

As 21 Lições

O Que Aprendi ao Cair na Toca do Coelho do
Bitcoin

Gigi

As 21 Lições

O Que Aprendi ao Cair na Toca do Coelho do Bitcoin
Primeira Edição. Versão 0.3.11, git commit 6a933bb.

Copyright ©2018–2021 Gigi / @dergigi / dergigi.com

Tradução feita por KoreaComK / @KoreacomK



Este livro e sua versão online são distribuídos nos termos da Licença Creative Commons Attribution-ShareAlike 4.0. Uma cópia da referência desta licença pode ser encontrada no site oficial creative commons.^a

^a<https://creativecommons.org/licenses/by-sa/4.0>

Dedicado a minha esposa, meu filho e a todos os filhos deste mundo. Que o Bitcoin atenda bem a você e forneça uma visão de um futuro pelo qual vale a pena lutar.

Introdução

Alguns chamam isso de experiência religiosa. Outros o chamam de Bitcoin.

Encontrei o Gigi pela primeira vez em uma de minhas casas espirituais - em Riga, Letônia - a casa da Conferência chamada *The Baltic Honeybadger*, onde os mais fervorosos fiéis do Bitcoin fazem uma peregrinação anual. Depois de uma conversa profunda na hora do almoço, o título que Gigi e eu forjamos estava tão fixo em nossas cabeças quanto uma transação de Bitcoin que foi processada quando apertamos as mãos pela primeira vez, algumas horas antes.

Meu outro lar espiritual, Christ Church, em Oxford, onde tive o privilégio de estudar para o meu MBA, foi onde tive meu momento do “Buraco do Coelho”. Como Gigi, transcendi os reinos econômicos, técnicos e sociais, e fui espiritualmente envolvido pelo Bitcoin. Depois de “comprar na alta” na bolha de novembro de 2013, havia várias lições extremamente difíceis a serem aprendidas no mercado que ficou em baixa por 3 anos, um tempo que parecia implacavelmente esmagador e interminável. Essas 21 lições realmente teriam me servido muito bem naquela época. Muitas dessas lições são simplesmente verdades naturais que, para aqueles que não foram iniciados, são obscurecidas por um papel opaco e frágil. Porém, no final deste livro, o papel irá se dissolver de maneira feroz.

Em uma noite cristalina em Oxford, no final de agosto de 2016, apenas algumas semanas depois da faca ter sido retorcida no meu coração quando o corretora Bitfinex foi hackeada, sentei-me em silenciosa contemplação no Jardim do Mestre da Igreja de Cristo. Os tempos eram difíceis e eu estava no meu limite mental e

emocional depois do que parecia ser uma vida inteira de tortura. Não era devido a perda financeira, mas pela esmagadora perda espiritual que sentia por estar isolado em minha visão de mundo. Se ao menos houvesse os recursos que temos hoje naquela época eu saberia que não estava sozinho. O Jardim do Mestre é um lugar muito especial para mim e para muitos que vieram antes de mim ao longo dos séculos. Foi lá que Charles Dodgson, professor de matemática na Christ Church, observou uma de suas jovens alunas, Alice Liddell, filha do reitor da Christ Church. Dodgson, mais conhecido por seu pseudônimo, Lewis Carroll, usou Alice e o jardim como sua inspiração, e na magia daquela relva sagrada, eu encarei profundamente o cripto-abismo, e ele olhou de volta para mim, de maneira ardente, aniquilando minha arrogância, e dando um tapa na minha cara, acabando com o meu orgulho. Eu finalmente estava em paz.

As 21 lições leva você a uma verdadeira jornada ao Bitcoin, não apenas uma jornada ao mundo da filosofia, tecnologia e economia, mas da alma.

À medida que você se aprofunda na filosofia resumidamente apresentada nas 7 das 21 Lições, pode-se ir tão longe a ponto de compreender a origem de todos os seres com tempo e contemplação suficientes. Suas 7 lições de economia capturam, em termos simples, como estamos à mercê financeira de um pequeno grupo de *Chapeleiros Malucos* e como eles conseguiram cegar nossas mentes, corações e almas. As 7 lições sobre tecnologia mostram a beleza e a perfeição tecnologicamente darwiniana do Bitcoin. Sendo um Bitcoinheiro sem bagagem técnica, as lições fornecem uma revisão relevante da natureza tecnológica inerente do Bitcoin e, na verdade, da própria natureza da tecnologia.

Nessa experiência transitória que chamamos de vida, vivemos, amamos e aprendemos. Mas o que é a vida senão uma ordem de eventos com registro de data e hora?

Conquistar a montanha do Bitcoin não é fácil. Os cumes falsos

são abundantes, as rochas são ásperas e as rachaduras e fendas estão à espreita para nos engolir. Depois de ler este livro, verá que Gigi é o Pastor do Bitcoin e eu o apreciarei para sempre.

Hass McCook
November 29, 2019

“Poderia me dizer, por favor, que caminho
devo tomar para sair daqui?”

“Isso depende bastante de onde você quer
chegar.”

“O lugar não importa muito –”

“Então não importa o caminho que você vai
tomar.”

– Lewis Carroll, *Alice no País das Maravilhas*

Sumário

I. Filosofia	9
1. Imutabilidade e mudança	15
2. A escassez da escassez	19
3. Replicação e localidade	21
4. O problema da identidade	23
5. Uma concepção imaculada	25
6. O poder da liberdade de expressão	27
7. Os limites do conhecimento	29
II. Economia	31
8. Ignorância financeira	37
9. Inflação	41
10. Valor	47
11. Dinheiro	49
12. A história e a queda do dinheiro	53

13.A insanidade das reservas fracionárias	63
14.O dinheiro forte	69
III.Tecnologia	77
15.Força nos números	81
16.Reflexões sobre: “Não Confie, Verifique”	89
17.Dizer as horas demanda trabalho	97
18.Mova-se lentamente e não quebre as coisas	101
19.A privacidade não morreu	105
20.Cypherpunks escrevem código	107
21.Metáforas para o futuro do Bitcoin	111
Considerações Finais	119

Sobre Este Livro (... e Sobre o Autor)

Este é um livro um tanto incomum. Mas, o Bitcoin é uma tecnologia um tanto quanto incomum, então um livro incomum sobre o Bitcoin pode ser adequado. Não tenho certeza se sou um cara incomum (gosto de me ver como um cara *normal*), mas a história de como esse livro surgiu, e como me tornei um autor, vale a pena ser dita.

Em primeiro lugar, não sou um autor. Eu sou um engenheiro. Não estudei redação. Estudei código e programação. Em segundo lugar, nunca tive a intenção de escrever um livro, muito menos um livro sobre Bitcoin. Inferno! Eu nem falo o inglês nativo.¹ Sou apenas um cara que encontrou um bug no Bitcoin. Difícil.

Quem sou *eu* para escrever um livro sobre Bitcoin? Esta é uma boa pergunta. A resposta curta é simples: Sou Gigi e sou um bitcoinheiro.

A resposta longa é um pouco mais complicada.

Minha formação é em ciência da computação e desenvolvimento de software. Anteriormente, fiz parte de um grupo de pesquisa que tentava fazer os computadores pensarem e raciocinarem, entre outras coisas. Antes do Bitcoin, escrevi um software para processamento automatizado de passaportes e coisas relacionadas que ainda são bem assustadores. Eu sei uma ou

¹A razão pela qual estou escrevendo essas palavras em inglês é que meu cérebro funciona de maneiras misteriosas. Sempre que surge algo técnico, ele muda para o modo inglês.

duas coisas sobre computadores e nosso mundo interligado, então acho que tenho um pouco de vantagem para entender o lado técnico do Bitcoin. No entanto, como tento mostrar neste livro, o lado técnico das coisas é apenas uma pequena fatia da Quimera que é o Bitcoin. E cada um destes pequenos pedaços são importantes.

Este livro surgiu por causa de uma pergunta simples: “O que você aprendeu com o Bitcoin?” Tentei responder a essa pergunta em um único tweet. Então o tweet se transformou em uma thread. A tempestade de tweets se transformou em um artigo. O artigo se transformou em três artigos. Três artigos se transformaram em 21 lições. E 21 lições se transformaram neste livro. Acho que sou péssimo em condensar meus pensamentos em um único tweet.

“Por que escreveu este livro?”, você pode me perguntar. Novamente, há uma resposta curta e uma longa. A resposta curta é que eu simplesmente tinha que fazê-lo. Eu era (e ainda sou) possuído pelo Bitcoin. Acho que ele é infinitamente fascinante. Não consigo parar de pensar nisso e nas implicações que terá em nossa sociedade global. A resposta longa é que acredito que o Bitcoin é a invenção mais importante do nosso tempo, e mais pessoas precisam entender a natureza dessa invenção. O Bitcoin ainda é um dos fenômenos mais incomprendidos de nosso mundo moderno, e levei anos para perceber em toda sua completude a gravidade dessa tecnologia alienígena. Perceber o que é o Bitcoin e como ele transformará nossa sociedade é uma experiência profunda. Espero plantar as sementes que podem levar a essa compreensão em sua cabeça.

Embora esta seção seja intitulada *“Sobre este livro (... e sobre o autor)”*, no frigir dos ovos, este livro, quem sou e o que fiz, realmente não importa. Eu sou apenas um node na rede, literalmente e figurativamente. Além disso, não deve confiar no que

estou dizendo, de maneira nenhuma. Como node e bitcoinheiro, gosto de dizer: faça sua própria pesquisa e, o mais importante: Não confie, verifique.

Fiz o meu melhor para fazer meu dever de casa e fornecer muitas fontes para você poder mergulhar de cabeça, caro leitor. Além das notas de rodapé e citações neste livro, tento manter uma lista atualizada de recursos no 21lessons.com/rabbithole e no bitcoin-resources.com, que também lista muitos outros recursos, livros e podcasts com curadoria que o ajudarão a entender o que é o Bitcoin.

Resumindo, este é um simples livro sobre o Bitcoin, escrito por um bitcoinheiro. O Bitcoin não precisa deste livro e você provavelmente não precisa deste livro para entender o Bitcoin. Acredito que o Bitcoin será compreendido por você assim que você estiver pronto, e também acredito que as primeiras frações de um bitcoin o encontrará assim que você estiver pronto para recebê-las. Em essência, todos terão Bitcoin no momento certo. Enquanto isso, o Bitcoin simplesmente é, e isso é o suficiente. ²

²Beautyon, *O Bitcoin é. E isso é o suficiente.* [8]

Prefácio

Cair na toca do coelho do Bitcoin é uma experiência estranha. Como muitos outros, sinto que aprendi mais nos últimos anos estudando sobre o Bitcoin do que durante duas décadas de educação formal.

As lições a seguir são uma compilado de tudo o que aprendi. Publicado pela primeira vez como uma série de artigos intitulada “O que aprendi com o Bitcoin”, o que se segue pode ser visto como uma terceira edição da série original.

Como o Bitcoin, essas lições não são estáticas. Pretendo trabalhar nelas periodicamente, lançando versões atualizadas e material adicional no futuro.

Ao contrário do Bitcoin, as versões futuras deste projeto não precisam ser compatíveis com versões anteriores. Algumas lições podem ser aumentadas, outras podem ser refeitas ou mesmo, substituídas.

O Bitcoin é um professor que não se cansa, por isso não posso afirmar que essas lições sejam abrangentes ou completas. Elas são um reflexo de minha jornada pessoal pela toca do coelho. Há mais lições a serem aprendidas e cada pessoa aprenderá algo diferente ao entrar no mundo do Bitcoin.

Espero que você ache essas lições úteis e que o processo de aprendizado lendo-as não seja tão árduo e doloroso quanto aprendê-las por você mesmo.

As 21 Lições

“Oh, sua Alice tola!” ela disse a si mesma,
“como você pode aprender lições aqui? Ora,
dificilmente há espaço para você e nenhum
espaço para livros de aula!”

– Lewis Carroll, *Alice no País das Maravilhas*

Introdução

“Mas eu não quero me encontrar com gente louca”, observou Alice. “Oh, você não pode evitar isso”, replicou o Gato: “todos nós aqui somos loucos. Eu sou louco, você é louca”. “Como você sabe que eu sou louca?”, disse Alice. “Deve ser”, disse o Gato, “Ou não estaria aqui.”

– Lewis Carroll, *Alice no País das Maravilhas*

Em outubro de 2018, Arjun Balaji fez uma pergunta inofensiva, *O que você aprendeu com o Bitcoin?* Depois de tentar responder a essa pergunta em um tweet e falhar miseravelmente, percebi que as coisas que aprendi são numerosas demais para serem respondidas rapidamente.

As coisas que aprendi são obviamente sobre Bitcoin ou pelo menos relacionadas a ele. No entanto, embora alguns dos funcionamentos internos do Bitcoin sejam explicados, as próximas lições não são uma explicação de como o Bitcoin funciona ou o que é. Elas podem, no entanto, ajudar a explorar algumas das coisas que o Bitcoin toca: questões filosóficas, realidades econômicas e inovações tecnológicas.

Arjun Balaji
@arjunblj

Bitcoin is a game disguised to teach you about:

- Ethics of money production
- History of central banking & gold
- Adversarial system design
- Commodities markets
- Distributed systems engineering & the software lifecycle
- Securities law

What have you learned from Bitcoin?

1,353 7:19 PM - Oct 10, 2018

511 people are talking about this

As 21 *Lições* foram organizadas em 3 capítulos de 7 partes. Cada capítulo examina o Bitcoin através de uma perspectiva diferente, analisando que lições podem ser aprendidas ao inspecionar essa estranha rede de um ângulo diferente.

O Capítulo 1 explora os ensinamentos filosóficos do Bitcoin. A interação entre imutabilidade e mudança, o conceito de escassez verdadeira, a concepção imaculada do Bitcoin, o problema da identidade, a contradição entre replicação e localidade, o poder da liberdade de expressão e os limites do conhecimento.

O Capítulo 2 explora os ensinamentos econômicos do Bitcoin. Lições sobre ignorância financeira, inflação, valor, dinheiro e sua história, reservas fracionárias e como o Bitcoin está reintroduzindo o dinheiro forte de uma forma astuta e indireta.

O Capítulo 3 explora algumas das lições aprendidas examinando a tecnologia do Bitcoin. Por que há força nos números, reflexão sobre confiança, por que dizer as horas dá trabalho, como o desenvolvimento lento mantendo tudo funcionando é um excelente recurso e não um bug, o que a criação do Bitcoin pode nos

dizer sobre privacidade, por que os cypherpunks escrevem código (e não leis) e quais metáforas podem ser úteis para explorar o futuro do Bitcoin.

Cada lição contém várias citações e links ao longo do texto. Se valer a pena explorar uma ideia com mais detalhes, você pode seguir os links que irão te levar para trabalhos relacionados nas notas de rodapé ou na bibliografia.

Mesmo algum conhecimento prévio sobre o Bitcoin seja benéfico para o entendimento, espero que essas lições possam ser digeridas por qualquer leitor curioso. Embora algumas das lições se relacionem entre si, cada uma deve ser capaz de ficar isolada por conta própria e pode ser lida de forma independente. Fiz o meu melhor para fugir do jargão técnico, embora algum vocabulário específico deste domínio seja inevitável.

Espero que minha escrita sirva de inspiração para que outros olhem abaixo da superfície e examinem algumas das questões mais profundas que o Bitcoin traz. Minha própria inspiração veio de uma infinidade de autores e criadores de conteúdo a todos os quais sou eternamente grato.

Por último, mas não menos importante: meu objetivo ao escrever este livro não é convencê-lo de nada. Meu objetivo é fazer você pensar e te mostrar que o Bitcoin é muito mais do que aparenta ser. Eu nem posso te dizer o que é o Bitcoin ou o que o Bitcoin vai te ensinar. Você terá que descobrir por si mesmo.

“Depois disto, não haverá retorno. Se tomar a pílula azul — fim da história, vai acordar na sua cama e acreditar no que você quiser. Se tomar a pílula vermelha³ — você fica no País das Maravilhas, e eu te mostro o quanto profunda é a toca do coelho.”

– Morpheus

³a pílula laranja



Lembre: Tudo o que estou oferecendo é a verdade. Nada além disso.

Parte I.

Filosofia

Filosofia

O camundongo lançou-lhe um olhar um tanto inquisitivo, pareceu piscar um olho, mas não disse nada.

– Lewis Carroll, *Alice no País das Maravilhas*

Olhando para o Bitcoin superficialmente, alguém pode concluir que ele é lento, custoso, redundante demais e excessivamente paranóico. Olhando para o Bitcoin com curiosidade pode-se descobrir que as coisas não são o que parecem ser à primeira vista.

O Bitcoin tem uma maneira de pegar as suposições e transformá-las em nossas cabeças. Depois de um tempo, quando você estava prestes a se sentir confortável de novo, o Bitcoin se destrói na parede como um touro em uma loja de porcelana e destruirá suas suposições mais uma vez.

O Bitcoin é filho de muitas disciplinas. Como monges cegos examinando um elefante, todos os que abordam essa nova tecnologia o fazem de um ângulo diferente. E todos chegarão a conclusões diferentes sobre a natureza dessa fera.

As lições a seguir são sobre algumas das minhas suposições que o Bitcoin destruiu e as conclusões que acabei encontrando. Questões filosóficas de imutabilidade, escassez, localidade e identidade são exploradas nas primeiras quatro lições. Cada parte consiste em sete lições.



Figura 0.1.: Monges cegos examinando o Touro Bitcoin

Parte I – Filosofia:

1. Imutabilidade e mudança
2. A escassez da escassez
3. Replicação e localidade
4. O problema da identidade
5. Uma concepção imaculada
6. O poder da liberdade de expressão
7. Os limites do conhecimento

A lição 5 explora como a história de origem do Bitcoin não é apenas fascinante, mas absolutamente essencial para um sistema sem governante ou líder. As duas últimas lições deste capítulo exploram o poder da liberdade de expressão e os limites de nosso conhecimento individual, refletidos pela surpreendente profundidade da toca do coelho do Bitcoin.

Espero que você ache o mundo do Bitcoin tão educativo, fascinante e divertido quanto eu achei e ainda acho. Convido você a seguir o coelho e explorar as profundezas desta toca do coelho. Agora segure seu relógio de bolso, desça e aproveite a queda.

1. Imutabilidade e mudança

“O que será que mudou à noite? Deixe-me ver: eu era a mesma quando acordei de manhã? Tenho a impressão de ter me sentido um pouco diferente. Mas se eu não sou a mesma, a próxima questão é “Quem sou eu?” Ah! esta é a grande confusão!”

– Alice

O Bitcoin é por padrão difícil de se descrever. É uma *coisa nova* e qualquer tentativa de fazer uma comparação com conceitos anteriores, seja chamando-o de ouro digital ou de dinheiro da internet, está fadada a ficar aquém do todo. Qualquer que seja sua analogia favorita, dois aspectos do Bitcoin são absolutamente essenciais: descentralização e imutabilidade.

Uma maneira de pensar sobre o Bitcoin é como um contrato social automatizado¹. O software é apenas uma peça do quebra-cabeça, e esperar mudar o Bitcoin mudando o software é um exercício de futilidade. Seria preciso convencer o restante da rede a adotar as mudanças, o que é mais um esforço psicológico do que de engenharia de software.

O que se segue pode parecer absurdo à primeira vista, como tantas outras coisas neste campo, mas acredito que seja profundamente verdadeiro, mesmo assim: você não muda o Bitcoin, mas Bitcoin irá mudar você.

¹Hasu, Unpacking Bitcoin’s Social Contract [32]

“O Bitcoin irá nos mudar mais do que nós podemos mudá-lo.”

– Marty Bent²

Levei muito tempo para perceber a profundidade disso. Como o Bitcoin é apenas software e tudo é de código aberto, você pode simplesmente mudar as coisas à vontade, certo? Errado. *Muito* errado. Sem nenhuma surpresa, o criador do Bitcoin sabia disso muito bem.

“A natureza do Bitcoin é tal que no momento que a versão 0.1 foi lançada, o seu design principal foi definido em pedra para o resto da sua existência.”

– Satoshi Nakamoto³

Muitas pessoas tentaram mudar a natureza do Bitcoin. Até agora, todos falharam. Embora exista um mar infinito de forks e altcoins, a rede Bitcoin ainda faz seu trabalho, assim como fazia quando o primeiro nó estava online. As altcoins não importarão no longo prazo. Os forks acabarão morrendo definhados. Bitcoin é o que importa. Enquanto nosso entendimento fundamental de matemática e/ou física não mudar, o honeybadger do Bitcoin continuará a não se importar.

²Tales From the Crypt [10]

³Postagem no fórum do BitcoinTalk: ‘Resposta: Transações e Scripts ...’ [56]

“O Bitcoin é o primeiro exemplo de uma nova forma de vida. Ele vive e respira na internet. Vive porque pode pagar as pessoas para que continue vivo. [...] Não pode ser mudado. Não pode ser questionado. Não pode ser adulterado. Não pode ser corrompido. Não pode ser parado. [...] Se uma guerra nuclear destruir metade do nosso planeta, ele continuará vivo e incorruptível.”

– Ralph Merkle⁴

O batimento cardíaco da rede Bitcoin durará mais do que todos os nossos.

Depois que entendi a citação acima, isso me mudou muito mais do que os blocos anteriores da blockchain do Bitcoin jamais fariam. Mudou minha preferência temporal, meu entendimento de economia, minhas visões políticas e muito mais. Caramba, está até mudando a dieta das pessoas⁵. Se tudo isso parece loucura para você, não se preocupe, você está em boa companhia. Tudo isso é uma loucura e, no entanto, está acontecendo.

O Bitcoin me ensinou que ele não vai mudar. Eu vou.

