual o *bitcoin* vai vencer. Existe um desequilíbrio maciço que a maioria das pessoas aqui desconhece. Cada pessoa aqui nesta sala tem acesso a uma conta bancária sem controle de moeda. Uma conta bancária da qual podem comprar ou vender qualquer moeda do mundo. Uma conta bancária da qual podem transferir dinheiro em qualquer lugar do mundo. Uma conta bancária da qual podem acessar mercados internacionais como a bolsa de Tókio ou da Alemanha. Um mercado pelo qual podem ter acesso a crédito e liquidez. Auto-empréstimos e hipotecas. Uma conta bancária que é poderosa. Esse poder está disponível para cerca de um bilhão de pessoas no planeta. Um bilhão de pessoas que têm acesso a facilidades bancárias de pleno direito, internacionais e de alta liquidez.

Existem ao todo 2 bilhões de pessoas que não têm quaisquer contas bancárias. Existem outras 4 bilhões de pessoas com acesso muito limitado a serviços bancários. Serviços bancários sem moedas internacionais, sem mercado internacional, sem liquidez. *Bitcoin* não é para o um bilhão. *Bitcoin* é para todos os outros 6 e 1/2 bilhões. As pessoas que atualmente são ignoradas pelos bancos internacionais. O que você acha que acontece quando você, de repente, transforma um simples telefone com mensagens de texto, ligado a um painel solar numa área rural da Nigéria, em um terminal bancário? Em um terminal de remessas da Western Union? Em um sistema internacional de originação de empréstimos? Um mercado de ações? Um impulsionador de IPO? No início, nada, mas espere alguns anos.

Nós vimos o que aconteceu com o desenvolvimento da tecnologia de celulares, que se alastrou na África mais rápido que qualquer outra tecnologia na história da humanidade. Nós vemos pequenas vilas, onde não existe água corrente, onde se cozinha com lenha e não há eletricidade - ainda assim, há

um pequeno painel solar no topo da cabana de barro, que não serve para gerar luz, mas para recarregar um telefone celular Nokia 1000. Esse aparelho informa sobre a previsão do tempo, os preços dos grãos no mercado e conecta as pessoas ao mundo. O que acontece se esse telefone se torna um banco? Porque com *bitcoin*, isso é possível. O que acontece se você conecta 6,5 bilhões de pessoas a uma economia global sem quaisquer barreiras de acesso?

> *"O que acontece se você conecta 6 1/2 bilhões de pessoas a uma economia global sem quaisquer barreiras de acesso?"*

Remessas, impactando vidas ao redor do mundo

Bitcoin não é uma moeda. *Bitcoin* é a internet do dinheiro. Enquanto tecnologia, pode trazer inclusão econômica e empoderamento para bilhões de pessoas no mundo. Eu vou dar um exemplo de uma aplicação simples que vai trazer mudanças na vida de mais de um bilhão de pessoas nos próximos cinco a dez anos.

Todos os dias, um imigrante de algum lugar recebe seu salário e fica em fila para transferir 50% de seu pagamento para seu país de origem a fim de alimentar sua família extendida. Aqui nos EUA, 60 milhões de pessoas não têm contas bancárias, mas ainda assim elas recebem seu pagamento e enviam para fora. No total, em todo o mundo, são enviados 550 bilhões de dólares em remessas de países de primeiro mundo. Grande parte desse dinheiro é enviado principalmente para cinco destinos: México, Índia, Filipinas, Indonésia e China. Em alguns desses lugares, as remessas representam mais de 40% da economia local. Sentada sobre esses 550 bilhões estão empresas como a Western Union, que tomam em média 9% de cada uma dessas transações dos bolsos das pessoas mais pobres do mundo.

> *"Imagine o que acontecerá quando um dia um desses imigrantes descobrir que eles podem enviar dinheiro de volta para seu país de origem em bitcoin. Não a uma taxa de 15%, nem 10% ou 5%, mas por 5 centavos." Não uma porcentagem; uma taxa fixa.*

Imagine o que acontecerá quando um dia um desses imigrantes descobrir que eles podem enviar dinheiro de volta para seu país de origem em *bitcoin*. Não a uma taxa de 15%, nem 10% ou 5%, mas por 5 centavos. Não uma porcentagem; uma taxa fixa. O que acontecerá quando eles puderem fazer isso? Eles podem, agora mesmo. Existe uma empresa emergente que faz a manipulação de remessas entre os Estados Unidos e as Filipinas. Eles estão fazendo alguns milhões agora, mas vão começar a crescer. Existem 500 bilhões de dólares estancados atrás desta represa. Quando se é um imigrante e pode mudar seu futuro financeiro por não pagar 9% para enviar dinheiro para casa, imagine o que acontece se todo mês, em vez de enviar 91 dólares para casa, puder enviar 100 dólares. Isso faz diferença. Existe um bilhão de pessoas, agora mesmo, com acesso à internet e recurso de aparelhos que podem usar

bitcoin como um serviço internacional de transferência de valores.

Bitcoin irá mudar o mundo

Resumido, *bitcoin* é a tecnologia mais interessante que eu já vi. Eu comecei a usar a internet em 1989, quando criança. Eu sabia que aquilo ia mudar o mundo antes que a maior parte das pessoas a descobrissem. Eu dizia para todos ao redor de mim: "Nós vamos fazer compras com isso. Nós vamos fazer serviços bancários com isso." As reações das pessoas eram bem previsíveis: "Tá bom, Andreas, vá fazer suas tarefas, limpe seu quarto." Quando eu vi o Linux pela primeira vez, eu disse: "Cara, isso vai mudar os sistemas operacionais para sempre. IBM vai falir." Todos riram de mim. Quando eu vi o primeiro navegador de internet e o primeiro *website*, eu disse: "Todas as empresas na América vão ter um *site* dentro de uma década." Todos riram de mim. Bem, deixe eu lhe dizer uma coisa, eu não sei o que vai acontecer com o *bitcoin*, mas eu sei que a invenção estrutural -- um sistema de dinheiros digitais que não tem bancos, nem governo nem controle central e está disponível para qualquer um usar sem permissão -- vai mudar o mundo.

Obrigado.

REDES BURRAS, INOVAÇÃO E O FESTIVAL DOS "COMMONS"

O'Reilly Radar Summit; São Francisco, California; Janeiro de 2015.

Link do vídeo: https://www.youtube.com/watch?v=x8FCRZoBUCw

No início do vídeo, Andreas agradece O'Reilly por concordar em publicar seu livro, *Mastering bitcoin*, sob uma licença *open-source*. Ele agradece ao público e toda a comunidade que o ajudou a escrever o livro.

Hoje, quero falar sobre redes burras. Eu quero falar sobre redes inteligentes. Eu quero falar sobre o valor do *open-source* quando encontra financiamento. E eu quero falar sobre o festival dos "Commons".

> *"Bitcoin é uma moeda, uma rede, uma tecnologia. E você não pode separar essas coisas."*

Bitcoin é uma moeda. *Bitcoin* é uma rede. *Bitcoin* é uma tecnologia. E você não pode separar essas coisas. Uma rede que por consenso baseia o seu valor em uma moeda não funciona sem a moeda. Você não pode fazer o *blockchain* sem uma moeda valiosa por trás dele, e a moeda não funciona sem a rede. *Bitcoin* é ambos. É a convergência de uma rede consensual e participativa e de uma moeda global, sem fronteiras que é fungível, rápida e segura.

Hoje, quero falar um pouco sobre a rede *bitcoin* e focar em um conceito que tem alguns paralelos com os primórdios da internet.

Redes inteligentes versus redes burras

Bitcoin não é uma rede inteligente. *Bitcoin* é uma rede burra. É realmente uma rede burra. É uma rede de processamento de transações burra. É uma rede burra para verificar uma linguagem de *script* muito simples. Ela não oferece uma gama completa de produtos e serviços financeiros. Não tem automação e incríveis características construídas nela.

> *"Bitcoin é simplesmente uma rede burra, e essa é uma das suas características mais fortes e mais importantes."*

Bitcoin é simplesmente uma rede burra, e essa é uma das suas características mais fortes e mais importantes. Quando você projeta redes, quando você arquiteta o sistema de rede, uma das escolhas mais fundamentais é esta: você

faz uma rede burra que ofereça suporte a dispositivos inteligentes, ou você faz uma rede inteligente que oferece suporte a dispositivos burros?

• A rede inteligente - telefones

A rede de telefone era uma rede muito inteligente. O telefone no final da rede era um dispositivo muito burro. Se você tivesse um telefone de discagem por pulso, essa coisa tinha talvez quatro componentes eletrônicos dentro dela. Era basicamente um interruptor em um fio com um alto-falante ligado a ele. Você conseguia discar se sacudisse o gancho para cima e para baixo suficientemente rápido.

O telefone foi um dispositivo burro; não tinha nenhuma informação de qualquer tipo. Tudo o que a rede de telefone fazia era dentro da rede. Identificador de chamada era um recurso de rede. Chamada em espera era um recurso de rede. E se você quisesse melhorar a experiência, você tinha que atualizar a rede, mas você não precisava atualizar o dispositivo. Isso foi uma decisão de *design* crítico porque, naquela época, havia a crença de que redes inteligentes eram melhores porque você poderia entregar serviços incríveis apenas atualizando a rede para todos.

> *"Como resultado do projeto de rede inteligente, inovação só acontece quando um recurso é necessário para todos os usuários da rede, quando ele é atraente o suficiente para provocar a disrupção da função de toda a rede para atualizá-lo."*

Há uma pequena desvantagem das redes inteligentes. Elas têm que ser atualizadas a partir do seu centro. E isso significa que a inovação ocorre no centro, por parte de um agente, e requer permissão. "Como resultado do projeto de rede inteligente, inovação só acontece quando um recurso é necessário para todos os usuários da rede, quando ele é atraente o suficiente para provocar a disrupção da função de toda a rede para atualizá-lo."

• Internet - a rede burra

A internet é uma rede burra. É burra como uma pedra. Tudo o que ela é capaz de fazer é mover dados do ponto A ao ponto B. Sem conhecer esses dados. Ela não é capaz de dizer a diferença entre uma chamada de *Skype* e uma página da *web*. Não consegue reconhecer se um dispositivo conectado é um computador, um celular, um aspirador de pó, uma geladeira ou um carro. Não sabe se esse dispositivo é poderoso ou não. Se ele pode rodar multimídia ou não. Ela não sabe essas coisas, e não se importa.

> *"Para rodar um aplicativo novo ou inovar em uma rede burra, tudo o que você precisa fazer é adicionar a inovação no periférico. Porque uma rede burra pode suportar dispositivos inteligentes, você não precisa mudar nada na rede."*

Para rodar um aplicativo novo ou inovar em uma rede burra, tudo o que você precisa fazer é adicionar a inovação no periférico. Porque uma rede burra pode suportar dispositivos inteligentes, você não precisa mudar nada na rede. Se você empurrar a inteligência para a periferia da rede, um aplicativo que tem apenas cinco usuários pode ser instalado se aqueles cinco usuários os atualizarem seus dispositivos para essa implementação. A rede burra vai transportar seus dados porque não sabe a diferença e não se importa.

• A rede burra do bitcoin

Bitcoin é uma rede burra suportando dispositivos muito inteligentes, e isso é um conceito incrivelmente poderoso porque *bitcoin* empurra toda a inteligência para os periféricos.

Não importa se o endereço *bitcoin* é o endereço de um multimilionário, de um banco central, de um contrato inteligente, de um dispositivo ou o endereço de um ser humano. A rede não sabe. Não importa se a transação está carregando muito dinheiro ou nem tanto assim. Não importa se o endereço for em Kuala Lumpur ou centro de Nova York. A rede não sabe, a rede não se importa.

A rede move dinheiro de um endereço para outro com base em um simples *script* de bloqueio. E isso significa que se você quer construir uma nova aplicação no topo do *bitcoin*, você pode atualizar os dispositivos e você pode conseguir isso. Você não precisa pedir permissão a ninguém para inovar. Escreva o app, lance-o em seu ponto de rede, e o *bitcoin* irá rodá-lo ali, porque *bitcoin* é uma rede burra.

Esse é o poder de inovação na internet. É a inovação sem permissão. É a inovação sem aprovação central. É a inovação sem uma atualização ampla da rede. E isso significa que o *bitcoin* não é uma rede financeira específica. Não é uma rede financeira para transações grandes ou pequenas, rápidas ou lentas. É para você usá-la como quiser, com base no que você escolher para fazer no seu ponto de rede.

Compare isso com o sistema bancário atual. O atual sistema bancário é construído em torno de redes muito inteligentes, absolutamente e rigidamente controladas para entregar aplicações muito específicas para pontos de rede muito burros. Mesmo no seu banco *on-line* mais sofisticado, tudo o que você consegue fazer é acessar algum HTML que fornece um conjunto de serviços que eles decidiram que iriam lhe dar. Você não tem acesso APIs, não é habilitado a executar aplicativos adicionais, nem atualizar, inovar ou mudar nada, a menos que toda a rede mude para apoiar a sua nova aplicação. O sistema atual tem redes para grandes pagamentos, pequenos pagamentos ou pagamentos rápidos, mas não tudo o que foi dito acima

sobre *bitcoin*. *Bitcoin* é todas essas coisas porque não discrimina, é neutro, não se importa, é burro.

> *"O sistema atual tem redes para grandes pagamentos, pequenos pagamentos ou pagamentos rápidos, mas não tudo o que foi dito acima sobre bitcoin. Bitcoin é todas essas coisas porque não discrimina, é neutro, não se importa, é burro."*

O poder de se empurrar a inteligência para a periferia, de não tomar decisões no centro, move a inovação para as mãos de seus usuários finais e dá a eles capacidade de criar aplicativos que são tão específicos que apenas um punhado de pessoas em todo o mundo precisa deles. E esses usuários podem construir esses aplicativos sem pedir permissão a ninguém.

A tragédia dos "commons"

Mas há mais uma coisa que é realmente única sobre *bitcoin* e é um dos motivos porque a moeda continua a sobreviver e suplantar as redes fechadas e centralizadas do passado, é que o *bitcoin* é uma rede aberta, com código aberto e não possui padronização.

Um dos conceitos-chave em economia é a ideia da tragédia dos "*commons*". Isso ocorre quando você tem um recurso comum que pode ser consumido sem limites por todos. Até que o recurso se esgota e todo o sistema entra em colapso. Trata-se de uma falha de mercado chamada "a tragédia dos *commons*". O exemplo mais famoso disso é o "common", como é chamada, no velho inglês britânico, uma grande área de pasto comunitária. Nesse exemplo existe um campo onde todos podem levar seu gado para pastar, mas se todo mundo resolve levar seu gado de forma irresponsável, em pouco tempo, você tem uma grande poça de lama sem grama nem gado. Porque todos exauriram o pasto, o recurso é esgotado.

Festival dos "commons"

Bitcoin não sofre da tragédia dos "*commons*" como ocorre com muitas redes financeiras, onde não se pode inovar na rede de outra pessoa. Quando a Visa inova, só ela ganha. Quando a MasterCard inova, só a Martercard ganha. Se um recurso é implantado na SWIFT, isso não parte do consumidor. Se o Bank of America faz algo novo e chique, eles fazem isso para competir e excluir todos os outros bancos que não implementaram o recurso.

Bitcoin é um recurso comum cujo uso aumenta o valor desse recurso, sem excluir de ninguém. Se uma empresa cria um novo recurso que pode ser usado em *bitcoin* sob uma licença *open-source*, esse recurso então pode ser usado por todos no ecossistema. Isso significa que a inovação enriquece todos na rede. Se uma empresa investe dinheiro no protocolo *bitcoin*, ela se benefi-

cia, mas também todos os outros na rede. Quando eles apostam na esfera *bitcoin*, eles beneficiam os investimentos de todos os outros neste espaço. Então, isso retorna várias vezes. Você participa dessa sinergia maravilhosa onde cada empresa que investe nesta incrível tecnologia a torna melhor para todo mundo. Não é um princípio de exclusão; em vez de uma tragédia dos "*commons*", temos um festival dos "*commons*". Algo que fica melhor quando mais empresas o usam.

> *"Não é um princípio de exclusão; em vez de uma tragédia dos commons, temos um festival dos "commons". Algo que fica melhor quando mais empresas o usam."*

- **Festival dos commons 2012-2014**

Basta olhar para alguns dos exemplos. O ano de 2014 foi supostamente o pior em *bitcoin*. Mas isso é apenas se você está focado no preço, porque em 2014, vimos a implantação de duas tecnologias incríveis. A primeira é a multi-assinatura *(multisig)*, que requereu uma pequena mudança no protocolo do núcleo, mas em seguida permitiu uma enorme quantidade de serviços e produtos a serem construídos na periferia. A segunda foi a tecnologia das carteiras hierárquicas determinísticas, o que não exigiu qualquer alteração no núcleo e nos permitiu ter essas experiências incrivelmente complexas e ricas no espaço das carteiras.

As empresas que inventaram e implantaram essas duas inovações, o fizeram em 2012, e hoje colhemos os benefícios. Todo um ecossistema de novos produtos e serviços tem sido construído a partir dessas duas invenções. O valor investido por uma empresa explode e cria uma gama inteira de produtos em uma nova indústria, dois anos mais tarde.

Em 2014, durante o pior ano da *bitcoin*, 500 *startups* receberam 500 milhões de dólares em investimentos, gerando dezenas de milhares de empregos, e nenhuma das inovações criadas geraram retorno, porque elas mal começaram. Todos os incríveis avanços da tecnologia que vimos em 2014 cresceram a partir de invenções criadas em 2012. Agora, o que acontece quando você joga 500 empresas e 10.000 desenvolvedores para resolver o problema? Dê-nos dois anos, e veremos algumas coisas espantosas em *bitcoin*. E essa é a vantagem do festival dos comuns.

Acelerando a inovação

Enquanto os jornalistas estão escrevendo mais um obituário para *bitcoin*, vejo um ecossistema de possibilidades. Vejo um ecossistema que está gerando empregos em uma economia que está quase morta. Vejo um ecossistema que tem algumas das pessoas mais inteligentes que já conheci criando as inovações mais surpreendentes. E o mais incrível é que nós todos nos beneficia-

mos com tudo isso. Realmente não estamos competindo uns contra os outros. Estamos participando do Festival dos recursos comuns, e como resultado, nós estamos vendo uma taxa de inovação que está acelerando. Já está a uma velocidade vertiginosa, e está acelerando.

Pegue um ecossistema aberto, descentralizado, com um festival de recursos comuns - código aberto, livre de padrões, rede aberta - e a inteligência e inovação empurrada para a periferia, assim os usuários têm controle sobre o que inovar e como eles investem seu tempo, dinheiro e espírito nesta tecnologia. Coloque isso contra um sistema fechado, controlado por um provedor central, no qual é necessário permissão para inovar e onde só há inovação mediante exclusão e concorrência frente a todas as outras empresas. Vamos esmagá-los.

As pessoas me perguntam: "Bem, o que aconteceria se Goldman Sachs construísse uma GoldmanSachsCoin?". Eu digo, deixem que ele o faça. Se a criação for realmente aberta e descentralizada, só provará o objetivo principal disso e nós podemos todos ir para casa, declarando vitória. Se ela for fechada e não permitir uma inovação aberta, ela se tornará estagnada em apenas alguns meses enquanto continuamos acelerando com mais e mais inovação e alimentando-nos das invenções uns dos outros.

Não é possível parar isso. É por isso que eu estou tão animado em estar no espaço *bitcoin*: uma rede burra que coloca toda a inteligência e inovação nas periferias para que nós possamos inovar sem pedir permissão a ninguém, e possamos participar deste festival incrível de recursos comuns.

Obrigado.

INVERSÃO DE INFRAESTRUTURA

Encontro Bitcoin de Zurique, Zurique; Suiça; Março de 2016

Link para o vídeo: https://www.youtube.com/watch?v=5ca70mCCf2M

Hoje, eu gostaria de falar sobre um conceito que eu gosto de chamar de "inversão de infraestrutura". Eu vou falar sobre como as coisas mudam quando uma nova tecnologia deve primeiro usar a infraestrutura antiga e como isso cria um conflito, pressão que pode levar a uma inversão de infraestrutura.

Novas tecnologias, cavalgando sobre velhas estruturas

Bitcoin é novo. *Bitcoin* é diferente. Quando uso o termo *bitcoin* aqui estou falando de maneira ampla. O que estou falando é de plataformas descentralizadas centradas em redes. Essas plataformas podem ser utilizadas para moeda, pagamentos ou outras aplicações de confiança. A plataforma poderia ser *bitcoin* ou outra coisa diferente. Para essa conversa, usarei o termo *bitcoin* para cobrir toda uma categoria de coisas que estão sendo criadas. É novidade e estamos tentando espremê-la sobre o atual sistema bancário. O resultado é uma bagunça.

Não somente é uma bagunça, como é uma oportunidade para os que apoiam o sistema financeiro tradicional de dizer: "Viu, não funciona. É devagar. Isso não funciona muito bem." Isso não é novidade. Este é um fenômeno que acontece cada vez que você tem uma tecnologia que é disruptiva, nos seus primeiros anos de adoção ela precisa ser carregada pela tecnologia que será disruptada por ela.

> *"Cada vez que você tem uma nova tecnologia que é disruptiva, nos seus primeiros anos de adoção ela precisa ser carregada pela tecnologia existente que será disruptada por ela."*

Vamos dar uma olhada histórica em como essas coisas se desenrolam. Quando você lê sobre uma tecnologia disruptiva 20, 30, 40 anos no futuro, é sempre muito suave. É óbvio porque visto de agora tudo parece mais claro. Por exemplo, automóveis foram uma grande invenção. E é claro que quando os automóveis foram inventados todos disseram "Yay! Nós não precisamos mais dos cavalos!" Correto? Não foi exatamente o que aconteceu. Em vez disso, eles disseram "Isso é loucura. Essas máquinas barulhentas e desconfortáveis irão provavelmente matar nós todos, elas nunca funcionarão. E por que alguém, além das estúpidas pessoas ricas brincando com seus brinquedos barulhentos, irá querer que usemos essas máquinas horríveis quando nós

temos cavalos perfeitamente bons?"

Isso é o que acontece realmente pela história quando são apresentadas tecnologias disruptivas. Você encontra resistência. Resistência é a primeira reação. Os que têm sucesso são os que continuam - mesmo que o restante da sociedade diga que são loucos - perseguindo uma ideia louca: automóveis, eletricidade, internet, *bitcoin*. Esses loucos pioneiros, que foram caçoados por todos os outros na sociedade por suas ideias loucas, persistiram até que todos pudessem ver que o que estavam fazendo estava correto.

• Infraestrutura para cavalos

Olhando para essa história, uma das coisas realmente interessantes para mim é que, no início, a tecnologia disruptiva deve viver em um mundo criado para a tecnologia que está substituindo. Quando você dirige seu novo automóvel em uma cidade, você está andando em estradas usadas por cavalos com infraestrutura projetada e usada para cavalos. Não há sinais luminosos. Não existem regras de trânsito. Não existem estradas pavimentadas.