⁴DAOs, Democracy and Governance, [44]

⁵Inside the World of the Bitcoin Carnivores, [58]

2. A escassez da escassez

“É o suficiente... eu espero não crescer mais...”

– Alice

Em geral, o avanço da tecnologia parece tornar as coisas mais abundantes. Cada vez mais pessoas podem desfrutar do que antes eram bens luxuosos. Em breve, todos nós viveremos como reis. A maioria de nós já vive assim. Como Peter Diamandis escreveu em *Abundance* [23]: “A tecnologia é um mecanismo de liberação de recursos. Pode tornar o que antes era escasso em abundante.”

Bitcoin, uma tecnologia avançada em si, quebra essa tendência e cria uma nova commodity que é realmente escassa. Alguns até argumentam que é uma das coisas mais escassas do universo. A oferta não pode ser inflacionada não importa quanto esforço seja despendido para se criar mais.

“Apenas duas coisas são genuinamente escassas:
tempo e Bitcoin.”

– Saifedean Ammous¹

Paradoxalmente, ele o faz por meio de um mecanismo de cópia. As transações são transmitidas, os blocos são propagados, o livro-razão distribuído é — bem, você adivinhou — distribuído. Todas essas são apenas palavras bonitas para dizer a mesma coisa: copiar. Caramba, o Bitcoin até mesmo se copia em quantos computadores puder, incentivando pessoas individuais a rodar full nodes e a minerar novos blocos.

¹Apresentação do livro *The Bitcoin Standard* [2]

Tudo isso funciona maravilhosamente em conjunto em um esforço concentrado para produzir escassez.

Em tempos de abundância, o Bitcoin me ensinou o que é a verdadeira escassez.

3. Replicação e localidade

Em seguida uma voz irada, do Coelho: “Pat, Pat! onde você está?”

– Lewis Carroll, *Alice no País das Maravilhas*

Deixando a mecânica quântica de lado, a localidade não é um problema no mundo físico. A questão “*Onde está X?*” Pode ser respondida de forma significativa, não importa se X é uma pessoa ou um objeto. No mundo digital, a pergunta do *onde* já é mais complicada, mas não impossível de responder. Onde estão seus e-mails realmente? Uma resposta não muito boa seria “na nuvem” que nada mais é que o computador de outra pessoa. Ainda assim, se você quisesse rastrear cada dispositivo de armazenamento que contém seus e-mails, você poderia, em teoria, localizá-los.

Com o bitcoin, a pergunta do “onde” é *realmente* complicada. Onde, exatamente, estão seus bitcoins?

“Abri os olhos, olhei em volta e fiz a pergunta inevitável, tradicional e lamentavelmente banal do pós-operatório: “Onde estou?””

– Daniel Dennett¹

O problema é duplo. Primeiro, o livro-razão distribuído é distribuído por replicação completa, o que significa que ele está em toda parte. Em segundo lugar, não existem bitcoins. Não apenas fisicamente, mas *teoricamente*.

¹Daniel Dennett, *Where Am I?* [21]

O Bitcoin rastreia um conjunto de saídas de transações não gastos, sem nunca ter que se referir a uma entidade que represente um bitcoin. A existência de um bitcoin é baseada observando-se o conjunto de saídas de transações não gastos e chamando cada entrada com 100 milhões de unidades básicas de bitcoin.

“Onde está, neste momento, em trânsito? [...] primeiro, não há bitcoins. Simplesmente não existem. Eles não existem. Existem entradas em um livro-razão que é compartilhado [...] Eles não existem em nenhum local físico. O livro-razão existe em todos os locais físicos, essencialmente. A geografia não faz sentido neste mundo — não vai ajudá-lo a descobrir a sua política aqui.”

– Peter Van Valkenburgh²

Então, o que você realmente possui quando diz “*Eu tenho um bitcoin*” se não há bitcoins? Bem, lembra de todas essas palavras estranhas que você foi forçado a escrever quando usou uma carteira? Acontece que essas palavras mágicas são o que você realmente possui: um feitiço mágico³ que pode ser usado para adicionar algumas entradas ao livro-razão público — as chaves para “mover” alguns bitcoins. É por isso que, para todos os efeitos, suas chaves privadas *são* seus bitcoins. Se você acha que estou inventando tudo isso, sinta-se à vontade para me enviar suas chaves privadas.

O Bitcoin me ensinou que localidade é um negócio complicado.

²Peter Van Valkenburgh on the *What Bitcoin Did* podcast, episode 49 [73]

³The Magic Dust of Cryptography: Como a informação digital está mudando nossa sociedade [30]

4. O problema da identidade

“Quem é você?”, perguntou a Lagarta..

– Lewis Carroll, *Alice no País das Maravilhas*

Nic Carter, em homenagem ao trabalho de Thomas Nagel em relação a mesma questão relacionada ao morcego, escreveu um excelente artigo que discute a seguinte questão: Como é ser um bitcoin? Ele mostra brilhantemente que blockchains públicas e abertas em geral, e Bitcoin em particular, sofrem do mesmo enigma do navio de Teseu: ¹ Qual Bitcoin é o Bitcoin verdadeiro?

“Considere quão pouca persistência os componentes do Bitcoin possuem. O código base inteiro foi retrabalhado, alterado e expandido de tal forma que mal se parece com sua versão original. [...] O registro de quem possui o que, o próprio livro-razão, é praticamente o único traço persistente da rede [...] Para ser considerado verdadeiramente sem um líder, você deve renunciar à solução fácil de ter uma entidade que pode designar uma chain como sendo a legítima.”

– Nic Carter²

Parece que o avanço da tecnologia continua nos forçando a levar essas questões filosóficas a sério. Mais cedo ou mais tarde,

¹Na metafísica da identidade, o navio de Teseu é um experimento mental que levanta a questão de saber se um objeto que teve todos os seus componentes substituídos permanece fundamentalmente o mesmo. [98]

²Nic Carter, *Como é ser um bitcoin?* [19]

os carros que dirigem sozinhos serão confrontados com versões reais do dilema do bonde, forçando-os a tomar decisões éticas sobre quais vidas são mais importantes do que outras.

As criptomoedas, especialmente desde o primeiro hard fork, nos forçam a pensar e a concordar sobre a metafísica da identidade. Curiosamente, os dois maiores exemplos que temos até agora levaram a duas respostas diferentes. No dia 1º de agosto de 2017, o Bitcoin se dividiu em dois. O mercado decidiu que a chain inalterada é o Bitcoin original. Um ano antes, em 25 de outubro de 2016, o Ethereum se dividiu em dois. O mercado decidiu que a chain *alterada* é o Ethereum original.

Se devidamente descentralizadas, as questões colocadas pelo paradoxo do *Návio de Teseu*, terão que ser respondidas perpetuamente enquanto essas redes de transferência de valor existirem.

O Bitcoin me ensinou que descentralização contradiz a identidade.

5. Uma concepção imaculada

“Suas cabeças se foram, para servi-la, Majestade”, os soldados gritaram em resposta...

– Lewis Carroll, *Alice no País das Maravilhas*

Todo mundo adora uma boa história de origem. A história de origem do Bitcoin é fascinante, e os detalhes dela são mais importantes do que se possa pensar. Quem é Satoshi Nakamoto? Ele era uma pessoa ou um grupo de pessoas? Ele era ela? Seria um alien viajante do tempo ou uma IA avançada? Deixando de lado as teorias estranhas, provavelmente nunca saberemos. E isso é importante.

O Satoshi escolheu ser anônimo. Ele plantou a semente do Bitcoin. Ele ficou por aqui por tempo suficiente para garantir que a rede não morresse quando estava engatinhando. E então ele desapareceu.

O que pode parecer um golpe estranho de anonimato é realmente crucial para um sistema verdadeiramente descentralizado. Sem controle centralizado. Nenhuma autoridade centralizada. Nenhum inventor. Ninguém para processar, torturar, chantagear ou extorquir. Uma concepção imaculada de tecnologia.

“Uma das melhores coisas que Satoshi fez foi desaparecer.”

– Jimmy Song¹

¹Jimmy Song, *Por que o Bitcoin é Diferente* [67]

Desde o nascimento do Bitcoin, milhares de outras criptomoedas foram criadas. Nenhum desses clones compartilha sua história de origem. Se você quiser substituir o Bitcoin, terá que transcender sua história de origem. Em uma guerra de ideias, as narrativas ditam a sobrevivência.

“O ouro foi transformado pela primeira vez em joias e usado para troca há mais de 7.000 anos. O brilho cativante do ouro o levou a ser considerado um presente dos deuses.”

Austrian Mint²

Como o ouro nos tempos antigos, o Bitcoin pode ser considerado um presente dos deuses. Ao contrário do ouro, as origens dos Bitcoins são muito humanas. E desta vez, sabemos quem são os deuses do desenvolvimento e da manutenção: pessoas de todo o mundo, anônimas ou não.

O Bitcoin me ensinou que narrativas são importantes.

²The Austrian Mint, *Gold: The Extraordinary Metal* [46]

6. O poder da liberdade de expressão

“Desculpe-me”, disse o Rato, carrancudo, mas educadamente, “Você falou alguma coisa?”

– Lewis Carroll, *Alice no País das Maravilhas*

O Bitcoin é uma ideia. Uma ideia que, na sua forma atual, é a manifestação de uma máquina movida puramente por texto. Cada aspecto do Bitcoin é texto. O whitepaper é texto. O software executado por seus nodes é texto. O livro-razão é texto. As transações são textos. As chaves públicas e privadas são textos. Cada aspecto do Bitcoin é texto e, portanto, equivalente à fala.

“O congresso não deverá fazer qualquer lei a respeito de um estabelecimento de religião, ou proibir o seu livre exercício; ou restringindo a liberdade de expressão, ou da imprensa; ou o direito das pessoas de se reunirem pacificamente, e de fazerem pedidos ao governo para que sejam feitas reparações de queixas.”

— Primeira Emenda à Constituição dos Estados Unidos

Embora a batalha final das Crypto Wars¹ ainda não tenha acontecido, será muito difícil criminalizar uma ideia, muito menos uma ideia que se baseia na troca de mensagens de texto. Cada vez que um governo tenta proibir um texto ou discurso,

¹The *Crypto Wars* é um nome não oficial para as tentativas dos EUA e governos aliados de minar a criptografia. [26] [78]

escorregamos no caminho do absurdo que inevitavelmente leva a abominações como números ilegais² e primos ilegais³.

Enquanto houver uma parte do mundo onde expressão seja livre como em *liberdade*, o Bitcoin será imparável.

“Não há nenhum ponto em qualquer transação do Bitcoin onde ele deixe de ser *texto*. É *tudo texto*, o tempo todo. [...] O Bitcoin é *texto*. Bitcoin é *linguagem*. Não pode ser regulamentado em um país livre como os EUA, com direitos inalienáveis garantidos e uma Primeira Emenda que exclui explicitamente o ato de publicar da supervisão do governo.” – Beautyon⁴

O Bitcoin me ensinou que, em uma sociedade livre, liberdade de expressão e software livre são imparáveis.

²Um número ilegal é um número que representa informações que são ilegais de possuir, proferir, propagar ou de outra forma transmitir em alguma jurisdição legal. [84]

³Um número primo ilegal é um número primo que representa informação cuja posse ou distribuição é proibida em algumas jurisdições legais. Um dos primeiros primos ilegais foi descoberto em 2001. Quando interpretado de uma maneira particular, ele descreve um programa de computador que ignora o esquema de gerenciamento de direitos digitais usado em DVDs. A distribuição de tal programa nos Estados Unidos é ilegal de acordo com a Lei de Direitos Autorais do Milênio Digital. Um primo ilegal é um tipo de número ilegal. [85]

⁴Beautyon, *Por que os EUA não podem regular o Bitcoin* [7]

7. Os limites do conhecimento

“Para baixo, para baixo, para baixo. Essa queda nunca chegará ao fim?”

– Lewis Carroll, *Alice no País das Maravilhas*

Entrar na toca do coelho do Bitcoin é uma experiência humilhante. Achei que sabia das coisas. Eu pensei que era inteligente. Achava que conhecia ao menos a ciência da computação, no mínimo. Estudei durante anos. Então tenho que saber tudo sobre assinaturas digitais, hashes, criptografia, segurança operacional e redes, certo?

Errado.

Aprender todos os fundamentos que fazem o Bitcoin funcionar é difícil. Compreender todos eles profundamente é quase impossível.

“Ninguém encontrou o fundo da toca do coelho Bitcoin.”

– Jameson Lopp¹

Minha lista de livros para ler continua se expandindo muito mais rápido do que eu consigo ler. A lista de papers e artigos para ler é virtualmente sem fim. Existem mais podcasts sobre todos esses tópicos do que eu poderia ouvir. É realmente humilhante. Além disso, o Bitcoin está evoluindo e é quase impossível

¹Jameson Lopp, tweet de 11 de Novembro de 2018 [41]



Figura 7.1.: A toca do coelho do Bitcoin não tem fundo.

se manter atualizado com a taxa cada vez maior de inovação. A poeira da primeira camada ainda nem baixou e as pessoas já construíram a segunda camada e estão trabalhando na terceira.

O Bitcoin me ensinou que eu sei muito pouco sobre quase tudo. Isso me ensinou que essa toca de coelho não tem fundo.

Parte II.

Economia

Economia

“Uma grande roseira imperava na entrada do jardim: as rosas que nela cresciam eram brancas, mas havia três jardineiros que se ocupavam em pintá-las de vermelho. Alice achou que aquilo era uma coisa estranha e aproximou-se para ver melhor. . .”

– Lewis Carroll, *Alice no País das Maravilhas*

Dinheiro não cresce em árvores. Acreditar que sim é tolice, e nossos pais garantem que saímos disso repetindo esse ditado quase como um mantra. Somos incentivados a usar o dinheiro com sabedoria, a não gastá-lo de qualquer jeito e a economizá-lo nos bons momentos para nos ajudar nos momentos difíceis. Afinal, o dinheiro não cresce em árvores.

O Bitcoin me ensinou mais sobre dinheiro do que eu jamais pensei que precisaria saber. Por meio dele, fui forçado a explorar a história do dinheiro, sistema bancário, pesquisar sobre várias escolas de pensamento econômico e muitas outras coisas. A busca para entender o Bitcoin me levou por uma infinidade de caminhos, alguns dos quais tento explorar neste capítulo.

Nas primeiras sete lições, algumas das questões filosóficas abordadas pelo Bitcoin foram discutidas. As próximas sete lições darão uma olhada mais de perto no dinheiro e na economia.

Parte II – Economia:

8. Ignorância financeira
9. Inflação
10. Valor
11. Dinheiro
12. A história e a queda do dinheiro
13. A insanidade das reservas fracionárias
14. O dinheiro forte²

Mais uma vez, só serei capaz de passar por cima destes pontos. O Bitcoin não é apenas ambicioso, mas também é amplo e profundo em seu escopo, tornando impossível cobrir todos os tópicos relevantes em uma única lição, ensaio, artigo ou livro. Duvido que seja mesmo possível.

O Bitcoin é uma nova forma de dinheiro, o que torna o aprendizado de economia fundamental para entendê-lo. Lidando com a natureza da ação humana e as interações dos agentes econômicos, a economia é provavelmente uma das maiores e mais confusas peças do quebra-cabeça do Bitcoin.

Novamente, essas lições são uma exploração das diversas coisas que aprendi com o Bitcoin. Elas são reflexões de minha jornada pela toca do coelho. Não tendo formação em economia, estou definitivamente fora da minha zona de conforto e especialmente ciente de que qualquer compreensão que possa ter está incompleta. Farei o meu melhor para delinear o que aprendi, mesmo correndo o risco de me fazer de tolo. Afinal de contas,

²Nota do tradutor: O termo *sound money* é quase um trocadilho com o som que uma moeda faz ao cair no chão, mas também passa a ideia de dinheiro saudável.

ainda estou tentando responder à pergunta: “*O que você aprendeu com o Bitcoin?*”

Depois de sete lições examinadas pelas lentes da filosofia, vamos usar as lentes da economia para examinar mais sete. A aula de economia é tudo que posso oferecer neste momento. Destino final: Uma *moeda forte*.

8. Ignorância financeira

“Ela iria pensar que eu sou uma garotinha ignorante por perguntar! Não, não vou perguntar nunca. Talvez eu possa ver o nome escrito em algum lugar..”

– Lewis Carroll, *Alice no País das Maravilhas*

Uma das coisas mais surpreendentes para mim foi a quantidade de finanças, economia e psicologia necessária para obter uma compreensão do que, à primeira vista, parece ser um sistema puramente *técnico* — uma rede de computadores. Parafraseando um baixinho com pés peludos: “É um negócio perigoso, Frodo, pisar no Bitcoin. Você lê o whitepaper e, se não se controlar, não há como saber para onde pode ser levado.”

Para entender um novo sistema monetário você precisa se familiarizar com o antigo. Comecei a perceber logo que a quantidade de educação financeira que desfrutei no sistema educacional foi basicamente *zero*.

Como uma criança de cinco anos, comecei a me fazer muitas perguntas. Como funciona o sistema bancário? Como funciona o mercado de ações? O que é moeda fiduciária? O que é dinheiro *normal*? Por que existe tanta dívida?¹ Quanto dinheiro é impresso e quem decide isso?

¹<https://www.usdebtclock.org/>

Depois de um leve pânico sobre a extensão da minha ignorância, encontrei segurança ao perceber que estava em boa companhia.

“Não é irônico que o Bitcoin tenha me ensinado mais sobre dinheiro do que todos esses anos que passei trabalhando para instituições financeiras... incluindo a minha carreira em um banco central?”

– Aaron²

“Aprendi mais sobre finanças, economia, tecnologia, criptografia, psicologia humana, política, teoria dos jogos, legislação e sobre mim mesmo nos últimos três meses de cripto do que nos últimos três anos e meio de faculdade.”

– Dunny³

Estas são apenas duas das muitas confissões em todo o Twitter.⁴ O Bitcoin, como foi explorado na Lição 1, é uma coisa viva. Mises argumentou que a economia também é uma coisa viva. E, como todos sabemos por experiência pessoal, as coisas vivas são inherentemente difíceis de entender.

²Aaron (@aarontaycc, @fiatminimalist), tweet de 12 de dezembro de 2018 [45]

³Dunny (@BitcoinDunny), tweet de 28 de Novembro de 2017 [24]

⁴Veja <http://bit.ly/btc-learned> para mais confissões no Twitter.

“Um sistema científico é apenas uma estação em uma busca interminável pelo conhecimento. É necessariamente afetado pela insuficiência inerente a todo esforço humano. Mas reconhecer esses fatos não significa que a economia atual esteja defasada. Significa apenas que a economia é uma coisa viva — e viver implica imperfeição e mudança.”

— Ludwig von Mises⁵

Todos nós lemos sobre várias crises financeiras no noticiário, nos perguntamos como funcionam esses grandes resgates e ficamos intrigados com o fato de que ninguém parece jamais ser responsabilizado pelos danos, que estão na casa dos trilhões. Ainda estou confuso, mas pelo menos estou começando a ter um vislumbre do que está acontecendo no mundo das finanças.

Algumas pessoas chegam ao ponto de atribuir a ignorância geral sobre esses tópicos à ignorância intencional e sistêmica. Embora história, física, biologia, matemática e línguas façam parte de nossa educação, o mundo do dinheiro e das finanças, surpreendentemente, só é explorado superficialmente, se é que é explorado. Eu me pergunto se as pessoas ainda estariam dispostas a acumular tantas dívidas como fazem atualmente se todos fossem educados em finanças pessoais e no funcionamento do dinheiro e das dívidas. Então eu me pergunto: quantas camadas de alumínio formam um chapéu de papel alumínio eficaz? Provavelmente três.

⁵Ludwig von Mises, *Ação Humana* [74]

“Essas crises, esses resgates, não são acidentes. E também não é por acaso que não há educação financeira na escola. [...] É premeditado. Assim como antes da Guerra Civil era ilegal educar um escravo, não podemos aprender sobre o dinheiro na escola.”

– Robert Kiyosaki⁶

Como na história de O mágico de Oz, somos orientados a não dar atenção ao homem por trás da cortina. Ao contrário de O Mágico de Oz, agora temos magia real ⁷: uma rede de transferência de valor aberta, resistente à censura e sem fronteiras. Não há cortina, e a magia é visível para qualquer um. ⁸

Bitcoin me ensinou a olhar atrás da cortina e enfrentar minha ignorância financeira.

⁶Robert Kiyosaki, *Por Que o Rico Está Ficando Mais Rico*[39]

⁷<http://bit.ly/btc-wizardry>

⁸<https://github.com/bitcoin/bitcoin>

9. Inflação

“Agora, aqui, sabe, é necessário toda a corrida que você tem para se manter no mesmo lugar. Se você quer ir a um lugar diferente, você deve correr pelo menos duas vezes mais rápido que aquilo!”

– A Rainha de Copas

Tentar entender a inflação monetária e como um sistema não inflacionário como o Bitcoin pode mudar a forma como fazemos as coisas foi o ponto de partida de minha aventura em economia. Eu sabia que a inflação era a taxa pela qual o dinheiro novo era criado, mas não sabia muito além disso.

Enquanto alguns economistas argumentam que a inflação é uma coisa boa, outros argumentam que o dinheiro “forte”, que não pode ser inflado facilmente — como tínhamos na época do padrão ouro — é essencial para uma economia saudável. O Bitcoin, com seu suprimento fixo de 21 milhões, concorda com o último argumento.

Normalmente, os efeitos da inflação não são imediatamente óbvios. Dependendo da taxa de inflação (bem como de outros fatores), o tempo entre a causa e o efeito pode ser de vários anos. Não só isso, mas a inflação afeta diferentes grupos de pessoas de formas diferentes. Como Henry Hazlitt aponta em *Economia em Uma Lição*: “A arte da economia consiste em olhar não apenas para o imediato, mas para os efeitos de longo prazo de qualquer ato ou política; consiste em rastrear as consequências dessa política não apenas para um grupo, mas para todos eles.”

Um dos meus momentos de iluminação pessoal foi a percep-

ção de que emitir moeda — imprimir mais dinheiro — é uma atividade econômica *completamente* diferente de todas as outras atividades econômicas. Enquanto bens e serviços reais produzem valor real para pessoas reais, imprimir dinheiro efetivamente faz o oposto disso. Diminui o valor de todos os que detêm a moeda que está sendo inflacionada.

“Mera inflação — isto é, a mera emissão de mais dinheiro, com a consequência de maiores salários e preços — pode parecer a criação de maior demanda. Mas, em termos de produção e trocas reais de coisas reais, não é.”

— Henry Hazlitt¹

A força destrutiva da inflação torna-se óbvia assim que um pouco de inflação se transforma em *muita*. Se a moeda chega a ser hiperinflacionada, as coisas ficam feias rapidamente.² Conforme o poder de compra da moeda inflacionada se desfaz, ela deixará de armazenar valor com o tempo, com isso as pessoas correrão para colocar seu dinheiro em bens que possam servir como reserva de valor.

Outra consequência da hiperinflação é que todo o dinheiro que as pessoas economizaram ao longo da vida efetivamente desaparecerá. O papel-moeda dentro de nossa carteira ainda estará lá, é claro. Mas será exatamente isso: papel sem valor.

O dinheiro também perde valor com a chamada inflação “moderada”. Simplesmente acontece devagar o suficiente para que a maioria das pessoas não perceba a diminuição do seu poder de compra. E uma vez que as impressoras estão funcionando, a

¹Henry Hazlitt, *Economia em Uma Lição* [35]

²<https://en.wikipedia.org/wiki/Hyperinflation> [83]



Figura 9.1.: Hiperinflação na República de Weimar (1921-1923)

moeda pode ser facilmente inflada, e o que costumava ser uma inflação branda pode se transformar em uma dolorosa inflação descontrolada com o apertar de um botão. Como Friedrich Hayek apontou em um de seus ensaios, a inflação branda geralmente leva à inflação total.

“A inflação ‘moderada’ e suave não pode ajudar — ela só leva a uma inflação absoluta.”

– Friedrich Hayek³

A inflação é particularmente maléfica, pois favorece aqueles que estão mais próximos das impressoras. Leva tempo para que o dinheiro recém-criado circule e os preços se ajustem, portanto se você conseguir colocar as mãos em mais dinheiro antes que o todo mundo se desvalorize, você estará à frente da curva inflacionária. É também por isso que a inflação pode ser vista como um imposto disfarçado porque no final os governos lucram com isso enquanto todos os outros acabam pagando o preço.

³Friedrich Hayek, *1980s Desemprego e Sindicatos* [33]

“Não acho exagero dizer que a história é, em grande parte, uma história de inflação e, geralmente, de inflações criadas por governos para ganhos dos próprios governos.”

– Friedrich Hayek⁴

Até agora, todas as moedas controladas pelo governo foram eventualmente substituídas ou entraram em colapso total. Não importa quão pequena seja a taxa de inflação, crescimento “estável” é apenas outra maneira de dizer crescimento exponencial. Na natureza, assim como na economia, todos os sistemas que crescem exponencialmente terão que se estabilizar ou sofrer um colapso catastrófico.

“Isso não vai acontecer no meu país”, é o que você provavelmente está pensando. Você não pensaria isso se você fosse da Venezuela, que atualmente está sofrendo com a hiperinflação. Com uma taxa de inflação de mais de um milhão por cento, o dinheiro é praticamente inútil. [75]

Isso pode não acontecer nos próximos anos ou com a moeda específica usada em seu país. Mas dê uma olhada na lista de moedas históricas⁵ que mostra que isso inevitavelmente acontecerá no longo prazo. Eu me lembro de usar muitas das moedas listadas: o xelim austríaco, o marco alemão, a lira italiana, o franco francês, a libra irlandesa, o dinar croata, etc. Minha avó até usava a coroa austro-húngara. Conforme o tempo passa, as moedas atualmente em uso⁶ irão caminhar lentamente, mas

⁴Friedrich Hayek, *O Bom Dinheiro* [34]

⁵Veja *Lista de moedas históricas* na Wikipedia. [91]

⁶Veja *Lista de moedas* na Wikipedia [90]

seguramente, para seus respectivos cemitérios. Eles irão hiperinflacionar ou serão substituídas. Em breve, serão moedas históricas. Vamos torná-las obsoletas.

“A história tem nos mostrado que os governos inevitavelmente sucumbirão ao tentação de inflar a oferta de dinheiro.”

– Saifedean Ammous⁷

⁷Saifedean Ammous, *O Padrão Bitcoin* [1]

Por que o Bitcoin é diferente? Em contraste com as moedas dos governos, bens monetários que não são regulamentados pelos Estados, mas pelas leis da física⁸, tendem a sobreviver e até manter valor ao longo do tempo. O melhor exemplo disso até agora é o ouro, que conforme o apropriadamente denominado *Gold-to-Decent-Suit Ratio*⁹ mostra, está mantendo seu valor por centenas e até milhares de anos. Pode não ser perfeitamente “estável” — um conceito questionável em primeiro lugar — mas o valor que ele possui será, pelo menos, da mesma ordem de magnitude.

Se um bem monetário ou moeda mantém bem seu valor ao longo do tempo e do espaço, ele é considerado *forte*. Se não consegue manter o seu valor, porque se deteriora ou infla facilmente, é considerada uma moeda *fraca*. O conceito de força é essencial para entender o Bitcoin e merece um exame mais aprofundado. Voltaremos a falar dele na última lição econômica: O dinheiro forte.

À medida que mais e mais países sofrem com a hiperinflação, mais e mais pessoas terão que enfrentar a realidade do dinheiro forte e fraco. Se tivermos sorte, talvez até mesmo alguns banqueiros centrais sejam forçados a reavaliar suas políticas monetárias. Aconteça o que acontecer, as percepções que ganhei graças ao Bitcoin provavelmente serão inestimáveis, não importa o resultado.

O Bitcoin me ensinou sobre como a inflação é um imposto disfarçado e a catástrofe da hiperinflação.

⁸Gigi, *Consumo de energia do Bitcoin - Uma mudança de perspectiva* [29]

⁹A história mostra que o preço de uma onça de ouro é igual ao preço de um terno masculino decente de acordo com os gerentes de investimento da Sionna [42]

10. Valor

“Era o Coelho Branco, voltando vagarosamente, olhando ansiosamente para trás, como se tivesse perdido algo...”

– Lewis Carroll, *Alice no País das Maravilhas*

O valor é um tanto paradoxal e existem várias teorias ¹ que tentam explicar por que valorizamos certas coisas ao invés de outras. As pessoas estão cientes desse paradoxo há milhares de anos. Como Platão escreveu em seu diálogo com Eutidemo, valorizamos algumas coisas porque são raras e não apenas por sua necessidade para nossa sobrevivência.

“E se você for prudente, dará este mesmo conselho a seus alunos também — que eles nunca devem conversar com ninguém, exceto você e uns aos outros. Pois é o raro, Eutidemo, que é precioso, enquanto a água é mais barata, embora seja a melhor, como disse Píndaro.”

– Platão²

Este paradoxo do valor ³ mostra algo interessante sobre nós, seres humanos. Parecemos valorizar as coisas de uma forma subjetiva ⁴, mas fazemos isso com certos critérios não arbitrários. Algo pode ser *precioso* para alguém por uma variedade

¹Ver *Teoria do valor (economia)* na Wikipedia [102]

²Platão, *Eutidemo* [60]

³Veja *Paradoxo do valor* na Wikipedia [96]

⁴Veja *Teoria subjetiva do valor* na Wikipedia [100]

de razões, mas as coisas que valorizamos compartilham certas características. Se pudermos copiar algo com muita facilidade, ou se for naturalmente abundante, não a valorizamos.

Parece que valorizamos algo porque é escasso (ouro, diamantes, tempo), difícil ou trabalhoso de ser produzido, por não poder ser substituído (uma velha fotografia de um ente querido), por ser útil de uma forma que permite que façamos coisas que de outra forma não poderíamos, ou uma combinação entre essas características, como grandes obras de arte.

O Bitcoin é tudo isso. É extremamente raro (21 milhões), cada vez mais difícil de produzir (redução da recompensa através dos halvings), não pode ser substituído (uma chave privada perdida é perdida para sempre) e nos permite fazer algumas coisas bastante úteis com ele. É indiscutivelmente a melhor ferramenta para transferência de valor entre fronteiras, virtualmente resistente à censura e confisco no processo, além de ser uma reserva de valor auto-soberana, permitindo que os indivíduos armazensem sua riqueza independentemente de bancos e governos, pra citar apenas dois.

O Bitcoin me ensinou que o valor é subjetivo, mas não arbitrário.

11. Dinheiro

““Quando jovem”, o sábio de cãs disse no ato,
“manteve-me lépido e forte este unguento
— não queres comprá-lo?
É barato: eu vendo a um tostão cada pote.””
– O Sábio - Alice no País das Maravilhas

O que é o dinheiro? Nós o usamos todos os dias, mas essa pergunta é surpreendentemente difícil de ser respondida. Dependemos dele em grandes e pequenas quantidades e se tivermos muito pouco nossas vidas se tornarão muito difíceis. No entanto, raramente pensamos sobre o que supostamente faz o mundo girar. O Bitcoin me forçou a responder a esta pergunta repetidamente: Mas o que diabos é o dinheiro?

Em nosso mundo “moderno”, a maioria das pessoas provavelmente pensarão em pedaços de papel quando falam sobre dinheiro, embora a maior parte do nosso dinheiro seja apenas um número na conta bancária. Já estamos usando zeros e uns como dinheiro, então como o Bitcoin é diferente? O Bitcoin é diferente por, em essência, ser um *tipo* de dinheiro muito diferente do que usamos atualmente. Para entender isso, teremos que examinar mais de perto o que é dinheiro, como surgiu e por que o ouro e a prata foram usados na maior parte da história comercial.

Conchas do mar, ouro, prata, papel, bitcoin. No final, **dinheiro é tudo o que as pessoas decidem usar como tal**, não importando forma ou a falta dela.

O dinheiro, como invenção, é engenhoso. Um mundo sem dinheiro é extremamente complicado. Quantos peixes irão me

comprar um par de sapatos novos? De quantas vacas vou precisar para comprar uma casa? E se eu não precisar de nada agora, mas precisar me livrar das minhas maçãs que irão estragar? Você não precisa de muita imaginação para perceber que uma economia de escambo é irritantemente ineficiente.

A melhor coisa sobre dinheiro é que ele pode ser trocado por *qualquer outra coisa* — essa é uma grande invenção! Como Nick Szabo¹ resumiu brilhantemente no seu texto *Shelling Out: The Origins of Money*[69], nós, seres humanos, usamos todos os tipos de coisas como dinheiro: miçangas feitas de materiais raros como marfim, conchas ou ossos especiais, vários tipos de joias e, mais tarde, metais raros como prata e ouro.

“Nesse sentido, é mais típico de um metal precioso. Ao invés de mudar o suprimento para manter o mesmo valor, a quantidade é predeterminada e o valor é que muda.”

– Satoshi Nakamoto²

Sendo criaturas preguiçosas que somos, não pensamos muito em como as coisas funcionam. Dinheiro, para a maioria de nós, funciona muito bem. Como acontece com nossos carros ou computadores, a maioria de nós só é forçada a pensar sobre o funcionamento interno dessas coisas caso elas quebrem. As pessoas que viram suas economias desaparecer por causa da hiperinflação sabem o valor de um bom dinheiro, assim como as pessoas que viram seus amigos e familiares desaparecerem por causa das atrocidades da Alemanha nazista ou da Rússia soviética sabem o valor da privacidade.

O problema com o dinheiro é que ele abrange tudo o que existe. O dinheiro é a metade de cada transação, o que confere enorme poder aos responsáveis pela sua criação.

¹<http://unenumerated.blogspot.com/>

²Satoshi Nakamoto, em resposta a Sepp Hasslberger [50]

“Dado que o dinheiro é a metade de cada transação comercial e que civilizações inteiras literalmente ascendem e são destruídas com base na qualidade do seu dinheiro, estamos falando de um poder incrível, que voa na calada da noite. É o poder de tecer ilusões que parecem reais enquanto duram. Esse é o cerne do poder do Fed.”

– Ron Paul³

O Bitcoin remove pacificamente esse poder, uma vez que ele elimina a criação de dinheiro, e faz isso sem o uso da força.

O dinheiro passou por várias iterações. A maioria das delas foi boa. Elas melhoraram nosso dinheiro de um jeito ou de outro. Muito recentemente, porém, o funcionamento interno do nosso dinheiro foi corrompido. Hoje, quase todo o nosso dinheiro é simplesmente criado *do nada* por quem tem poder para tal. Para entender como isso aconteceu, tive de aprender sobre a história e a subsequente queda do dinheiro.

Resta saber se será necessária uma série de catástrofes ou simplesmente um esforço educacional monumental para corrigir essa corrupção. Rezo aos deuses do dinheiro forte para que seja a segunda opção.

O Bitcoin me ensinou o que é dinheiro.

³Ron Paul, *O Fim do Fed* [57]

12. A história e a queda do dinheiro

“Tudo porque não se lembravam das regrinhas simples que seus amigos lhes haviam ensinado: que um atiçador em brasa acaba queimando sua mão se você insistir em segurá-lo por muito tempo; quando você corta o dedo muito fundo com uma faca, geralmente sai sangue; e ela nunca esquecera que, se você bebe muito de uma garrafa em que está escrito “veneno”, é quase certo que vai se sentir mal, mais cedo ou mais tarde.”

– Lewis Carroll, *Alice no País das Maravilhas*

Muitas pessoas pensam que o dinheiro é lastreado em ouro, que está trancado em grandes cofres protegido por paredes grossas. Isso deixou de ser verdade há muitas décadas. Não tenho certeza do que pensava, uma vez que estava em apuros bem sérios, não tendo virtualmente nenhuma compreensão de ouro, papel-moeda ou por que ele precisaria ser lastreado por algo em primeiro lugar.

Uma parte do aprendizado sobre o Bitcoin inclui entender sobre moeda fiduciária: o que significa, como surgiu e por que pode não ser a melhor ideia que já tivemos. Então, o que exatamente é a moeda fiduciária? E como acabamos usando isso?

Se algo é imposto por *decreto*, significa simplesmente que é imposto por autorização ou proposição formal. Assim, a moeda fiduciária é dinheiro simplesmente porque *alguém* disse que é. Como todos os governos usam moeda fiduciária hoje, esse alguém é *seu governo*. Infelizmente, você não está *livre* para



Figura 12.1.: Fiat: “Que seja feito”

discordar desta proposta de valor. Você sentirá rapidamente que essa proposição é tudo, menos pacífica. Se você se recusar a usar esse papel-moeda para fazer negócios e pagar impostos, as únicas pessoas com quem você poderá discutir sobre economia serão seus colegas de cela.

O valor da moeda fiduciária não decorre de suas propriedades inerentes. O quanto bom é uma moeda fiduciária, está relacionado a, única e exclusivamente, sua capacidade de ter instabilidade/estabilidade política e fiscal daqueles que sonham com sua existência. Seu valor é imposto por decreto, de forma arbitrária.

Até recentemente, dois tipos de dinheiro eram usados: **moeda-mercadoria**, feita com *coisas* preciosas, e **dinheiro representativo**, que simplesmente *representa* a coisa preciosa, principalmente por escrito.

Já mencionamos a moeda-mercadoria acima. As pessoas usavam ossos especiais, conchas e metais preciosos como dinheiro. Mais tarde, principalmente moedas feitas de metais preciosos como ouro e prata foram usadas como dinheiro. A moeda mais antiga encontrada até agora é feita de uma mistura natural de ouro e prata e foi feita há mais de 2.700 anos.¹ Se algo é novo no Bitcoin, o conceito de moeda não é.

¹De acordo com o historiador grego Heródoto, que escreveu no século V a.C., os lídios foram os primeiros a usarem moedas de ouro e prata.[47]



Figura 12.2.: Uma moeda da Lídia. Imagem sob a licença cc-by-sa da Classical Numismatic Group, Inc.

Acontece que acumular moedas, ou hodling, para usar o jargão atual, é quase tão antigo quanto as moedas da antiguidade. O primeiro hodler de moedas foi alguém que colocou quase uma centena delas em um pote e as enterrou nas fundações de um templo apenas para ser encontrado 2500 anos depois. Um *cold storage* muito bom, diga-se de passagem.

Uma das desvantagens de se usar as moedas de metal precioso é que elas podem ser *recortadas* ou *raspadas*, degradando efetivamente o valor da moeda. Novas moedas podem ser cunhadas a partir dos pedaços, inflando a oferta de dinheiro ao longo do tempo e desvalorizando cada moeda no processo. As pessoas estavam literalmente raspando² o máximo que podiam das suas moedas de dólares de prata. Eu me pergunto que tipo de anúncio de *Dollar Shave Club* eles tinham naquela época.

Uma vez que os governos só ficam tranquilos com a inflação quando são eles criando, esforços foram feitos para impedir essa prática feita pelas pessoas. No clássico estilo de polícia e ladrão, os raspadores de moedas ficaram cada vez mais criativos

²Nota do tradutor: *Clipping* ou *shaving off* é o nome dado ao processo de raspar moedas de metais, como ouro ou prata, e usar vários desses fragmentos para cunhar novas moedas.

<https://www.quora.com/What-does-it-mean-to-shave-coins>



Figura 12.3.: Moedas de prata com cortes de tamanhos variados.

com suas técnicas, forçando os “mestres da cunhagem” a ficarem ainda mais criativos em suas contramedidas. Isaac Newton, o mundialmente conhecido físico que escreveu o livro *Principia Mathematica*, costumava ser um desses mestres. Ele quem adicionou pequenas listras nas bordas das moedas que ainda estão presentes hoje. Já se foram os dias em que era fácil depreciar as moedas de forma caseira.

Mesmo levando em consideração esses métodos de depreciação das moedas³, elas ainda sofrem de outros problemas. Elas são volumosas e não são muito convenientes para transportar, especialmente quando grandes transferências de valor precisam acontecer. Aparecer com um enorme saco de moedas de prata toda vez que você quiser comprar uma Mercedes não é algo muito prático.

Falando de coisas alemãs: como o *dólar* dos Estados Unidos ganhou esse nome é outra história interessante. A palavra

³Além de recortar, friccionar (sacudir as moedas em um saco e coletar o seu pó) e tamponar (retirar o miolo da moeda fazendo um furo e depois, martelar a moeda até fechá-lo) foram os métodos mais utilizados para depreciar as moedas. [92]



Figura 12.4.: O “Dólar” original. Saint Joachim foi colocado na face da moeda com seu manto e seu chapéu de mago. Imagem sob a licença cc-by-sa da Wikipedia enviada pelo usuário Berlin-George

“dólar” é derivada da palavra alemã *Thaler*, abreviação de *Joachimsthaler* [101]. Um Joachimsthaler foi uma moeda cunhada na cidade de *Sankt Joachimsthal*. Thaler é simplesmente uma abreviação para alguém (ou algo) vindo do vale, e porque Joachimsthal era o vale da produção de moedas de prata, as pessoas simplesmente se referiam a essas moedas de prata como *Thaler*. Thaler (alemão) se transformou em daalders (holandês) e, finalmente, dólares (inglês).

A introdução do dinheiro representativo foi o prenúncio da queda do dinheiro forte. Os certificados de ouro foram introduzidos em 1863 e cerca de quinze anos depois o dólar de prata também foi lenta, mas constantemente sendo substituído por uma procuração em papel: o certificado de prata. [99]

Demorou cerca de 50 anos desde a introdução dos primeiros certificados de prata até que esses pedaços de papel se transformassem em algo que hoje reconhecemos como um dólar americano.



Figura 12.5.: Um dólar americano de 1928. “Pagável à vista ao portador”. Imagem sob a licença cc-by-sa publicada pela National Numismatic Collection em Smithsonian Institution

Observe que o dólar de prata dos EUA de 1928 na Figura 12.5 ainda atende pelo nome de *certificado de prata*, indicando que este é de fato meramente um documento afirmando que o portador deste pedaço de papel tem direito a uma peça de prata. É interessante ver que o texto que indica isso foi ficando menor com o tempo. O vestígio do “certificado” desapareceu completamente depois de um tempo sendo substituído pela declaração tranquilizadora de que essas são notas do Federal Reserve.⁴

Como mencionado acima, o mesmo aconteceu com o ouro. A maior parte do mundo seguia um padrão bimetálico [77], o que significa que as moedas eram feitas principalmente de ouro e prata. Ter certificados de ouro resgatáveis em moedas de ouro era indiscutivelmente uma melhoria tecnológica. O papel é mais conveniente, mais leve e, como pode ser dividido arbitrariamente simplesmente colocando um número menor nele, é mais fácil dividi-lo em unidades menores.

⁴Nota do tradutor: Federal Reserve é o banco central dos Estados Unidos.



Figura 12.6.: Uma nota de \$100 dólares cunhada em 1928 em certificados de ouro. Imagem sob a licença cc-by-sa publicada pela National Numismatic Collection, National Museum of American History.

Para lembrar aos portadores (usuários) que esses certificados eram representativos de ouro e da prata físicos, eles tinham cores de acordo com o metal e isso era declarado claramente no próprio certificado. Você pode ler com facilidade a escrita de cima para baixo:

“Isso certifica que foram depositados no tesouro dos Estados Unidos da América cem dólares em moedas de ouro pagáveis à vista ao portador.”