> *"Você está numa sociedade de cavalos e você é o maluco conduzindo um desses veículos sem cavalos."*

Há algumas coisas sobre cavalos que os carros não têm. Esses carros antigos possuíam tração apenas nas rodas dianteiras. Então, apenas duas rodas girando. Os cavalos são veículos de quatro patas de tração, o que lhes dá muita flexibilidade. Eles também têm o equilíbrio. Você tinha uma estrada que foi projetada para cavalos e não foi pavimentada. Algumas delas tinham paralelepípedos, mas a grande maioria das estradas não era pavimentada. Elas também não eram secas. Elas eram geralmente cobertas de lama e cocô de cavalo (porque é isso que os cavalos fazem). Esse é o ambiente no qual o automóvel teve que se impor na prática. Não começou com "Sim, ótimo, inventamos um automóvel agora. Permitam-me demonstrar as suas capacidades na autoestrada." Em vez disso, as pessoas ricas e loucas que estavam experimentando essa tecnologia estavam dirigindo seus carros em estradas com buracos profundos, onde os cavalos tinham passado. Em estradas não projetadas para automóveis, na lama. O que aconteceu? Os carros ficavam presos porque não tinham equilíbrio nem quatro patas.

Os críticos disseram: "Ah, nós avisamos que isso nunca iria funcionar. Olhem para vocês. Você não consegue sequer sair da lama."

Além disso, onde você vai pegar gasolina? Existe apenas um posto de gasolina. O que acontece se você ficar sem gasolina antes de chegar lá? Significa que se seu cavalo tiver fome, você poderá pelo menos andar mais algumas milhas, mas se sua nova ideia maluca de carro ficar sem gasolina, aí acabou,

você está preso. Você já estava preso por causa da lama, mas agora você está realmente preso porque ficou sem gasolina. Isso nunca vai funcionar."

• De cavalos para veículos

Muitas vezes, a nova tecnologia deve primeiro usar a infraestrutura da tecnologia que no fim das contas irá substituir. No início, os automóveis tinham que usar estradas projetadas para cavalos. Por fim, começamos a pavimentar estradas. Então, algo realmente interessante aconteceu. Quando você pavimenta as estradas e torna-as adequadas para os veículos, a antiga tecnologia (cavalos) ainda pode usá-las. Se você quer fazer um agradável passeio a cavalo por Zurique, tenho a certeza de que o cavalo seria perfeitamente confortável. Os cavalos são muito confortáveis no asfalto, como *skates, Segways*, motocicletas e bicicletas -- tecnologias que não existiam. Na verdade, para que essas tecnologias existissem, você primeiro teve que construir a infraestrutura para automóveis.

As estradas planas e pavimentadas não só permitem que o automóvel exista, permitem que o cavalo exista confortavelmente, mas também abrem portas para novas tecnologias. Agora, você tem pessoas que andam em *Segways*, *scooters*, *skates*, patins, empurrando carrinhos de bebê e todas as outras coisas que estão se movendo em nossas ruas.

Isso é uma inversão de infraestrutura. Você começa com a nova tecnologia vivendo na infraestrutura da velha e, então, ela muda. Você constrói infraestrutura e a velha infraestrutura também utiliza a infraestrutura projetada para a nova tecnologia.

> *"Isso é uma inversão de infraestrutura. Você começa com a nova tecnologia vivendo na velha infraestrutura e, então, uma substitui a outra."*

Vamos ver mais exemplos.

• Infraestrutura para gás natural

Uma das grandes coisas sobre a história é que algumas das proclamações mais certas são muitas vezes ridicularizadas por séculos, porque são tão ridículas. Por exemplo, quando a eletrificação foi introduzida durante a Feira Mundial em Paris, o prefeito de Paris na época disse: "A eletricidade é uma moda e, assim que fecharmos a feira e derrubarmos a Torre Eiffel, a eletricidade desaparecerá na história". Errado por duas razões.

A Torre Eiffel está ainda de pé e a eletricidade ganhou.

Mas pense no momento em que a eletricidade estava apenas começando: não havia infraestrutura. Então, como exatamente você coloca eletricidade

em uma casa? Em primeiro lugar, o único motivo para colocar eletricidade na casa é porque você é uma dessas pessoas ricas e loucas. Provavelmente uma das mesmas pessoas que comprou um automóvel. Agora você está basicamente colocando raios em suas paredes, o que certamente é uma ideia maluca que resultará em sua casa queimando. Isso foi o que os jornais escreveram. Eles escreveram sobre todas as casas que incendiaram e como essas pessoas malucas estavam colocando eletricidade em suas casas.

O que era a infraestrutura na época? Naquela época, a maior parte da infraestrutura foi projetada para fornecer gás. Na verdade, a iluminação a gás nas principais cidades era bastante comum. Havia tubulações que poderiam fornecer gás principalmente para luzes de rua, mas também para luzes domésticas, bem como para aquecimento. Você não poderia usar essa infraestrutura para a eletricidade. Você não poderia usá-la para distribuir a eletricidade para as casas.

No início, o único uso da eletricidade era realmente para as fábricas, porque é aí que se poderia tirar o máximo proveito da eletricidade. Antes da eletricidade, uma fábrica podia ter um grande motor a gás parado no canto da fábrica. O motor distribuía energia através de uma série de correias e polias espalhadas em toda a fábrica para rodar todos os outros equipamentos. Era basicamente uma turbina a gás, que permitiu distribuir a eletricidade diretamente para todos os equipamentos e utilizar motores elétricos.

Obviamente, as fábricas podem se beneficiar da eletricidade, mas por que colocá-la em sua casa? Por que você usaria eletricidade já que você tinha luz e aquecimento a gás que funcionavam bem? E não havia infraestrutura. A infraestrutura para o gás não era útil para a eletricidade. Se você quisesse, você teria que construir novas infraestruturas.

Então, vemos o outro aspecto dessa inversão de infraestrutura, que é a daqueles investidos no *status quo* que apontam para seus novos projetos elétricos e dizem: "Não existe uma rede de distribuição suficientemente grande para criar clientes. E não há clientes suficientes para demandar uma rede de distribuição. Isso nunca vai acontecer." Foi exatamente o que disseram sobre carros. Eles disseram: "Não existem postos de gasolina suficientes para abastecer seus carros e não há clientes o bastante para demandar postos de gasolina. Isso nunca vai acontecer."

• Do gás natural à eletricidade

Então, a eletrificação começa a acontecer e as pessoas descobrem que uma vez que você estabelece uma infraestrutura da eletricidade, você pode usá-la não só para desenvolver as possibilidades da eletricidade, mas também para desenvolver aplicações antigas. Você pode fazer luz e aquecimento e pode

fazê-lo mais eficientemente, em alguns casos, com a eletricidade. Mas agora, você pode fazer coisas novas. Você pode fazer ventiladores, ar condicionados, pode fazer motores, misturadores e secadores de cabelo e, de um modo geral, as casas não pegam fogo por causa da eletricidade com frequência.

Novamente, vemos a inversão de infraestrutura. Nos primeiros anos, você tem que operar na infraestrutura antiga. É quase impossível. Teoricamente você pode ligar um gerador de gás em sua casa e alimentá-lo com gás e gerar eletricidade localmente, mas isso não era muito eficiente. Em seguida, você constrói a infraestrutura para a nova tecnologia, e essa infraestrutura acomoda a tecnologia antiga com bastante conforto - iluminação, aquecimento ou cavalos, no caso das estradas. Mas também abre as portas para novas aplicações que você não podia desenvolver antes. E o mundo muda.

> *"Alterar a infraestrutura abre as portas para novas aplicações que você não poderia desenvolver antes. E o mundo muda."*

• Infraestrutura para vozes humanas

Meu terceiro exemplo é um pouco mais técnico. É aqui que você verá o público separado entre aqueles com mais de 35 anos e aqueles com menos de 35 anos. Diga-me se você pode reconhecer este som.

Andreas replica o som de um modem dial-up.

Pessoas com menos de 35 anos estão me olhando como eu se eu fosse um louco, e as pessoas com mais de 35 anos dizem: "Isso é um modem. Eu tinha um desses!" É assim que nos conectávamos à internet. Perdoem-me enquanto entramos na história antiga. Um modem é um modulador-demodulador. É um dispositivo que emite dados através de uma linha telefônica. É o seguinte: se você pensar sobre isso, a linha telefônica é como uma estrada de terra e você está tentando dirigir um carro por ela.

Uma linha de telefone é um sistema projetado para transportar a voz humana. Quando eu era adolescente, as linhas telefônicas ainda eram analógicas e tínhamos sistemas de discagem por pulso. Costumamos, às vezes, tentar tocar música para nossos amigos pela linha telefônica. Se você já tentou isso, você descobriu que realmente não funcionava. A razão pela qual não funcionava é porque as frequências permitidas por uma linha telefônica são muito estreitas.

Veja, a rede telefônica é projetada para fazer uma coisa e apenas uma coisa. É altamente especializada, assim como a rede de gás, que entrega gás para as casas, é projetada apenas para fornecer gás. Não água, eletricidade ou óleo. Apenas gás, e é especializada. O sistema telefônico foi projetado para fornecer apenas voz, e a voz humana é muito precisa. Nossa frequência

principal é 1 *kilohertz*; ficamos perto desse intervalo, às vezes indo um pouco acima e um pouco abaixo. Existem algumas poucas pessoas que podem ir um pouco além de um alcance comum. Adolescentes podem alcançar frequências que não consigo nem ouvir mais. Mas, devido ao uso especializado da voz e às dificuldades de transmitir vozes, especialmente em grandes distâncias, os engenheiros reduziram o alcance aceitável. Se você permitir uma gama completa, você obtém voz, mas você também recebe ruídos estáticos, interferências elétricas em altas frequências. Você também tem barulhos estranhos, interferência elétrica de motores em frequências muito baixas. O que acontece se sua linha telefônica tem ruídos estáticos e ruídos estranhos? Você adiciona um filtro que corta as baixas e outro filtro que corta as altas. Agora, a conexão é mais limpa, mas a voz humana começa a parecer mais estranha porque está sendo comprimida.

Esta estrada comprimida é uma estrada muito difícil de transportar dados porque, quando você está transmitindo dados, você precisa obter muita informação em uma faixa de frequência muito estreita. O som de apito que você ouve com o modem é, na verdade, dois modems tentando testar a faixa de frequência disponível nessa conexão específica. Todos esses ruídos são os modems dizendo, em diferentes frequências: "Você pode me ouvir agora?". E o outro dizendo "Eu ouvi você. Você pode me ouvir?". Indo e voltando até que o intervalo disponível seja estabelecido.

Essa é uma maneira insana de se fazer transmissão de dados. Basicamente você tem dois dispositivos que estão cantando um para o outro através de um canal muito estreito, tentando de alguma forma comprimir a maior quantidade de dados possível através de um canudo pequeno e estreito. Então, nós os atualizamos e eles ficam melhores e melhores em fazer isso.

As empresas de telefonia detestaram: "Não foi para isso que projetamos as redes. Esta é uma rede de comunicação de voz pura e de ponta. Que diabos vocês estão fazendo?". Na verdade, no país onde cresci - em Atenas, na Grécia -, se você tentasse fazer uma chamada de longa distância com o modem, o que você ouviria seria o início de uma conexão de modem e em seguida um clique abrupto. O quê? O que aconteceu? Eles cortavam as linhas se detectassem um modem. Por quê? Porque estava competindo com a companhia telefônica. Como os bancos, fechando contas de empresas *bitcoin*. Ou, basicamente, exatamente o mesmo.

O que eles disseram na época? Eles disseram: "Poderíamos implementar conexões de dados - fibra, cabos coaxiais, conexões de dados diretos em banda larga. Mas antes de tudo, ninguém precisa de banda larga, porque o que eles farão? Transmitir voz? Já temos uma rede de voz. É fantástico. Não precisamos dessas coisas novas. Em segundo lugar, você não tem usuários suficientes para implantar o cabo coaxial. E você não tem cabo coaxial sufi-

ciente para criar uma base de usuários. Isso nunca acontecerá." Exatamente a mesma ideia.

• Da voz aos dados

Então, tivemos um dos exemplos mais espetaculares da inversão de infraestrutura que eu já vi e que me lembro da história. Quando, primeiro, a internet não era desejada e carregava as linhas telefônicas relutantemente. Depois, a internet foi transportada por linhas telefônicas por empresas de telefonia que se tornaram provedores de serviços da internet. Em seguida, gradualmente, a sua espinha dorsal passou a ser orientada para dados. Então, toda a sua rede torna-se digital. Então, toda a sua rede começa a funcionar pela internet. Logo, eles começam a executar todas as suas linhas telefônicas sobre a internet. Hoje, todos os telefonemas que você faz em qualquer parte do mundo são transmitidos pela internet, com poucas exceções nas periferias em alguns países em desenvolvimento. Uma inversão completa da infraestrutura.

> *"Hoje, todos os telefonemas que você faz em qualquer parte do mundo são transmitidos pela internet, com poucas exceções nas periferias em alguns países em desenvolvimento. Uma inversão completa da infraestrutura."*

Acontece que é muito difícil transferir dados através de uma linha de telefone limitada projetada para voz, mas se você inverter a equação, colocar a voz sobre uma conexão de dados, é insignificantemente fácil. Qual é a diferença? Um é extremamente especializado. Já escolheu o aplicativo para você. O aplicativo é voz; os dados são a exceção que você está tentando comprimir. O outro é muito genérico. Os dados significam alguma coisa, e a voz é apenas uma das aplicações realizadas confortavelmente.

Eu acho que a ironia final para as empresas de telefonia é algo especial chamado "geração de ruído de conforto". Se você é engenheiro de comunicações, você sabe do que estou falando. Isso é a coisa mais irônica do mundo. Depois de anos e anos, pessoas de minha idade, acostumadas à sua linha telefônica estática o tempo todo, começam a ter telefonia celular e linhas telefônicas digitais perfeitas, elas não apresentam ruído. No momento em que a outra pessoa parasse de falar, o que você teria era o silêncio completo. Então, foi como "Oh, ok, acho que desligaram."

Eles não tinham desligado. Eles ainda estavam lá. Não havia nada de estática. Então, as empresas de telefonia inventaram a tecnologia mais brilhante existente, que é a geração de ruído de conforto. Este é um dispositivo que fica no outro extremo do seu telefone e parece ver se a conexão ainda está aberta e, se estiver, sussurra estática em seu ouvido apenas para fazer você se sentir tranquilo que a outra pessoa ainda está lá. Na verdade, ele gera ruído

de alta frequência de propósito, artificialmente na sua ponta - ruído que não está no sistema, apenas para que você não pense que a outra pessoa desligou.

As mesmas empresas que disseram "Nunca seremos capazes de fazer voz de qualidade pela internet. Não queremos a internet em nossas linhas telefônicas", agora estão injetando ruído para simular o terrível desempenho da rede anterior porque estamos oferecendo qualidade de CD ou um melhor som em todos os continentes. Uma inversão completa da infraestrutura.

Do sistema bancário para bitcoin

Agora, temos o *bitcoin*. Temos uma plataforma de confiança descentralizada que pode fazer a liquidação de transações em nível mundial, sem intermediários. Mas, ainda estamos vivendo no velho sistema. Hoje, temos que usar câmbios vinculados a contas bancárias tradicionais, ou usar transferências bancárias IBAN ou cartões de crédito. Hoje, dirigimos o automóvel ao longo das estradas enlameadas do sistema bancário. O supercarro *bitcoin*, o Fórmula 1 das finanças, está andando nas estradas enlameadas de 1970 do sistema bancário, baseado no *mainframe* da década de 1970, e é uma estrada esburacada.

> *"O supercarro bitcoin, o Fórmula 1 das finanças, está andando nas estradas enlameadas de 1970 do sistema bancário, baseado no mainframe da década de 1970, e é uma estrada esburacada."*

Os bancos apontam para isso e dizem: "Não funciona. Olha, você tem que seguir toda a regulamentação que nós temos de seguir. Você tem que fazer toda a identificação que nós temos que fazer. Você tem que diminuir tudo até a velocidade do sistema bancário tradicional. Isso nunca vai funcionar. Não apenas isso, mas você não tem usuários suficientes para criar infraestrutura, e você não possui infraestrutura suficiente para atrair novos usuários. Então, isso claramente nunca vai funcionar.".

Mas o que temos, como a eletricidade e o automóvel e a internet, é uma nova tecnologia com uma promessa em seu interior de mil outras aplicações que eles ainda nem imaginaram.

Prevejo que, nos próximos 15 a 20 anos, veremos uma grande inversão de infraestrutura acontecer nas finanças. Primeiro, os bancos resistirão. Então, os bancos adotarão. Os bancos executarão seus sistemas ao lado dos sistemas de *blockchain* e *bitcoin* e, finalmente, eles executarão todos os sistemas bancários tradicionais como uma aplicação no topo de um livro-razão descentralizado de confiança. Porque, embora seja muito difícil de fazer um livro-razão descentralizado de confiança que esteja ligado a todos esses sistemas bancários antigos, simular um sistema bancário antigo em cima de um livro-razão descentralizado, em cima do *bitcoin*,

um *blockchain* global aberto, é trivial. Tudo o que você precisa fazer é usar todas as suas capacidades e desacelerá-las. Por exemplo, eu posso criar um aplicativo que faz sua transação de *bitcoins* e a liquida em três a cinco dias úteis por um custo de 5 dólares. Eu implementei o sistema bancário tradicional. É como uma geração de ruído de conforto.

> *"Nos próximos 15 a 20 anos, veremos uma grande inversão de infraestrutura acontecer nas finanças."*

Para aqueles dentre nós tão acostumados com o sistema bancário de uma geração anterior que diz "Eu não gosto desse financiamento rápido. Me sinto desconfortável. Eu quero sentar na mesa da minha cozinha todos os domingos e conferir meu talão de cheques e certificar-me de que nenhum dos meus cheques tenha voltado. Eu não gosto dessa transferência eletrônica instantânea global. Isso me assusta", nós podemos desacelerá-lo.

Essa inversão de infraestrutura nos permitirá rodar aplicações de sistemas bancários tradicionais confortavelmente sobre um livro-razão global distribuído - um *blockchain* aberto como o *bitcoin*, o *blockchain* aberto, provavelmente o *bitcoin* abriu o *blockchain* e, simultaneamente, abriu a porta para outras aplicações, para aplicações que nunca vimos antes. Essas novas aplicações terão uma aparência diferente do sistema bancário tradicional. Tão diferente quanto um *Segway* ou um *skate* parece para aqueles que estão comprometidos com carruagens tradicionais. Tão diferente quanto a mudança para a eletricidade em uma era de iluminação a gás em casas vitorianas tradicionais. Tão estranho quanto o ruído de conforto na comunicação de voz de dados de alta qualidade pela internet, que é capaz de muito mais.

Habilitar o futuro no seu sistema antigo é muito difícil. Enquanto você está tentando fazer isso, todos estão apontando para o futuro e dizendo: "Olhe. Isso não funciona.". Uma vez que você reverteu a infraestrutura, a simulação do passado na rede do futuro torna-se extremamente fácil.

> *"Uma vez que você reverteu a infraestrutura, a simulação do passado na rede do futuro torna-se extremamente fácil."*

Agora nós fazemos parte dos estágios iniciais à medida que olhamos para o futuro do dinheiro e os primeiros estágios da maior inversão de infraestrutura que o mundo já viu.

Obrigado.

A MOEDA COMO UMA LINGUAGEM

Bitcoin Expo 2014 - Principal Palestrante; Toronto, Ontário, Canadá; Abril de 2014

Link para o vídeo: https://www.youtube.com/watch?v=jw28y81s7Wo

Isso será mais como uma palestra filosófica sobre o futuro das criptomoedas e o que eu aprendi aqui neste evento. Este evento é chamado de *Bitcoin* Expo 2014. Ele poderia ter sido chamado de *Bitcoin* and *Ethereum* Expo 2014. Não sei se você reparou, mas o *Ethereum* teve uma presença um tanto quanto forte aqui. Surge uma pergunta interessante, na realidade um número significante de pessoas me perguntou: "O *Ethereum* ameaça o futuro do *bitcoin*? Ele rouba um pouco da sua força?". Essas são perguntas que eu ouvi muitas vezes, ouvi também pessoas se referindo a essa questão ao tentar entender as *altcoins* -- imaginando se as *altcoins* ameaçam a dominância do *bitcoin*, se elas enfraquecem o *bitcoin*, se o valor da rede passa a ser demasiadamente distribuído.

Nascido na moeda

Eu venho pensando sobre esta questão por um bom tempo. Fundamentalmente, é uma questão que evoca o velho paradigma das moedas. Todos crescemos em um mundo onde as moedas são impostas a nós de forma monopolista, onde as moedas são definidas estritamente pela localização geográfica em que ocorrem, e onde a escolha da moeda não é sua. É um acidente de nascimento, como muitas outras coisas em nossas vidas. Em um acidente de nascimento, nasci em uma família de classe média alta na Grécia, acompanhado de uma loteria de privilégios na minha vida. Eu também adquiri o dracma. Eu não escolhi o dracma, assim como não escolhi ser um homem branco, assim como não escolhi nascer em uma família de pessoas instruídas. Essas coisas simplesmente aconteceram comigo.

> *"A moeda é um objeto da nação. Ela nos impõe uma certa restrição. Não escolhemos nossa moeda; ela nos escolhe."*

Moeda, da forma como a entendemos, é um artefato do estado-nação. Ela nos impõe certas restrições. Não escolhemos nossa moeda; ela nos escolhe. Somos obrigados a usar essa moeda em todas as nossas interações. Não temos escolha -- isso mudou em 2008. Agora vivemos em um mundo um pouco diferente, mas muitos dos antigos paradigmas ainda habitam

nossos pensamentos.

Em um mundo onde a moeda é um objeto monopolista da nação restrito pela geografia, é um jogo de soma zero. A moeda é a bandeira, é a nação. É a expressão do valor econômico do seu Estado. Ele define suas interações num mundo de geopolítica, em uma luta global pela dominação entre nações. Não cabe escolha individual. Não tem nada a ver com o indivíduo, exceto o indivíduo cujo rosto estampa a moeda corrente -- até recentemente, aqui no Canadá, este rosto era o de uma senhora branca chamada Elizabeth.

A moeda como meio de expressão

Agora, vivemos em um novo mundo, um mundo onde a moeda é uma escolha, não apenas em termos de uso. Não é só uma questão de ser capaz de escolher qual moeda usamos como indivíduos. É também, uma forma de expressão. Qualquer um de nós pode, agora, criar uma moeda usando um simples formulário na internet.

> *"Agora, vivemos em um novo mundo, um mundo onde a moeda é uma escolha, não apenas em termos de uso... É também uma forma de expressão."*

Enquanto pensava sobre a evolução das *altcoins*, como são chamadas, eu percebi que estava fazendo as perguntas erradas. Quantas moedas vão existir? Quantas *altcoins* vão existir? De que forma as *altcoins* competirão no mundo das criptomoedas enquanto caminhamos para o futuro? Haverá centenas de *altcoins*? Se existirem centenas de *altcoins*, o que isso significará para o valor de cada uma individualmente? Como elas competem? Essa é a forma errada de pesar sobre essa questão. Eu via as moedas como um jogo de soma zero, tal como tinha sido imposto sobre a minha visão de mundo pelas nações que as criaram. Então, comecei a pensar a moeda como uma aplicação. Em seguida, passei a pensar a moeda como uma forma de expressão.