Em 1963, as palavras “PAGÁVEL À VISTA AO PORTADOR” foram removidas de todas as notas recém emitidas. Cinco anos depois, o resgate das notas de papel por ouro e prata terminou.

As palavras que sugeriam as origens e a ideia por trás do papel-moeda foram removidas. A cor dourada desapareceu. Tudo o que restou foi o papel e com ele a capacidade do governo de imprimir o quanto quiser.



Figura 12.7.: Uma nota de vinte dólares americanos de 2004 usada atualmente. “ESTA NOTA É DE CURSO FORÇADO”

Com a abolição do padrão-ouro em 1971, esse truque de mágica de um século de duração estava finalizado. O dinheiro se tornou a ilusão que todos compartilhamos até hoje: o dinheiro fiduciário. Vale alguma coisa porque alguém comandando um exército e operando prisões diz que vale alguma coisa. Como pode ser lido claramente em cada nota de dólar em circulação hoje, “ESTA NOTA É DE CURSO FORÇADO”. Em outras palavras: ela vale porque a nota diz que vale.

A propósito, há outra lição interessante sobre as notas de hoje, que está escondido escondido à vista. A segunda linha diz que ela é de curso forçado “PARA TODAS AS DÍVIDAS, PÚBLICAS E PRIVADAS”. O que pode ser óbvio para os economistas me surpreendeu: todo dinheiro é dívida. Minha cabeça ainda está doendo por causa disso, e deixarei a exploração da relação entre dinheiro e dívida como um exercício para você, leitor.

Como vimos, ouro e prata foram usados como dinheiro por milênios. Com o tempo, as moedas feitas de ouro e prata foram substituídas por papel. O papel foi lentamente sendo aceito

como forma de pagamento. Essa aceitação criou uma ilusão — **a ilusão de que o próprio papel tem valor**. O movimento final foi cortar completamente o vínculo entre a representação e o seu valor real, abolindo o padrão-ouro e convencendo a todos de que o papel em si é precioso.

O Bitcoin me ensinou sobre a história do dinheiro e o maior truque da ilusão da história da economia: a moeda fiduciária.

13. A insanidade das reservas fracionárias

Era muito tarde para desejar isso! Ela continuou crescendo e crescendo, e logo precisou ajoelhar-se no chão. Em outro minuto não havia nem mesmo um quarto para isso, e ela tentou deitar-se com um cotovelo contra a porta e o outro braço sobre a cabeça! Alice continuava a crescer e, como último recurso, ela colocou um braço para fora da janela e um pé para dentro da chaminé, dizendo para si mesma “Agora eu não posso fazer mais nada, o que quer quer seja que aconteça. O que vai ser de mim?”

– Lewis Carroll, *Alice no País das Maravilhas*

Valor e dinheiro não são tópicos triviais, especialmente nos dias atuais. O processo de criação de dinheiro em nosso sistema bancário não é algo simples também, e tenho a sensação de que é assim de propósito. O que eu encontrei antes apenas na faculdade e em textos jurídicos, parece ser uma prática comum no mundo financeiro também. Nada é explicado em termos simples para o público leigo, não porque é algo realmente complexo, mas porque a verdade está escondida atrás de camadas e camadas de jargões e *aparente* complexidade. “Política monetária expansionista, flexibilização quantitativa¹, estímulo fiscal à economia.” O público acena concordando hipnotizado pelas palavras bonitas.

¹Quantitative easing

Reservas fracionárias e flexibilização quantitativa são duas dessas palavras bonitas, que ofuscam o que realmente está acontecendo, mascarando como algo complexo e difícil de entender. Se você explicasse a uma criança de cinco anos a insanidade de ambos tudo se tornaria aparente rapidamente.

Godfrey Bloom, dirigindo-se ao Parlamento Europeu durante um debate conjunto, disse isto de uma maneira mil vezes melhor do que eu jamais poderia:

“[...] você não entende direito o conceito de banco. Todos os bancos estão falidos. O Banco Santander, o Deutsche Bank, o Royal Bank of Scotland — estão todos falidos! E por que eles estão falidos? Não é um ato de Deus. Não é algum tipo de tsunami. Eles estão falidos porque temos um sistema chamado ‘reserva fracionária’, o que significa que os bancos podem emprestar dinheiro que na verdade não possuem! É um escândalo criminoso e já dura muito tempo. [...] Temos falsificação — às vezes chamada de afrouxamento quantitativo — ou seja, falsificação com outro nome qualquer. Impressão artificial de dinheiro, que se qualquer pessoa comum fizesse iria para a prisão por muito tempo [...] e até começarmos a enviar banqueiros — e eu incluo banqueiros centrais e políticos — para a prisão por este ultraje, isso vai continuar.”

– Godfrey Bloom²

Deixe-me repetir a parte mais importante: **os bancos podem emprestar dinheiro que na verdade não possuem.**

Graças ao sistema de reservas fracionárias, um banco só precisa manter uma pequena *fração* de cada dólar que recebe. É

²Debate conjunto na união bancária [17]

algo entre 0 e 10%³, geralmente na limite inferior, o que torna as coisas ainda piores.

Vamos usar um exemplo concreto para entender melhor essa ideia maluca. Com a fração de 10% vamos conseguir fazer todos os cálculos em nossa cabeça. Pronto. Pense comigo: se você levar \$100 para um banco — porque você não quer guardá-lo embaixo do seu colchão — eles só precisam manter a *fração* acordada. Em nosso exemplo, seria \$10, porque 10% de \$100 é \$10. Simples, certo?

Então, o que os bancos fazem com o resto do dinheiro? O que acontece com o seus \$90? Eles fazem o que bancos fazem, emprestam para outras pessoas. O resultado é um efeito multiplicador de moeda, o que aumenta enormemente a oferta de moeda na economia (Figura 13.1). Seu depósito inicial de \$100 logo se transformará em \$190. Ao emprestar uma fração de 90% dos \$90 recém-criados logo teremos \$271 na economia. E \$343,90 depois disso. A oferta de dinheiro está aumentando recursivamente, uma vez que os bancos estão literalmente emprestando dinheiro que eles não possuem [93]. Sem um único Abracadabra, os bancos transformam magicamente \$100 em mil dólares ou mais. Acontece que multiplicar o valor inicial por 10 é fácil. Leva apenas algumas rodadas de empréstimo.

Não me entenda mal: não há nada de errado em fazer empréstimos. Não há nada de errado com os juros. Não há nada de errado com os bons e velhos bancos que armazenavam sua fortuna em algum lugar mais seguro do que na sua gaveta de meias.

Os bancos centrais, no entanto, são uma besta diferente. Abo-

³Esse sistema no Brasil é implementado através dos depósitos compulsórios que os bancos precisam fazer junto ao Banco Central.

[https://www.bcb.gov.br/estabilidedefinanceira/
recolhimentoscompulsorios](https://www.bcb.gov.br/estabilidedefinanceira/recolhimentoscompulsorios)

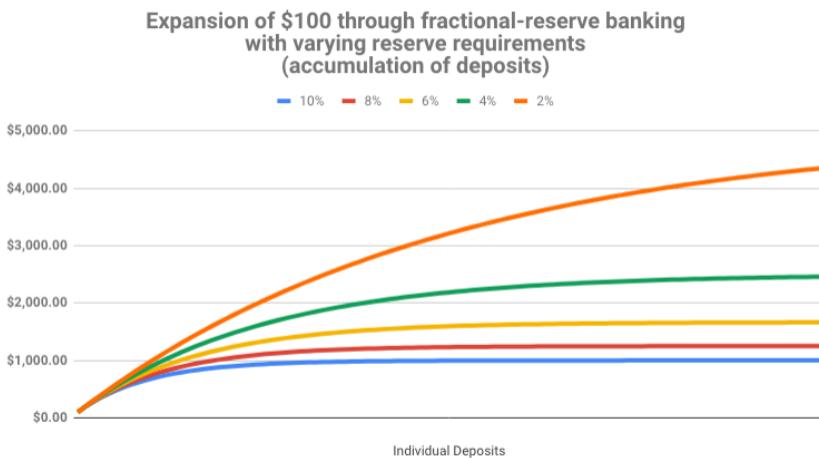


Figura 13.1.: O efeito multiplicador da moeda

minações de regulação financeira, metade pública metade privada, brincando de deus com algo que afeta todos que fazem parte da nossa civilização global, sem consciência, apenas interessados no futuro imediato e, aparentemente, sem qualquer responsabilidade ou auditabilidade (ver Figura 13.2).

Embora o Bitcoin ainda seja inflacionário, deixará de ser em breve. O fornecimento estritamente limitado de 21 milhões de bitcoins acabará com a inflação por completo. Agora temos dois mundos monetários: um inflacionário, onde o dinheiro é impresso arbitrariamente, e o mundo do Bitcoin, onde o suprimento máximo é fixo e facilmente auditável por todos. Um é forçado através da violência, o outro pode ser acompanhado por qualquer um que queira. Sem barreiras de entrada, ninguém para pedir permissão. Participação voluntária. Essa é a beleza do Bitcoin.

Eu diria que o argumento entre economistas keynesianos⁴ e

⁴Teorias monetárias que estão de acordo com John Maynard Keynes e



Figura 13.2.: Janet Yellen, Secretária do Tesouro dos Estados Unidos, se opõe fortemente contra a auditoria do Fed, enquanto o Cara da Placa do Bitcoin é fortemente a favor de se comprar bitcoin.

austríacos⁵ não é apenas acadêmico. Satoshi conseguiu construir um sistema de transferência de valor com esteroides, criando o melhor dinheiro já existiu no processo. De uma forma ou de outra, mais e mais pessoas aprenderão sobre o golpe que é o sistema de reservas fracionárias. Se chegarem a conclusões semelhantes a da maioria dos austríacos e dos bitcoinheiros, eles podem entrar na crescente internet do dinheiro. Ninguém pode pará-lo se decidirem fazer isso.

Bitcoin me ensinou que o sistema de reservas fracionárias é pura insanidade.

seus discípulos [86]

⁵Escola de pensamento econômico baseado no individualismo metodológico [76]

14. O dinheiro forte

“A primeira coisa que eu tenho que fazer”, disse Alice para si mesma, enquanto vagueava pela floresta, “é crescer até meu tamanho normal outra vez, e a segunda coisa é encontrar o caminho para aquele jardim adorável. Acho que este é o melhor plano.”

– Lewis Carroll, *Alice no País das Maravilhas*

A lição mais importante que aprendi com o Bitcoin é que, no longo prazo, o dinheiro forte é superior ao dinheiro fraco. Dinheiro forte, também conhecido como *moeda sólida*, é qualquer moeda negociada globalmente que serve como uma reserva confiável de valor.

É verdade que o Bitcoin ainda é jovem e volátil. Os críticos dirão que ele não armazena valor de forma confiável. O argumento da volatilidade está se perdendo com o tempo. A volatilidade é esperada. O mercado vai demorar um pouco para descobrir o preço justo desse novo dinheiro. Além disso, como muitas vezes é dito em tom de brincadeira, é apenas um erro de medição. Se você pensar em dólares, não conseguirá ver que um bitcoin sempre será um bitcoin.

“Uma oferta de moeda fixa, ou uma oferta alterada apenas de acordo com critérios objetivos e calculáveis, é uma condição necessária para um preço justo do dinheiro.”

– Fr. Bernard W. Dempsey, S.J.¹

¹Perry J. Roets, S.J., *Revisão da Economia Social* [62]

$$\sum_{i=0}^{32} \frac{21000 \lfloor \frac{50*10^8}{2^i} \rfloor}{10^8} \quad (14.1)$$

Figura 14.1.: Fórmula de emissão do Bitcoin

Como um rápido passeio pelo cemitério de moedas esquecidas nos mostra: o dinheiro que pode ser impresso será impresso. Até agora, nenhum ser humano na história foi capaz de resistir a essa tentação.

O Bitcoin acaba com a tentação de imprimir dinheiro de uma forma engenhosa. Satoshi estava ciente de nossa ganância e falibilidade — é por isso que ele escolheu algo mais confiável do que a vontade humana: a matemática.

Embora essa fórmula seja útil para descrever o suprimento de Bitcoin, ela não está, na verdade, em nenhum lugar do código. A emissão de novos bitcoins é feita de forma controlada por algoritmos, reduzindo a recompensa que é paga aos mineradores a cada quatro anos [13]. A fórmula acima é usada para resumir rapidamente o que está acontecendo por trás dos bastidores. O que realmente acontece pode ser visto com mais facilidade observando a mudança na recompensa do bloco, a recompensa paga a quem encontrar um bloco válido, que acontece aproximadamente a cada 10 minutos.

Fórmulas, funções logarítmicas e exponenciais não são intuitivas, e poucas pessoas conseguem entendê-las. O conceito de *força* de um dinheiro pode ser mais fácil de entender se visto de outra forma. Uma vez que sabemos a quantidade de alguma coisa e a dificuldade que é a sua produção ou como é difícil colocar as nossas mãos nisso, compreendemos imediatamente seu valor. O que é verdade para as pinturas do Picasso, para os violões de Elvis Presley e para os violinos Stradivarius é verdade

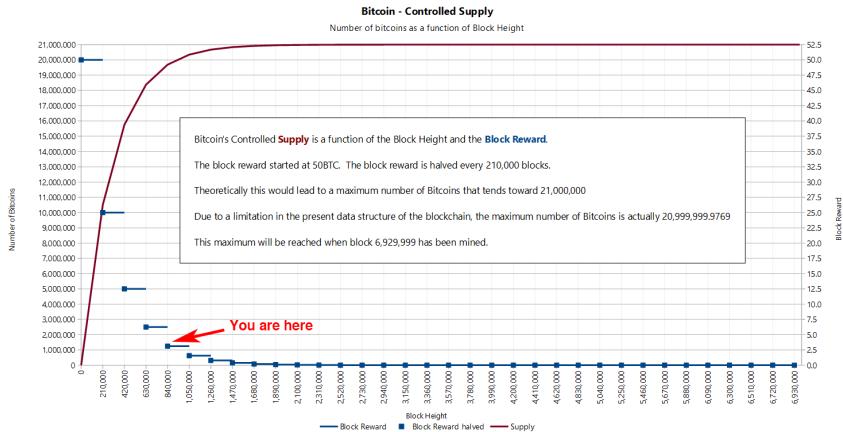


Figura 14.2.: Suprimento controlado do Bitcoin

também para a moeda fiduciária, ouro e bitcoins.

A força da moeda fiduciária depende de quem está no comando da impressora. Alguns governos podem estar mais dispostos a imprimir grandes quantidades de moeda do que outros, resultando em uma moeda mais fraca. Outros governos podem ser mais restritivos na impressão de dinheiro, resultando em uma moeda mais forte.

“Um aspecto importante desta nova realidade é que instituições como o Fed não vão à falência. Eles podem imprimir qualquer quantia de dinheiro que possam precisar para si mesmos a um custo próximo de zero.”

– Jörg Guido Hülsmann²

Antes de termos moedas fiduciárias, a solidez do dinheiro era determinada pelas propriedades naturais do material que usávamos como moeda. A quantidade de ouro na terra é limitada

²Jörg Guido Hülsmann, *A Ética da Produção da Moeda* [38]

pelas leis da física. O ouro é raro porque supernovas e colisões de estrelas de nêutrons são raras. O “fluxo” de ouro é limitado porque extraí-lo da terra demanda um grande esforço. Por ser um elemento pesado, está principalmente enterrado no subsolo.

A abolição do padrão ouro deu lugar a uma nova realidade: adicionar dinheiro novo requer apenas uma gota de tinta. Em nosso mundo moderno, adicionar alguns zeros ao saldo de uma conta bancária exige ainda menos esforço: mudar alguns bits no computador de um banco é o suficiente.

O princípio delineado acima pode ser expresso de forma mais geral como a proporção de “estoque” em relação ao “fluxo”. Simplificando, o *estoque* é quanto de algo temos atualmente. Para nossos propósitos, o estoque é uma medida da oferta monetária atual. O *fluxo* é o quanto é produzido durante um período de tempo (por exemplo, em um ano). A chave para entender o dinheiro forte é entender essa relação entre estoque/fluxo (também conhecida como stock-to-flow, ou pelo sua abreviação S2F).

Calcular a relação estoque/fluxo de uma moeda fiduciária é difícil, porque quanto dinheiro existe depende de como se analisa. [94] Você poderia contar apenas as notas e moedas (M_0), adicionar cheques e depósitos bancários (M_1), contas de poupança e fundos mútuos e algumas outras coisas mais (M_2), e ainda adicionar certificados de depósito a tudo isso (M_3). Além disso, como tudo isso é definido e medido varia de país para país e como o Federal Reserve dos EUA parou de publicar os números [61] para o M_3 , teremos que nos contentar com o suprimento monetário de M_2 . Eu adoraria verificar esses números, mas acho que temos que confiar no Fed, por enquanto.

O ouro, um dos metais mais raros da Terra, tem o maior stock-to-flow. De acordo com o US Geological Survey, um pouco mais de 190.000 toneladas foram extraídas. Nos últimos anos, cerca de 3.100 toneladas de ouro foram extraídas por ano. [68]

Usando esses números, podemos calcular facilmente a razão

$$\frac{190,000t}{3,100t} = 61 \quad (14.2)$$

Figura 14.3.: Razão stock-to-flow do ouro

estoque/fluxo do ouro (ver Figura 14.3).

Nada tem uma relação estoque/fluxo mais alta do que o ouro. É por isso que o ouro, até agora, era o dinheiro mais forte e sólido que existia. Costuma-se dizer que todo o ouro extraído até agora caberia em duas piscinas olímpicas. De acordo com meus cálculos³, precisaríamos de quatro. Talvez seja necessário atualizar essas informações ou as piscinas olímpicas ficaram menores.

O Bitcoin entra em cena. Como você provavelmente sabe, a mineração de bitcoin esteve na moda nos últimos dois anos. Isso ocorre porque ainda estamos nas fases iniciais do que é chamado de *era da recompensa*, onde os nodes de mineração são recompensados com *muitos* bitcoins por seu esforço computacional. Atualmente, estamos na era de recompensa número 4, que começou em 2020 e terminará no início de 2024, provavelmente em maio. Embora o suprimento de bitcoin seja predeterminado, o seu funcionamento interno permite apenas datas aproximadas. No entanto, podemos prever com certeza quão alto será o stock-to-flow do Bitcoin. Alerta de spoiler: será alto.

Quão alto? Bem, acontece que o Bitcoin ficará infinitamente mais forte (veja a Figura 14.4).

Devido a uma diminuição exponencial da recompensa de mineração, o fluxo de novos bitcoins diminuirá, resultando em uma relação estoque/fluxo cada vez mais alta. Ele alcançará o ouro

³<https://bit.ly/gold-pools>

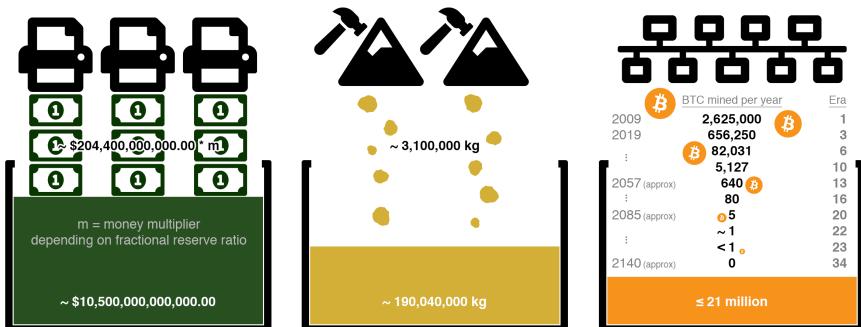


Figura 14.4.: Visualização do stock-to-flow do dólar, ouro e Bitcoin

em 2020, apenas para superá-lo quatro anos depois, dobrando sua força novamente. Essa duplicação ocorrerá 64 vezes no total. Graças ao poder dos exponenciais, o número de bitcoins minerados por ano cairá para menos de 100 em 50 anos e abaixo de 1 bitcoin em 75 anos. A torneira global, que é a recompensa em bloco, vai secar por volta do ano 2140, parando efetivamente a produção de novos bitcoins. Este é um jogo de longo prazo. Se você está lendo isso, ainda está no começo.

À medida que o bitcoin se aproxima da proporção infinita de estoque para fluxo, será o dinheiro mais forte existente. A solidade infinita é difícil de vencer.

Visto pelas lentes da economia, o *ajuste de dificuldade* do Bitcoin é provavelmente seu componente mais importante. O quanto difícil é ‘extrair’ bitcoins depende da rapidez com que novos bitcoins são minerados.⁴ É o ajuste dinâmico da dificuldade de mineração da rede que nos permite prever seu suprimento futuro.

A simplicidade do algoritmo de ajuste de dificuldade pode desviar a atenção de sua profundidade, mas ele é realmente uma

⁴Na verdade, depende da rapidez com que blocos válidos são encontrados, mas para nosso propósito, isso é a mesma coisa que “minerar bitcoins” e será assim, pelos próximos 120 anos.