Veja, o dinheiro, no fundo, é uma linguagem. É uma linguagem que usamos para expressar valor uns aos outros. Quando eu te dou uma nota de um dólar, estou dizendo que quero entregar-lhe o valor equivalente a essa nota. Estou comunicando minha vontade de trocar esse valor com você, porque eu valorizo algo que você faz ou algo que você pode me dar. Estou usando o dinheiro como um símbolo de linguagem.

> *"O dinheiro, no fundo, é uma linguagem. É uma linguagem que usamos para expressar valor uns aos outros. Quando eu te dou uma nota de um dólar, estou dizendo que quero entregar-lhe o valor equivalente a essa nota. Estou comunicando a minha vontade de trocar esse valor com você."*

• Inventando moedas no playground

Isso acontece nas sociedades humanas onde existem moedas formais ou não. Se você não tem uma moeda com um rosto estampado nela, você a inventa. Uma das coisas que realmente me cativou foi entender que se você tem um ambiente de escola primária e observa as crianças em seu hábitat natural (um hábitat não muito natural na maioria das escolas), para as crianças pequenas não existe moeda, e elas não entendem o conceito de moeda.

Mas elas inventam moedas. Elas começam a negociar. Elásticos, cartas de Pokemon, Tamagotchis, 'gestos' de afeto, 'gestos' de popularidade. Seres humanos criam as moedas como um meio de expressar seus desejos, de expressar sua individualidade. Eu pensei, o que aconteceria se uma criança de 5 anos numa escola primária pudesse usar um *website* para criar a "Joãocoin" e competir contra a "Mariacoin" em um jogo de popularidade dentro da escola?

Em seguida, ocorreu-me que perguntar "quantas moedas existirão?" é equivalente a perguntar "quantos de nós se tornarão blogueiros na internet?". A resposta é simples: todos nós.

A moeda, agora, é um meio de expressão. Mas se todo mundo pode criar uma moeda, como quantificar o seu valor e o que isso significa? Qual é a diferença entre a moeda como uma forma de expressar popularidade, como a expressão de um desejo, de um meme, de um modismo, de uma marca? Lá, agora – *Andreas aponta para fora do auditório* –, um concurso de ídolos adolescentes canadense está acontecendo. Um dos competidores, Amir, tem um grupo grande de fãs. Talvez, Amir queira criar o "Amircoin" para que seus fãs possam expressar a vontade de assistir mais à sua dança. Por que não? As pessoas falaram sobre eu estar fazendo o "Andreascoin". Eu acho que é um pouco bobo. Mas, por que não? Eu acho que em algum momento veremos coisas como esta acontecerem.

Não teremos centenas de *altcoins*. Não teremos milhares de *altcoins*. Teremos centenas de milhares, milhões de *altcoins*. Em seguida, haverá milhares de *altcoins* sendo criadas todos os dias para organizar comunidades locais, para expressar modismos, para criar competições de popularidade, para codificar o mais recente meme da internet.

> *"Não teremos centenas de altcoins. Não teremos milhares de altcoins. Teremos centenas de milhares, e depois milhões de altcoins."*

Autoridade por produção

Com tantas *altcoins*, como saber quais possuem valor e quais não? Para tentar responder a esse tipo de pergunta eu, frequentemente, reflito sobre o

surgimento do primeiro sistema descentralizado que eu conheci, a internet. O que ele fez para a compreensão de informações, escassez de informação, opinião e autoridade da opinião. O que ele fez para nós, como sociedade, enquanto a internet emergia no cenário global.

Costumava haver um tempo em que, se você quisesse ler uma opinião confiável, você comprava um pedaço de jornal de uma organização que tinha uma impressora num prédio de três andares de altura e quatro campos de futebol de comprimento e tinha um nome realmente excelente, como The New York Times. Aquela organização poderia comprar tinta por barril e, através da propriedade dessa enorme fábrica, eles tinham o peso da autoridade. Nós atribuímos autoridade a essas instituições, e usávamos essa autoridade para decidir quais opiniões importavam ou não. Nós os usávamos como portadores de autoridade para nos dar orientação na compreensão da opinião.

Então, a internet destruiu tudo isso, de repente qualquer um podia imprimir, qualquer um podia publicar.

Autoridade por mérito

No início, as pessoas perguntavam: "Como saberemos quais opiniões importam se qualquer um pode ter uma opinião?". O mundo irá chegar ao fim, pensaram. Mas uma coisa engraçada aconteceu. Nós mudamos de um mundo em que a autoridade e a opinião vieram do emissor, da autoridade da publicação por representação, num mundo onde devemos considerar a opinião sobre seus próprios méritos, sobre o conteúdo dessa opinião. Nós chegamos em um mundo onde The New York Times imprime balela que envia uma nação inteira para a guerra, e um blogueiro egípcio nas linhas de frente de uma revolução imprime uma verdade que ninguém quer ouvir. De repente, o mundo está de ponta-cabeça. Autoridade não é mais uma pessoa que possui uma imprensa. Agora, a pessoa que tem o conteúdo é o que importa. Nós acabamos de fazer isso com a moeda.

> *"Autoridade não é mais uma pessoa que possui a imprensa. Agora, a pessoa que tem o conteúdo é o que importa."*

Valorizando moedas pelo uso

Agora, a autoridade não é derivada da soberania do emissor, da imprensa de uma nação que pode declarar através do monopólio e uso da força que esta é a moeda que você usará. Agora, nós podemos escolher a moeda, e uma criança de cinco anos pode criar uma moeda. Talvez a moeda que a criança de cinco anos criou tenha valor monetário, talvez não. Provavelmente, não terá. Mas algumas terão. Precisamos nos acostumar com um mundo onde devemos julgar a moeda não por quem a emitiu, mas por quem a usa. Ou melhor,

por quantas pessoas usam e pra que elas usam.

> *"Precisamos nos acostumar com um mundo onde devemos julgar a moeda não por quem a emitiu, mas por quem a usa. Ou melhor, por quantas pessoas usam e pra que elas usam."*

Vamos imaginar um mundo onde a moeda é usada de forma generalizada, e ninguém lembra quem criou a moeda ou o porquê. Eles somente sabem que dentro de suas comunidades locais isso tem um poder aquisitivo. Como um pequeno pensamento ilusório: imagine uma década a partir de hoje, em um vilarejo rural desanexado das nações desenvolvidas, os aldeões trocando duas moedas. Uma tem na frente um Shiba Inu, uma raça de cachorro japonês, e é chamada *Dogecoin*. Eu não tenho certeza de como pronunciar, e isso realmente não importa, mas você pode comprar uma dúzia de ovos com ela. Os outros aldeões estão negociando outra moeda que tem uma velha senhora branca chamada Elizabeth. Eles não têm ideia de quem é Elizabeth. Eles não sabem por que ela colocou sua foto na moeda. Talvez tenha escrito uma bela canção. Talvez tenha vencido o *Teen Idols* do Canadá. Ninguém lembra mais, mas você pode comprar seis ovos com ela.

Para essas pessoas, não importa quem emitiu a moeda; o que importa é se tem poder aquisitivo ou não. A moeda é agora avaliada puramente em sua base monetária, por causa de sua adoção, por causa de seu uso. Existe uma diferença fundamental entre essas duas moedas. Uma tem um suprimento previsível, estável, algorítmico. A outra tem uma velha senhora branca chamada Elizabeth nela. Então, na verdade, uma delas tem algum valor intrínseco porque removeu alguma incerteza do sistema monetário com ela. A outra não necessariamente.

Nós precisamos nos preparar para viver em um mundo onde múltiplas moedas coexistam.

• Múltiplas moedas coexistindo

Moeda como meio de expressão, moeda como ferramenta de linguagem, não é mais sobre o emitente. Cabe a nós como indivíduos fazer a escolha de usar aquela moeda, e nós daremos valor a ela através do nosso uso. Nós daremos valor a ela através da adoção. Nós nos surpreenderíamos por algumas moedas que irão emergir a partir de uma moda, de alguma piada, às vezes até de uma piada de mal gosto, e então explodir em uma consciência viral na internet e depois se tornar real seu poder monetário em uso em toda uma vasta população.

Como nós devemos operar em um mundo desse tipo? O que significaria haver competição entre moedas se existem milhões? O que seria se a escassez digital realmente ocorresse, mas apenas em uma base local e somente no

contexto de cada uma dessas moedas? Se a escassez não fosse derivada pelo emitente, mas fosse derivada em termos de adoção e em termos do símbolo em si?

> *"Moeda como meio de expressão, moeda como ferramenta de linguagem, não é mais sobre o emitente. Cabe a nós como indivíduos fazer a escolha de usar aquela moeda, e nós daremos valor a ela através do nosso uso."*

Nós iremos ter moedas para diferentes usos. Portanto, você já tem o *bitcoin* que provê um tipo muito específico de política monetária. Você tem a *Ethereum* que pode prover uma plataforma de contratos. Existe a *Namecoin* para convenções nominativas distribuídas. Existem muitas outras, e irão existir muitas outras que irão resolver outros problemas: enovelar proteínas, a busca por vida extraterrestre. Talvez nós tenhamos moedas que serão melhores para microtransações e micropagamentos com uma resolução muito rápida. Talvez nós tenhamos moedas que são melhores para grandes transações, como imóveis. Quem sabe. Se você pensa em moeda como um aplicação, então você percebe que isso realmente não importa.

Na internet, o *e-mail* foi o vovô de todos eles. Ou vovó deles. *E-mail*, como *bitcoin*, foi a aplicação matadora que nos permitiu ver o poder das comunicações descentralizadas e adotar essa nova plataforma. Foi o suficiente para criar utilidade para expandir a rede por todo o mundo, mas isso foi só a primeiro aplicação. Depois, mensagens instantâneas, fóruns, quadros de boletim, Facebook, Twitter. Você receia que o Twitter vá destruir o *e-mail*? Você tem medo que o Facebook vá destruir as mensagens instantâneas? Você teme que o valor do *e-mail* seja corroído de alguma maneira pela existência do Twitter? Nós não nos preocupamos com essas coisas porque entendemos que cada um serve a um propósito diferente. Alguns nos permitem expressar uma modalidade de comunicação instantânea e em tempo real. Alguns nos permitem uma comunicação assimétrica, onde usando o Twitter posso me dirigir a um público de milhares de pessoas e receber *feedback* em tempo real sem precisar de ter uma comunicação bidirecional e síncrona. Alguns, como o *e-mail*, nos permitem ter uma comunicação mais assíncrona, de longo prazo, entre as pessoas.

O que fazemos é construir interfaces, nós construímos abstrações, criamos ferramentas unificadoras que nos permitem usar todas essas modalidades a partir de uma única interface e mover-nos fluidamente de uma para a outra. Então, podemos começar a transmitir pequenas mensagens de texto para alguém, entrar em uma conversa, convertê-la para uma conversa de áudio, decidir que queremos mostrar-lhes o nosso cachorro, ligamos o vídeo, convertemos em uma videoconferência e, quando terminamos a conversa, encaminhamos um *e-mail* para resumir tudo o que foi conversado. Agora, passamos por cinco modalidades diferentes de comunicação em uma única

interface unificada.

> *"O que fazemos é construir interfaces, construímos abstrações, criamos ferramentas unificadoras que nos permitem usar todas essas modalidades a partir de uma única interface e nos mover fluidamente de uma para outra".*

• Moeda como um aplicativo

Eu penso que isso é o que vai acontecer com a moeda. Vamos começar a tratar a moeda como um aplicativo e, para fazer isso, precisaremos de interfaces que nos permitam uma experiência monetária unificada, que nos permita ter uma única carteira com talvez 150 moedas diferentes nela. Por causa de invenções como as *sidechains*, corretoras (exchanges) descentralizadas, sistemas líquidos fluidos e a total ausência de monopólio, de bloqueio, de situações de reféns em torno das moedas, poderemos instantaneamente e com muito baixo custo converter *bitcoin* para *Namecoin*, para *Dogecoin*, para *Ethereum*. Se pudermos fazer isso, então não importa porque nós não faremos isso; nossa interface de carteira unificada fará isso, tentando ver o que estamos tentando alcançar com nossa moeda. Se estou comprando uma casa, poderei expressar minha vontade transacional na modalidade de *bitcoin* porque é a moeda mais adequada. Quando eu tentar nomear o domínio para aquela casa, ele irá converter alguns para *Namecoin*. O contrato será pago em *ether*. Quando eu der uma gorjeta para o garçom pela xícara de café naquela manhã, darei em *Doge*. Minha interface irá esconder todas essas diferenças.

> *"Nós estamos começando a tratar moeda como um aplicativo, e para fazer isso vamos precisar de interfaces que nos permitam experienciar a moeda unificada, que nos permitam uma única carteira com talvez umas 150 moedas diferentes nela."*

Posso ver um mundo em que possamos suavemente nos mover entre moedas de forma multimodal. Existe mais uma coisa que vem por aí, que a possibilidade real de abstrairmos o valor em taxa de câmbio a partir da moeda real. Se nós temos um sistema de comunicação multimodal, nós não precisamos mais olhar os valores individuais e as taxas de câmbio de todos esses commodities, ativos, moedas, chame-os como você quiser.

• Moeda índice

Existe uma real possibilidade de que teremos uma moeda índice, uma moeda que não é em si negociável, que não tem uma utilidade intrínseca como mercadoria transacional, mas no lugar disso é usada para expressar o poder aquisitivo *vis-à-vis* das várias moedas em nossa carteira.

Eu posso ter mil unidades de moeda unificada. Você não pode comprar unidades de moeda unificada. Você pode comprar *bitcoin* e depois me dizer o

quanto de unidades de moeda unificada vale. Eu valorizo tudo em unidades de moeda unificada, e depois eu pago em *Dogecoin* ou *Namecoin* ou *bitcoin* ou *ether*, dependendo de como eu quero usar.

> *"Posso ver um mundo onde nós possamos suavemente nos mover entre moedas em uma forma multimodal."*

Nós já fazemos isso no mercado financeiro. De fato, você pode negociar o S&P 500. Você não está comprando uma única empresa; o que você está comprando é um agregado de várias coisas diferentes que estão na bolsa de valores como uma expressão do valor total do mercado. Você pode usar esse meta-instrumento para precificar as transações. Por exemplo, o London Interbank Offered Rate é usado como meta-taxa de juro para, contratualmente, ligar as coisas em um conjunto de taxa de juros globais. Você não precisa dizer "Eu vou comprar tudo isso que o Bundesbank diz." Você diz, "Eu vou comprar isso na LIBOR+2," e então você tem um ponto de referência estável para transações.

Eu espero que possamos ver muito disso com moedas. Nós, provavelmente, iremos ver muitas meta-moedas cujo propósito é agregar valor para todas as carteiras e todas as moedas, e nos permitindo entender o valor abstrato que existe independentemente da moeda com a qual escolhemos nos expressar.

Escolhendo moedas e comunidades

Então, essa é uma perspectiva ligeiramente filosófica. É por isso que eu acho que isso não importa: *Ether* não está competindo com *bitcoin*; *bitcoin* não está competindo com *Litecoin*. Elas todas são meios de se expressar na modalidade transacional que queremos usar em algum ponto para alcançar nosso objetivo. Com isso vem uma ferramenta muito importante e poderosa. Nas escolhas que fazemos com essas moedas, estamos também escolhendo nos alinhar com essas comunidades.

> *"Adoção não é o simples ato de usar uma moeda; é também participar de uma comunidade que também tenha escolhido adotar essa moeda."*

Adoção não é o simples ato de usar uma moeda; é também participar de uma comunidade que tenha escolhido adotar essa moeda. Quando eu escolho adotar o *bitcoin*, eu acredito em uma política monetária de um total de 21 milhões de moedas como fonte estável de valor. Se eu escolher adotar *Freicoin*, é porque acredito em uma moeda com base inflacionária, moeda de sobreestadia que tem uma taxa de juros negativa, que impõe o consumo e desencoraja a acumulação. Estou escolhendo minhas políticas através da minha moeda, e através dessa escolha estou associando a mim mesmo com uma comunidade global que fez a mesma escolha que eu e está expressando essa escolha através da moeda. Assim como eu escolho

qual aplicativo de internet quero me comunicar, estou também me alinhando com a comunidade correspondente. Eu não uso Twitter só porque é um mecanismo de comunicação conveniente. Eu uso o Twitter porque eu também concordo com muitos dos conceitos e filosofias que a comunidade de outras pessoas que escolheram usar o Twitter.

> *"Nós entramos no reino da meta-política, da política por algoritmos, da habilidade para comunidades globais de formarem em torno de um consenso comum de políticas através da escolha da moeda."*

Com a moeda, essa escolha se torna muito mais poderosa politicamente. Nós entramos no reino da meta-política, da política por algoritmos, da habilidade para comunidades globais de formarem em torno de um consenso comum de políticas através da escolha da moeda. Você quer inflação? Use uma moeda inflacionária. Você é um pró-ouro? Use uma moeda deflacionária. Você quer uma moeda que crie uma renda mínima garantida para os pobres? Use uma moeda que expresse essas políticas. Você quer uma moeda que dê brindes por diminuir o carbono? Use uma moeda que expresse essas políticas verdes. Estamos começando a ver comunidades, políticas e moedas convergirem e nos permitir fazer essas escolhas. Assim como posso dar apoio à *Joeycoin* para dizer que Joey é de fato o mais legal entres os garotos de 5 anos, eu posso apoiar *Greencoin* porque eu me importo com o aquecimento global. Ou não. Eu posso apoiar a *Meatcoin* se eu realmente gosto de carne vermelha. Tanto faz. *LigaMundialDeLutaLivreCOIN*, não tem problema algum. Haverá algumas dessas também.

Realmente, todas essas coisas são formas de expressão e que podem retornar ao ponto original: a moeda, no fim, é uma forma de linguagem. É uma linguagem pela qual podemos comunicar nossas expectativas de desejo de valores, e agora que podemos fazer isso em uma escala tão massiva, que todos podem criar moedas, nossas escolhas realmente importarão. Passamos do jogo de somas de zero. Isso não é mais sobre nações-estado. Isso não é sobre quem adotou primeiro o *bitcoin* ou as criptomoedas, porque a internet está adotando as criptomoedas, e a internet é a maior economia global. É a primeira economia transnacional, e precisa de uma moeda transnacional.

> *"Isso não é mais sobre nações-estado. A internet é a maior economia global. É a primeira economia transnacional, e precisa de uma moeda transnacional."*

Moeda cria soberania

Para resumir, nós invertemos os mais básicos e mais fundamentais na equação da moeda. Por milênios, até o ano de 2008, soberania definia a moeda. Soberania era a base na qual seria criada a moeda, e a moeda permitia que a soberania fosse expressada. O sistema monopolístico de moeda é a base da soberania. Agora, a internet tem uma moeda. A internet vai usar essa moeda

para criar soberania.

> *"Depois de 2008, a moeda cria soberania."*

Depois de 2008, a moeda cria soberania. A internet tem sua própria moeda, que significa que a internet tem seu poder aquisitivo. O que significa que a internet tem liberdade econômica. O que significa que a internet pode exercer a liberdade financeira numa forma pós-nacionalista, de uma forma que ignora fronteiras, mas não torna as nações-estado obsoletas, só simplesmente menos relevantes. Quando um blogueiro egípcio pode não somente postar sobre a revolução como pode financiar a revolução com *bitcoins*, e ele pode se conectar com pessoas de todo o mundo que compartilham suas ideias de autodeterminação e liberdade, ele está expressando sua própria soberania como indivíduo e está expressando a soberania como uma comunidade que utiliza daquela moeda.

Esse é o mundo em que vivemos agora: um mundo onde moedas podem coexistir e onde moedas e sua adoção criam soberania.

Obrigado.

PRINCÍPIOS DO DESIGN DO BITCOIN

Esta palestra foi ministrada em junho de 2015 no Harvard Innovation Lab em Boston, Massachusetts, como parte de uma oficina de design do IDEO Lab. Durante este workshop de dois dias, os estudantes competiram para criar protótipos de aplicativos baseados no bitcoin e na tecnologia blockchain.

Link do vídeo: https://www.youtube.com/watch?v=Ur037LYsb8M

Bom dia, pessoal. Uau, que tarefa difícil vocês têm. Em um nível muito básico, vocês têm que tentar entender o que é o *bitcoin*. Eu posso responder a essa pergunta em quatro palavras. *Bitcoin* é dinheiro digital, Mas isso não o captura de verdade. É mais como a internet do dinheiro. Na realidade o *bitcoin* é uma rede de consenso descentralizada baseada na tecnologia do *blockchain* e em um algoritmo de prova de trabalho que permite que um *token* digital aja como um sistema de recompensa para uma competição, baseada em teoria dos jogos, entre um conjunto descentralizado de mineradores que validam e – "ah meu deus..." – imediatamente cai no penhasco.

Mesmo depois de alguns anos explorando "O que é *bitcoin*?", você verá que ainda estará aprendendo, você ainda estará tentando entender o que é o *bitcoin*. Parte da razão disso é porque o *bitcoin* é uma tecnologia muito nova, é uma tecnologia realmente disruptiva, mas também é a abstração de uma tecnologia muito antiga. Essa tecnologia é o dinheiro. Dinheiro é uma ferramenta, é uma tecnologia. Na verdade ela compartilha semelhanças com estruturas linguísticas, isso porque a usamos quase como uma linguagem para comunicar o valor entre nós mesmos em uma sociedade.

A história do dinheiro

Quem quer me dizer aqui qual é a idade do dinheiro? *Membro da audiência*: "5 mil anos?". Tudo bem, esse é um bom palpite. Um pouco mais velho. Tente novamente. O problema em tentar entender a história do dinheiro é que o dinheiro é mais velho que a história. Podemos seguir e dar uma olhada nos textos sobre dinheiro. Dinheiro é mais velho do que a própria escrita. Isso pode confundi-lo um pouco. Você está como, "o dinheiro é mais velho do que a escrita? Não pode ser." Na verdade, se você olhar para as primeiras formas de escrita que podemos encontrar, elas são planilhas. São livros de contabilidade. A primeira coisa arranhada em tabletes criados com madeira e coisas assim são os livros de contabilidade. Eles representam quantas ânforas de óleo foram dadas ao faraó. Se voltarmos ainda mais no tempo, podemos en-

contrar formas antigas de dinheiro entre as ruínas de antigas civilizações: miçangas, penas, conchas, pedras gigantes. O dinheiro assumiu muitas formas, mas ele existe e tem existido há quase tanto tempo quanto a linguagem. Essa é uma tecnologia verdadeiramente antiga. Então, não tem 5 mil anos. Provavelmente está perto de 500 mil anos.

• Primatas e dinheiro

Na verdade, vimos o dinheiro surgir com outras espécies. Espécies altamente inteligentes como os primatas, certos tipos de pássaros como corvos, mesmo mamíferos marinhos como golfinhos têm formas de sinais que eles usam para expressar valor entre si. Ou eles podem aprender muito rapidamente o mecanismo do dinheiro. Você pode ensinar primatas que, se virarem o seixo, ganharão uma banana. E, em seguida, verá, dentro de um curto período de tempo, como isso não só se torna parte da cultura dos primatas, mas é transmitido até a próxima geração, e eles começam a inventar atividades econômicas. Não atividades econômicas legais. Eles inventam assalto à mão armada: batem nos outros macacos e pegam seus seixos, para que possam ganhar bananas. Eles inventam favores sexuais por seixos, para que possam ganhar bananas. Eles inventam algumas das primeiras atividades econômicas.

> *"Espécies de elevada inteligência como os primatas, certos tipos de pássaros como corvos, e mesmo mamíferos marinhos como golfinhos têm formas de créditos que eles usam para expressar valor entre si."*

Dinheiro é antigo. É uma tecnologia absolutamente antiga, e nenhum de nós realmente o compreende. Se você quiser uma demonstração desse fato, sente-se e converse com uma criança de quatro anos de idade e tente explicar a ela o dinheiro. Você vai descobrir rapidamente que a criança de quatro anos tem perguntas muito boas que você não é capaz de responder. Você pode assistir aos pais passarem por isso, é hilário:

"– Mamãe, de onde vem o dinheiro?"

"– Os bancos o fazem."

"– Como eles o fazem?"

"– Bem, eles o imprimem."

"– Por que não podemos ter mais, então."

"– Vá limpar seu quarto."

Você está a quatro perguntas de "vá limpar seu quarto" numa conversa sobre dinheiro porque adultos realmente não entendem o que é o dinheiro. Mesmo que seja um artefato cultural que tem existido em nossa espécie por centenas de milhares de anos, não entendemos como funciona.

Características do dinheiro

Nós passamos por várias iterações tecnológicas do dinheiro. Começamos com formas muito básicas de dinheiro. Essas formas básicas tinham características únicas que as tornaram boas como dinheiro. O que torna o dinheiro bom? Algo que é raro, conchas, penas. Você pode utilizar conchas como dinheiro, a menos que você more na praia; se você mora na praia, você não pode usar conchas como dinheiro. Você pode transportar o valor facilmente. Então, tem que ser portátil. Com poucas exceções, a maioria dos tipos de dinheiro são altamente portáteis. Se a quantidade de dinheiro que você precisa para comprar uma vaca é mais pesada do que a vaca, então não é dinheiro bom. É por isso que não vemos com frequência, por exemplo, o ouro sendo usado em grandes transações. É muito pesado. Outras características do dinheiro. Tem que ser difícil de falsificar; tem que ser difícil de criar mais dele. Você deve ser capaz de identificar rapidamente ou de forma relativamente fácil que é autêntico; Deve ser fungível. Se eu estiver usando conchas, então esta concha ou aquela concha são ambas o mesmo dinheiro. Se eu lhe der um dólar, não importa qual dólar lhe dei; é fungível. Cada dólar pode ser substituído por qualquer outro dólar.

"O dinheiro em si é uma abstração. Se não é uma abstração, então não é dinheiro — é permuta."

Essas são as tecnologias, e gradualmente, ao longo do tempo, nós criamos abstrações. "O dinheiro em si é uma abstração. Se não é uma abstração, então não é dinheiro — é permuta." Se eu lhe der bananas em troca do seu bode, isso não é dinheiro. As bananas não são dinheiro porque você as come. Você não pode usá-las para fazer mais trocas. Portanto, isso é permuta. Você está trocando uma mercadoria por outra. Se é abstrato — se não tem nenhum uso prático em si — então trata-se de uma abstração de dinheiro, algo que representa outra coisa, algum valor compartilhado.

Essa reflexão nos leva a uma conclusão inescapável sobre dinheiro: dinheiro é uma alucinação cultural compartilhada. É uma ilusão compartilhada. Nós andamos por aí e nos relacionamos com outras pessoas sendo intermediados por pedaços de algodão impressos com tinta verde cheios de germe. Se você fosse um antropólogo alienígena que pousou na terra a observar esse comportamento, você provavelmente pensaria que é muito, muito estranho. Que só através da troca dessas peças de algodão, você pode ter relações sociais, fazer transações e participar do comércio — se alimentar, abrigar-se, etc., etc. Não faz muito sentido, mas isso é baseado em uma alucinação compartilhada. É baseado no pressuposto de que se você me der um dólar hoje, alguém vai aceitar aquele dólar em troca de algo de valor amanhã. Enquanto se acreditar que isso é verdade, então o dólar tem valor. Valor vem do pressuposto de que posso usá-lo novamente.

"O dinheiro é uma alucinação cultural compartilhada."

• Somente mais uma abstração do dinheiro

Bitcoin é apenas a mais recente iteração de abstração. Já fizemos abstração antes, mas cada vez que fazemos abstração de dinheiro, a sociedade se assusta porque essa coisa nova não pode ser dinheiro real. Olhe para trás e veja o que aconteceu com a introdução das moedas estampadas em metal não precioso, e então finalmente notas de papel. Quando as primeiras notas de papel circularam, ninguém acreditava que elas tinham valor. A alucinação compartilhada não tinha tomado conta ainda. Foi muito difícil persuadir as pessoas a trocarem moedas de ouro verdadeiro ou moedas de prata por pedaços de papel que atestavam que eles tinham ouro em um cofre. Em seguida, dê um passo além, desapareça com o ouro do cofre e diga, "Acontece que, agora, é só o papel."

"... cada vez que fazemos abstração de dinheiro, a sociedade enlouquece porque essa nova coisa não pode ser dinheiro de verdade."

Você pergunta para as pessoas sobre o *bitcoin* e uma das primeiras coisas que se ouve da maioria é que não é dinheiro real, pois não tem lastro por ouro, como o dólar dos EUA — o que eu acho surpreendente. O dólar não tem lastro por ouro desde 1936. No entanto, a maioria das pessoas acredita que, em algum lugar no cofre, possivelmente em Fort Knox, ou algum outro local presente em filmes, existem barras de ouro que correspondem lingote por lingote aos pedaços de papel que elas têm no seu bolso. Eles não correspondem. Isso não existe. Por que o *bitcoin* é dinheiro? Porque as outras pessoas pensam que é dinheiro. Você pode escrever uma dúzia de dissertações de doutorado explicando exatamente porque *bitcoin* não é dinheiro... e eu vivi isso por dois anos. Portanto, não importa o que diz a sua tese. Para mim, é dinheiro, porque eu o vivenciei por dois anos. Do mesmo modo que outras milhares de pessoas. Portanto, para mim, é um dinheiro muito real.

Bitcoin e design

Você recebeu a tarefa de criar *designs* e conceitos em torno da mais antiga tecnologia do mundo que pouquíssimas pessoas realmente entendem. Trata-se da mais recente e abstrata ideia, nova em folha e completamente separada das expressões anteriores sobre dinheiro e extremamente complexa enquanto tecnologia. Essa é uma difícil tarefa. Quando confrontado com esse desafio, a técnica que parece mais favorável é o uso de metáforas. Metáforas são ferramentas extremamente poderosas. Elas nos permitem criar expectativas. Metáforas são as ferramentas pelas quais criamos expectativas. Quando você tem um computador e ele tem uma área de trabalho, você assume que alguma coisa vai acontecer quando arrasta alguma coisa pela área de

trabalho. Isso porque você já trabalhou antes em uma área de trabalho real, o que influencia suas expectativas. Você espera que o ambiente virtual se comporte tal como aquele objeto que imita. Isso é metáfora de *design*. Metáforas de *design* são extremamente poderosas, mas também podem ser muito perigosas se mal aplicadas.

> *"Metáforas de design são extremamente poderosas, mas também podem ser muito perigosas se mal aplicadas. Em se tratando de bitcoin, todos os termos metafóricos são errados e falhos."*

• As carteiras não são carteiras

Em se tratando de *bitcoin,* todos os termos metafóricos são errados e falhos. Vamos repassar a lista. Você provavelmente esbarrou neles ao se envolver com a tecnologia de *bitcoin* e descobrir toda uma terminologia. Primeiro de tudo, uma "carteira". O que é uma carteira? Uma carteira é algo que armazena dinheiro. Não em *bitcoin*. O dinheiro não está na carteira; o dinheiro está na rede. A carteira contém chaves. Então, não é uma carteira; é um chaveiro. Como você pode dizer que não é uma carteira? Você pode copiar uma carteira? Não. Mas você pode copiar uma chave. Um chaveiro é uma metáfora muito melhor. Se eu tenho um chaveiro — imaginar um grande anel de chaves como um faxineiro ou um depositário —, eu tenho um monte de chaves e posso entrar em uma loja, posso ter todas essas chaves duplicadas e posso criar um segundo chaveiro. Ambos os chaveiros funcionarão indistintamente em todas as fechaduras que o chaveiro original funcionou. É como funciona um chaveiro. Se você entende o que faz um chaveiro, então você vai entender como funciona uma carteira *bitcoin*. Você pode copiá-la, você pode fazer cópias das chaves. Se você dá a alguém uma cópia da chave, essa pessoa pode também abrir a porta. Sem precisar de outra permissão sua para fazer isso.

Então, uma "carteira" não é uma carteira; é um chaveiro. Essa é uma metáfora terrível. Você tem expectativas de que vai fazer uma carteira. Ela irá guardar coisas. E que o conteúdo ficará escondido e enumerado. Nada disso existe no *bitcoin*.

• Não há moedas em bitcoin

Vamos ao básico: "*Bit - Coin*." Moeda (Coin). Uma palavra péssima. E uma marca péssima. Moeda. Pegue a forma mais abstrata de dinheiro que já criamos, que é baseada em uma rede completamente descentralizada que não tem moedas, e em seguida, nomeie-a "*bitcoin*". Só para confundir todos. Uma moeda, que é uma tecnologia de duas gerações passadas e uma representação física de dinheiro muito menos abstrata e muito mais tangível. Você pega a representação mais abstrata do dinheiro e a batiza com a representação mais tangível de dinheiro. Somente um engenheiro seria capaz de criar essa marca.

Aqui vai um pequeno segredo: não há nenhuma moeda no *bitcoin*. Quando se opera a mineração, não se criam moedas, mas sim registros de lançamentos. Essas transações não enumeram moedas. Eles têm saídas (*outputs*) — transações de saída — que são frações de valor que são infinitamente divisíveis e recombináveis. Moedas não fazem isso. Você não pode rastrear uma moeda em *bitcoin*, porque não há nenhuma moeda.

Então, você tem uma "carteira" que não contém "moedas" — porque as moedas na verdade estão na rede e não são moedas, são registros de saídas —, e o que você realmente tem é um chaveiro. As transações não são de um remetente a um destinatário. Endereços não têm saldo em *bitcoin*. Não há tal coisa como o saldo de um endereço. Um endereço controla as transações de saída, e se você rastrear o *blockchain* e somar todas as transações de saída, você pode extrair algum valor nocional. Se isso poderia mesmo ter sido gasto ou quanto o é, é realmente muito difícil de determinar. Não há nenhum "saldo". Você não tem nenhuma "conta" no *bitcoin*.

Todos os termos são falhos. O problema é que, da perspectiva do *design*, em vez desses termos metafóricos informarem as nossas expectativas, eles nos confundem. Está preparando o terreno para um enorme equívoco, porque pensamos que algo vai funcionar de certa maneira, mas isso acaba se comportando de forma completamente diferente e inesperada. Um exemplo é o ambiente Windows. Não sei se você alguma vez já comparou um ambiente Mac a um Windows. Para mim, o Windows não tem consistência. A metáfora aí é completamente falha. Você espera que ele faça uma coisa, mas acaba fazendo algo completamente diferente, o que confunde. A essência de um bom *design* é escolher a metáfora que informa as expectativas.

"A essência de um bom design é escolher a metáfora que informa as expectativas."

• Figuras skeuomórficas

Aqui está o próximo grande problema com metáforas e *design*. Existe um determinado conceito chamado skeumorfismo. A palavra *skeuomorphic* significa "uma sombra de seu eu anterior". Sua forma é como uma sombra.

O que significa que, quando você cria elementos no projeto, isso lhe dá referências ou dicas de algum modelo anterior. Um exemplo clássico, na primeira iteração de iPads, o *software* iOS tinha vários elementos skeumórficos. Se você abrisse a sua lista de contatos, o *layout* imitava couro. Um couro com costura. Essa costura não servia para nada. Era apenas um elemento de *design* que não tinha nenhuma finalidade funcional, cuja intenção era colocá-lo em contato com algo familiar, para que você pudesse entender a metáfora. Quando você está jogando um jogo de cartas no seu computador e tem um fundo falso de feltro sob as cartas, é porque está tentando remeter à metáfora

de um cassino, introduzindo esse elemento de *design*. As figuras skeumórficas são extremamente poderosas. Também são extremamente perigosas. Se você não usá-las de forma correta, novamente, pode criar expectativas diferentes do que vai acontecer a seguir.

Em *bitcoin*, temos vários skeumorfismos. O meu favorito e mais odiado é a imagem que você verá em cada artigo escrito sobre *bitcoin*: uma pilha de moedas de ouro com uma letra B nelas, geralmente a moeda Casascius desenhada por Mike Caldwell, e, às vezes, alguma outra versão dela. Pegou-se a pior metáfora do projeto do *bitcoin*, a palavra moeda, e a partir dela criou-se uma bela ilustração digital que reforça a ideia de algo físico. Essa é uma figura skeumórfica, que engana completamente todo mundo. As pessoas estão realmente indo ao eBay e comprando o que elas acham que é *bitcoin*. Estão comprando moedas físicas douradas, que não têm nada a ver com o *blockchain*, mas apenas a letra B estampada. "Olha, eu me juntei à revolução do dinheiro digital" dizem, mas essas réplicas tangíveis raramente têm qualquer valor em *bitcoin*. Esse é o resultado. Então, as pessoas escrevem artigos e olham para a imagem e pensam, "isso é o que parece um *bitcoin*." Isso não é o que um *bitcoin* se parece, porque, se você se lembra, talvez eu tenha mencionado que não há nenhuma moeda em *bitcoin*. Esse é o perigo.

Design para inovação

É realmente difícil pensar em boas metáforas para *bitcoin* porque não existe paralelos. Isso nunca foi feito. Formam-se armadilhas pela tentativa de extrapolar as experiências anteriores. Elas são inevitáveis. Tecnologias disruptivas fazem isso. Em tecnologias incrementais, utilizando o conhecimento existente e adicionando um miligrama a mais de visão e estendendo-a só mais um pouco, entende-se a nova tecnologia porque ela é somente a expansão do passado. *Bitcoin* é uma quebra radical com o passado, assim o entendimento tradicional do funcionamento de dinheiro não ajuda o entendimento do *bitcoin*. Se serve para algo, serve para dificultar o entendimento dos *bitcoins*. Quem menos entende de *bitcoin* são os economistas monetaristas. Não conseguem colocar seus pensamentos neles. Escreverão longas teses sobre como o *bitcoin* não é dinheiro, apesar do fato de eu ter vivido deles por anos.

> *"Bitcoin é uma quebra radical com o passado, assim o entendimento tradicional do funcionamento de dinheiro não ajuda o entendimento do bitcoin."*

Compreensão de tecnologias disruptivas é ainda mais difícil do que compreender tecnologias incrementais, porque as coisas mais interessantes não têm paralelo anterior. Pense assim. Olhe para *Star Trek* na década de 1970. O que eles acertaram? Haviam tricorders. Haviam comunicadores portáteis. Havia vídeo telefonia. Havia tudo o que era previsível com a tecnologia da

década de 1970. Não conseguiram prever a internet. Não conseguirem entender a ideia de armazenamentos de informações em rede. Eles tinham computadores fantásticos que poderiam falar com você, mas não tinham acesso a quaisquer dados. Eles não conseguiram prever coisas como meios de comunicação sociais. O mais importante, prestando atenção, nota-se algo muito estranho. *Star Trek* não tem dinheiro. Não há dinheiro em qualquer lugar no universo de *Star Trek*. Por que isso? Porque sua visão mais distante é uma sociedade sem dinheiro, uma sociedade sem um idioma para transmissão de valor, que é provavelmente a mais radical ruptura da realidade.

• Prevendo o futuro

Quando tentamos prever o futuro, encontramos certas áreas que são completamente escuras. Essas são as áreas que nunca foram vistas antes. Essas são as aplicações que não podemos imaginar porque, para que venham a existir, muitas coisas têm que se encaixar. Para a rede acontecer, foi necessário um protocolo padronizado de transmissão comum. Para a rede dar à luz a mídia social, foi necessária a penetração maciça de correio eletrônico básico e conexões TCP/IP. Era necessária a penetração dessas conexões em um estado permanente. Eram necessários dispositivos móveis com alta capacidade de computação na palma da mão conectados à internet. Todas essas coisas tinham que se concretizar para que as mídias sociais fossem possíveis.

> *"Se você olhar para internet em 1992, você achará que ela iria substituir o telefone. Esta é a única experiência que você tem."*

"Se você olhar para internet em 1992, você achará que ela iria substituir o telefone. Esta é a única experiência que você tem.". A internet é um telefone chique. Talvez seja um telefone chique/fax, talvez uma impressora multifuncional/fax/telefone. É muito chique. Então, as empresas de telefone olham para isso e dizem "Oh, é um telefone chique. Nós podemos fazer isso." Eles estavam errados, felizmente. De outra maneira, cada vez que fosse para uma chamada no *Skype*, iria precisar de um pequeno buraco do lado do meu computador onde eu teria que depositar 0,25$ a cada 3 segundos para fazer uma ligação de *Skype*. Felizmente, não foram as empresas de telefone que escreveram as regras. Eles possivelmente não poderiam prever os resultados que vimos na internet, por que a maioria das coisas interessantes não eram melhorias incrementais ou extensões das coisas prévias. Eram simplesmente partidas radicais do passado, por que eles criaram condições para coisas que não eram possíveis antes.

Vamos voltar para o *bitcoin* e pensar nisso por um segundo. Considere que estamos falando sobre transações financeiras, sistema bancário e pagamentos. "É um cartão de crédito chique." "É o Paypal, basicamente. É um Paypal global." Mas não é. É algo completamente, radicalmente, diferente, mas nós

não podemos ver onde isso vai dar. As aplicações que vão acontecer no *bitcoin*, as aplicações realmente interessantes, são aquelas que só acontecem quando você tem adoção e penetração suficientes nesta tecnologia, a habilidade para fazer transações transfronteiriças num nível nunca antes feito na história humana.

> *"Considere que estamos falando sobre transações financeiras, sistema bancário e pagamentos. "É um cartão de crédito chique." "É o Paypal, basicamente. É um Paypal global." Mas não é. É algo completamente, radicalmente, diferente."*

Hoje, são 3 bilhões de pessoas sem qualquer tipo de facilidades bancárias. Mais que 3 bilhões de pessoas "desbancarizadas" como as chamamos - nenhum acesso ao crédito ou financiamento internacional. Você ou eu podemos ir em um *site* de uma corretora agora mesmo e dentro de 24 horas teremos uma conta em dólares que pode negociar na bolsa de valores de Tokyo. Isso é um privilégio. Isso é uma facilidade concedida para menos de um bilhão de pessoas no mundo. Um para cada sete. E os outros 6 bilhões? Eles mal têm um controle básico. Muitos deles vivem em sociedades baseadas em dinheiro ou permuta. Então, as questões que você tem que entender são: o que acontece com um fazendeiro no Kenya que tem um Nokia 1000 com mensagens de celular, e de repente o telefone se torna um terminal da Bloomberg, um terminal de empréstimos, um terminal de remessa da Western Union, uma bolsa de valores, é um banco, não um terminal de banco, mas um banco, no telefone? E o que acontece quando isso é fornecido para os outros 6 bilhões em todo o mundo?

Parte da razão do *bitcoin* ser imparável é por que existe uma grande necessidade para essa tecnologia. Bancos nos mundos em desenvolvimento não podem estender serviços a essas populações. Recentemente, eu estava conversando com um banqueiro que me disse, "Metade da nossa população está a 100 milhas da filial mais próxima, subindo o rio, de canoa. Nós não conseguimos atendê-los." Mas até na vila mais remota das bacias amazônicas tem uma torre de celular, e alguém, naquela vila, tem painel de energia solar e um celular Nokia 1000. Existem mais telefones da marca Nokia no mundo do que qualquer outro tipo de aparelho eletrônico. É o dispositivo mais produzido em grande escala que a humanidade já produziu. Quase 5 bilhões de pessoas têm acesso a telefones celulares. Quase 3 bilhões de pessoas têm acesso ao celular e não têm acesso à água potável. Pense nisso. Telefones celulares são mais difundidos do que a água em nosso planeta. O que acontece quando cada um desses que falamos é um banqueiro. Para mim, a visão do *bitcoin* não é para levar o banco para os outros 6 bilhões, é para desbancarizar todos nós. Nós podemos fazer isso. Serviços bancários são uma aplicação.

> *"Para mim, a visão do bitcoin não é para levar o banco para os outros 6 bilhões, é para desbancarizar todos nós."*

Inovação intersticial

Esse é apenas o começo. As coisas realmente interessantes no *bitcoin* acontecem no que eu chamo de "inovação intersticial" - a inovação em intervalos, os lugares onde hoje os sistemas não alcançam. As tecnologias têm um efeito interessante onde elas subitamente mudam os pressupostos básicos. Algumas das coisas mais poderosas acontecem com a internet, acontecem não por causa da conectividade, mas por causa do custo marginal da transmissão de informação à distância. Antes da internet, a informação movia-se do ponto A para o ponto B e custava muito dinheiro. A internet levou o custo quase a zero. O resultado foi que milhões de aplicações que não poderiam acontecer com os custos anteriores, mesmo se nós só imaginássemos, de repente se tornaram possíveis. Por que você iria transmitir música ao invés de comprá-la e armazená-la localmente? Por que não custa nada. Uma vez que não custa nada e você pode transmitir música, você de repente percebe que direito de propriedade é meio que supervalorizado. Se uma geração inteira percebesse isso, então a propriedade intelectual também estaria meio supervalorizada. Adeus gravadoras! Esses efeitos acontecem por que a tecnologia modifica os custos fundamentais de fazer as coisas.

Vamos pensar o que acontece quando o *bitcoin* altera o custo fundamental de transação -- transação sobre distância, valor transmitido, gravação de informação e gravação de informação em uma maneira imutável. O que acontece quando, pela primeira vez, existe um sistema que pode avaliar as regras sem a intervenção humana e pode ser confiável sem ter que depositar confiança em qualquer ser humano? No *bitcoin*, nós chamamos isso de remoção do risco de contrapartida. Se eu crio uma transação e assino, todos na rede de *bitcoin* podem validar essa transação independentemente. E eles não precisam perguntar pra ninguém. Eles podem ir através do *blockchain* no próprio computador, onde eles sabem que é correto e verdadeiro, porque vem sendo rastreado e construído como prova de trabalho. Eles podem checar aquela transação, 350 *bytes*, e eles podem validar aquela transação sem pedir para ninguém. Um sistema autoverificável, um sistema de regras que existe independente de atores humanos, que existe baseado na topologia de rede.