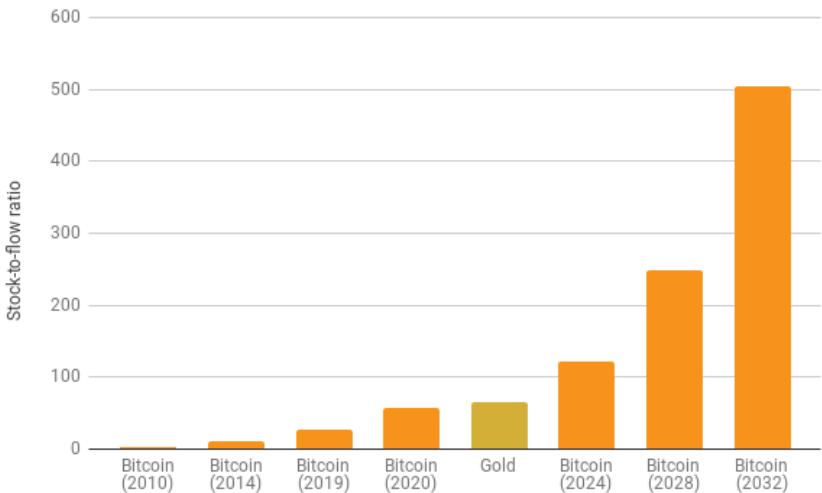


Figura 14.5.: Aumento da razão estoque/fluxo do bitcoin em comparação com o ouro

revolução de proporções einsteinianas. Isso garante que, não importa o quanto de esforço, muito ou pouco, seja gasto na mineração, a emissão controlada de Bitcoin não será interrompida. Ao contrário de todos os outros recursos, não importa quanta energia alguém coloque na mineração de bitcoins, a recompensa total não aumentará.

Assim como $E = mc^2$ dita o limite de velocidade universal em nosso universo, o ajuste de dificuldade do Bitcoin dita o **limite do dinheiro** no universo Bitcoin.

Se não fosse por esse ajuste de dificuldade, todos os bitcoins já teriam sido minerados. Se não fosse por esse ajuste de dificuldade, o Bitcoin provavelmente não teria sobrevivido a sua infância. É o que protege a rede em sua era de recompensa. É o

que garante uma distribuição estável e justa⁵ de novos bitcoins. É o termostato que regula a política monetária do Bitcoin.

Einstein nos mostrou algo novo: não importa o quanto você empurre um objeto, em certo ponto você não conseguirá obter mais velocidade dele. Satoshi também nos mostrou algo novo: não importa o quanto você procure por esse ouro digital, em certo ponto você não conseguirá ‘extrair’ mais bitcoins. Pela primeira vez na história da humanidade, temos um bem monetário que, não importa o quanto você tente, não será capaz de produzir mais.

O Bitcoin me ensinou que dinheiro forte é essencial.

⁵Dan Held, *A distribuição do Bitcoin foi justa* [36]

Parte III.

Tecnologia

Tecnologia

“Desta vez vou me sair melhor”, disse para si mesma, e começou por pegar a chavezinha de ouro e destrancar a porta que dava para o jardim.

– Lewis Carroll, *Alice no País das Maravilhas*

Chaves de ouro, relógios que só funcionam por acaso, corridas para resolver enigmas estranhos e construtores que não têm rostos nem nomes. O que parecem histórias de faz de conta é comum no mundo do Bitcoin.

Como exploramos no Capítulo II, grandes partes do sistema financeiro atual estão sistematicamente quebradas. Como Alice, só podemos esperar administrar melhor desta vez. Mas graças a um inventor pseudoanônimo temos uma tecnologia incrivelmente sofisticada para nos apoiar desta vez: o Bitcoin.

Resolver problemas em um ambiente radicalmente descentralizado e hostil requer soluções únicas. O que de outra forma seriam problemas triviais para resolver são tudo menos isso neste mundo estranho. O Bitcoin depende de uma criptografia forte para a maioria das soluções, pelo menos quando analisado através das lentes da tecnologia. Iremos explorar o quão forte essa criptografia é em uma das lições a seguir.

A criptografia é o que o Bitcoin usa para remover a confiança em autoridades. Ao invés de depender de instituições centralizadas, o sistema depende da autoridade final do nosso universo: a física. Alguns pequenos grãos de confiança ainda são necessários, no entanto. Examinaremos isso na segunda lição deste capítulo.

Parte III – Tecnologia:

15. Força nos números
16. Reflexões sobre: “Não Confie, Verifique”
17. Dizer as horas demanda trabalho
18. Mova-se lentamente e não quebre as coisas
19. A privacidade não morreu
20. Cypherpunks escrevem código
21. Metáforas para o futuro do Bitcoin

As últimas duas lições exploram o *ethos* do desenvolvimento tecnológico no Bitcoin, que é indiscutivelmente tão importante quanto a própria tecnologia. O Bitcoin não é o próximo aplicativo revolucionário no seu celular. É a base de uma nova realidade econômica, razão pela qual o Bitcoin deve ser tratado como um software financeiro de nível nuclear.

Onde estamos nesta revolução financeira, social e tecnológica? Redes e tecnologias do passado podem servir como metáforas para o futuro do Bitcoin, que são exploradas na última lição deste capítulo.

Mais uma vez, aperte o cinto e aproveite o passeio. Como todas as tecnologias exponenciais, estamos prestes a nos tornar parabólicos.

15. Força nos números

“Deixe-me ver: quatro vezes cinco é doze, e quatro vezes seis é treze, e quatro vezes sete é... ai, ai! deste jeito nunca vou chegar a vinte!”

– Lewis Carroll, *Alice no País das Maravilhas*

Os números são uma parte essencial do nosso dia a dia. Números grandes, entretanto, não são algo com que a maioria de nós esteja muito familiarizado. Os maiores números que podemos encontrar na vida cotidiana estão na faixa dos milhões, bilhões ou trilhões. Podemos ler sobre milhões de pessoas na pobreza, bilhões de dólares gastos em resgates aos bancos e trilhões de dívida pública. Embora seja difícil entender essas manchetes, estamos um tanto quanto confortáveis com o tamanho desses números.

Embora essas cifras de bilhões e trilhões nos pareçam confortáveis, nossa intuição já começa a falhar com números dessa magnitude. Você sabe quanto tempo teria que esperar para que um milhão/bilhão/trilhão de segundos passassem? Se você for como eu, vai estar perdido sem realmente fazer as contas.

Vamos dar uma olhada neste exemplo: a diferença entre cada um é um aumento de três ordens de magnitude: 10^6 , 10^9 , 10^{12} . Pensar em segundos não é muito útil, então vamos traduzir isso em algo que possamos entender com mais clareza:

- 10^6 : Um milhão de segundos se passou há 1 semana e meia.
- 10^9 : Um bilhão de segundos são aproximadamente 32 anos.

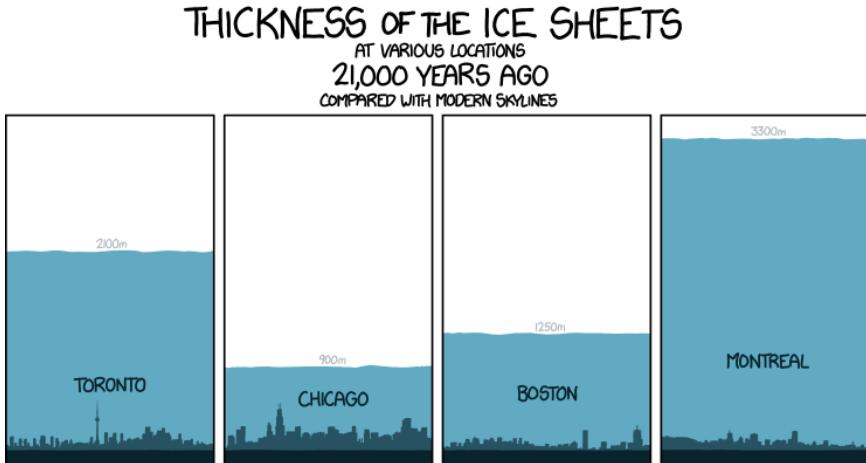


Figura 15.1.: Há aproximadamente um trilhão de segundos no passado. Fonte: xkcd 1225

- 10^{12} : Um trilhão de segundos atrás, Manhattan estava coberta por uma camada grossa de gelo.¹

Assim que entramos na escala astronômica da criptografia moderna, nossa compreensão falha catastroficamente. O Bitcoin é construído em torno de grandes números e da impossibilidade adivinhá-los facilmente. Esses números são muito, muito maiores do que qualquer coisa que possamos encontrar no nosso dia a dia. Muitas ordens de magnitude maiores. Entender o quanto grandes esses números realmente são é essencial para entender o Bitcoin como um todo.

Vamos pegar o SHA-256², uma das funções hash³ usada no Bitcoin como um exemplo concreto. É natural pensar em 256

¹Um trilhão de segundos (10^{12}) foi há 31710 anos. A última Era Glacial foi há 33,000 anos. [88]

²O SHA-256 faz parte da família SHA-2 de funções criptográficas de hash desenvolvidas pela NSA. [97]

³O Bitcoin usa SHA-256 em seu algoritmo de hashing de bloco. [12]

bits como “duzentos e cinquenta e seis”, que não é um número grande. No entanto, o número depois do SHA-256 está falando sobre ordens de grandeza astronômicas — algo com que nossos cérebros não estão bem equipados para lidar.

Embora o comprimento do bit seja uma métrica conveniente, o verdadeiro significado da segurança dos 256 bits se perde na tradução. Semelhante aos milhões (10^6) e bilhões (10^9) acima, o número do SHA-256 é de ordem de grandeza (2^{256}).

Então, quão forte o SHA-256 é exatamente?

“SHA-256 é muito forte. Não é como uma mudança incremental de MD5 para SHA1. Pode durar várias décadas, a menos que haja algum avanço no ataque.”

— Satoshi Nakamoto⁴

Vamos esclarecer as coisas. 2^{256} é igual ao seguinte número:

115 quatuorvigintilhão 792 trevigintilhões 89 duovigintilhões 237 unvigintilhões 316 vigintilhões 195 novendecilhões 423 octodecilhões 570 septendecilhões 985 sexdecilhões 8 quindecilhões 687 quatuordecilhões 907 tredecilhões 853 duodecilhões 269 undecilhões 984 decilhões 665 nonilhões 640 octilhões 564 septilhões 39 sextilhões 457 quintilhões de 584 quadrilhões 7 trilhões 913 bilhões 129 milhões 639 mil 936.

São muitos nonilhões! Tentar fazer com que esse número entre na sua cabeça é praticamente impossível. Não há nada no universo físico para compararmos. É muito maior do que o número de átomos no universo observável. O cérebro humano simplesmente não foi feito para dar sentido a essa magnitude.

⁴Satoshi Nakamoto, em resposta a pergunta sobre as colisões no SHA-256.
[54]

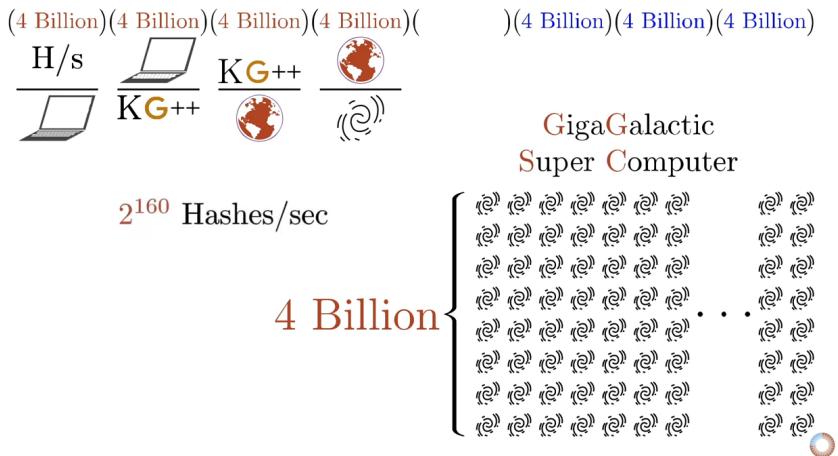


Figura 15.2.: Ilustração da segurança do SHA-256. Gráfico original feito por Grant Sanderson, conhecido como *3Blue1Brown*.

Uma das melhores visualizações da verdadeira força do SHA-256 é um vídeo de Grant Sanderson. Apropriadamente nomeado “*Quão forte é a segurança de 256 bits?*”⁵, onde ele mostra maravilhosamente o quão grande é um número de 256 bits. Faça um favor a si mesmo e reserve cinco minutos para assisti-lo. Como todos os outros vídeos do *3Blue1Brown*, este não é apenas fascinante, mas também excepcionalmente bem feito. Alerta: você pode cair na toca do coelho da matemática.

Bruce Schneier [65] usou os limites físicos da computação para colocar este número em perspectiva: mesmo que consigamos construir um computador perfeito, que poderia usar energia proveniente de qualquer tipo de matriz energética para mudar bits perfeitamente [87], construir uma esfera de Dyson⁶ envolta do

⁵ Assista ao vídeo acessando o link https://youtu.be/S9JGmA5_unY

⁶ Uma esfera Dyson é uma mega estrutura hipotética que poderia envolver uma estrela e capturar uma grande porcentagem da sua energia ema-

sol e deixar este computador rodando por 100 bilhões de bilhões de anos, ainda assim teríamos apenas 25% de chance de encontrar a agulha no palheiro de 256 bits.

“Estes números não tem nada a ver com a tecnologia dos nossos dispositivos, eles são o máximo que a termodinâmica nos permite. E eles implicam fortemente que um ataque de força bruta contra chaves de 256 bits seja inviável até que os computadores possam ser construídos com alguma coisa além da matéria e que ocupem algo além do espaço físico que conhecemos.”

– Bruce Schneier⁷

É difícil exagerar a profundidade disso. A criptografia forte inverte o equilíbrio de poder do mundo físico com o qual estamos tão acostumados. Coisas inquebráveis não existem no mundo real. Aplique força suficiente e poderá abrir qualquer porta, caixa ou baú de tesouro.

O baú do tesouro do Bitcoin é muito diferente. É protegido por uma criptografia fortíssima, que não dá lugar à força bruta. E enquanto as suposições matemáticas se mantiverem, a força bruta é tudo o que temos. Existem também a opção de um ataque global, usando uma chave inglesa de \$5 dólares (Figura 15.3), mas a tortura não funcionará para todos os endereços do Bitcoin, e as paredes criptográficas dessa moeda derrotarão os ataques de força bruta. Mesmo se alguém tente atacar com a força de mil sóis. Literalmente.

Este fato e suas implicações foram resumidos de forma pujante em *Call to Cryptographic Arms*: “*Nenhuma quantidade de força coercitiva resolverá um problema matemático.*”

nada. [81]

⁷Bruce Schneier, *Applied Cryptography* [64]

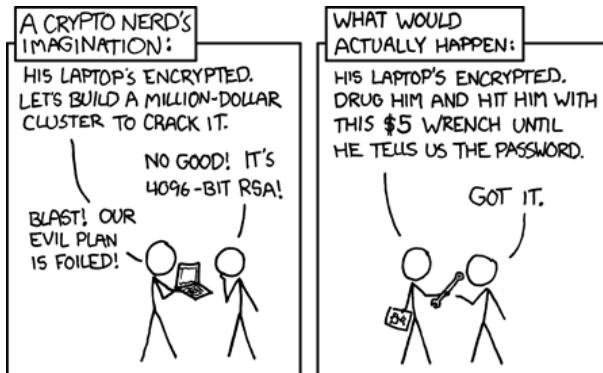


Figura 15.3.: Ataque de chave inglesa de \$5 dólares. Fonte: xkcd 538

“Não é óbvio que o mundo teve que funcionar dessa maneira. Mas de alguma forma o universo sorri para a criptografia.”

– Julian Assange⁸

Ninguém ainda sabe ao certo se esse sorriso é genuíno ou não. É possível que nossa suposição de assimetrias matemáticas esteja errada e então descobriremos que P na verdade é igual a NP [95], ou encontraremos soluções surpreendentemente rápidas para problemas específicos [79] que atualmente assumimos serem difíceis. Se for esse o caso, a criptografia como a conhecemos deixará de existir e as implicações disso provavelmente mudariam o mundo como o conhecemos hoje radicalmente.

“Vires in Numeris” = “Força nos Números”⁹

⁸ Julian Assange, *A Call to Cryptographic Arms* [5]

⁹ *Vires in Numeris* foi a primeira proposta de lema para o Bitcoin, feita pelo usuário *epii* [25] no fórum bitcointalk.

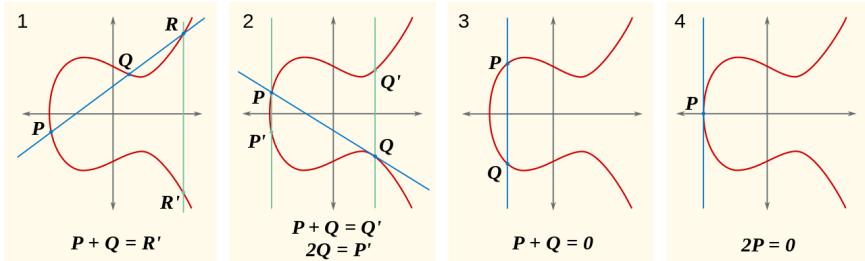


Figura 15.4.: Exemplo de curvas elípticas. Gráficos sob a licença cc-by-sa disponibilizadas por Emmanuel Boutet.

Vires in numeris não é apenas um lema cativante usado por bitcoinheiros. A compreensão de que existe uma força que não pode ser freada e que foi encontrada nos números é profunda. Entender isso e a inversão dos equilíbrios de poder existentes foi o que permitiu mudar minha visão de mundo e do futuro que está à nossa frente.

Um resultado direto disso é o fato de você não precisar pedir permissão a ninguém para participar do Bitcoin. Não existe uma página para se inscrever, nenhuma empresa responsável, nenhuma agência governamental para enviar os formulários de inscrição. Basta gerar um grande número e você estará pronto para prosseguir. A autoridade central de criação de contas é a matemática. E só Deus sabe quem está encarregado disso.

O Bitcoin é construído com base em nosso melhor entendimento da realidade. Embora ainda existam muitos problemas abertos na física, ciência da computação e matemática, temos muita certeza sobre algumas coisas. Que existe uma assimetria entre encontrar soluções e validar a correção dessas soluções, é uma delas. Que para computar precisamos de energia, é outra. Em outras palavras: encontrar uma agulha em um palheiro é mais difícil do que verificar se a coisa pontuda em sua mão é mesmo uma agulha ou não. E encontrar a agulha dá um trabalho.

A vastidão do espaço de endereços do Bitcoin é verdadeiramente estonteante. O número de chaves privadas é ainda mais. É fascinante como muito de nosso mundo moderno se resume à improbabilidade de encontrar uma agulha em um palheiro incommensuravelmente grande. Agora estou mais ciente desse fato do que nunca.

O Bitcoin me ensinou que existe força nos números.

16. Reflexões sobre: “Não Confie, Verifique”

“Agora, para as evidências”, disse o Rei, “e depois para a sentença.”

– Lewis Carroll, *Aventuras de Alice no subterrâneo*¹

O Bitcoin visa substituir à moeda convencional, ou pelo menos fornecer uma alternativa a ela. A moeda convencional está vinculada a uma autoridade central, não importa se estamos falando de moeda de curso forçado como o dólar americano ou dinheiro do Monopoly moderno, o V-Bucks do Fortnite. Em ambos os exemplos você deve confiar na autoridade central para emitir, gerenciar e distribuir seu dinheiro. O Bitcoin acaba com essa necessidade, e o principal problema que ele resolve é o justamente o da *confiança*.

“A raiz do problema com a moeda convencional é toda a confiança necessária para fazê-la funcionar. [...] O que precisamos é de um sistema de pagamento eletrônico baseado em prova criptográfica ao invés de confiança.”

– Satoshi Nakamoto²

O Bitcoin resolve o problema de confiança por ser completamente descentralizado, sem a necessidade de um servidor central ou de partes confiáveis. Nem mesmo são necessários *terceiros* confiáveis, mas partes confiáveis, ponto final. Quando não

¹Nota do tradutor: Manuscrito que deu origem a ‘Alice no País das Maravilhas’.

²Satoshi Nakamoto, anúncio oficial do Bitcoin [51] e whitepaper [48]

há autoridade central, simplesmente *não há* ninguém em quem confiar. A descentralização completa é a inovação. É a raiz da resiliência do Bitcoin, a razão pela qual ele ainda está vivo. A descentralização também é o motivo pelo qual temos a mineração, nodes, hardware wallets e, sim, a blockchain. A única coisa que você tem que “confiar” é que nosso entendimento de matemática e física não está totalmente errado e que a maioria dos mineradores age honestamente (eles são incentivados a agir assim).

Enquanto o mundo normal opera sob o pressuposto de “*confie, mas verifique*”, o Bitcoin opera sob o pressuposto de “*não confie, verifique*”. Satoshi destacou a importância de remover a confiança, tanto na introdução, quanto na conclusão do whitepaper do Bitcoin.

“Conclusão: Propomos um sistema para transações eletrônicas sem dependência da confiança.”

– Satoshi Nakamoto³

Observe que *sem dependência da confiança* é usado em um contexto muito específico aqui. Estamos falando de terceiros confiáveis, ou seja, outras entidades nas quais você confia para produzir, manter e processar seu dinheiro. Presume-se, por exemplo, que você pode confiar no seu computador.

Como Ken Thompson mostrou em sua palestra ao receber um Prêmio Turing, confiança é uma coisa extremamente complicada no mundo computacional. Ao executar um programa, você deve confiar em todos os tipos de software (e hardware) que, em teoria, podem alterar o programa que você está tentando executar de forma maliciosa. Como Thompson resumiu em seu livro *Reflexões sobre a necessidade de confiar na confiança*: “A lição é óbvia. Você não pode confiar em um código que não foi totalmente criado por você mesmo.” [70]

³Satoshi Nakamoto, whitepaper do Bitcoin [48]

```

char s[ ] = {
    '\V',
    '0',
    '\n',
    'I',
    'J',
    'K',
    'V',
    'W',
    'T',
    'R',
    '\n',
    (213 lines deleted)
    0
};

/*
 * The string s is a
 * representation of the body
 * of this program from '0'
 * to the end.
 */
main( )
{
    int i;

    printf("char s[ ] = {\n");
    for(i=0; s[i]; i++)
        printf("\t\"%c\",", s[i]);
    printf("\n};\n");
}

```

I
Here are some simple transliterations to allow non-C programmer to read this code.