> *"O que acontece quando, pela primeira vez, existe um sistema que pode avaliar as regras sem a intervenção humana e pode ser confiável sem ter que depositar confiança em qualquer ser humano? No bitcoin, nós chamamos isso de remoção do risco de contrapartida."*

O que isso significa? O que isso faz para o comércio, para as transações? Podemos entender o que isso faz para o serviço bancário. Podemos entender também que a Western Union está caindo nessa década. Cobrar 30% da população mais pobre do planeta, você merece ser derrubado por uma tecnologia disruptiva. Ano passado, o CEO da Western Union disse, "A médio

prazo, nós não estamos preocupados com o *bitcoin*." Eu quero isso enquadrado na minha parede. É uma dessas frases, como o chefe da Kodak dizendo coisas assim enquanto a Nokia roubava seu almoço. A Kodak era a maior empresa de câmeras fotográficas do mundo até uma empresa que não era do ramo vender mais de 1 bilhão de câmeras em um ano e destruir sua indústria. Eles nunca viram isso antes. Nokia, a propósito, é o maior fabricante mundial de câmeras, sem dúvida. Isso é o que vai acontecer ao Western Union.

Essa é fácil. O que acontece quando você é capaz de fazer essa validação de regras sem a participação de terceiros? Isso muda várias instituições sociais fundamentais que temos hoje. Isso muda o que chamamos de "coeficiente de Coase", que trata das despesas organizacionais. Se queremos fazer algo como uma equipe, duas pessoas podem fazer mais do que uma. Três pessoas podem conseguir ainda mais. Mas há um limite para isso. Uma vez que você fica muito grande, os gastos gerais de comunicação entre os participantes do grupo são maiores do que o aumento marginal da eficiência. Então, adicionar mais pessoas piora, porque o grupo está crescendo muito rápido. *Bitcoin* muda isso, porque agora reduz as despesas de organização, transação e comércio, baseando-se em validação independente, em uma escala extremamente grande. Agora podemos contar com 1 milhão de pessoas, cerca de 5 mil máquinas, para aprovar a situação de um registro a cada dez minutos com custos extremamente baixos. Isso nunca aconteceu antes. Abre a porta para coisas que não podemos sequer imaginar. *Bitcoin* é uma radical descontinuação do passado.

Vamos dar um exemplo simples: pessoalidade. Pessoalidade é exigida para a posse financeira. Para ter seu próprio dinheiro, controlar os fundos, ter uma conta bancária, receber uma conta, pagar alguém, etc., você precisa ser uma pessoa. Em todos os lugares do mundo em cada pagamento e rede financeira que existe, pessoas possuem dinheiro. Eles podem possuir sob a forma de corporações, mas elas são apenas pessoas agrupadas. Eles podem usar procuradores, agentes, coisas assim, mas são só pessoas trabalhando juntas. *Bitcoin* não exige pessoalidade. Um agente de *software* pode possuir dinheiro. Um pedaço de *software* pode estar controlando autonomamente dinheiro sem qualquer intervenção humana. Isso é totalmente inédito na história do homem. Nós nunca presenciamos o que acontece a seguir.

Aqui está um pequeno experimento de imaginação. Vamos pegar três tecnologias radicalmente disruptivas e misturá-las. *Bitcoin* + Uber + Carros que dirigem sozinhos. O que acontece quando você mistura os três? O carro autoproprietário. Um carro que paga por sua concessão Toyota, seu seguro e sua gasolina, oferecendo corridas às pessoas. Um carro que não é propriedade de uma corporação. Um carro que é uma corporação. Um carro que é um acionista e dono de sua própria corporação. Um carro que existe como uma entidade financeira autônoma com nenhuma propriedade humana. Isso nun-

ca aconteceu antes, e isso é só o começo. *Suspiros da audiência*: "Caramba!"

> *"Vamos pegar três tecnologias radicalmente disruptivas e misturá-las. Bitcoin + Uber + Carros que dirigem sozinhos. O que acontece quando você mistura os três? O carro autoproprietário."*

Eu posso garantir que uma das primeiras corporações autônomas distribuídas será um vírus *ransomware*, totalmente autônomo, baseado em inteligência artificial que sairá roubando o *bitcoin* das pessoas *on-line*, e usará esse dinheiro para desenvolver-se para pagar melhores programas para comprar hospedagem e para divulgação. Essa é uma visão de futuro. Outra visão de futuro é uma caridade digital autônoma. Imagine um sistema que recebe doações das pessoas e usa essas doações para monitorar as redes sociais, como Twitter e Facebook. Quando um certo patamar é alcançado e vê que 100 mil pessoas estão falando de um desastre natural como um furacão nas Filipinas, pode ordenar as doações e automaticamente financiar auxílio na área, sem um quadro de diretores, sem acionistas. 100% da doação vai diretamente para as causas beneficentes. Qualquer um pode ver as regras através da qual essa caridade autônoma e altruísta funciona. Estamos começando a abordar as coisas de uma maneira nunca vistas antes. Isso não é somente uma moeda.

Agora, vamos olhar como a comunidade do *bitcoin* está endereçando esse potencial incrível com suas escolhas de *design* e metáforas. Ah, rapaz, é uma bagunça.

Experiência com caixas eletrônicos

Vamos pegar um exemplo simples. Quantos de vocês tiveram uma experiência com caixa eletrônico de *bitcoin*, ou BTM, como é conhecido? Como foi essa experiência? Quem gostou? Ninguém, isso é certo. O que é um caixa eletrônico comum? Essas máquinas têm cerca de 25 anos de existência. Qual o propósito delas? Qual é seu objetivo? *Membros da audiência*: "É um dispensário de dinheiro". Okey. Quando você interage enquanto pessoa com um desses dispositivos, você tem uma relação já existente com o banco ou instituição financeira, você tem um saldo preexistente. Seu objetivo principal quando vai até um desses é entrar, sacar dinheiro e sair. Vinte segundos é muito tempo. Três cliques são demais. A mais incrível inovação dos caixas eletrônicos nos últimos 25 anos foi o dinheiro rápido. Isso é tudo. Eles não mudaram muito desde então. Você aperta um botão. Então, eu posso ter dinheiro em um clique. Uau! 15 segundos, e pronto. Por que isso é importante? Porque um dos principais usos de caixas eletrônicos é que às 13:00h, 100 pessoas fazem fila na frente de quatro ou cinco caixas eletrônicos no centro da cidade para tirar 20 dólares e comprar o almoço. Você vê isso em qualquer lugar do mundo.

Qual é o propósito de um caixa eletrônico? Para um banco, é reduzir a despe-

sa de ter um ser humano e reduzir a interação para o menor tempo possível para alguém que tem uma relação preexistente com aquele banco. O que isso tem em comum com um caixa de *bitcoin*? Absolutamente nada.

Experiência com caixa eletrônico de bitcoin

Agora vamos olhar para a experiência de um BTM (caixa eletrônico de *bitcoin*). O usuário médio de um BTM é alguém que nunca viu *bitcoin* antes. É uma pessoa que não entende o que é *bitcoin*, e um BTM é a sua primeira experiência com essa moeda. É uma pessoa que não tem uma relação preexistente com ninguém no contexto *bitcoin*. É uma pessoa que geralmente não tem uma carteira, porque não sabe que precisa de uma. Eles não sabem o que é uma carteira, certamente não sabem que se trata, na verdade, de um chaveiro. Vão até essa máquina que foi projetada por engenheiros para simular a experiência de um caixa eletrônico comum, que não se assemelha absolutamente em nada com a usualidade do *bitcoin*.

Então, você vai até um BTM e tenta movimentar *bitcoins* em tão poucos cliques possíveis e com um mínimo de interação. É uma boa maneira de construir a fidelidade da marca? É uma maneira de construir a experiência do usuário? É uma boa maneira de introduzir novos usuários? Quer dizer, essas máquinas jogam o *bitcoin* em você. Você não está preparado para isso. Por favor, abra seu celular e mostre seu código QR. – Você: "O quê? O que é um código QR? Um momento, vou pesquisar no Google por 'QR code'... Existe um app para escaneá-los... talvez eu deva usar aquele. Ou não deva usar esse outro. Talvez eu devesse usar uma carteira de *bitcoin*. Oh! existem 26 delas. Qual delas será melhor? Eu não sei. Vou usar a *Circle*. Ah, essa requer uma relação preexistente. Opa! Eu vou usar *Coinbase*. Ah, essa requer uma relação preexistente. Opa!"

Finalmente, tenho a minha carteira e exibo o código QR, coloco algum dinheiro nela e eu agora tenho *bitcoins*. O que eu vou fazer com isso? Eu tenho todas essas dúvidas. Quem aceita o *bitcoin*? Onde posso gastá-lo? Como faço para enviá-lo? Como faço para protegê-lo? Ele vai se perder se eu perder meu celular? Não faço a menor ideia. Por quê? Porque esta máquina infernal maldita não me informa nada. Ela só jogou o *bitcoin* em mim, e em 15 segundos está pronta para o próximo cliente.

Se eu estivesse projetando caixas eletrônicos para *bitcoin*, antes de tudo, as colocaria em adegas. Em segundo lugar, não usaria inglês neles. Seria tudo em espanhol porque usaria o modelo de remessa. Em terceiro lugar, a primeira função desse caixa eletrônico seria "Enviar dinheiro para a Cidade do México". É isso. Porque quero que as pessoas usem *bitcoin* para algo. Em quarto lugar, haveria um grande botão na frente escrito "Falar com um huma-

no". Eu tenho um dispositivo conectado à internet com uma câmera e uma tela e não estou usando isso para fazer o vídeo atendimento, isso é algum tipo de brincadeira? Boom: *Skype*. Uma pessoa. "Que diabos é *bitcoin*? Onde posso gastar eles?" "Oh, senhor, vejo que você está numa loja de vinhos na Avenida 25. Existem outras três lojas que aceitam *bitcoin* em sua área. Deixe-me mostrar-lhe um breve vídeo introdutório. Reúna todas as crianças na loja e poderemos dançar uma canção *bitcoin*. Vamos ver outro vídeo." Não quero interagir por somente 15 segundos. Quero interagir por duas horas e garantir que todos os meus amigos sentem em frente da máquina e assistam a vídeos de *bitcoin* e aprendam sobre *bitcoin*. Tem cores bonitas e me diz onde posso gastá-los. Ele me dá sugestões sobre carteiras. Ele pode enviar diretamente para o meu celular. Ele está construindo lealdade, marca e experiência. Não é uma interação de 15 segundos. Esta é a primeira experiência que muitas pessoas terão com *bitcoin*. Você tem a oportunidade de ter uma experiência profunda, significativa, educacional. Mas você não tem.

Crianças usam bitcoin

Aqui está outra pequena pista: as crianças estão usando *bitcoin*. Em média, ao redor do mundo, a idade mínima para abrir uma conta bancária é 16 anos de idade. Quando esses jovens de 16 anos de idade forem para o banco, quero que eles já tenham pelo menos seis anos de experiência com uso ativo do *bitcoin*. Porque então, quando eles enfrentarem o primeiro banqueiro, serão "Três a cinco dias?!" "Dias úteis!? Que diabo é um dia útil?" "Como assim você fecha às 17:00? Eu mal saí do trabalho a essa hora!" "Como assim eu tenho que pagar para você guardar meu dinheiro. Isso é ridículo!" "Ainda existem pessoas que sequer ouviram falar de *bitcoin*?!"

> *"Para muitos jovens, bitcoin será sua primeira experiência econômica. Quando esses jovens chegarem a um banco, eles estarão prontos para lidar com o sistema bancário."*

É a experiência que eu quero. Adivinha o quê? Crianças de 10 anos para cima abrindo contas *bitcoin*. Sabe por quê? Eles podem baixar o app na internet e estar no controle do dinheiro pela primeira vez. Então, os pais precisarão ter a conversa sobre pássaros e abelhas, mas também sobre chaves privadas. Essa é uma enorme disparidade geracional. "Para muitos jovens, *bitcoin* será sua primeira experiência econômica. Quando esses jovens chegarem a um banco, eles estarão prontos para lidar com o sistema bancário." Isso é uma enorme vantagem.

Tecnologia nova em folha, termos velhos de sempre

Então, como você atrai uma população completamente nova? Parte do truque é não tentar ser um banco. Não tentar fazer nada parecido com o sistema

bancário tradicional. Tudo o que esse sistema faz é poluir sua mente. Você quer que os novos usuários tenham uma nova experiência com *bitcoin* que seja diferente de qualquer banco que eles verão. Você não quer nada parecido com uma conta corrente. Deus me livre de você usar a palavra conta. Abra qualquer uma das bolsas agora — *Circle*, *Coinbase*. Qual é o nome do seu cadastro no *Coinbase*? É uma conta corrente e tem um saldo, e mostra-lhe um extrato. Quem é que contrataram para fazer este *layout*? O que significa a palavra conta? Significa uma conta na qual você pode escrever cheques. Eu sei que isso é a América, e estamos 25 anos atrasados no *fintech*. O resto do mundo não faz cheques, garanto. O que é um cheque? Um cheque é o dispositivo pelo qual uma avó pode fazer 20 pessoas na fila atrás no supermercado reclamar simultaneamente. Eu uso para pagar meu aluguel todo mês. Eu não sei porquê. Eu não posso fazer isso de outra forma. É uma loucura que eu esteja assinando um pedaço de papel e enviando pelo correio em 2015, para que meu senhorio possa caminhar até o banco e depositá-lo. Para que ele possa ter o dinheiro três a cinco dias úteis depois, afinal eles já lhe cobraram cinco dólares para possuir seu próprio dinheiro.

Não será preciso grande esforço para vender o *bitcoin* como algo melhor que bancos. Tudo que você precisa para ganhar dos bancos é que uma pessoa use *bitcoin* por uma semana e, em seguida, o banco cuidará do resto. Eles vão congelar sua conta, eles vão dizer que estão fechados, vão fazê-lo esperar por três a cinco dias úteis. Venderam *bitcoin*. Os bancos vão vendê-lo para você, sempre.

• As alegrias da transferência bancária internacional

Fui convidado para fazer uma palestra no Bundesbank, o Banco Federal alemão. Eles estavam me pagando para essa palestra, mas não sabiam como usar *bitcoin*, o que é um problema sério, porque eu geralmente recebo em *bitcoin*. Então, concordamos em fazer uma transferência bancária. Demorou 16 dias. Primeiro, eles pediram o número da minha conta. Então, no dia seguinte, eles disseram que precisavam do código SWIFT. A essa altura, meu banco estava fechado, e não consegui o número. Na manhã seguinte, eu consegui o tal código e mandei para os alemães. Mas, então, o banco estava fechado. Na manhã seguinte, eles testaram o número SWIFT e descobriram que era o número errado. Era o código usado para dólares americanos, não para moeda estrangeira. Então, eles me mandaram um *e-mail*, mas meu banco estava fechado. No dia seguinte, eu consegui o outro número e mandei para os alemães, mas naquele momento, o banco deles estava fechado. Finalmente fizeram a transferência. Meu banco deu uma olhada e disse, "Bundesbank. Nunca ouvi falar deles. Parece-me duvidoso. Vamos congelar isso durante 14 dias, para o caso de não ter fundos." Esse é o terceiro maior banco central no mundo. Esse é o Banco Federal alemão. Eles não dão cheques sem fundos. 14

dias mais tarde — e esta é a melhor parte — eles disseram, "dinheiro retido. Dinheiro liberado." Eles lançaram 80 dólares do montante total, que era uma quantidade de quatro dígitos. 80 dólares. Por que 80? Que diabos é isso? O que eu vou fazer com isso? Fique com tudo logo. Você está me provocando? Isso não faz sentido.

O problema com metáforas bancárias tradicionais

Isso é o que nós estamos abordando com *bitcoin*. Se você está introduzindo um novo produto no mercado e você é um *designer*, quais partes dessa metáfora você quer reutilizar no seu produto? De acordo com o mercado *bitcoin*, todas elas, aparentemente para convencer as pessoas de que trata-se da mesma coisa que seu banco. Não foram aproveitadas coisas relacionadas a bancos que são boas — como a habilidade de facilmente reverter transações, para obter um reembolso se você perder sua senha privada. Realmente nenhuma. Também nenhuma das partes ruins dos bancos, mas não prestamos atenção a isso. Então, nós criamos expectativas que são totalmente enganosas.

> *"Bitcoin precisa desesperadamente de um design. Até o momento isso está a cargo de engenheiros e está totalmente incompreensível."*

Inovação, design e assimilação

"*Bitcoin* precisa desesperadamente de um *design*. Até o momento isso está a cargo de engenheiros e está totalmente incompreensível. Mas eu tenho esperança, porque já fizemos isso antes. Eu me lembro da internet de 1989, e na época era ilegal fazer atividades comerciais na internet. Pertencia à National Science Foundation e era só para acadêmicos (ou, digamos, adolescentes de 15 anos que, por acaso, conseguiam a senha para um sistema acadêmico). Na época, o DNS estava ainda em sua infância. A maioria dos sistemas não tinha nomes DNS atribuídos. As coisas não estavam muito bem estruturadas. A maioria das coisas interessantes você só poderia encontrar através de um endereço IP. Eu andava com uma lista de endereços IP na minha carteira, então eu tive acesso a essas coisas. Para usá-los, era necessário habilidade de linha de comando UNIX.

Não havia nenhuma chance de minha mãe conseguir usar aquilo. Minha mãe me ligou e disse que seu aparelho de som estava quebrado, e eu tentei entender o porquê. Ela disse, "ele está exibindo uma mensagem de erro. Está piscando para mim '0:00'". Levei alguns minutos para entender que ela tinha puxado o plugue e o relógio tinha resetado. Então, o relógio estava esperando para ser configurado novamente e estava piscando "0:00." Essa é a pessoa que eu queria que usasse a internet para conversarmos, mas isso não ia acontecer. Demorou quase 20 anos entre o dia em que eu mandei meu primeiro *e-mail* e o dia que minha mãe mandou o primeiro *e-mail* dela. Para isso, um

monte de coisas tinha que acontecer. O mais importante, o iPad. Ela foi capaz de fazê-lo com um clique, o que era a única coisa capaz de tornar isso possível. Não tinha como a internet, em 1989, ser usada pelo público em geral.

• UX e sociedade

Existe um fantástico trecho de um programa matinal de TV, de 1994, que não foi ao ar. Ele mostra os jornalistas em grupo pouco antes do programa. Eles estão discutindo seu próximo assunto, que é história da internet, e estão tentando acertar suas informações. Um jornalista está perguntando aos outros jornalistas: "Então, espera, a internet é a coisa com o sinal 'no'?" "Não, não, isso é o *e-mail*. A internet é a coisa com os 'www', com os pontos e as barras." "Eu pensei que era o *e-mail*." "Não, isso é a internet." "Mas isso não é a *web*?" Então há essa discussão circular. Um sistema projetado por engenheiros. Impossível de entender. Duas coisas aconteceram. Uma, feita de tecnologia muito mais fácil de entender, muito melhor, mais refinada. Outra coisa importante aconteceu: a sociedade mudou. Hoje, um cidadão médio sabe exatamente a diferença entre um sinal de @ e um www, mesmo que seja um *design* horrível. A sociedade, aprendeu a língua da internet porque era importante o suficiente esse aprendizado.

> *"A sociedade aprendeu a língua da internet porque era importante o suficiente esse aprendizado."*

Enquanto fizemos a internet mais fácil, a sociedade fez sua parte compreendendo também as partes realmente ininteligíveis da internet. A mesma coisa está acontecendo com *bitcoin*. Vou a conferências abertas onde as pessoas nunca ouviram falar de *bitcoin* antes e eu digo: "Escute, não se preocupe. Alguém na sua vida pode te explicar sobre *bitcoin*. Quando terminarem de arrumar seu quarto, peça-lhes para te ensinar". Suas crianças de 10 anos de idade vão entender sobre isso. Já conheci crianças que usam interfaces baseadas na *web* para criar suas próprias criptomoedas.

Uma das perguntas interessantes que muitas vezes me fazem é "Quantos tipos de criptomoedas haverá?" A resposta é exatamente equivalente a "quantos blogueiros haverá na internet?" Todos nós. Todos eles. Não centenas de moedas, milhares, dezenas de milhares de moedas. Quando uma criança de 6 anos de idade pode criar uma moeda chamada *Joeycoin* para lançar em sua escola como uma disputa de popularidade, o fato de que a sua moeda possui escalabilidade é global, infalsificável e pode ser usada internacionalmente, não importa para o Joey, enquanto seus cinco amigos realmente gostarem de usar *Joeycoin*. Infelizmente, um concorrente, *Mariacoin*, é lançado na cena, e começa uma antiquada guerra de moedas. Isso vai acontecer. Parte do motivo pelo qual afirmarmos isso é porque crianças criam moedas. Você deixa as crianças em um jardim de infância por elas mesmas, e elas vão inventar

moedas — elásticos, cartões de Pokémon, cubinhos. Elas vão começar a acumular, trocar, vender por favores e então eventualmente brigar pela sua moeda imaginária que acabaram de inventar. Essa é uma experiência humana.

Nós apenas inventamos a moeda mais incrível do mundo. Seu trabalho agora é criar o *design* e as metáforas corretas para fazê-las funcionar para todo mundo.

Muito obrigado.

DINHEIRO COMO TIPO DE CONTEÚDO

Bitcoin conferência Sul; Queenstown, Nova Zelândia; novembro de 2014

Link do vídeo: https://www.youtube.com/watch?v=6vFgBGdmDgs

Bom dia pessoal. Hoje eu quero falar sobre um novo tópico em que trabalhei: dinheiro como tipo de conteúdo. *Bitcoin* introduziu uma transformação fundamental na forma em como o dinheiro vai ser visto no futuro, tornando o dinheiro completamente independente do meio de transporte básico e transformando-o em um tipo de conteúdo autônomo.

O que eu quero dizer com isso? Uma transação de *bitcoin* é uma estrutura de dados assinada, que pode ser executada em qualquer lugar do mundo. Muitas pessoas pensam que uma transação *bitcoin* tem de ser transmitida na rede *bitcoin*. Isso não é verdade. Uma transação *bitcoin* deve chegar aos mineradores e ser incluída em um bloco, mas não precisa ser transmitida pela rede *bitcoin*. Não há nada especial sobre a rede *bitcoin*. Ele apenas transmite transações e blocos. Uma transação pode ser transmitida por qualquer forma ou meio de comunicação.

Uma das coisas sobre *bitcoin* mágicas é que uma transação não incorpora mecanismos de segurança em si. A segurança está na prova de trabalho fornecida pelos mineradores, e a assinatura digital na transação é colocada por usuários finais com as chaves que eles armazenam. Não há nada de secreto na transação *bitcoin*. Deixe-me explicar o que quero dizer com isso.

Cartões de crédito: fragilidade do sistema

Se você estiver interessado em usar um sistema de ponto de venda e um cartão de crédito, o que é transmitido ao comerciante (através de uma longa série de intermediários) é o número de cartão de crédito, dados de validade e código de CCV2 na parte de trás do cartão. Na verdade, estou transmitindo as chaves secretas. Estou transmitindo os códigos de acesso à minha conta. Essa informação é obrigatória. Se essa informação for capturada, minha conta pode ser comprometida. Eu posso ser cobrado novamente, pelo comerciante ou por um dos intermediários, ou por qualquer *hacker* que tenha tirado essa informação de qualquer um dos intermediários. As informações do meu cartão de crédito precisam ser cuidadosamente protegidas.