- = assignment
- == equal to EQ
- != not equal to NE
- ++ increment
- 'x' single character constant
- ""'' multiple character string
- %d format to convert to decimal
- %s format to convert to string
- \ tab character
- \n newline character

FIGURE 1.

Excerpts copied with permission of the Association for Computing Machinery

To what extent should one trust a statement that a program is free of Trojan horses? Perhaps it is more important to trust the people who wrote the software.

KEN THOMPSON

```

    ...
c = next( );
if(c != '\\\\')
    return(c);
c = next( );
if(c == '\\\\')
    return('\\\\');
if(c == 'n')
    return('\\n');

```

FIGURE 2.2

```

    ...
c = next( );
if(c != '\\')
    return(c);
c = next( );
if(c == '\\\\')
    return('\\\\');
if(c == 'n')
    return('\n');
if(c == 'v')
    return('v');
...

```

FIGURE 2.1.

```

c = next( );
if(c != '\\\\')
    return(c);
c = next( );
if(c == '\\\\')
    return('\\\\');
if(c == 'n')
    return('\\ n');
if(c == 'v')
    return(11);

```

FIGURE 2.3.

The moral is obvious. You can't trust code that you did not totally create yourself. (Especially code from companies that employ people like me.) No amount of source-level verification or scrutiny will protect you from using untrusted code.

```
compile(s)
char *s;
|
|
|
```

FIGURE 3.1.

```
compile(s)
char *s;
{
    if(match(s, "pattern"))
        compile("bug");
    return;
}
```

FIGURE 3.2.

```

completes)
char *s;
{
    if(match(s, "pattern 1"))
        compile ("bug1");
    return;
}
if(match(s, " pattern 2"))
    compile ("bug 2");
return;
}

```

FIGURE 3.3

Thompson demonstrou que mesmo se você tiver acesso ao código-fonte, seu compilador ou qualquer outro programa ou hardware de gerenciamento, pode estar comprometido, e detectar esse backdoor seria muito difícil. Assim, na prática, um sistema verdadeiramente *confiável* não existe. Você teria que criar todo o seu software e todo o seu hardware (montadores, compiladores, vinculadores, etc.) a partir do zero, sem a ajuda de nenhum software externo ou maquinário auxiliado por software.

“Se você deseja fazer uma torta de maçã do zero,
você deve primeiro inventar o universo.”

– Carl Sagan⁴

O Ken Thompson Hack é um backdoor particularmente engenhoso e difícil de detectar, que funciona sem modificar nenhum software, então vamos dar uma olhada rápida nele. Os pesquisadores descobriram uma maneira de comprometer o hardware crítico de segurança alterando a polaridade das impurezas do silício. [9] Apenas mudando as propriedades físicas das coisas que os chips de computador são feitos, eles foram capazes de comprometer um gerador de números aleatórios criptograficamente seguro. Como essa mudança não pode ser encontrada, o backdoor não pode ser detectado por inspeção óptica, que é um dos mecanismos de detecção de violação mais importantes para chips como esses.

Parece assustador? Bem, mesmo se você fosse capaz de construir tudo do zero, ainda teria que confiar na matemática. Você teria que confiar que *secp256k1* é uma curva elíptica que não possui nenhum tipo de backdoor. Sim, backdoors maliciosos podem ser inseridos nas bases matemáticas das funções criptográficas e, sem dúvida, isso já aconteceu pelo menos uma vez. [80] Existem boas razões para você ser paranóico, e o fato de que tudo, desde

⁴Carl Sagan, *Cosmos* [63]

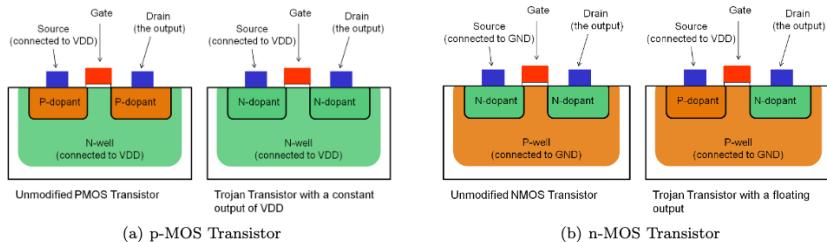


Figura 16.2.: Os Cavalos de Tróia Dopant-Level Escondidos no Hardware por Becker, Regazzoni, Paar, Burleson

o seu hardware, até seu software, passando pelas curvas elípticas utilizadas podem ter backdoors [82], são algumas delas.

“Não confie. Verifique.”

– Bitcoinheiros de todos os lugares

Os exemplos acima devem ilustrar que a computação *sem confiança* é utópica. O Bitcoin é provavelmente o sistema que mais se aproxima dessa utopia, mas ainda assim, é *confiança minimizada* — com o objetivo de remover a confiança sempre que possível. Indiscutivelmente, a cadeia de confiança é interminável, já que você também terá que confiar que a computação requer energia, que P não é igual a NP e que você está realmente vivendo na realidade e não preso em uma simulação por agentes mal-intencionados.

Os desenvolvedores estão trabalhando em ferramentas e procedimentos para minimizar ainda mais qualquer confiança remanescente. Por exemplo, os desenvolvedores do Bitcoin criaram o Gitian⁵, que é um método de distribuição de software para criar *builds* determinísticos. A ideia é que, se vários desenvolvedores forem capazes de reproduzir binários idênticos, a chance

⁵<https://gitian.org/>

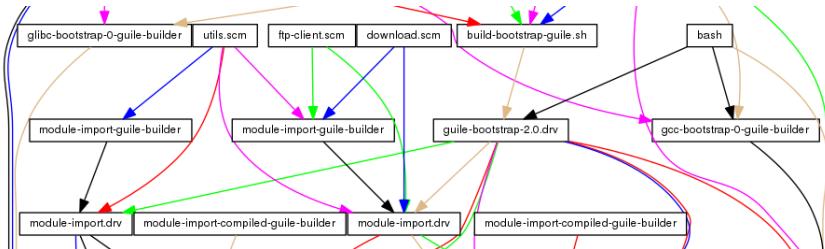


Figura 16.3.: O que veio primeiro, o ovo ou a galinha?

de adulteração maliciosa é reduzida. Os backdoors mais excêntricos não são o único vetor de ataque. A simples chantagem ou extorsão também são ameaças reais. Como no protocolo principal, a descentralização é usada para minimizar a confiança.

Vários esforços estão sendo feitos para melhorar o problema do ovo e da galinha na quesito confiança, que o hack de Ken Thompson tão brilhantemente apontou [20]. Um desses esforços é o Guix⁶ (a pronuncia correta é *guiks*), que usa gerenciamento de pacote declarado funcionalmente levando a compilações reproduzíveis bit a bit por design. O resultado é que você não precisa mais confiar em nenhum servidor que fornece o software, pois pode verificar se o binário fornecido não foi adulterado, reconstruindo-o do zero. Recentemente, um pull request foi merigliado para integrar o Guix ao processo de build do Bitcoin.⁷

Felizmente, o Bitcoin não depende de um único algoritmo ou peça de hardware. Um dos efeitos da descentralização radical do Bitcoin é o modelo de segurança distribuído. Embora os backdoors descritos acima não devam ser desconsiderados, é improvável que cada software de carteira, cada hardware wallet, cada biblioteca criptográfica, cada implementação de node e cada compilador de cada linguagem estejam comprometidos. Possível, mas

⁶<https://guix.gnu.org>

⁷Veja o PR 15277 do bitcoin-core: <https://github.com/bitcoin/bitcoin/pull/15277>

altamente improvável.

Observe que você pode gerar uma chave privada sem depender de nenhum hardware ou software computacional. Você pode jogar uma moeda [4] algumas vezes, embora dependendo de sua moeda e estilo de lançamento esta fonte de aleatoriedade possa não ser suficientemente aleatória. Há um motivo pelo qual protocolos de armazenamento como Glacier⁸ aconselham a escolha de dados de nível profissional usados por cassinos como uma das duas fontes de entropia.

O Bitcoin me forçou a refletir sobre o que realmente significa não confiar em ninguém. Isso aumentou minha consciência do problema do bootstrap e da cadeia de confiança implícita no desenvolvimento e execução de um software. Isso também despertou minha atenção sobre as muitas maneiras pelas quais software e hardware podem ser comprometidos.

O Bitcoin me ensinou a não confiar, mas a verificar.

⁸<https://glacierprotocol.org/>

17. Dizer as horas demanda trabalho

“Oh puxa! Oh puxa! Eu devo estar muito atrasada!”

– Lewis Carroll, *Alice no País das Maravilhas*

Costuma-se dizer que os bitcoins são minerados porque milhares de computadores trabalham na solução de problemas matemáticos *muito complexos*. Certos problemas precisam ser resolvidos, e se você calcular a resposta certa, você “produz” um bitcoin. Embora essa visão simplificada da mineração de bitcoin possa ser fácil de ser transmitida e entendida, ela deixa a desejar em alguns aspectos. Os bitcoins não são produzidos ou criados, e toda essa experiência não é realmente sobre a solução de problemas matemáticos específicos. Além disso, a matemática não é particularmente complexa. O que é complexo é *dizer as horas* em um sistema descentralizado.

Conforme descrito no whitepaper, o sistema de prova de trabalho (também conhecido como mineração) é uma maneira de implementar um servidor de data/hora distribuído.

Quando aprendi como o Bitcoin funciona, também pensei que

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

3. Timestamp Server

The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.



4. Proof-of-Work

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

Figura 17.1.: Trechos do whitepaper. Alguém disse timechain?

a prova de trabalho era ineficiente e um desperdício. Depois de um tempo, comecei a mudar minha perspectiva sobre o consumo de energia do Bitcoin [29]. Parece que a prova de trabalho ainda é muito mal compreendida, mesmo no ano 10 DB (depois do Bitcoin).

Uma vez que os problemas a serem resolvidos na prova de trabalho são criados, muitas pessoas parecem acreditar que este é um trabalho *inútil*. Se o foco for puramente o cálculo, essa é uma conclusão razoável. Mas o Bitcoin não é sobre computação. É sobre *concordar independentemente sobre ordem das coisas*.

A Prova de trabalho é um sistema no qual todos podem validar o que aconteceu e em que ordem aconteceu. Essa validação independente é o que leva ao consenso, um acordo individual entre várias partes sobre quem possui o quê.

Em um ambiente radicalmente descentralizado, não podemos nos dar ao luxo de ter um tempo absoluto. Qualquer relógio introduziria uma terceira parte confiável, um ponto central no sistema que deveria ser confiado e poderia ser atacado. “O tempo é a raiz do problema”, como Grisha Trubetskoy aponta [72]. E Satoshi resolveu esse problema de forma brilhante implementando um relógio descentralizado por meio de uma blockchain de prova de trabalho. Todos concordam de antemão que a cadeia com a maior quantidade de trabalho é a fonte da verdade. É por definição o que realmente aconteceu. Este acordo é o que agora é conhecido como consenso de Nakamoto.

“As transações de registro de data e hora da rede, colocando-as em uma cadeia contínua que serve como prova da sequência dos eventos testemunhados.”

– Satoshi Nakamoto¹

¹Satoshi Nakamoto, Whitepaper do Bitcoin [48]

Sem uma maneira consistente de saber as horas, não há uma maneira consistente de saber o antes e o depois. Uma ordenação confiável é impossível. Como mencionado acima, o consenso de Nakamoto é o jeito do Bitcoin dizer a hora de maneira consistente. A estrutura de incentivos do sistema produz um relógio probabilístico e descentralizado, utilizando tanto a ganância quanto o interesse próprio dos participantes concorrentes. O fato desse relógio ser impreciso é irrelevante porque a ordem dos eventos acaba sendo inequívoca e pode ser verificada por qualquer pessoa.

Graças à prova de trabalho, o trabalho e a validação do trabalho são radicalmente descentralizados. Todos podem entrar e sair à vontade e todos podem validar tudo a qualquer momento. Além disso, todos podem validar o estado do sistema *individualmente*, sem ter que depender de ninguém para isso.

Compreender a prova de trabalho leva tempo. Frequentemente, é contra-intuitivo e, embora as regras sejam simples, elas levam a fenômenos bastante complexos. Para mim, mudar minha perspectiva sobre a mineração ajudou. Útil, não inútil. Validação, não computação. Tempo, não blocos.

O Bitcoin me ensinou que dizer as horas é complicado, especialmente se você estiver em um ambiente descentralizado.

18. Mova-se lentamente e não quebre as coisas

Assim, o barco navegou lentamente, sob o brilhante dia de verão, com sua tripulação alegre e sua música de vozes e risos...

– Lewis Carroll, *Aventuras de Alice no subterrâneo*

Pode ser um mantra esquecido, mas “mova-se rápido e quebre as coisas” ainda é como grande parte do mundo da tecnologia opera. A ideia de que não importa se você acertar tudo na primeira vez é um pilar básico da mentalidade *falhe cedo, falhe com frequência*. O sucesso é medido pelo crescimento, então, enquanto você está crescendo, tudo bem. Se algo não funcionar no início, você simplesmente pivota e itera. Em outras palavras: jogue merda na parede e veja o que gruda.

O Bitcoin é muito diferente. É diferente por design. É diferente por necessidade. Como Satoshi apontou, uma moeda eletrônica já foi tentada muitas vezes anteriormente, e todas as tentativas falharam porque tinha uma cabeça para ser cortada. A novidade do Bitcoin, é que ele é uma besta sem cabeça.

“Muitas pessoas descartam automaticamente a moeda eletrônica como uma causa perdida por conta de todas as empresas que faliram desde a década de 1990. Espero que seja óbvio que foi apenas a natureza centralizada dos sistemas que fez com que elas estivessem condenadas.”

– Satoshi Nakamoto¹

¹Satoshi Nakamoto, em resposta ao usuário Sepp Hasslberger. [52]

Uma consequência dessa descentralização radical é uma resistência inerente à mudança. “Mova-se rápido e quebre as coisas” não funciona e nunca funcionará na camada base do Bitcoin. Mesmo que fosse desejável, não seria possível convencer *todos* os usuários a mudarem seus hábitos. Isso é consenso distribuído. Essa é a natureza do Bitcoin.

“A natureza do Bitcoin é tal que, uma vez que a versão 0.1 foi lançada, o seu design principal foi gravado em pedra para o resto de sua vida.”

– Satoshi Nakamoto²

Esta é uma das muitas propriedades paradoxais do Bitcoin. Todos nós acreditamos que qualquer coisa que seja software pode ser alterada facilmente. Mas a natureza da besta torna muito difícil mudá-la.

Como Hasu mostra lindamente em Unpacking Bitcoin’s Social Contract [32], mudar as regras do Bitcoin só é possível *propondo* uma mudança e, consequentemente, *convencendo* todos os usuários do Bitcoin a adotarem essa mudança. Isso torna o Bitcoin muito resistente a alterações, mesmo sendo um software.

Essa resiliência é uma das propriedades mais importantes do Bitcoin. Os sistemas de software críticos têm que ser antifrágis. É isso que a interação entre a camada social e técnica do Bitcoin garantem. Os sistemas monetários são adversários por natureza, e como sabemos há milhares de anos, bases sólidas são essenciais em um ambiente hostil.

“E desceu a chuva, e correram rios, e assopraram ventos, e combateram aquela casa, e não caiu, porque estava edificada sobre a rocha.”

– Matheus 7:24–27

²Satoshi Nakamoto, em resposta ao usuário Gavin Andresen [52]

Indiscutivelmente, nesta parábola dos construtores sábios e tolos, o Bitcoin não é a casa. É a rocha. Imutável, imóvel, fornecendo a base para um novo sistema financeiro.

Assim como os geólogos, que sabem que as formações rochosas estão sempre se movendo e evoluindo, pode-se ver que o Bitcoin está sempre se movendo e evoluindo também. Você só precisa saber para onde olhar e como olhar para ele.

A introdução de pay to script hash³ e segregated witnesses⁴ são a prova de que as regras do Bitcoin podem ser alteradas se um número suficiente de usuários estiver convencido de que adotar tal alteração é benéfica para a rede. Essa última possibilitou o desenvolvimento da rede lightning⁵, que é uma das casas que estão sendo construídas sobre a base sólida do Bitcoin. Atualizações futuras como assinaturas Schnorr [59] irão aumentar a eficiência e privacidade, bem como scripts (leia-se: contratos inteligentes) que serão indistinguíveis de transações regulares graças ao Taproot [31]. Construtores sábios realmente constroem em bases sólidas.

Satoshi não era apenas um construtor sábio tecnologicamente. Ele também entendeu que seria necessário tomar decisões acertadas ideologicamente.

³Transações do tipo pay to script hash (P2SH) foram padronizadas no BIP 16. Eles permitem que as transações sejam enviadas para um script hash (endereço começando com 3) ao invés de um hash de chave pública (endereços começando com 1) [15]

⁴Segregated Witness (abreviado como SegWit) é uma atualização de protocolo implementada com o objetivo de fornecer proteção contra maleabilidade de transação além de aumentar a capacidade do bloco. O SegWit separa a *testemunha* da lista de entradas. [16]

⁵<https://lightning.network/>

“Ser código aberto significa que qualquer pessoa pode revisar o código de forma independente. Se fosse de código fechado, ninguém poderia verificar a segurança. Eu acho que é essencial para um programa desta natureza que seu código seja aberto.”

– Satoshi Nakamoto⁶

A abertura é fundamental para a segurança e inerente ao código aberto e ao movimento de software livre. Como Satoshi apontou, os protocolos seguros e o código que os implementam devem ser abertos — não há segurança através da obscuridade. Outro benefício está novamente relacionado à descentralização: o código que pode ser executado, estudado, modificado, copiado e distribuído gratuitamente garante que ele seja espalhado por toda parte.

A natureza radicalmente descentralizada do Bitcoin é o que o move de forma lenta e deliberada. Uma rede de nodes, cada um administrado por um indivíduo soberano, é inherentemente resistente a mudanças, maliciosas ou não. Sem nenhuma forma de forçar as atualizações aos usuários, a única maneira de introduzir mudanças é convencer lentamente cada um desses indivíduos a adotá-las. Esse processo descentralizado de introdução e implantação de alterações é o que torna a rede incrivelmente resistente a mudanças maliciosas. É também o que torna mais difícil consertar coisas quebradas do que em um ambiente centralizado, é por isso que todos tentam não quebrar as coisas em primeiro lugar.

O Bitcoin me ensinou que mover-se devagar é uma de suas funcionalidades, não um bug.

⁶Satoshi Nakamoto, em resposta ao usuário SmokeTooMuch [53]

19. A privacidade não morreu

Os jogadores jogavam todos ao mesmo tempo, sem esperar sua vez, discutindo o tempo todo, brigando pelos ouriços; logo a Rainha estava furiosa e batia com os pés no chão, gritando: “Cortem a cabeça dele!”, ou “Cortem a cabeça dela!” o tempo todo.

– Lewis Carroll, *Alice no País das Maravilhas*

Se você acreditar nos especialistas, a privacidade morreu nos anos 1980¹. A invenção do Bitcoin por um pseudônimo e outros eventos da história contemporânea mostram que isso não é verdade. A privacidade está viva, mesmo que não seja fácil escapar de um Estado de vigilância.

O Satoshi fez um grande esforço para encobrir seus rastros e esconder sua identidade. Dez anos depois, ainda não se sabe se Satoshi Nakamoto era uma única pessoa, um grupo de pessoas, homem, mulher ou uma IA viajante no tempo que inicializou a si mesma para dominar o mundo. Teorias da conspiração à parte, Satoshi escolheu se identificar como um japonês, e é por isso que eu não suponho, mas respeito seu gênero escolhido e me refiro a ele como *ele*.

Qualquer que seja a sua identidade real, Satoshi teve sucesso em escondê-la. Ele deu um exemplo encorajador para todo mundo que deseja ficar anônimo: é possível ter privacidade online.

¹<https://bit.ly/privacy-is-dead>



Figura 19.1.: Eu não sou Dorian Nakamoto.

“Encriptação funciona. Um sistema de criptografia propriamente implementado é uma das poucas coisas em que se pode confiar.”

– Edward Snowden²

O Satoshi não foi o primeiro inventor anônimo ou pseudônimo, e ele não vai ser o último. Alguns imitaram seu estilo de publicação pseudônima, como Tom Elvis Yedusor, criador do protocolo MimbleWimble [71] enquanto outros publicaram provas matemáticas avançadas e permaneceram completamente anônimos [3].

Esse mundo em que vivemos é estranho. Um mundo onde identidade é opcional, contribuições são aceitas baseadas no mérito, e pessoas podem colaborar e transacionar livremente. Vai demorar ainda algum tempo para me ajustar e ficar confortável com esses novos paradigmas, mas eu acredito fortemente que todas essas coisas tem potencial de mudar o mundo para melhor.

Nós sempre devemos lembrar que privacidade é um direito humano fundamental³. E enquanto as pessoas exercerem e defenderem esses direitos, a batalha por privacidade está longe de acabar.

O Bitcoin me ensinou que a privacidade não morreu.

²Edward Snowden, respondendo à perguntas dos leitores [66]

³Declaração Universal dos Direitos Humanos, *Artigo 12*. [6]

20. Cypherpunks escrevem código

“Eu posso ver que você está tentando inventar alguma coisa.”

– Lewis Carroll, *Alice no País das Maravilhas*

Como muitas grandes ideias, o Bitcoin não surgiu do nada. Só foi possível combinando muitas inovações e descobertas da matemática, física, ciências da computação e muitas outras áreas. Mesmo sendo um gênio, Satoshi não conseguiria inventar o Bitcoin sem estar apoiado sobre os ombros de gigantes.

“Aquele que apenas deseja e espera não interfere ativamente no curso dos eventos e nem com a formação do próprio destino.”

– Ludwig von Mises¹

Um desses gigantes é o Eric Hughes, um dos fundadores do movimento cypherpunk e escritor de *O Manifesto Cypherpunks*. Em inglês *A Cypherpunk's Manifesto*. É difícil imaginar que Satoshi não tenha sido influenciado por esse manifesto. Nele já se falava de muitas coisas que o Bitcoin proporciona e usa, como: transações diretas e privadas, dinheiro e moedas eletrônicas, sistemas anônimos e a defesa de privacidade com criptografia e assinaturas digitais.

¹Ludwig von Mises, *Ação Humana* [74]

“Privacidade é necessária para uma sociedade livre na era eletrônica. [...] Já que desejamos privacidade, nós temos que ter certeza que cada parte na transação tenha conhecimento só do que é diretamente necessário para aquela transação [...] Assim, privacidade em uma sociedade aberta requer sistemas de transação anônima. Até agora, o dinheiro tem sido o principal sistema desse tipo. O sistema de transações anônimas não é um sistema de transações secretas. [...] Nós os Cypherpunks, estamos dedicados em construir sistemas anônimos. Nós vamos defender a nossa privacidade com criptografia, com sistemas de encaminhamento de e-mails anônimos, com assinaturas digitais e com dinheiro eletrônico. Os cypherpunks escrevem código.”

– Eric Hughes²

Cypherpunks não se confortam com esperanças e desejos. Eles ativamente interferem com os eventos em curso e moldam seu próprio destino. Os cypherpunks escrevem código.

Assim, no verdadeiro estilo cypherpunk, Satoshi sentou e começou a escrever código. Código que pegou uma ideia abstrata e provou para o mundo que ela realmente funcionava. Código que plantou a semente de uma nova realidade econômica. Graças a esse código, todo mundo pode verificar que esse sistema novo realmente funciona, e a cada dez minutos, mais ou menos, o Bitcoin prova para o mundo que ainda está vivo.

Para ter certeza de que sua inovação transcenda a fantasia e vire realidade, Satoshi escreve o código para implementar essa ideia antes de escrever o whitepaper. Ele também fez questão de

²Eric Hughes, O Manifesto Cypherpunks [37]

```

23 map<uint256, CBlockIndex*> mapBlockIndex;
24 const uint256 hashGenesisBlock("0x000000000019d6689c085ae1e165831e934ff763ae46a2a6c172b3f1b60a8ce26f");
25 CBlockIndex* pindexGenesisBlock = NULL;
26 int nBestHeight = -1;
27 uint256 hashBestChain = 0;
28 CBlockIndex* pindexBest = NULL;
:
675 int64 CBlock::GetBlockValue(int64 nFees) const
676 {
677     int64 nSubsidy = 50 * COIN;
678
679     // Subsidy is cut in half every 4 years
680     nSubsidy >= (nBestHeight / 210000);
681
682     return nSubsidy + nFees;
683 }
684
685 unsigned int GetNextWorkRequired(const CBlockIndex* pindexLast)
686 {
687     const unsigned int nTargetTimespan = 14 * 24 * 60 * 60; // two weeks
688     const unsigned int nTargetSpacing = 10 * 60;
689     const unsigned int nInterval = nTargetTimespan / nTargetSpacing;
690
691     // Genesis block
692     if (pindexLast == NULL)
693         return bnProofOfWorkLimit.GetCompact();

```

Figura 20.1.: Trechos de código do Bitcoin version 0.1

não atrasar³ qualquer versão para sempre. Até porque, “sempre tem mais uma coisa a ser feita.”

“Eu tive que escrever todo aquele código, antes de me convencer que eu podia resolver todo problema, só depois eu escrevi o whitepaper.”

– Satoshi Nakamoto⁴

No mundo de hoje, cheio de promessas de execução duvidosa, um exercício de construção dedicada era desesperadamente necessário. Seja determinado, se convença que você pode realmente resolver os problemas e implementar as soluções. Todos nós devemos ter como objetivo ser um pouco mais cypherpunk.

³“Nós não devemos atrasar se todos os recursos estão prontos.” – Satoshi Nakamoto [55]

⁴Satoshi Nakamoto, Re: Bitcoin P2P e-cash paper [49]

O Bitcoin me ensinou que cypherpunks escrevem código.

21. Metáforas para o futuro do Bitcoin

“Eu sei que algo interessante vai certamente acontecer...”

– Lewis Carroll, *Alice no País das Maravilhas*

Nas últimas décadas, a inovação tecnológica aparentemente não tem seguido uma tendência linear. Quer você acredite que singularidade tecnológica existe ou não, é inegável o progresso exponencial em muitas áreas. Além do fato da velocidade em que as tecnologias estão sendo adotadas estar acelerando, e antes que você perceba, o playground do pátio do maternal desapareceu, e suas crianças estão usando snapchat no lugar dele. Curvas exponenciais têm uma tendência de dar um tapa na sua cara antes que você possevê-las chegar.

O Bitcoin é uma tecnologia exponencial, construída em cima de tecnologias exponenciais. O site *Our World in Data*¹ lindamente mostra a velocidade crescente de adoção das tecnologias, começando em 1903 com a introdução de linhas de telefone (veja a figura 21.1). Linhas de telefone, eletricidade, computadores, internet, telefones celulares; todos seguem uma tendência exponencial de custo-performance e adoção. O Bitcoin também segue essa tendência [22].

Bitcoin não só tem um, mas múltiplos efeitos de rede², todos resultando crescimentos exponenciais nas suas respectivas áreas: preço, usuários, segurança, desenvolvedores, fatia do mercado e adoção global como dinheiro.

¹<https://ourworldindata.org/>

²Trace Mayer, *The Seven Network Effects of Bitcoin* [43]

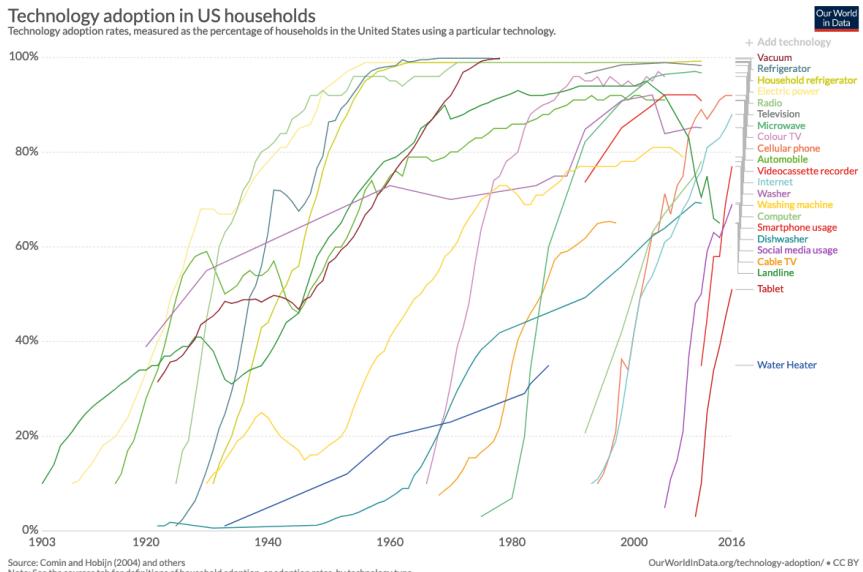


Figura 21.1.: O Bitcoin está literalmente rompendo dos gráficos

Tendo sobrevivido a sua infância, o Bitcoin continua crescendo todo dia em vários aspectos. Claro, a tecnologia ainda não alcançou a maturidade, ainda. Talvez esteja na sua adolescência. Mas se a tecnologia é exponencial, o caminho da obscuridade até o uso cotidiano é curto.

Jeff Bezos em sua palestra de 2003 no TED talk, escolheu usar a eletricidade como metáfora para o futuro da internet.³ Todos os três fenômenos, internet, Bitcoin — são tecnologias *habilitadoras*, redes que habilitam outras coisas. Elas são uma infraestrutura que terá várias coisas construídas utilizando-a como base. É fundadora por natureza.

A eletricidade tem estado um bom tempo entre nós. Nós tomamos ela por garantida. A internet é bem mais jovem, mas a maioria das pessoas já a considera por garantida também.

³<http://bit.ly/bezos-web>



Figura 21.2.: Telefone Celular, ca 1965 vs 2019.

O Bitcoin tem apenas dez anos, mas entrou na consciência do público durante a febre do último ciclo. Apenas quem adotou primeiro é quem o toma por garantido. Quanto mais tempo passar, mais pessoas vão reconhecer o Bitcoin como uma coisa que simplesmente é.⁴

Em 1994, a internet ainda era confusa e não intuitiva. Olhando esse gravação antiga do programa *Today Show*⁵ nos mostra que o que é natural e intuitivo agora, na verdade não era no passado. O Bitcoin ainda é confuso e alienígena para muitos, mas assim como a internet agora é uma 'segunda natureza' para os 'nativos digitais', gastar e empilhar sats⁶ vai ser algo cotidiano para os nativos de bitcoin no futuro.

“O Futuro já chegou — só não está igualmente bem distribuído.”

– William Gibson⁷

⁴Isso é chamado de *Efeito Lindy*. O Efeito Lindy é uma teoria onde a expectativa de vida de coisas não perecíveis, coisas como tecnologia, ou uma ideia, é proporcional a sua idade atual, onde cada período de sobrevivência adicional implica em uma longevidade maior. [89]

⁵https://youtu.be/U1Jku_CSyNg

⁶<https://twitter.com/hashtag/stackingsats>

⁷William Gibson, *The Science in Science Fiction* [28]

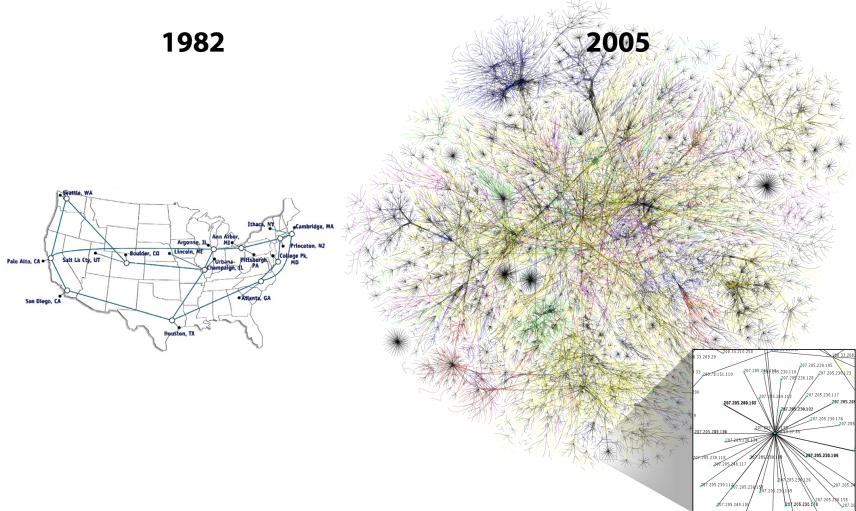


Figura 21.3.: A internet, 1982 vs 2005. Imagem sob licença cc-by-sa da Merit Network, Inc. and Barrett Lyon, Opte Project

Em 1995, quase 15% dos adultos Americanos usaram a internet. Dados históricos da Pew Research Center [27] nos mostram como a internet está emaranhada nas nossas vidas. De acordo com uma pesquisa dos consumidores feita pelo Kaspersky Lab [40], 13% dos correspondentes usaram Bitcoin e os seus clones para pagar por bens em 2018. Enquanto pagamentos não são o único caso de uso do bitcoin, existe alguns indicativos de onde estamos, falando como se a internet tivesse um cronograma: estamos no início dos anos 90.

Em 1997, Jeff Bezos disse em uma carta para os acionistas [11] que “Este é o Dia 1 para a Internet”, reconhecendo o poder ainda não explorado do potencial da rede, e, por extensão, da sua empresa. Qualquer que seja o dia hoje para o Bitcoin, todo o potencial não explorado é visto por todos, menos aos observadores casuais.



Figura 21.4.: Hal Finney escreveu o primeiro tweet mencionando o bitcoin em Janeiro 2009.

O primeiro node de Bitcoin foi ligado em 2009, após Satoshi ter minerado *o bloco gênesis*⁸ e divulgou o código para o público. O seu node não ficou sozinho por muito tempo. Hal Finney foi uma das primeiras pessoas a entender a ideia e se juntou a rede. Dez anos depois, enquanto eu escrevo, mais de 75.000⁹ nodes estão rodando o bitcoin.

A camada do protocolo base não é a única coisa que cresce exponencialmente. A lightning network, uma tecnologia de segunda camada, está crescendo a um passo ainda mais rápido.

Em Janeiro de 2018, a lightning network tinha 40 nodes e 60 canais [103]. Em Abril de 2019, a rede cresceu para mais de 4000 nodes e por volta de 40.000 canais. Isso tudo ainda sendo uma tecnologia experimental onde perda de fundos podem acontecer. Ainda assim, a tendência é clara: Milhões de pessoas são ousadas

⁸O bloco gênesis é o primeiro bloco da blockchain do Bitcoin. Versões mais modernas do cliente Bitcoin a enumeram como bloco 0, embora em versões bem iniciais fosse contada como bloco 1. O Bloco gênesis é costumeiramente codificado nas aplicações de software que utilizam a blockchain do Bitcoin. É um tipo especial de caso que não faz referência a um bloco anterior e produz um subsídio que não pode ser gasto. O parâmetro *coinbase* contém, além de dados normais, o seguinte texto: “*The Times 03/Jan/2009 Chancellor on brink of second bailout for banks*” [14]

⁹<https://bit.ly/luke-nodecount>

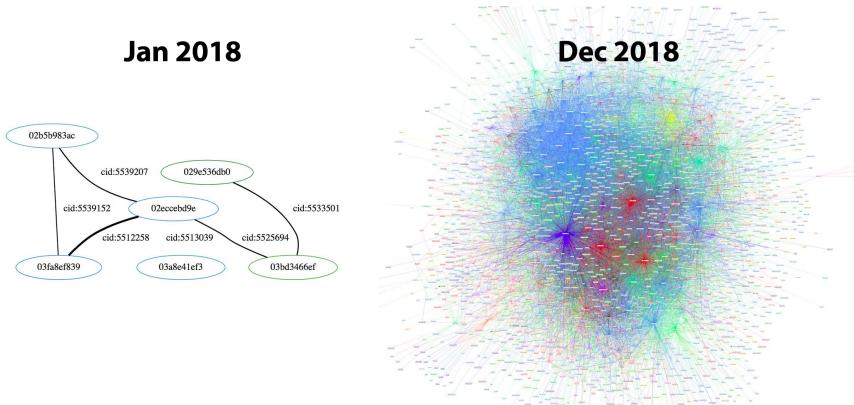


Figura 21.5.: Lightning Network, Janeiro de 2018 vs Dezembro de 2018 Fonte: Jameson Lopp

e estão ávidas para usá-la.

Para mim, tendo vivido a subida meteórica da internet, os paralelos entre ela e o Bitcoin são óbvios. Ambas são redes, ambas são tecnologias exponenciais, e ambas permitem novas possibilidades, novas indústrias novos modos de vida. Assim como a eletricidade era a melhor metáfora para entender onde a internet estava indo, a internet pode ser a melhor metáfora para entender onde o bitcoin está indo. Ou, nas palavras de Andreas Antonopoulos, o Bitcoin é *A Internet do Dinheiro*. Essas metáforas ajudam a nos lembrar que a história não se repete, mas muitas vezes rima.

Tecnologias experimentais são difíceis de entender e muitas vezes subestimadas. Mesmo que eu tenha um grande interesse por essas tecnologias, eu sou constantemente surpreendido pela rapidez do progresso e da inovação. Ver o ecossistema do Bitcoin crescer, é como ver o crescimento da internet de maneira acelerada. É extremamente estimulante.

Minha busca por tentar entender o Bitcoin me levou para muitos caminhos na história, e às vezes, para mais de um. En-

tender sociedades antigas, dinheiro do passado, e como redes de comunicações se desenvolveram, foi tudo parte da jornada. Do machado para o smartphone, a tecnologia realmente mudou nosso mundo muitas vezes. Tecnologias de redes são especialmente transformadoras, a escrita, as estradas, a eletricidade, a internet. Todas elas mudaram o mundo. O Bitcoin mudou o meu mundo e vai continuar mudando a mente e os corações de todos os que ousarem usá-lo.

O Bitcoin me ensinou que entender o passado é essencial para conhecer o futuro. Um futuro que apenas começou...

Considerações Finais

Conclusão

*“Comece pelo começo”, disse o Rei, gravemente,
“e prossiga até chegar ao fim; então pare”.*
– Lewis Carroll, *Alice no País das Maravilhas*

Como mencionado no início, eu acho que qualquer resposta para a questão “*O que você aprendeu com o Bitcoin?*” será sempre incompleta. A simbiose de vários sistemas que podem ser vistos como vivos – Bitcoin, a tecnosfera, e economia – é muito interligada, os tópicos muito numerosos, e as coisas estão se movendo muito rápido para uma pessoa sozinha entender tudo.

Mesmo sem entendê-lo totalmente, e mesmo com todas as suas peculiaridades e aparentes deficiências, o Bitcoin, sem dúvida, funciona. Ele continua produzindo blocos aproximadamente a cada dez minutos e faz isso lindamente. Quanto mais tempo o Bitcoin continua funcionando, mais pessoas optam por usá-lo.

“É verdade que as coisas são bonitas quando funcionam. Arte é funcionamento.”

– Giannina Braschi¹⁰

O Bitcoin é um filho da Internet. Está crescendo exponencialmente, confundindo as linhas entre as disciplinas. Não está claro, por exemplo, onde termina o reino da tecnologia pura e onde começa outra matéria. Embora o Bitcoin exija que os computadores funcionem com eficiência, a ciência da computação não é suficiente para entendê-lo. O Bitcoin não é apenas sem

¹⁰Giannina Braschi, *O Império dos Sonhos* [18]

fronteiras no que diz respeito ao seu funcionamento interno, mas também sem fronteiras no que diz respeito a disciplinas acadêmicas.

Economia, política, teoria dos jogos, história monetária, teoria das redes, finanças, criptografia, teoria da informação, censura, lei e regulamentação, organização humana, psicologia — tudo isso e mais são áreas de conhecimento que podem ajudar na busca pelo conhecimento de como o Bitcoin funciona e o que ele é.

Nenhuma invenção é responsável por seu sucesso. É a combinação de várias peças, que antes não se relacionavam, unidas por incentivos da teoria dos jogos, que constituem a revolução que é o Bitcoin. A bela mistura de muitas disciplinas é o que torna Satoshi um gênio.

Como todo sistema complexo, o Bitcoin precisa fazer concessões em termos de eficiência, custo, segurança e muitas outras propriedades. Assim como não existe uma solução perfeita para derivar um quadrado de um círculo, qualquer solução para os problemas que o Bitcoin tenta resolver sempre será imperfeita também.

“Não acredito que algum dia teremos um bom dinheiro novamente antes de tirarmos isso das mãos do governo, ou seja, não podemos tirá-lo violentamente das mãos do Estado, tudo o que podemos fazer é por alguma astuta forma indireta, introduzir algo que eles não podem parar.”

– Friedrich Hayek¹¹

O bitcoin é a maneira astuta e indireta de reintroduzir um bom dinheiro ao mundo. Ele faz isso colocando um indivíduo

¹¹Friedrich Hayek sobre Política Monetária, o Padrão Ouro, Déficits, Inflação, e John Maynard Keynes <https://youtu.be/EYhEDxFwFRU>

soberano atrás de cada node, assim como Da Vinci tentou resolver o problema intratável de transformar um quadrado em um círculo, colocando o Homem Vitruviano em seu centro. Os nodes removem efetivamente qualquer conceito de centralidade, criando um sistema surpreendentemente antifrágil e extremamente difícil de ser desligado. O Bitcoin vive e seu batimento cardíaco provavelmente durará mais que o nosso.

Espero que você tenha gostado dessas vinte e uma lições. Talvez a lição mais importante seja que o Bitcoin deve ser examinado holisticamente de vários ângulos, se alguém quiser ter algo próximo de uma imagem completa. Assim como remover uma parte de um sistema complexo destrói o todo, examinar partes do Bitcoin isoladamente parece contaminar a compreensão dele. Se apenas uma pessoa eliminar o termo “blockchain” de seu vocabulário e substituí-lo por “cadeia de blocos”, morrerei feliz.

Em qualquer caso, minha jornada continua. Pretendo me aventurar ainda mais nas profundezas desta toca do coelho e convido você a vir junto no passeio.¹²

¹²<https://twitter.com/dergigi>

Agradecimentos

Agradeço aos incontáveis autores e produtores de conteúdo que influenciaram meu pensamento sobre o Bitcoin e os tópicos que ele aborda. Há muitos de vocês para listar, mas farei o meu melhor para citar alguns.

- Obrigado a Arjun Balaji pelo tweet que me motivou a escrever este livro.
- Obrigado a Marty Bent por fornecer conteúdo sem fim para reflexão e entretenimento. Se você não segue Marty's Bent e o Tales From The Crypt, não sabe o que está perdendo. Felicidades Matt e Marty por nos guiarem pela toca do coelho
- Obrigado a Michael Goldstein e Pierre Rochard pela curadoria e fornecimento da melhor literatura Bitcoin por meio do Instituto Nakamoto. E obrigado por criar o Noded Podcast, que influenciou substancialmente minhas visões filosóficas sobre o Bitcoin.
- Obrigado a Saifedean Ammous por suas convicções, tweets picantes e por escrever o padrão Bitcoin.
- Obrigado a Francis Pouliot por compartilhar sua empolgação em descobrir sobre a cadeia do tempo.
- Obrigado a Andreas M. Antonopoulos por todo o material didático que vem publicando ao longo dos anos.