Desde o momento em que o cartão de crédito sai do meu bolso até que o di-

nheiro esteja na conta do comerciante, ele é transportado pela rede em uma série de carros blindados virtuais. Tem criptografia do ponto de venda ao retorno do comerciante. No retorno do comerciante, é criptografado através da Visa para processamento em lote. Da Visa, é criptografado através do banco de origem para o banco de destino, criptografando esse *token* em cada passo do caminho porque essa chave é secreta. Se a criptografia falhar em qualquer ponto da cadeia, a segurança do meu cartão de crédito é comprometida.

Os dados do cartão de crédito também são armazenados em muitos pontos de trânsito. Ele é armazenado para fins históricos. O que é uma péssima ideia, porque isso cria um tesouro centralizado, um alvo para o ataque de *hackers*. Já vimos isso acontecer repetidamente. Nos EUA, o Target e o Home Depot, dois grandes varejistas, tiveram seus sistemas hakeados, e foram roubados entre 50 e 60 milhões de cartões de crédito. JPMorgan Chase teve 75 milhões das contas comprometidas recentemente. Todas essas coisas não estão acontecendo porque essas empresas são negligentes na proteção dos dados dos cartões de crédito.

> *"Há realmente dois tipos de empresas lá fora: aquelas que não conseguiram tomar as medidas necessárias para garantir os cartões de crédito que você os confiou e aquelas que em breve deixarão de tomar as medidas de segurança necessárias para proteger os cartões de crédito que você os confiou... Os cartões de crédito são quebrados por design porque o token em si é a chave secreta. Se você transmite esse token, expõe sua conta inteira a riscos."*

Existem realmente dois tipos de empresas lá fora: aquelas que não conseguiram tomar as medidas necessárias para garantir a segurança dos cartões de crédito que você os confiou e aquelas que em breve deixarão de tomar as medidas de segurança necessárias para proteger os cartões de crédito que você os confiou. Você também já foi hackeado ou você vai ser hackeado - essas são as duas categorias. Ninguém está imune a isso. Ninguém pode inventar uma maneira de proteger milhões de tokens de acesso seguro contra ataques motivados. É impossível de fazer. Nós não sabemos como fazê-lo. Não há nenhum truque de segurança de informações que possa proteger todos os tipos de possíveis ataques. Cartões de crédito são violados facilmente, porque o *token* em si é a chave secreta. Se você transmite esse *token*, expõe sua conta a riscos.

Transações bitcoin: segurança na estrutura

Bitcoin é fundamentalmente diferente. O que é transmitido não é uma chave, mas simplesmente uma mensagem assinada. É uma autorização. Essa autorização tem duas referências externas: (1) de onde o dinheiro está vindo, fazendo referência a um resultado não gasto na cadeia de blocos; e (2) uma referência para onde eu quero enviar o dinheiro - criando um contrato, uma nova limitação sobre quem pode gastar o dinheiro, geralmente um endereço

de chave pública ou endereço *bitcoin*. Essa transação não contém dados confidenciais. Se você roubar a informação da transação, tudo o que você sabe é de qual endereço veio o dinheiro, para qual endereço o dinheiro está sendo enviado, e quanto. E isso é tudo. A assinatura não revela nada. Os endereços não revelam nada. Não existem identificações pessoais dos fornecedores. Você poderia fazer a transação e imprimi-la. Você pode publicá-la em um *outdoor*. Você poderia gritar do terraço. Uma transação de *bitcoin* pode ser transmitida por um Wi-Fi completamente inseguro. Por sinal de fumaça. Através de um sinal luminoso. Com pombos correio. Não importa. Nada nessa mensagem pode ser comprometido.

> *"Uma transação de bitcoin pode ser transmitida por Wi-Fi completamente inseguro. Por sinal de fumaça. Através de um sinal luminoso. Com pombos. Não importa. Nada nessa mensagem pode ser comprometido."*

O dinheiro como um tipo de conteúdo

A maioria das pessoas não percebe o que significa converter dinheiro em um tipo de conteúdo. Nós tomamos a transação, que é apenas 250 *bytes*, e a separamos do meio de transporte, portanto, não depende de qualquer segurança subjacente. Fazemos com que ele fique sozinho para que ele possa ser verificado por qualquer nó que tenha uma cópia completa do *blockchain*. Uma vez verificado de forma independente como gastável, é autenticado e validado pelo sistema que tem uma cópia completa do *blockchain* - na verdade, até mesmo por sistemas que possuem apenas uma cópia parcial do *blockchain*. Essa transação pode ser verificada em segundos. Tudo o que tem que ser feito é alcançar um nó na rede que possa conversar com os mineradores. E isso é tudo. Uma vez que é injetada na rede *bitcoin*, ela se propaga e você pode ter quase certeza de que a transição será incluída posteriormente e se tornará válida. Se eu olhar para qualquer transação, eu posso calcular se tem taxas suficientes e, então, posso fazer certas premissas sobre como os mineradores vão tratar a transação, porque conheço as regras pelas quais eles operam em uma rede de consenso. Eu sei que uma vez que a transação seja propagada o suficiente, ela aparecerá em um bloco, em breve.

Parar as transações de bitcoin é impossível

Não há nada de mágico em uma transação de *bitcoin*. Vamos pensar sobre isso por um segundo. Como você pode codificar 250 *bytes* e transmiti-los pela rede?

Alguém recentemente me perguntou e eu me perguntei muito: "Os governos tirânicos não podem bloquear ou proibir a transmissão de transações de *bitcoin*?" A resposta é NÃO, mas não acho que as pessoas não entendem bem por que a resposta é não. Vou dar-lhe alguns exemplos teóricos para mostrar

o que quero dizer.

- **Transmitir bitcoin transações via skype como caracteres**

Meu primeiro exemplo é uma codificação das operações de *bitcoin* como combinações de caracteres no *Skype*. O *Skype* possui um alfabeto emoji de 128 caracteres que lhe permite enviar várias carinhas franzidas, sorridentes, polegares para cima, polegares para baixo, dias ensolarados, corações batendo, bolos de aniversário, você sabe, essas variáveis é que possibilitam todos esses tipos de coisas. Agora, vamos olhar para uma perspectiva de conteúdo de informação. Isso é um conjunto de caracteres, certo? Se eu for cientista da computação, vou olhar para isso e dizer, ok, agora tenho um esquema de codificação. Isso permite que eu envie uma transação de 250 *bytes* em cerca de 500 caracteres. 500 sorrisos. Uma transação de *bitcoin* em caracteres.

Posso literalmente escrever um pequeno *script* matematicamente, isso daria provavelmente duas linhas de Python. Se você é realmente eficiente, em uma só linha. Não foram necessárias bibliotecas. No roteiro criptográfico, posso usar uma representação hexadecimal de uma transação de *bitcoin* e codificá-la em *emoticons*. Então, eu posso copiar na janela do *Skype* em qualquer lugar no mundo. Enquanto o destinatário que recebe essa série de *smiles* digita-o em um *script* de decodificador e, em seguida, simplesmente o injeta na rede *bitcoin*, essa transação acontecerá. O destinatário pode ser um robô. O destinatário pode ser uma estação de escuta automatizada que é projetada para decodificar os caracteres em transações e transmiti-las para a rede *bitcoin*.

Agora, explique-me como alguém pode fazer isso parar, sem desligar o *Skype*. Se fecharem o *Skype*, use o Facebook. Se fecharem o Facebook, você usará Craigslist. Se fecharem a Craigslist, vou colocar minha transação em uma postagem no TripAdvisor. Se fecharem o TripAdvisor, eu publicarei como um comentário numa história dentro de um artigo da Wikipédia. Se fecharem, vou postar isso como pano de fundo de uma imagem JPEG nas minhas fotos de férias.

> *"O dinheiro agora é conteúdo de informação completamente desconectado."*

O dinheiro agora é conteúdo de informação completamente desconectado. Não há nada que você possa fazer para impedir as informações de viajarem de qualquer lugar do mundo para qualquer lugar do mundo, quando você tem uma abundância de mecanismos de comunicação multimídia totalmente interligadas como temos hoje.

- **Transmitir transações bitcoin via rádio de ondas curtas**

Digamos que não tivéssemos a internet. Inventei um plano maluco e ridículo, que é uma transmissão de transações de *bitcoin* via rádio de ondas curtas, frequência-*hopping*, explosão. Isso seria usado ao estilo dos guerrilheiros.

Durante a Segunda Guerra Mundial, na França ocupada, os Aliados lançaram milhares de rádios de ondas curtas - *kits* completos com pequenos paraquedas - dos aviões, de modo que os partidários pudessem escondê-los em celeiros, nas escavações de árvores, em edifícios abandonados, sob pontes e usá-los para se comunicar com vários centros de comando aliados em toda a Europa, bem debaixo do nariz das forças nazistas ocupantes. Uma das coisas sobre o rádio de ondas curtas: ele não só tem enorme alcance, mas você pode também, em determinadas frequências, ricochetear a mensagem na estratosfera. Na época, eles usaram isso para comunicação de voz, comunicação de números codificados, código Morse usando vários esquemas de criptografia de maneira única.

Hoje, posso obter um *kit* que me permite conectar um transmissor de rádio de ondas curtas muito simples ao meu *laptop* via USB. Agora tudo o que preciso é de uma antena. O legal é que – para usar um rádio de ondas curtas – uma antena consiste, simplesmente, em um metal suficientemente longo,- uma linha ferroviária, um varal metálico de roupa, um fio elétrico quebrado, um fio de cerca de arame farpado. Já reparei que aqui na Nova Zelândia, vocês têm muitos. Há cercados de ovelhas por toda a parte.

Agora, a transmissão de uma transação de *bitcoin* envolve a conexão de um *laptop*; anexando-a a um poste de vedação, pressionando "*enter*" e transmitindo uma transação explosiva. Em 25 segundos já há uma estação receptora em algum lugar com um raio de milhares de milhas e conectado à rede *bitcoin*. Você pode ocultar uma estação receptora onde você quiser, um ouvinte passivo não pode ser triangulado, e esse dispositivo de escuta injeta a transação para a rede. Se eu sou guerrilheiro e quero comprar algo, eu construo a transação *off-line*, e quando estiver pronta, saio para o meio do campo, conecto meu transmissor em um varal metálico, pressiono "*enter*", transmito-a por 25 segundos, guardo minhas coisas e desapareço na floresta. Como é que paramos isso? Ninguém para isso. Essa é uma resposta simples, ninguém. Mas isso é só o começo.

Separando o meio da mensagem

Uma vez que você percebe que o dinheiro se tornou um tipo de conteúdo, essas transações desconectadas do meio criam algumas características secundárias realmente importantes. Você vê que o meio é uma mensagem, como alguém disse uma vez. A razão principal pela qual o meio é uma men-

sagem é porque o meio comprime, transforma e, em muitos casos, distorce a mensagem.

Quando o meio é TV, a mensagem tem 18 minutos de duração, depois é interrompida por espaços publicitários. Essa é a mensagem. Não há nenhum outro formato que você possa encaixar lá. Então, você faz uma mensagem que se adapta a esse meio. E você começa a atribuir o valor de sua mensagem numa medida equivalente aos custos de produção. TV, por exemplo, impõe um determinado custo para produção de vídeo. As pessoas que estão nesse negócio fazem a suposição equivocada de que o custo de produção de TV é o mesmo que o valor desse *show*. Quanto mais você gastar, mais valioso ele será.

Você pode imaginar o susto quando aparece algo como YouTube que reduz os custos de produção para zero. Qual a suposição imediata que as pessoas dessa indústria fazem? Se o custo é zero, o conteúdo deve ser inútil. Esse é um mal-entendido fundamental sobre o que acontece quando você separa o conteúdo do meio. Separando a mensagem do meio, a percepção de valor desloca-se do custo de produção para o valor real que tem para o consumidor final quando eles consomem o conteúdo.

> *"Quando o custo da impressão são valores astronômicos e os meios de impressão estão disponíveis apenas para alguns selecionados, o único que você imprime é a Bíblia de Gutenberg."*

Deixe-me dar-lhes um exemplo ainda mais antigo. "Quando o custo de impressão são valores astronômicos e os meios de impressão estão disponíveis apenas para alguns selecionados, o único que você imprime é uma Bíblia de Gutenberg". O meio define o alcance da expressão da mensagem e restringe-a apenas às mensagens grandiosas e mais importantes que a sociedade terá. O meio limita o alcance da expressão impondo enormes custos de produção.

O que você acha que Gutenberg pensaria do Twitter, que leva o custo de produção a zero, tornando tudo disponível universalmente, para todos e gratuitamente. Você vai da impressão da Bíblia de Gutenberg para a resposta de um *tweet* com uma de minhas expressões favoritas, uma opinião de três caracteres, "BMC", que significa “Balançando Minha Cabeça". "Quando ‘Professor Bitcorn’ diz que, "o *bitcoin* vai a zero," eu posso expressar toda minha gama de opiniões e análises ponderadas como, balançando a cabeça com a mão na face. Uso três caracteres e expresso minha opinião para o mundo. Se você olhar para isso de uma perspectiva objetiva, certamente, essa mensagem é inútil. Quando você parte da premissa equivocada de que se o custo de produção for zero, e a mensagem aparentar ser trivial, então a combinação inteira de meio e mensagem deve ser inútil, trivial, e não ter nenhum valor - é um erro que as pessoas costumam cometer em momentos de mudanças de era.

Quando o Twitter surgiu, as pessoas acharam que seria usado apenas para

o trivial. E ainda um ano atrás, eu estava assistindo à CNN International cobrindo a revolução egípcia, e eram transmissões ao vivo de tweets de revolucionários egípcios nas ruas do Cairo, dando vida à reportagem que estava acontecendo minuto a minuto. E os âncoras da CNN não estavam fazendo nada. Estavam apontando para a tela e dizendo: "Olha, temos outro *tweet*.". E aqui outro *tweet* de alguém que não conhecemos. Aqui outro *tweet*. "Eles foram reduzidos ao papel de um modelo de programa de televisão dizendo: "E aqui um maravilhoso refrigerador que será seu se você acertar o prêmio atrás da porta número 1." Eu acho isso extremamente gratificante ao assistir a esses tagarelas, como Anderson Cooper, basicamente reduzido a um leitor de tweets da tela.

Por que tiravam sarro dele. Eles erraram em assumir que se o custo da produção é zero, o valor da mensagem é zero. Confundiram o meio para a mensagem. Eles fizeram o erro de assumir que seu controle sobre o meio foi a fonte de qualidade. E muito depois que a qualidade desapareceu, agarraram-se ao controle e pensaram que o controle seria a única maneira de alcançar qualidade, e se você removesse controle, você removeria qualidade. Isso é o fétido e desmascarado elitismo em seu pior absoluto. Isso assume que os porteiros são fonte de qualidade quando são apenas porteiros. Eles assumem que o fato de eles possuírem o meio mais caro significa que essa é a mensagem que vale a pena ouvir.

> *"Eles erraram em assumir que se o custo da produção é zero, o valor da mensagem é zero. Confundiram o meio para a mensagem. Eles fizeram o erro de assumir que seu controle sobre o meio foi a fonte de qualidade. E muito depois que a qualidade desapareceu, agarraram-se ao controle..."*

No momento em que você rasga essa mensagem longe do meio e você a abre para toda uma gama de expressão, sim, expressará as mensagens mais triviais de sua cultura, incluindo "SMH". Mas também expressará as mensagens mais interessantes de sua cultura, eventualmente.

Hoje nas escolas americanas, as crianças leem O Jornal Federalista, que é uma coleção de ensaios públicos escritos no século 18 por algum dos pais fundadores debatendo o significado de uma democracia para a nova república. Em 100 anos, as pessoas estarão lendo Os Tweets Federalistas da Revolução do Cairo. Essa não é uma ideia insana. Esse é o caminho da civilização humana. Nós já vimos isso acontecer uma e outra vez.

Agora eles zombam do Twitter como trivial por que eles não entendem a distinção entre mensagem e meio. A televisão já foi ridicularizada como um passatempo trivial por que ela obscurecia a arte da cinematografia. Cinematografia foi um passatempo trivial por que banalizou e vulgarizou a arte do teatro. O teatro foi um passatempo vulgar e banal dos vitorianos por que banalizou as grandes peças dramáticas dos romanos e antigos gregos. Continue por

esse caminho que você eventualmente chegará até Aristóteles dizendo que a filosofia está morta por que hoje em dia as crianças todas querem assistir a apresentações dramáticas no lugar de ler seus livros de filosofia. Ele provavelmente irá reclamar sobre seus cabelos compridos também. Toda geração confunde o meio com o conteúdo e considera a renovação desses meios - que ampliam acesso e disponibilidade, que estendem a gama de expressão - como triviais, vulgares, depreciadores da mensagem.

> *"Toda geração confunde o meio com o conteúdo e considera a renovação desses meios - que ampliam acesso e disponibilidade, que estendem a gama de expressão - como triviais, vulgares, depreciadores da mensagem."*

Eles não entendem que quando você banaliza o meio, isso liberta a mensagem e a eleva. Agora é possível expressar uma vasta gama de mensagens. Sim, as primeiras serão triviais e a razão disso é que as mídias preexistentes não permitiam essa expressão. Elas não estavam habilitadas para essa expressão. Sim, temos memes. Mas também tweets ao vivo sobre a revolução do Cairo. Com o tempo, eles descobrirão que nova mídia é a qualidade da mensagem. Então, poderemos virar e chamar a próxima mídia de vulgar e banal.

O dinheiro é a mensagem, agora liberado do meio

Dinheiro é um tipo de conteúdo, e só o arrancamos do meio. O meio tem sido uma série de redes interconectadas que segregam o dinheiro pelo tamanho e pelo destinatário. Temos redes de pagamento para quantias pequenas de dinheiro. Temos redes de pagamento para quantias grandes de dinheiro. Temos redes de pagamento para dinheiro rápido. Temos redes de pagamento para dinheiro lento. Redes de pagamento para as empresas pagarem as empresas. Redes de pagamento para os governos pagarem os governos. Redes de pagamento para os consumidores pagarem as empresas. Redes de pagamento para os consumidores pagarem os consumidores. Oh. espere, na realidade não temos. Não temos redes de pagamento para os consumidores pagarem outros consumidores. Não temos redes de pagamento para fazer pequenos pagamentos porque o meio tradicional não permite esse intervalo de expressão.

> *"O dinheiro é um tipo de conteúdo, e acabamos de liberá-lo do meio".*

Não posso enviar 20 centavos em todo o mundo, de um indivíduo para outro, porque o meio restringe a mensagem. O custo de produção não permite expressar essa transação. Mas agora, temos a mensagem separada do meio. Criamos dinheiro como um tipo de conteúdo. Esse dinheiro agora é capaz, perto de zero custo de produção, de expressar toda a gama de expressões transacionais — desde o minúsculo para o enorme, de consumidor a consumidor, de governo para governo.

O que acontece a seguir? Os *gatekeepers* lhe dizem que essa rede não é séria. Eles confundem o baixo custo dessa rede de pagamentos com o valor do seu serviço e vão te dizer que essa nova forma de pagamento é vulgar e barata. Que é algo usado somente para trivialidades. Todas as pessoas sérias vão permanecer na rede de pagamento do passado, sólida e de qualidade. Porque se eles conseguem controlar e restringir a gama de expressões possíveis, eles acham que isso significa qualidade. Não é verdade. É apenas um custo de produção inflado. Trata-se de puro elitismo, no seu pior. Eles se prendem ao meio e não conseguem ver que agora a mensagem pode ser transportada independente de qualquer meio a um custo zero e instantaneamente.

Qual é o primeiro uso desse novo modelo? Qual é o primeiro uso desse novo meio de enviar mensagem? Agora nós podemos enviar pagamentos triviais. Eu pego dicas no Twitter. Essa é uma demonstração que eu posso fazer que claramente mostra às pessoas a diferença. Eu posso fazer algo que não podia antes. Mas, para muitas pessoas isso é trivial. Para muitas pessoas, quando eu mostro a parte mínima da gama de expressões, simplesmente reforço a ideia de que se trata de um meio vulgar e ordinário. O que elas não conseguem entender é que esse meio não é apenas para o trivial; ele alcança uma variedade inteira de transações, das mais modestas às enormes.

> *"O blockchain pode englobar uma inteira gama de transações, de um twitter de 10 centavos a uma venda a débito de 100 bilhões."*

Um dia, os países vão comprar petróleo com *blockchain*. Um dia, companhias multinacionais serão compradas através do *blockchain*. Um dia, você poderá vender um porta-aviões pelo *blockchain*. O *blockchain* pode englobar uma gama inteira de transações, de um twitter de 10 centavos a uma venda a débito de 100 bilhões. Nós apenas não percebemos ainda. Isso pode ser feito sem qualquer limitação imposta pelo meio. Isso não se deve apenas ao fato de que essas transações, como conteúdo, podem ser transportadas por meio de um *smiley* no *Skype*. Trata-se de um simples sintoma do fato de que nós estamos nos libertando das limitações dos meios de transporte comuns. Nós criamos o reino do conteúdo.

Grande arco da tecnologia

Quando o conteúdo começou a ser domínio da exclusividade, elitismo e do acesso limitado, foi usado por grandes mestres para criar obras primas. A Bíblia de Gutemberg. As primeiras fotografias. O pouso na Lua, televisionado pela primeira vez. Os grandes filmes do passado. Obras primas criadas por grandes mestres.

Então, o meio muda porque a tecnologia o torna mais acessível. Pessoas começam a usá-la para uma grande variedade de expressões, mas os porteiros

(guardiões) ainda se agarram às ideias velhas. Eles ainda tentam fazer coisas grandiosas com esses meios. Eles imprimem livros pesados em couro e capa dura. Então os meios expandem novamente e as coisas passam a ser em capa mole e fotografias se tornam acessíveis no dia a dia das pessoas em 24 poses. Os guardiões do passado ainda se agarram ao velho, mas agora não podem mais fingir que isso é grandioso, então eles apenas fazem grandeza. Eles dizem: "Há um certo *jene sais quoi* para filmar." "Há uma certa qualidade para o vinil que os CDs nunca capturarão." "Uma âncora de TV realmente tem autoridade. Você se lembra do Walter Cronkite? "Um jornal é a fonte de opinião oficial, e o seu valor está no papel onde é impressa." Arrogantemente. A grandiosidade se foi. A qualidade se foi. Agora é uma questão de se agarrar ao controle e fingir que isso ainda significa qualidade.

Finalmente, em seu grande arco, a tecnologia atinge o estágio final. No estágio final, as únicas pessoas que acreditam em coisas grandiosas são os avós. No grande arco da tecnologia, o que começou como obra-prima, agora é consumido apenas por aqueles em sua última etapa de vida. Os primeiros cheques escritos no passado foram usados pela realeza para financiar grandes aventuras, como a Companhia das Índias para abrir a rota das especiarias e o comércio com o leste. Naquele tempo, somente a realeza tinha talões de cheque. Hoje, se você está em um supermercado e a vovó na fila a sua frente, deus a proteja, abre a sua bolsinha e tira um talão de cheques, 15 pessoas na fila vão reclamar audivelmente, pois percebem que essa transação demorará, no mínimo, 15 minutos. Nada da grandiosidade que havia ao financiar a Companhia das Índias permanece quando você paga feijões e torradas com um talão de cheques no supermercado. É o estágio final.