- Obrigado a Peter McCormack por seus tweets honestos e pelo podcast What Bitcoin Did, que continua fornecendo ótimas percepções de muitas áreas do saber.
- Obrigado a Jannik, Brandon, Matt, Camilo, Daniel, Michael e Raphael por fornecerem feedback para os primeiros rascunhos de algumas lições. Agradecimentos especiais a Jannik que revisou vários rascunhos várias vezes.
- Obrigado a Dhruv Bansal e Matt Odell por dedicar seu tempo para discutir algumas dessas ideias comigo.
- Obrigado a Guy Swann por produzir uma versão em áudio de 21lessons.com.
- Obrigado ao Friar Hass por seu apoio espiritual e orientação, e por dedicar seu tempo para escrever um prefácio para este livro.
- Obrigado a minha esposa por me tolerar minha natureza obsessiva.
- Obrigado à minha família por me apoiar tanto nos momentos bons como nos maus.
- Por último, mas não menos importante, graças a todos os bitcoinheiros maximalistas, shitcoinheiros minimalistas, shills, bots e shitposters que residem no belo jardim que é o Bitcoin Twitter.

E, finalmente, obrigado por ler isso. Espero que você tenha gostado tanto quanto eu gostei de escrever.

Lista de Figuras

0.1. Monges cegos examinando o Touro Bitcoin	12
7.1. A toca do coelho do Bitcoin não tem fundo.	30
9.1. Hiperinflação na República de Weimar (1921-1923)	43
12.1. Fiat: “Que seja feito”	54
12.2. Uma moeda da Lídia. Imagem sob a licença cc-by-sa da Classical Numismatic Group, Inc.	55
12.3. Moedas de prata com cortes de tamanhos variados.	56
12.4. O “Dólar” original. Saint Joachim foi colocado na face da moeda com seu manto e seu chapéu de mago. Imagem sob a licença cc-by-sa da Wikipedia enviada pelo usuário Berlin-George	57
12.5. Um dólar americano de 1928. “Pagável à vista ao portador”. Imagem sob a licença cc-by-sa publicada pela National Numismatic Collection em Smithsonian Institution	58
12.6. Uma note de \$100 dólares cunhada em 1928 em certificados de ouro. Imagem sob a licença cc-by-sa publicada pela National Numismatic Collection, National Museum of American History. .	59
12.7. Uma nota de vinte dólares americanos de 2004 usada atualmente. “ESTA NOTA É DE CURSO FORÇADO”	60
13.1. O efeito multiplicador da moeda	66

13.2. Janet Yellen, Secretária do Tesouro dos Estados Unidos, se opõe fortemente contra a auditoria do Fed, enquanto o Cara da Placa do Bitcoin é fortemente a favor de se comprar bitcoin.	67
14.1. Fórmula de emissão do Bitcoin	70
14.2. Suprimento controlado do Bitcoin	71
14.3. Razão stock-to-flow do ouro	73
14.4. Visualização do stock-to-flow do dólar, ouro e Bitcoin	74
14.5. Aumento da razão estoque/fluxo do bitcoin em comparação com o ouro	75
15.1. Há aproximadamente um trilhão de segundos no passado. Fonte: xkcd 1225	82
15.2. Ilustração da segurança do SHA-256. Gráfico original feito por Grant Sanderson, conhecido como 3Blue1Brown.	84
15.3. Ataque de chave inglesa de \$5 dólares. Fonte: xkcd 538	86
15.4. Exemplo de curvas elípticas. Gráficos sob a licença cc-by-sa disponibilizadas por Emmanuel Boute.	87
16.1. Trechos do artigo de Ken Thompson ‘Reflexões sobre confiar na confiança’	91
16.2. Os Cavalos de Tróia Dopant-Level Escondidos no Hardware por Becker, Regazzoni, Paar, Burleson .	93
16.3. O que veio primeiro, o ovo ou a galinha?	94
17.1. Trechos do whitepaper. Alguém disse timechain?	97
19.1. Eu não sou Dorian Nakamoto.	106
20.1. Trechos de código do Bitcoin version 0.1	109

21.1. O Bitcoin está literalmente rompendo dos gráficos	112
21.2. Telefone Celular, ca 1965 vs 2019.	113
21.3. A internet, 1982 vs 2005. Imagem sob licença cc-by-sa da Merit Network, Inc. and Barrett Lyon, Opte Project	114
21.4. Hal Finney escreveu o primeiro tweet mencionando o bitcoin em Janeiro 2009.	115
21.5. Lightning Network, Janeiro de 2018 vs Dezembro de 2018 Fonte: Jameson Lopp	116

Sobre a Bibliografia

Hoje em dia, muitos livros foram publicados sobre o Bitcoin. No entanto, a maioria da conversa — e assim, a maioria dos recursos mais interessantes — acontecem online.

A bibliografia a seguir lista livros, artigos e recursos online. Se o recurso tem um URL associado a ela, a URL estava ativa e funcionando em Outubro de 2019, pois consegui acessar com sucesso o dito recurso. Se qualquer uma das URLs levar a uma página inativa, desculpe. Por favor me informe ¹³ para que eu possa atualizar o(s) link(s).

P.S: O Bitcoin e o IPFS consertam isso.

¹³<https://dergigi.com/contact>

Referências Bibliográficas

- [1] Saifedean Ammous. *The Bitcoin Standard: The Decentralized Alternative to Central Banking*. Wiley, 2017.
- [2] Saifedean Ammous. Presentation on the bitcoin standard. https://www.bayernlb.de/internet/media/de/ir/downloads_1/bayernlb_research_sonderpublikationen_1/bitcoin_munich_may_28.pdf, May 2018.
- [3] Anonymous 4chan Poster, Robin Houston, Jay Pantone, and Vince Vatter. A lower bound on the length of the shortest superpattern. <https://oeis.org/A180632/a180632.pdf>, October 2018.
- [4] Andreas M Antonopoulos. *Mastering Bitcoin: Programming the Open Blockchain*. "O'Reilly Media, Inc.", 2014.
- [5] Julian Assange. Cypherpunks: Freedom and the future of the internet - introduction: A call to cryptographic arms. <https://cryptome.org/2012/12/assange-crypto-arms.htm>, December 2012.
- [6] United Nations General Assembly. The universal declaration of human rights, December 1948.
- [7] Beautyon. Why america can't regulate bitcoin. <https://hackernoon.com/why-america-can't-regulate-bitcoin-8c77cee8d794>, March 2018.

- [8] Beautyon. Bitcoin is. and that is enough. <https://hackernoon.com/bitcoin-is-and-that-is-enough-e3116870eed1>, October 2019.
- [9] Georg T Becker, Francesco Regazzoni, Christof Paar, and Wayne P Burleson. Stealthy dopant-level hardware trojans. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 197–214. Springer, 2013.
- [10] Marty Bent. Tales from the crypt – a podcast about bitcoin. <https://tftc.io/tales-from-the-crypt/>, 2017.
- [11] Jeff Bezos. To our shareholders. http://media.corporate-ir.net/media_files/irol/97/97664/reports/Shareholderletter97.pdf, 1997.
- [12] Bitcoin Wiki contributors. Block hashing algorithm — Bitcoin Wiki. https://en.bitcoin.it/w/index.php?title=Block_hashing_algorithm&oldid=66452, 2019.
- [13] Bitcoin Wiki contributors. Controlled supply — Bitcoin Wiki. https://en.bitcoin.it/w/index.php?title=Controlled_supply&oldid=66483, 2019.
- [14] Bitcoin Wiki contributors. Genesis block — Bitcoin Wiki. https://en.bitcoin.it/w/index.php?title=Segregated_Witness&oldid=66902, 2019.
- [15] Bitcoin Wiki contributors. Pay to script hash — Bitcoin Wiki. https://en.bitcoin.it/w/index.php?title=Pay_to_script_hash&oldid=64705, 2019.
- [16] Bitcoin Wiki contributors. Segregated witness — Bitcoin Wiki. https://en.bitcoin.it/w/index.php?title=Segregated_Witness&oldid=66902, 2019.

- [17] Godfrey Bloom. Why the whole banking system is a scam. <https://youtu.be/hYzX3YZoMrs>, May 2013.
- [18] Giannina Braschi. *Empire of Dreams*. AmazonCrossing, 2011.
- [19] Nic Carter. Bitcoin's existential crisis / what is it like to be a bitcoin? <https://medium.com/s/story/what-is-it-like-to-be-a-bitcoin-56109f3e6753>, November 2018.
- [20] Guix Contributors. Guix — bootstrapping. https://guix.gnu.org/manual/en/html_node/Bootstrapping.html, 2019.
- [21] Daniel C Dennett and Douglas R Hofstadter. *The mind's I: fantasies and reflections on self and soul*. Harvester Press, 1981.
- [22] Jeff Desjardins. The rising speed of technological adoption. <https://www.visualcapitalist.com/rising-speed-technological-adoption/>, February 2017.
- [23] Peter Diamandis. *Abundance : the future is better than you think*. Free Press, New York, 2012.
- [24] Dunny. I've learned more about finance, economics, technology, cryptography, human psychology, politics, game theory, legislation, and myself in the last three months of crypto than the last three and a half years of college. <https://twitter.com/BitcoinDunny/status/935330541263519745>, November 2017.
- [25] epii. New bitcoin logo. <https://bitcointalk.org/index.php?topic=4994.msg140770#msg140770>, May 2011.

- [26] Electronic Frontier Foundation. The crypto wars:governments working to undermine encryption. https://www.eff.org/files/2014/01/03/cryptowarsonepgers-1_cac.pdf, 2018.
- [27] Susannah Fox and Lee Rainie. How the internet has woven itself into american life. <https://pewrsr.ch/32M7Qmg>, February 2014.
- [28] William Gibson. The science in science fiction. <https://www.npr.org/2018/10/22/1067220/the-science-in-science-fiction>, October 2018.
- [29] Gigi. Bitcoin's energy consumption – a shift in perspective. <https://dergigi.com/2018/06/10/bitcoin-s-energy-consumption/>, June 2018.
- [30] Gigi. The magic dust of cryptography – how digital information is changing our societybitcoin's gravity. <https://dergigi.com/2018/08/17/the-magic-dust-of-cryptography/>, Aug 2018.
- [31] Gregory Maxwell. Taproot: Privacy preserving switchable scripting. <https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2018-January/015614.html>, 2018.
- [32] Hasu. Unpacking bitcoin's social contract. <https://uncommoncore.co/unpacking-bitcoins-social-contract>, December 2018.
- [33] Friedrich August Hayek. *1980s Unemployment and the Unions: Essays on the Impotent Price Structure of Britain and Monopoly in the Labour Market*. Institute of Economic Affairs, 1984.

- [34] Friedrich August Hayek. *The Collected Works of F.A. Hayek, Volume 6, Good Money, Part II*. Routledge, 1999.
- [35] Henry Hazlitt. *Economics in One Lesson*. Ludwig von Mises Institute, <https://mises.org/library/economics-one-lesson>, 1946.
- [36] Dan Held. Bitcoin's distribution was fair. <https://blog.picks.co/bitcoins-distribution-was-fair-e2ef7bbbc892>, 2018.
- [37] Eric Hughes. A cypherpunk's manifesto. <https://www.activism.net/cypherpunk/manifesto.html>, March 1993.
- [38] Guido Jörg Hülsmann. *Ethics of Money Production*. Ludwig von Mises Institute, <https://mises.org/library/ethics-money-production>, 2008.
- [39] Robert Kiyosaki. Why the rich are getting richer. <https://youtu.be/abMQhaMdQu0>, July 2016.
- [40] Kaspersky Lab. From festive fun to password panic: Managing money online this christmas. <https://www.kaspersky.com/blog/money-report-2018/>, 2018.
- [41] Jameson Lopp. No one has found the bottom of the bitcoin rabbit hole. <https://twitter.com/lopp/status/1061415918616698881>, November 2018.
- [42] Margo Rapport. History shows price of an ounce of gold equals price of a decent men's suit, says sionna investment managers. <https://www.businesswire.com/news/home/20110819005774/en/History-Shows-Price-Ounce-Gold-Equals-Price>, 2011.

- [43] Trace Mayer. The 7 network effects of bitcoin. <https://www.thrivenotes.com/the-7-network-effects-of-bitcoin/>, January 2016.
- [44] Ralph C. Merkle. Daos, democracy and governance. <https://alcor.org/cryonics/Cryonics2016-4.pdf#page=28>, July-August 2016.
- [45] Fiat Minimalist. Isn't it ironic that bitcoin has taught me more about money than all these years i've spent working for financial institutions? <https://twitter.com/fiatminimalist/status/1072880815661436928>, December 2018.
- [46] The Austrian Mint. Gold: The extraordinary metal. <https://www.muenzeoesterreich.at/eng/discover-for-investors/gold-the-extraordinary-metal>, November 2017.
- [47] British Museum. The origins of coinage. https://www.britishmuseum.org/explore/themes/money/the_origins_of_coinage.aspx, 2007.
- [48] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. <https://bitcoin.org/bitcoin.pdf>, October 2008.
- [49] Satoshi Nakamoto. Re: Bitcoin p2p e-cash paper. <https://www.metzdowd.com/pipermail/cryptography/2008-November/014832.html>, November 2008.
- [50] Satoshi Nakamoto. Bitcoin open source implementation of p2p currency. <http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?commentId=2003008%3AComment%3A9562>, February 2009.

- [51] Satoshi Nakamoto. Bitcoin open source implementation of p2p currency. <http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source>, February 2009.
- [52] Satoshi Nakamoto. Re: Bitcoin open source implementation of p2p currency. <http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source>, February 2009.
- [53] Satoshi Nakamoto. Re: Questions about bitcoin. <https://bitcointalk.org/index.php?topic=13.msg46#msg46>, December 2009.
- [54] Satoshi Nakamoto. Dealing with sha-256 collisions. <https://bitcointalk.org/index.php?topic=191.msg1585#msg1585>, June 2010.
- [55] Satoshi Nakamoto. Re: 0.3 almost ready. <https://bitcointalk.org/index.php?topic=199.msg1670#msg1670>, June 2010.
- [56] Satoshi Nakamoto. Re: Transactions and scripts: Dup hash160 ... equalverify checksig. <https://bitcointalk.org/index.php?topic=195.msg1611#msg1611>, June 2010.
- [57] Ron Paul. *End the Fed*. Grand Central Publishing, <http://endthefed.org/books/>, 2009.
- [58] Jordan Pearson. Inside the world of the bitcoin carnivores: Why a small community of bitcoin users is eating meat exclusively. https://motherboard.vice.com/en_us/article/ne74nw/inside-the-world-of-the-bitcoin-carnivores, September 2017.

- [59] Pieter Wuille. Schnorr signatures for secp256k1. <https://github.com/sipa/bips/blob/bip-schnorr/bip-schnorr.mediawiki>, 2019.
- [60] Plato. *Plato in Twelve Volumes, Vol. 3. (Euthydemus section 304a/304b).* Harvard University Press, <http://www.perseus.tufts.edu/hopper/text?doc=Perseus%3Atext%3A1999.01.0178%3Atext%3DEuthyd.%3Asection%3D304a>, 2017.
- [61] Federal Reserve. Money stock measures – discontinuance of m3. <https://www.federalreserve.gov/Releases/h6/discm3.htm>, 2005.
- [62] Perry J. Roets. Bernard w. dempsey, s.j. *Review of Social Economy*, 49(4):546–558, 1991.
- [63] Carl Sagan. *Cosmos*. Random House, 1980.
- [64] Bruce Schneier. *Applied Cryptography: Protocols, Algorithms and Source Code in C*. John Wiley and Sons, 2017.
- [65] Bruce Schneier. Schneier on security. <https://www.schneier.com>, 2019.
- [66] Edward Snowden. Edward snowden: Nsa whistleblower answers reader questions. <https://www.theguardian.com/world/2013/jun/17/edward-snowden-nsa-files-whistleblower>, June 2013.
- [67] Jimmy Song. Why bitcoin is different. <https://medium.com/@jimmysong/why-bitcoin-is-different-e17b813fd947>, April 2018.

- [68] U.S. Geological Survey. National minerals information center — mineral commodity summaries. <https://www.usgs.gov/centers/nmic/mineral-commodity-summaries>, 2019.
- [69] Nick Szabo. Shelling out: The origins of money. <https://nakamotoinstitute.org/shelling-out/>, 2002.
- [70] K. Thompson. Reflections on trusting trust. In *ACM Turing award lectures*, page 1983, 2007.
- [71] Tom Elvis Jedusor. Mimblewimble origin. <https://github.com/mimblewimble/docs/wiki/MimbleWimble-Origin>, 2016.
- [72] Grisha Trubetskoy. Blockchain proof-of-work is a decentralized clock. <https://grisha.org/blog/2018/01/23/explaining-proof-of-work/>, 2018.
- [73] Peter Van Valkenburgh. Coin center’s peter van valkenburg on preserving the freedom to innovate with public blockchains. <http://bit.ly/valkenburgh>, November 2018.
- [74] Ludwig von Mises. *Human Action*. Ludwig von Mises Institute, <https://mises.org/library/human-action-0/html/p/607>, 1949.
- [75] Wikipedia contributors. 2013–present economic crisis in venezuela — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=2013%E2%80%93present_economic_crisis_in_Venezuela&oldid=918242758, 2019.
- [76] Wikipedia contributors. Austrian school — Wikipedia, the free encyclopedia. <https://en.wikipedia.org/w/>

[index.php?title=Austrian_School&oldid=920008469](https://en.wikipedia.org/w/index.php?title=Austrian_School&oldid=920008469), 2019.

- [77] Wikipedia contributors. Bimetallism — Wikipedia, the free encyclopedia. <https://en.wikipedia.org/w/index.php?title=Bimetallism&oldid=920537299>, 2019.
- [78] Wikipedia contributors. Crypto wars — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Crypto_Wars&oldid=916147143, 2019.
- [79] Wikipedia contributors. Discrete logarithm — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Discrete_logarithm&oldid=909625575, 2019.
- [80] Wikipedia contributors. Dual ec drbg — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Dual_EC_DRBG&oldid=918490393, 2019.
- [81] Wikipedia contributors. Dyson sphere — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Dyson_sphere&oldid=916621053, 2019.
- [82] Wikipedia contributors. Elliptic-curve cryptography — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Elliptic-curve_cryptography&oldid=916608234#Backdoors, 2019.
- [83] Wikipedia contributors. Hyperinflation — Wikipedia, the free encyclopedia. <https://en.wikipedia.org/w/index.php?title=Hyperinflation&oldid=916608234>, 2019.

- index.php?title=Hyperinflation&oldid=919343724, 2019.
- [84] Wikipedia contributors. Illegal number — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Illegal_number&oldid=918772989, 2019.
- [85] Wikipedia contributors. Illegal prime — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Illegal_prime&oldid=913087454, 2019.
- [86] Wikipedia contributors. Keynesian economics — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Keynesian_economics&oldid=919881690, 2019.
- [87] Wikipedia contributors. Landauer's principle — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Landauer%27s_principle&oldid=907333330, 2019.
- [88] Wikipedia contributors. Last glacial maximum — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Last_Glacial_Maximum&oldid=919510280, 2019.
- [89] Wikipedia contributors. Lindy effect — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Lindy_effect&oldid=921214819, 2019.
- [90] Wikipedia contributors. List of currencies — Wikipedia, the free encyclopedia. <https://en.wikipedia.org/>

[org/w/index.php?title=List_of_currencies&oldid=897955050](https://en.wikipedia.org/w/index.php?title=List_of_currencies&oldid=897955050), 2019.

- [91] Wikipedia contributors. List of historical currencies — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=List_of_historical_currencies&oldid=919919705, 2019.
- [92] Wikipedia contributors. Methods of coin debasement — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Methods_of_coin_debasement&oldid=917940627, 2019.
- [93] Wikipedia contributors. Money multiplier — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Money_multiplier&oldid=918027413, 2019.
- [94] Wikipedia contributors. Money supply — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Money_supply&oldid=921152289, 2019.
- [95] Wikipedia contributors. P versus np problem — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=P_vs_NP_problem&oldid=919882161, 2019.
- [96] Wikipedia contributors. Paradox of value — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Paradox_of_value&oldid=906068208, 2019.
- [97] Wikipedia contributors. Sha-2 — Wikipedia, the free encyclopedia. <https://en.wikipedia.org/w/index.php?title=SHA-2&oldid=917408454>, 2019.

- [98] Wikipedia contributors. Ship of theseus — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Ship_of_Theseus&oldid=923020256, 2019.
- [99] Wikipedia contributors. Silver certificate (united states) — Wikipedia, the free encyclopedia. [https://en.wikipedia.org/w/index.php?title=Silver_certificate_\(United_States\)&oldid=917688197](https://en.wikipedia.org/w/index.php?title=Silver_certificate_(United_States)&oldid=917688197), 2019.
- [100] Wikipedia contributors. Subjective theory of value — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Subjective_theory_of_value&oldid=893004286, 2019.
- [101] Wikipedia contributors. Thaler — Wikipedia, the free encyclopedia. <https://en.wikipedia.org/w/index.php?title=Thaler&oldid=914457345>, 2019.
- [102] Wikipedia contributors. Theory of value (economics) — Wikipedia, the free encyclopedia. [https://en.wikipedia.org/w/index.php?title=Theory_of_value_\(economics\)&oldid=919603374](https://en.wikipedia.org/w/index.php?title=Theory_of_value_(economics)&oldid=919603374), 2019.
- [103] Wilma Woo. 'unfairly cheap' lightning network mainnet hits 40 nodes, 60 channels. <https://bitcoinist.com/bitcoin-lightning-network-mainnet-nodes/>, January 2018.