As únicas pessoas que ainda assistem Fox News são vovôs, pois nós todos lemos nossas notícias na internet. O que já foi trivial é agora nossa fonte confiável de notícias e informações. Você não poderá explicar isso aos velhos guardiões do passado. Nós lemos nossos livros digitalmente. Algumas pessoas vão dizer: "Existe algo especial em sentir o papel." Sim. É muito pesado carregar 20 livros em uma mala, e eu leio essa quantidade em quatro ou cinco semanas, então eu preciso carregar. Não existe nada sobre sentir papel, isso é se agarrar ao passado.

> *"Enquanto nos mudamos para esse mundo onde o dinheiro é uma forma de conteúdo, os guardiões do velho sistema de pagamentos vão se agarrar à ilusão de que os bancos tradicionais são a qualidade. Que eles próprios são a qualidade. Mas não é aí que a qualidade está."*

Enquanto nós nos mudamos para esse mundo onde o dinheiro é uma forma de conteúdo, os guardiões do velho sistema de pagamentos vão se agarrar à ilusão de que os bancos tradicionais são a qualidade. Que eles próprios são a qualidade. Que qualidade é inerente ao controle à censura, às limitações. Mas não é aí que a qualidade está. Nós estamos seguindo em frente e abrindo

a gama de expressões possíveis com dinheiro para níveis inimagináveis, permitindo coisas que nunca aconteceram antes. Eles seguirão agarrados a suas ideias de grandiosidade: os velhos grandes bancos com tetos abobadados e cofres cromados que estarão vazios, onde um dia poderemos fazer visitas guiadas aos domingos para ver como os bancos costumavam ser. Poderemos rodar o mundo, e os grandes cofres dos velhos bancos, agora, serão bares onde se pode tomar um coquetel, porque os bancos não conseguirão mais manter seus prédios. Eles não servem para nada além de grandiosidade. Eles ainda tentarão persuadi-lo de que, sob seu controle, o protegerão do mal, dos terroristas, dos lavadores de dinheiro. Tudo que eles fazem é proteger sua posição na competição.

Nós agora separamos a mensagem do meio. Dinheiro agora é uma forma de conteúdo e isso não vai voltar atrás.

Obrigado.

Nota do Andreas: *Nessa conversa eu tentei me aventurar totalmente a improvisar matemática enquanto falava. Eu não sou bom em matemática. E eu consigo ser pior improvisando matemática. A matemática ruim não invalida os pontos que mencionei, mas isso deve ser editado e apurado para proteger meu ego. ssssh! :)! Não diga a ninguém que eu sugiro improvisar matemática.*

ELEMENTOS DE CONFIANÇA: LIBERANDO A CRIATIVIDADE

Encontro Blockchain; Berlin, Alemanha; março 2016

Link do vídeo: https://www.youtube.com/watch?v=uLpSM3HWU6U

Hoje, eu vou falar da química do dinheiro, especificamente da química do *bitcoin*. Esse é um dos aspectos que faz o *bitcoin* ser tão excitante e tão interessante. É o que a maioria de nós nem sequer percebe quando estuda *bitcoin* por um ano ou dois.

O *bitcoin* é como uma cebola. Você tem que desembrulhá-lo. Conforme você o desembrulha, você encontra mais uma camada. Eu comecei cinco anos atrás. Estou ainda descascando. Estou encontrando mais e mais coisas que me surpreendem todos os dias sobre *bitcoin*.

A ilusão de remetentes, receptores e contas

Quando eu encontrei o *bitcoin* pela primeira vez, fiquei surpreso por ver que isso parecia muito com um sistema bancário familiar. Visitei sites bem conhecidos de *bitcoin*, como o *blockchain*.info, e pude ver as transações. Eu cliquei sobre as transações e pude ver um remetente, um receptor e uma conta. Eu pensei, isso é bastante familiar. Operações bancárias. Ótimo. Então, eu decidi ver o código fonte e ver como isso funcionava.

Como um cientista da computação, eu imaginei que se leria o código-fonte, e tentaria entender como o sistema fazia essas coisas, mas, quando eu pesquisei o código fonte para remetente, receptor e contas, não encontrei nada. Porque nenhuma dessas coisas, na verdade, existem no *bitcoin*. Isso realmente me surpreendeu porque, quando eu olhei o código fonte, nada dessas coisas que eu esperava achar estavam realmente lá. Você esperaria que um sistema bancário, como parecia ser, tinha sido projetado para fazer certas coisas de formas muito específicas. *Bitcoin* não é assim. Não é assim de jeito nenhum.

> *"Quando eu pesquisei o código-fonte para remetente, receptor ou contas, eu não achei nada. Porque nenhuma dessas coisas realmente existem no bitcoin."*

Quantos de vocês olharam no código-fonte ou entenderam os fundamentos

técnicos? Poucas pessoas nesta sala. Quando você escava o código, você não encontra nenhum saldo, nenhum remetente, mas há UTXO saídas de transações não utilizadas, e existem entradas.

Mas aquelas entradas não correspondem realmente aos remetentes. E a transação tem saídas, que realmente não correspondem aos receptores. De repente, você percebe que o que você está olhando é quase essa natureza quântica ou atômica do *bitcoin*.

Estrutura atômica do bitcoin

Em química, temos elementos como cobre, ferro e hélio. A química oferece essa enorme complexidade de coisas que você pode combinar para fazer coisas interessantes. Como pessoas. E torradeiras. Mas quando você aprofunda na química, você percebe que cobre não é uma coisa. O cobre é um padrão de prótons, nêutrons e elétrons. Não existe cobre. Um próton é exatamente como outro próton; ele pode ser tão feliz como parte de um hélio ou de um cobre, ele não se importa. Não há nada sobre aquele próton específico que o torne parte do cobre.

Química é uma camada, mas abaixo disso há física atômica. Essa camada é muito simples. Tem um punhado de elementos. Este punhado de poucos elementos torna-se tudo o que sabemos de química, um pouco mais de 100 elementos na natureza que possuem propriedades diferentes e únicas, que são completamente diferentes. Alguns deles são líquidos, alguns deles são metais, alguns deles são gases. Eles se comportam diferentemente. Alguns são ácidos, outros não são. Mas nada disso é a composição básica. Estes são apenas padrões.

Bitcoin tem essa estrutura fundamental atômica, essa estrutura elemental. Os elementos de *bitcoin* são componentes de transações e os elementos de linguagem de programação. Esses elementos não têm nada a ver com as operações de banco tradicional. Não existe conta ou saldos, ou remetentes e receptores. Em vez disso, os elementos básicos do *bitcoin* estão procurando por propriedades matemáticas fundamentais e propriedades criptografadas -- como um *hash* que é igual a outro *hash*, como uma assinatura de curva elíptica que corresponde a outra assinatura de curva elíptica, manipulação de números, etc., etc. O que você vê na superfície -- as transações -- são somente conceitos. Eles são uma maneira específica de triturar os elementos que criam algo que se parece com um banco. O que é ótimo porque, se você é novo ao *bitcoin* e alguém lhe diz, "Bem, há uma conta, um remetente e um receptor", você pensa: Ok, eu entendo isso.

> *"O que você vê na superfície -- as transações -- são somente conceitos. Eles são uma maneira específica de triturar os elementos que criam algo que se parece com um banco."*

Depois você aprende que você tem uma carteira, mas sua carteira não tem moedas, e sim chaves, e essas chaves podem ser copiadas, e agora você está pensando: "Não estou acompanhando". Isso não combina com minha experiência. As coisas se complicam porque o *bitcoin* não é o que você pensa que é. É uma plataforma. Não é um sistema de pagamentos. Não é uma moeda. Não é um sistema bancário. É uma plataforma que garante certas funções de confiança. Se acontecer de você ter uma plataforma que garante certas funções de confiança, uma aplicação muito útil para construir uma moeda e uma rede de pagamento, você pode construir mais coisas.

> *"Bitcoin não é o que você pensa que é. É uma plataforma. Não é um sistema de pagamento. Não é uma moeda. Não é um sistema bancário. É uma plataforma que garante certas funções de confiança."*

• Blocos de lego

Quando eu era criança, meu brinquedo favorito era Lego. A razão de ser meu brinquedo favorito não foi por causa do que estava na caixa. Porque eu não construí o que estava na caixa. Se na caixa tinha um caminhão de bombeiros vermelho, eu construiria um dragão, ou um hipopótamo-girafa, alguma coisa que não existia ou alguma ideia que eu tivesse. Era por isso que eu gostava. Eu poderia pegar esses blocos de construção básicos e poderia construir o que eu quisesse.

De uma perspectiva abstrata, Lego é uma bagunça. E a coisa que eu construí não parecia muito com um caminhão de bombeiro ou uma nave espacial. Se alguém tivesse me dado um brinquedo que era um caminhão de bombeiros, com plástico injetado, bordas suaves, um caminhão de bombeiros vermelho completo, seria o caminhão perfeito. Mas só poderia ser um caminhão de bombeiros, e depois de 20 minutos de brincadeira eu já estaria entediado. Porque meu suave, arredondado caminhão é somente um caminhão de bombeiros, é um caminhão de bombeiro perfeito. Mas nunca seria um hipopótamo-girafa ou um tomate ou uma nave espacial. Mas o Lego permite mais.

• Blocos de cozinha

Conforme eu fui crescendo, eu comecei a cozinhar como um *hobby*. O que eu amei sobre a culinária é que é a combinação perfeita da arte e da ciência. É de entendimento fundamental de como os ingredientes funcionam, como eles se comportam, como a química muda quando eles são combinados ou quando se adiciona um catalisador como sal ou quando você aplica calor sobre eles, o que você pode criar. Você pode criar praticamente qualquer coisa. Contanto que você entenda como os ingredientes trabalham, você pode executar e entregar qualquer coisa que deseja criar.

• Blocos de criatividade

O *bitcoin* engloba aquela natureza elementar. Não lhe dá um resultado final. Oferece um conjunto de ingredientes e uma receita. Oferece um conjunto de blocos de Lego e uma foto na caixa que se parece com um caminhão de bombeiros vermelho. Quando apresentamos isso ao mundo, as empresas financeiras olham e dizem, "Bom, seu caminhão de bombeiros tem bordas afiadas e é feito de pequenos blocos idiotas. Em *bitcoin*, pegamos os ingredientes, os colocamos juntos e fazemos um sistema de pagamento bancário. O banco olha para isso como se estivesse dizendo para nós: "Seu hambúrguer está ok, mas no McDonald's podemos fazê-lo em 45 segundos e podemos vender bilhões deles.". Então, porque nós precisaríamos de um *chef*, de ingredientes, de uma receita, se simplesmente podemos produzir 1 bilhão deles?" Eles não estão vendo um ponto.

> *"Bitcoin engloba aquela natureza elementar. Não lhe dá um resultado final. Dá-lhe um conjunto de ingredientes e uma receita."*

O ponto não é gerar bilhões de cópias do mesmo produto inferior. O ponto não é obter o caminhão vermelho de plástico moldado por injeção do qual vou ficar entediado em 5 segundos. O ponto é liberar minha criatividade, dando-me as ferramentas e os elementos de que preciso para construir algo único.

Eu não construí um hambúrguer mais rápido ou mais barato que o McDonald's, e meu caminhão de bombeiros não é mais suave que a cópia moldada. Mas posso fazer almôndegas com molho de tomate vermelho. Também posso fazer um hipopótamo-girafa. Você não pode fazer isso com um brinquedo pré-fabricado. Você não pode fazer isso na cozinha do McDonald's. Eu liberei minha criatividade.

• Blocos de bitcoin

Nós estamos começando a ver pessoas entenderem que o *bitcoin* é um conjunto de ingredientes e você tem uma receita, mas você pode fazer diferentes receitas. Pessoas estão agora tentando combinar esses ingredientes.

Nós estamos construindo projetos de *crowdfunding* por combinar transações atômicas com somas de entrada versus saídas e assinaturas digitais. Ao combinar esses ingredientes, podemos criar uma transação única que pode ser financiada por várias pessoas, mas a transação só será válida se o limite de financiamento for cumprido. Esses são os mesmos elementos que eu uso para fazer um pagamento de um dólar para você através da rede de pagamento do *bitcoin*, mas você pode recombiná-los de forma diferente, e agora você tem uma plataforma *crowdfunding*.

Estamos criando canais de pagamento combinando assinaturas de 2 de 2, multi-assinaturas, com tempo de bloqueio de transação. Isso nos permite cobrar por *streaming* de vídeo a cada segundo. Essa é uma receita totalmente nova.

Estamos trabalhando em canais de pagamentos. Levando-os e adicionando um novo ingrediente, contratos bloqueados por tempo *Hash*, nós podemos conectar múltiplos canais juntos. Então, temos uma rede relâmpago, e uma nova receita que ninguém havia visto antes.

> *"Estamos tentando liberar a criatividade de uma geração inteira. Estamos construindo um sistema, onde mais de mil aplicativos que requeiram a confiança possam ser construídos."*

Os bancos não estão dizendo: "Seu caminhão tem quinas afiadas e seu hambúrguer é tão caro e leva mais de 45 segundos." O que eles estão realmente dizendo é: "Suas taxas de transações são tão altas e vocês são tão lentos que possivelmente não conseguirão produzir em escala." Falta um ponto. O ponto é que não estamos tentando vender um bilhão de hambúrgueres a cada 45 segundos; estamos tentando liberar a criatividade de uma geração inteira. Estamos construindo um sistema onde mais de mil aplicativos que requeiram a confiança possam ser construídos.

Economias de grupo focal

Quando você tem os ingredientes, quando você tem esses elementos básicos, a receita que você constrói depende inteiramente de você. Porque, quando eles construíram o pequeno caminhão de bombeiro vermelho, eles poderiam construir uma fábrica inteira somente para fazer pequenos caminhões de bombeiro vermelhos. Estou certo de que eles irão lhe dizer: "Ouça, nossas estatísticas dizem que 95% das crianças querem um caminhão de bombeiro vermelho. Nós testamos com grupos focais e equipes de *marketing*. Nós podemos produzi-los aos milhões. Eles custam apenas 3 centavos. Eles têm uma pequena parcela de tinta de chumbo, e hidrocarbonetos cancerígenos tóxicos e venenosos, mas não é um problema. Nós podemos fazer isso bem barato e lucrativo." E eles só podem construir caminhões de bombeiro.

Quando você constrói uma cozinha como o McDonald's, você pode produzir hambúrguer a cada 45 segundos, mas você não pode fazer almôndegas. Você não pode fazer nada além disso. Você é aperfeiçoado para fazer uma coisa e uma única coisa e, enquanto isso servir a sua linha de lucro, está tudo bem. Porque estou certo de que você testou em um grupo-alvo para ter certeza de que é o que todos querem.

Esta é uma péssima maneira de construir uma economia. Esta é uma péssima maneira de construir um sistema financeiro. Esta é uma péssima maneira de construir uma rede de pagamentos.

Privilégio bancário e vigilância

Efetivamente, o que os bancos estão nos dizendo é: "Nós nos concentramos em testar isso. O que as pessoas querem é a habilidade, em vez de passar o cartão Visa delas, para digitar algo no leitor, economizando quase dois segundos e reduzindo o esforço em pelo menos quatro calorias. Eu quero dizer, nós poderíamos lidar com 4 bilhões de pessoas que não têm acesso ao banco ou à água limpa. Nós poderíamos lidar com o fato de que o nosso mundo é uma bagunça fragmentada, onde a grande maioria da humanidade não tem acesso aos serviços financeiros. Ou, nós poderíamos reduzir os esforços dos compradores e transformar o cartão em um cartão flutuante.

Nós poderíamos encarar o fato de que a razão para mais de 4 bilhões de pessoas não terem banco é porque nós necessitamos que cada um se identifique em cada lado em todas as transações, então podemos construir um sistema de vigilância total que causaria inveja à Stasi, para monitorar cada transação financeira em cada canto do planeta. Por que nós convencemos a nós mesmos de que nosso senso burguês de segurança nos protegerá, não por resolver a pobreza, não por reduzir, talvez, o bombardeio de outros países, mas, em vez disso, por vigiar a todos todo o tempo quando compram um hambúrguer - por via das dúvidas.

Nós poderíamos submeter-nos a esse mecanismo que agora simplifica a si mesmo, e como uma fábrica que somente produz pequenos caminhões de bombeiro vermelhos, este é um sistema que só pode entregar serviços financeiros para uma pequena faixa da elite da população mundial, com vigilância totalitária atrelada a regulações em cada país, com barreiras nas fronteiras não permitindo comércio internacional. O sistema financeiro onde o governo pode aplicar pressão para que você pare de negociar com o WikiLeaks, só porque não gostam deles, mas você ainda pode mandar doações ao Ku Klux Klan - e isso não é uma piada. É exatamente o que aconteceu.

Eles construíram um sistema que só pode fazer uma coisa: nos escravizar. Que só pode fazer uma coisa: empobrecer-nos. Um sistema que remove a liberdade da maneira mais eficiente possível para gerar lucros. O sistema está quebrado, e isso não se adapta. Mas se é isso o que você está tentando fazer, é o mais eficiente que você já viu.

Por comparação, o pequeno e louco sistema de mistura que construímos com o *bitcoin*, que é errado, que é devagar e que não pode ser escalonável, é ineficiente e não é tão sério e sofisticado como os sistemas bancários internacionais, mas oferece liberdade e permite liberar a criatividade.

Muito obrigado.

ESCALABILIDADE DO BITCOIN

Bitcoin Meetup em Paralelni Polis; Praga; Tcheca; março 2016

Link do vídeo: https://www.youtube.com/watch?v=bFOFqNKKns0

Histórias de escalabilidade

Hoje, eu vou falar sobre a escalabilidade. Muitos de vocês provavelmente notaram que há um debate muito interessante sobre como o *bitcoin* é escalável. Esse é o tema que eu quero abordar, não de uma perspectiva técnica, mas de uma perspectiva mais ampla, para tentar entender o que significa escalar.

• Usenet (a utilização da rede) vai destruir a internet

Reúnam-se e falaremos sobre muito tempo atrás. Em 1989, a internet era discada. Não apenas uma conexão entre usuários de internet; na maioria dos casos, os *backbones* de internet eram discados. Entre as universidades, entre as estações de pesquisa, haviam algumas conexões permanentes de alta velocidade - 256 *kbits*, 512 *kbits*. Mas a internet era principalmente à rede discada. O correio eletrônico, *e-mail*, ainda não tinha se estabelecido, mas havia um lugar especial na internet chamado Usenet. Usenet era um sistema de grupos de discussão onde você podia publicar uma mensagem de texto, outras pessoas a veriam e então responderiam.

Não se tratava de mensagens instantâneas. Era uma comunicação lenta porque, para que o Usenet funcionasse, todas as mensagens dependiam de uma transmissão através de um sistema de acesso telefônico e eram propagadas de um nó para outro, em um sistema chamado *store and forward* - ou "armazene e encaminhe". Você publicaria uma mensagem e ela levaria entre 24 e 48 horas para chegar a todos. Então, eles poderiam responder, e levaria outras 24 a 48 horas para que você pudesse ver as respostas. Hoje, compararíamos isso com a tentativa de estabelecer comunicação com Matt Damon em Marte, como no filme *The Martian*.

Naquele momento, havia uma grande discussão entre os engenheiros da internet, porque Usenet estava ficando muito popular e seu uso estava se tornando grande. *Kilobytes* e depois *megabytes* de informações de texto precisavam ser transmitidas. Inicialmente, levaríamos cerca de 30 minutos em uma conexão discada para obter as mensagens do Usenet de um só dia.

Então, com a popularidade crescente do sistema, mais mensagens se convertiam em mais dados e mais tempo. Logo, passou a demorar uma hora, duas horas e três horas. E os especialistas previram o fim. Eles diziam que, se você traçar um ponto onde estamos hoje e um ponto seis meses à frente e conectá-los em uma linha, em breve, levará 26 horas para transmitir as mensagens de um só dia e isso é um enorme problema, porque só temos 24 horas.

O que acontece então? A internet entrará em colapso! Claramente, não pode escalar. Não será possível escalar.

- **Grupos alt irão destruir a internet**

Na época, haviam duas partes para a Usenet. Havia a parte regular da Usenet, estruturada para grupos de discussões acadêmicas, e uma outra pequena parte da Usenet chamada "The Alt", usada por grupos alternativos. O *alt* era opcional. Como um provedor Usenet, você poderia carregar o uso *alt*, se você quisesse oferecer essa opção. Os provedores realmente interessantes ofereceram uma opção aos grupos *alt*. Claro, todas as coisas interessantes surgiam nos grupos *alt*: alguns dos primeiros grupos eram surpreendentes, alt.folklore.computers, alt.security, e claro, como tudo o que se desenvolve em escala na internet, alt.sex.

E esses grupos alternativos, sendo opcional, se tornaram o foco do grande debate. Nós deveríamos alimentá-los? E, nesse momento, começamos a ver o primeiro spam do mundo. Lembro-me de ter recebido o primeiro spam. Era uma mensagem enviada por dois advogados e que era postada em todos os grupos de Usenet. Você não fez isso. E isso não foi legal. Milhares de pessoas disseram-lhes que não foi legal. Essa foi uma primeira reação em massa via internet.

A discussão era, nós permitiremos os grupos *alt*? Porque se nós permitirmos os grupos *alt*, a internet certamente irá derreter e não haverá possibilidade alguma de ganhar escala. Se isso se tornar popular, as pessoas vão discutir mais, e se elas discutirem mais, não teremos capacidade suficiente para lidar com essa quantidade de dados. Essa conversa durou mais de dois anos. Havia alguns provedores de serviço corajosos que mantiveram os grupos *alt*, usando grandes unidades de disco rígido - discos rígidos enormes de 5MB. Novamente, a ideia principal era, se você tomar o caminho do "onde-estamos-agora" e "para-onde-vamos-lá-na-frente", acabamos batendo contra um muro.

> *"Se nós permitirmos os grupos alt, a internet certamente irá derreter e não haverá possibilidade alguma de ganhar escala."*

Assim, a internet não poderia ganhar escala. Esse foi o começo da problema-

tização da internet ganhar escala. Obviamente, não poderia e não iria ganhar escala. Muitas pessoas escreveram suas teses de doutorado sobre por que não ganharia escala.

Mas, obviamente, a questão é que redes não ganham escala. Redes falham em ganhar escala. Algumas redes fracassam elegantemente em ganhar escala por décadas, e são essas as que triunfam no final das contas.

> *"Algumas redes fracassam elegantemente em ganhar escala por décadas, e são essas as que triunfam no final das contas."*

Eventualmente, nós resolvemos o problema da Usenet. As conexões digitais foram atualizadas, mais sistemas foram conectados com linhas alugadas e conexões diretas. A conexão discada foi gradualmente substituída por linhas alugadas. As pessoas começaram a investir na infraestrutura e assim foi possível hospedar a Usenet confortavelmente. Então, as pessoas começaram a usar o *e-mail*. E o problema da capacidade de escalar voltou.

• O e-mail e os anexos dos e-mails vão destruir a internet

Na medida em que o *e-mail* tornou-se popular, ele começou a substituir e eclipsar o tamanho da Usenet. Agora, o problema era ainda maior, porque as pessoas queriam se comunicar diretamente. Agora, uma mensagem que antes levava 24 horas passou a cruzar a internet em duas horas, o que significava que as pessoas começaram a ter conversas em tempo real -- ou quase em tempo real. O uso de *e-mail* explodiu. E, novamente, a internet não poderia ganhar escala, porque se você olhar para onde o *e-mail* está hoje e onde estava há seis meses e desenhar uma linha, não é possível ganhar escala. A internet vai derreter. As pessoas escreviam mais teses de doutorado sobre como a internet morreria sob a carga de *e-mail* e nunca ganharia escala.

Gradualmente, começamos a otimizar. Nós resolvemos o problema do *e-mail*. E quando eu digo "nós", na verdade eu estava apenas assistindo, pois eu tinha 16 anos de idade e não tinha a menor ideia do que estava acontecendo. Mas nós, como pessoas, como humanidade, resolvemos o problema. Ganhamos escala. A internet falhou na escala para o Usenet e conseguiu escalar o Usenet para que ele não conseguisse escalar o *e-mail*. Então, como foi possível ganhar escala para os e-mails, um espertinho foi e inventou o MIME, mensagens multimídia na internet, o que significava que você poderia anexar as coisas ao *e-mail*. Esses anexos tinham 10 vezes o tamanho do texto, pois pessoas começaram a enviar coisas maiores, como desenhos, fotos e, claro, sexo.

Então, era possível ganhar escala para os e-mails, mas não para os anexos dos e-mails. Todo mundo estava em um alvoroço: "Nós nunca vamos ganhar escala para aguentar os anexos dos e-mails. A internet vai certamente der-

reter!" Então, nós resolvemos isso também. Até que um cara britânico, Sir Tim Berners Lee (que até então era apenas Tim) inventou a *web*. Agora, você pode colocar as imagens como fotos em quadros.

- **A web destruirá a internet**

Foi em 1992, quando eu baixei e executei o primeiro navegador da *web*, NCSA Mosaic, no meu laboratório universitário. Nos reunimos em três ou quatro amigos. Trabalhamos por horas para que o NCSA Mosaic fosse baixado, compilado e instalado. Então, nós o acessamos e visitamos a *web*. Foi assim. Posso dizer que, em 1992, visitei toda a *web* em uma tarde. Ambos os sites. Porque havia apenas dois. Eu visitei ambos os sites e pensei: Oh, meu Deus. Isso vai ser grande! A internet nunca será dimensionada. E imagine o que você poderia fazer com o sexo na *web*! Claro que isso se tornou o aplicativo de escala, como todos sabemos. Tem impulsionado o desenvolvimento da internet desde o início, mas não falamos sobre isso numa sociedade polida.

> *"Posso dizer que, em 1992, visitei toda a web em uma tarde. Ambos os sites. Porque havia apenas dois. Pensei: Oh meu Deus, vai ser enorme! A internet nunca será dimensionada."*

A internet estava falhando em escala para suportar a *web*. E as pessoas diziam: "Nós não podemos dar suporte para todas essas imagens, documentos e hipertextos. Isso falhará na escala.". E mais teses de PhD foram escritas, e mais discussões foram sendo realizadas. A internet ainda estava falhando em escala. Mas agora, mesmo falhando por mais de uma década, muito elegantemente e mantendo o seu sucesso.

- **VOIP irá destruir a internet**

Então, alguém inventou o Voice Over IP. Algumas outras pessoas decidiram, por que não substituímos o sistema telefônico inteiro pela internet? Essa foi uma ideia maluca. As companhias de telefonia começaram uma campanha maciça para nos informar porque as redes com comutação de pacotes nunca poderiam transmitir voz. Eles disseram que, na verdade, a abordagem de qualidade verdadeira para a voz sempre seriam redes de comutadores hierárquicas pertencentes ao monopólio de empresas de telecomunicações nacionais, porque a internet não poderia escalar para atender as chamadas telefônicas do mundo.

Essas mesmas empresas de telefonia (as que ainda estão no mercado) agora roteiam todas as chamadas telefônicas pela internet. Primeiro, eles não queriam a internet em suas redes telefônicas. Depois, eles permitiram a internet em suas redes de telefone. Então, eles construíram suas redes de telefone em cima da internet.

"Primeiro, eles não queriam a internet em suas redes telefônicas. Depois, eles permitiram a internet em suas redes de telefone. Então, eles construíram suas redes de telefone em cima da internet."

- **Vídeos de gatinhos irão destruir a internet**

Em seguida, começamos a enviar vídeos. E então a internet não poderia escalar novamente porque o YouTube iria derreter a internet. Claramente, precisávamos de alguma qualidade de conteúdo e filtragem, porque não podemos permitir que todos os idiotas vejam e publiquem um vídeo sobre seu gato. Eles disseram: "Já existem milhares de vídeos de gatos. Se você traçar uma linha de quantos vídeos de gatos havia ontem para quantos vídeos de gatos existem hoje e, extrapolando, até o final desta década, haverá um bilhão de vídeos de gatos na internet!" Foi exatamente o que aconteceu.

E nós escalamos. Agora, podemos fazer o vídeo 3D e vídeo 4K.

- **Netflix irá destruir a internet**

Quando Netflix apareceu, vimos o mesmo erro. Em 1992, quando visitei o primeiro *site*, meu pensamento foi: A TV está tão morta que um dia poderemos transmitir filmes instantaneamente. Se você falasse isso a um respeitável pesquisador de rede em 1992, ele o chamaria de idiota. Porque, claramente, se tivéssemos Netflix em 1992, um fluxo de vídeo único para um único usuário iria derreter toda uma internet. No entanto, aqui estamos hoje. A propósito, a internet está falhando em escala para a Netflix e também para todas as outras empresas que estão fazendo vídeos ao vivo.

Vai continuar a falhar na escala incrementalmente e graciosamente. Em breve, nós vamos estar fazendo Oculus Rift holográfica 3D, 4K, VR. Então, ele realmente falhará na escala. Pessoas ainda vão escrever suas teses de Phd sobre por que a internet está prestes a derreter.

Escalabilidade é um alvo em movimento

Escalabilidade é um alvo em movimento. A escala define uma borda das capacidades de hoje. Como ela se move para a frente, a capacidade aumenta. A razão para isso é realmente simples: é porque a escala não é um objetivo a atingir; é uma definição do que você pode fazer com a rede hoje. No momento em que você aumenta a capacidade, a própria definição do que você pode fazer com uma rede, hoje, muda, porque alguém diz: "Espere um segundo. Quer dizer que agora posso fazer 'X', que tem 10 vezes mais demanda do que eu fiz antes? Vamos fazer algo disso.". E, então, você não pode continuar novamente. Escalabilidade é um alvo em movimento. Escala define uma borda das capacidades de hoje. Como ela se move para a frente, a capacidade aumenta.

"Escalabilidade é um alvo em movimento. Escala define uma borda das capacidades de hoje. Como ela se move para a frente, a capacidade aumenta."

Bitcoin está falhando na escala. Se tivermos sorte realmente, *bitcoin* continuará a falhar na escala graciosamente por 25 anos, como a internet. Os mesmos tipos de empresas que diziam que a internet nunca poderia suportar e funcionar para todo o *e-mail*, nunca funcionará para fazer chamadas de voz de qualidade, nunca poderá funcionar com vídeo de qualidade, agora estão fazendo o mesmo tipo de argumentos corporativos sobre por que o *bitcoin* nunca pode fazer pagamentos de varejo, nunca poderá ter a escala da Visa, nunca poderá fazer escala global e, se for realmente adotado, ele entrará em colapso.

Agora, há uma dúzia de pessoas escrevendo sua tese de PhD sobre como o *bitcoin* falhou, vai falhar, está morrendo, está morto e morrerá novamente.

"Bitcoin está falhando na escala. Se tivermos sorte realmente, o bitcoin continuará a falhar a escala graciosamente por 25 anos, como a internet."

Há um belo *site* chamado bitcoinobituaries.com, onde você pode ler os prognósticos da morte de *bitcoin* desde 2009 -- regularmente, como um relógio, a cada três a seis meses, grandes jornais, cientistas, etc. dizem: "É Isso. *Bitcoin* está morto.". Na verdade, isso agora se tornou uma incrível oportunidade de recrutamento, porque tudo o que você tem a fazer é esperar que as pessoas saibam que o *bitcoin* morreu, o CEO do *bitcoin* foi preso, ou o *bitcoin* foi interrompido por Putin e, quatro meses depois, alguém diz: "Você sabe que existem algumas novas aplicações interessantes com o *bitcoin*". E eles olham e pensam: "*Bitcoin* ainda está lá?"

"*Bitcoin* ainda está lá" é o slogan de *marketing* dessa comunidade. Se pudermos continuar falando o "*bitcoin* ainda está lá", as pessoas ficarão surpresas e confusas. Não combina com suas expectativas. Não é possível que *bitcoin* ainda esteja lá, porque pessoas muito sérias com títulos muito sérios, trabalhando para empresas muito ricas, disseram-lhes que o *bitcoin* não estaria lá. Mas o *bitcoin* ainda está lá, porque estamos falhando em escalar graciosamente.

• Taxa de otimização e escalabilidade

Quando falhamos a escala durante um teste de estresse ou um teste de capacidade, quando a rede é inundada com transações, o que acontece? Alguns usuários experimentam uma situação terrível. Eles fazem uma transação com uma taxa de 0,1 *milibit*, como sempre, e demora três dias para confirmar. Durante esse tempo, eles estão enlouquecendo, especialmente se eles são novos usuários. Os novos usuários assumem que o dinheiro deixou sua conta (não há contas no *bitcoin*) e o dinheiro está a caminho da conta de destino (novamente repito que não há contas em *bitcoin*) e, portanto, o dinheiro está

em algum lugar no meio do limbo. O dinheiro ainda está em sua conta, só que sua carteira diz que ainda não foi confirmada. É na origem ou no destino, atomicamente com uma transação. Não existe um estágio intermediário. Não pode ser no limbo porque *bitcoin* não transmite, instala-se.

Nós experimentamos esses problemas súbitos, e algumas carteiras se comportam de forma inteligente e aumentam suas taxas, às vezes, em 100%. O que isso significa é que, em vez de custar 4 centavos para enviar uma transação global em segundos e para qualquer lugar do mundo sem censura, com inovação aberta e acesso aberto a todos, é preciso 8 centavos para efetuar essa transação! Claramente, isso é uma indicação, junto com as pessoas que esperaram três dias para confirmar sua transação, que *bitcoin* está morto agora. E alguns dos desenvolvedores dizem: "Oh, eu desisto. *Bitcoin* está morto." Os jornais escrevem:"*Bitcoin* está morto. As transações não estão sendo realizadas.".

As transações estão acontecendo. Eles passaram por mim. Eu estava executando uma carteira que era inteligente; estava fazendo seus cálculos de taxa de transação. O que acontece após a crise de capacidade? Temos carteiras melhores.

Essa é realmente a essência de um sistema dinâmico que responde à pressão, porque, à medida que melhoramos as carteiras, essas melhores carteiras calculam as taxas mais corretamente. E é muito mais fácil atolar a rede se houver um monte de carteiras burras fazendo taxas de 0,1 *milibit*. Então, tudo o que você precisa é fazer 0,11 *milibits* de taxa e você agora é o rei da colina. Porque os outros idiotas não atualizaram e travaram a rede com suas transações. Mas se eles conseguirem 0,12 *milibits*, agora você terá que fazer 0,13. Agora, estamos em uma corrida e, antes que você perceba, você está gastando 0,5 *milibits* em uma transação onde você é um usuário legítimo, isso é nada. Se você está tentando bloquear a rede, as taxas começam a ficar muito altas, rapidamente.

Transações de spam, transações legítimas, transações ilegítimas

Levantam questões interessantes: o que é uma transação de spam? O que é uma transação legítima? O que é uma transação ilegítima? Há duas maneiras de responder a isso. Uma é uma abordagem paternalista, vinda de cima para baixo, que diz, isso é permitido, isso não é permitido e, fazendo uma lista, evitaremos que a rede seja preenchida até a capacidade. Mas que quebra uma capacidade fundamental do *bitcoin*, que é a neutralidade da rede. *Bitcoin* não quer saber quem é o remetente ou o receptor, qual o aplicativo usado, qual a aplicação, nem qual é o valor envolvido na transação. Tudo o que

importa é: você pagou a taxa? Se você pagou a taxa, sua transação é legítima por definição, porque você achou legítimo o suficiente para anexar essa taxa. O próprio ato de pagamento da taxa legitima a transação. Se começarmos a tomar decisões sobre o que é spam e o que não é, agora estamos escolhendo o futuro do *bitcoin* e restringindo-o a um conjunto de aplicativos que podemos imaginar. Uma pessoa brilhante, que cria um novo aplicativo que nem podemos imaginar - e que pode parecer ser spam para nós - não é transportada pela rede, porque nós tomamos uma decisão unanime para dizer se essa transação é ilegítima.

> *"O próprio ato de pagamento de taxa legitima a transação. Se começarmos a tomar decisões sobre o que é spam e o que não é, estaremos escolhendo o futuro do bitcoin e restringindo-o a um conjunto de aplicativos que podemos imaginar."*

A outra maneira de fazer isso é imaginar, como usar o mercado para resol-ver esse problema. Temos um mercado. Temos uma moeda. Use o mercado para resolver esse problema: permita ao mercado estabelecer a taxa mínima que atende aos requisitos de fornecimento através dos mineradores e sua necessidade de propagação rápida de blocos e a demanda dos usuários para as aplicações que lhes interessam. Se você paga a taxa, sua transação é legitimada. Não há transação de spam. Não existe uma transação ilegítima. Há apenas transações que foram mineradas e transações que não tinham taxa suficiente para serem mineradas.

Décadas de falha na escala

É assim que o *bitcoin* joga fora. Isso não vai ser resolvido; teremos uma discussão de escalabilidade anualmente por décadas no futuro, espero. Todos os anos falharemos em escala para uma próxima aplicação, e sucessivamente como nas escalas anteriores. Assim que melhorarmos, as pessoas vão inventar novas aplicações e teremos que redimensionar novamente.

> *"Todos os anos, falharemos em escala para uma próxima aplicação e sucessivamente avançaremos como nas escalas anteriores."*

Internet: falhando e escalando graciosamente, por 25 anos. *Bitcoin*: vamos continuar falhando e escalando graciosamente, e o *bitcoin* ainda não está morto.

Obrigado.

UMA MENSAGEM DE ANDREAS

Pedido de revisão

Obrigado por ler este livro. Espero que tenha gostado de ler, tanto quanto eu gostei de criá-lo. Se você gostou deste livro, por favor, dedique um minuto para visitar a página do livro em internetdodinheiro.com, ou onde quer que você tenha comprado, e deixe um comentário. Isso ajudará o livro a obter maior visibilidade nos *rankings* de busca e alcançar mais pessoas que possam estar aprendendo sobre *bitcoin* pela primeira vez. Seu comentário honesto também ajudará a tornar o meu próximo livro ainda melhor.

Obrigado

Quero aproveitar esta oportunidade para agradecer formalmente a comunidade pelo apoio ao meu trabalho. Muitos de vocês compartilham este trabalho com amigos, família e amigos; participam de eventos em pessoa, por vezes, viajam longas distâncias; e aqueles que são capazes de me apoiar na plataforma Patreon. * Sem vocês, eu não poderia fazer este trabalho importante, um trabalho que eu amo, e eu sempre serei grato. *

Obrigado.

Atualizando-se com Andreas

Saiba mais sobre Andreas, inclusive quando ele está planejando visitar sua cidade, seu *website* é https://www.antonopoulos.com.

Você pode também segui-lo em seu Twitter http://www.twitter.com/aantonop ou se inscreva no canal do YouTube em https://www.youtube.com/aantonop.

E claro, Andreas não seria capaz de realizar seu trabalho sem suporte financeiro da comunidade através da Patreon. Saiba mais sobre o seu trabalho e ganhe acesso prévio a vídeos e outros conteúdos exclusivos por se tornar um patrono em https://www.patreon.com/aantonop.

Impressão, audioBook e ebook volume dois

Este é o primeiro livro de uma série chamada "A Internet do dinheiro". Se você gostou deste livro, você provavelmente irá gostar também do Volume Dois, que está disponível em forma impressa, ebook e audiobook para os Estados Unidos, Reino Unido, Europa, Austrália e em outros lugares pelo mundo. Em breve também estará disponível em língua portuguesa.

O Volume Dois contém a seção "Perguntas frequentes" e algumas das conversas mais populares, incluindo:

Introdução ao *Bitcoin*: Conferência IPP do Singularity University; Silicon Valley, California; setembro 2016;

Blockchain versus Conversa Fiada: Conferência da África Blockchain em Grupos Focais; Joanesburgo, África do Sul; março de 2017;

Notícia falsa, Dinheiro falso: Encontro do Vale do Silício no Plug & Play Tech Center; Sunnyvale, Califórnia; abril de 2017;

Imutabilidade e Prova de Trabalho, O Monumento Digital em Escala Planetária: Encontro de *Bitcoin* do Vale do Silício; Sunnyvale, Califórnia; setembro 2016

Guerras Monetárias: Coinscrum Minicom no Imperial College; Londres, Inglaterra; dezembro 2016;

O Menino Bolha e o Rato de Esgoto: Workshop DevCore na Universidade Draper, San Mateo, Califórnia; outubro 2015;

O que é Transmissão de Dinheiro?: Encontro de Quarta-feira de *Bitcoin* no Eye Film Museu; Amsterdã, Holanda; outubro 2016;

Ciência de Foguete e Aplicativo Matador de *Ethereum*: Encontro *Ethereum* Cape Town em Deloitte Greenhouse; Cape Town, África do Sul; março 2017;

Estamos apenas começando.

Para complementar o assunto introduzido com o livro A Internet do Dinheiro, a EmRede Editora trouxe para o Brasil uma coleção de mais 3 livros sobre esse assunto tão importante e transformador.

Os livros apresentados a seguir serão distribuídos em breve, para acompanhar as novidades basta seguir nossos canais de comunicação.

A Máquina da Verdade - O Blockchain e o Futuro de Tudo
Michael Case e Paul Vigna

Os grandes bancos cresceram e se entrincheiraram. A privacidade existe apenas até o próximo hack. Fraude de cartão de crédito é um fato da vida. Muitos dos "sistemas legados", antes concebidos para tornar nossas vidas mais fáceis e nossa economia mais eficiente, não estão mais à altura da tarefa. No entanto, existe uma maneira de ultrapassar tudo isso - um novo tipo de sistema operacional com o potencial de revolucionar vastas áreas de nossa economia: o blockchain.

No livro A máquina da verdade, Michael J. Casey e Paul Vigna desmistificam o blockchain e explicam por que ele pode restaurar o controle pessoal sobre nossos dados, ativos e identidades;

conceder para bilhões de pessoas excluídas acesso à economia global; e mudar o equilíbrio de poder para reavivar a fé da sociedade em si mesma. Eles revelam a ruptura que promete vir para as indústrias, incluindo finanças, tecnologia, transporte, cultura, meio ambiente e muitas outras.

Casey e Vigna expõem o desafio de substituir instituições confiáveis (e não tão confiáveis) nas quais confiamos por séculos com um modelo radical que as ultrapassa. A Máquina da Verdade revela o empoderamento possível quando os intermediários interessados em se interessarem dão lugar à transparência do blockchain, ao mesmo tempo em que destacam as perdas de emprego, a afirmação de interesses especiais e a ameaça à coesão social que acompanhará essa mudança. Com a mesma perspectiva equilibrada que trouxeram para A Era das Criptomoedas, Casey e Vigna mostram por que todos nós devemos nos importar com o caminho que a tecnologia blockchain está trilhando - levando a humanidade adiante, não para trás.

A Era das Criptomoedas - como o Bitcoin e o Blockchain estão desafiando a ordem econômica global
Michael Case e Paul Vigna

Bitcoin tornou-se um chavão durante a noite. Um ciber-enigma com seguidores entusiasmados, ele aparece nas manchetes e estimula o debate interminável da mídia. Você pode aparentemente usá-lo para comprar qualquer coisa, desde café até carros, mas poucas pessoas parecem realmente entender o que é. Isso levanta a questão: por que alguém deveria se preocupar com o bitcoin?

Em A Era das Criptomoedas, os jornalistas de Wall Street, Paul Vigna e Michael J. Casey, dão a resposta definitiva a essa questão. A Criptomoeda está pronta para lançar uma revolução, que poderia reinventar as estruturas financeiras e sociais tradicionais, ao mesmo tempo em que traz os bilhões de indivíduos "sem banco" do mundo para uma nova economia global. Criptomoeda mantém a promessa de um sistema financeiro sem intermediários, pertencentes às pessoas que o usam e salvaguardados da devastação de um acidente do tipo de 2008.

Mas o bitcoin, o mais famoso das criptomoedas, carrega uma reputação de instabilidade, flutuação selvagem e negócios ilícitos; alguns temem que ele tenha o poder de eliminar empregos e derrubar o conceito de um estado-nação. Implica, acima de tudo, mudança monumental e abrangente - para melhor e para pior. Mas está aqui para ficar e você o ignora por sua conta em risco.

Vigna e Casey desmistificam a criptomoeda - suas origens, sua função e o que você precisa saber para navegar em uma economia cripto. O mundo da criptomoeda será muito diferente do mundo da moeda de papel; A Era das Criptomoedas vai te ensinar como estar pronto.

O livro de Satoshi - os escritos coletados do criador do Bitcoin Satoshi Nakamoto
Phil Champagne

Você, como o resto do mundo, especulou sobre a identidade de Satoshi Nakamoto, criador anônimo do Bitcoin?

A primeira criptomoeda do mundo, o Bitcoin entrou em operação em 2009 e desde então revolucionou nossos conceitos de moeda e dinheiro. Não suportado por nenhum governo ou banco central, completamente eletrônico, o Bitcoin é uma moeda virtual baseada em sistemas criptográficos avançados.

Como a moeda que ele criou, a identidade do criador do Bitcoin, Satoshi Nakamoto, é virtual, existindo apenas online. A persona Nakamoto, que pode representar um indivíduo ou um grupo, existe apenas nas publicações on-line que introduziram e explicaram o Bitcoin durante seus primeiros dias. Aqui, coletadas e publicadas profissionalmente pela primeira vez, estão os escritos essenciais que detalham a criação do Bitcoin. Estão incluídos:

• E-mails e postagens de Satoshi Nakamoto em fóruns informatizados apresentados em ordem cronológica

• Fundamentos do Bitcoin apresentados em termos simples

• Implicações econômicas potenciais e profundas do Bitcoin

• O paper seminal que começou tudo

O livro de Satoshi oferece uma maneira conveniente de analisar o que o criador do Bitcoin escreveu ao longo dos dois anos que constituíram sua "vida pública" antes de ele desaparecer da Internet ... pelo menos sob o nome de Satoshi Nakamoto.

A verdadeira identidade de Nakamoto pode nunca ser conhecida. Portanto, os escritos reproduzidos aqui são, provavelmente, tudo que o mundo jamais ouvirá dele a respeito da criação, funcionamento e base teórica do Bitcoin. Quer aprender mais sobre o Bitcoin? Vá diretamente para a fonte - os escritos do próprio criador, Satoshi Nakamoto.