

# O MUNDO MÁGICO DO BITCOIN



# O MUNDO MÁGICO DO BITCOIN

Uma visão não usual sobre o dinheiro  
mágico da internet e seu culto de fanáticos.

**Leta**

PATROCÍNIO



Este livro não existiria se não fosse o Mateus da Livecoins, a quem eu só tenho a agradecer pela parceria. Desde a primeira vez que eu comentei sobre a possibilidade de juntar os textos em um livro, só recebi apoio e incentivo.

A Livecoins é, na minha opinião, a referência nacional em conteúdos bitcoinheiros. Lá não é portal com foco em shitcoin, o que é louvável, visto que todos os incentivos do sistema contribuem para essa abordagem.

Para mim, é uma honra ser um dos colunistas deste portal, que conta com grandes mestres como o Korea, o Alan Schramm e a Madu escrevendo para lá de tempos em tempos. Lembro como se fosse ontem o texto do Korea sobre o maximalismo tóxico, foi nesse dia que minha admiração pelo portal começou: ter coragem de publicar esse texto não é para qualquer um, só para quem tem adesão ao nosso ethos de bitcoinheiro.

Enfim, meu muito obrigado ao Mateus em específico e à Livecoins como um todo. Vocês com certeza contribuem significativamente para o nosso ecossistema.

## AGRADECIMENTO

Um agradecimento especial a todos os heróis, coloquialmente chamados de revisores, que ajudaram no processo de me fazer parecer menos analfabeto.

Meu muito obrigado a Elisa, Liev e Lázaro, que deram a primeira demão de revisão ao texto e enfrentaram o grosso do problema e olharam os textos ainda na sua forma inicial, separados do contexto do restante do livro. Também estendo esse agradecimento ao Korea, Fernando Guimarães, Oscar B Jr., Alex Lage e Marco Tulio Nascimento que ajudaram a polir todas as arestas que ainda estavam presentes.

Um agradecimento especial ao meu amigo Norbert, que, além de co-autor de um dos capítulos, também sempre me incentivou e compartilhou ideias comigo.

Um muito obrigado também a minha prima Tati, que cuidou das ilustrações e diagramação desta obra.



A todos os plebs.  
Aos meus pais, a quem devo tudo e aos meus  
sobrinhos Gregorio, Helena, Luisa e Julia.

*Eu não acredito que teremos um bom dinheiro de novo antes de tirá-lo das mãos do governo, isto é, não podemos tirá-los violentamente das mãos do governo, tudo o que podemos fazer é, por algum o caminho indireto, introduzir algo que eles não podem parar.*

**Friedrich Hayek em 1984**

## PREFÁCIO

Quando criamos o canal 'Bitcoinheiros', há quase 210 mil blocos, uma das minhas principais motivações (ou necessidades) era aprender mais sobre bitcoin. Ter encontros semanais para produzir conteúdo com o Allan Raicher, Becas e o Dov, pessoas que eu admiro e reconheço pela capacidade intelectual e conhecimento profundo sobre bitcoin, parecia uma boa desculpa para me incentivar a estudar o assunto de maneira mais dedicada. Mas o impacto foi muito maior do que eu poderia imaginar. Em poucos anos tivemos mais de 1,5 milhão de visualizações no youtube, e o que era apenas uma forma egoísta de me aplicar ao estudo de um dos temas mais revolucionários e instigantes da história da humanidade, acabou por repercutir e atingir outras pessoas.

Depois de produzirmos centenas de vídeos, tutoriais, discussões e entrevistas com as mentes mais brilhantes que já haviam sido sugadas pelo bitcoin, comecei a me questionar por que ainda não tinham surgido outros canais ou podcasts focados no tema. Não era possível que não houvesse outros indivíduos com competência comunicativa para produzir conteúdo 'bitcoin only' em português. Verbalizei essa frustração em alguns programas, até que na altura do bloco 714954 recebemos um tal de 'Bitcoin Explica' para uma entrevista. Imediatamente reconheci um remanescente que além de compreender com clareza o bitcoin, trazia uma perspectiva única do assunto, com seu olhar de profundo conhecedor das ciências naturais. Minha reação

foi perguntar: “Quando você irá começar seu próprio podcast?”.

Não é surpresa que sua produção intelectual foi muito além de fazer um podcast. Comecei a escrever este texto no exato momento em que terminei de ler o livro “O Mundo Mágico do Bitcoin”, e ainda me sinto tomado pela emoção causada pelo último capítulo, que conta a história e o caminho pessoal percorrido pelo autor. A qualidade do conteúdo e sua escrita leve, profunda e irreverente é algo único que você dificilmente encontrará em outros livros sobre bitcoin. Ao começar pelo entendimento sobre “o que é dinheiro” e quais são os problemas do atual sistema monetário, o autor estabelece os fundamentos básicos para começar a falar sobre essa revolução, conduzindo o leitor pelos trilhos da sua jornada na toca do coelho. Com seu olhar criativo, fala sobre “A melhor empresa do mundo” em uma metáfora para explicar as qualidades únicas dessa rede, e na busca por oferecer uma visão completa deste novo mundo, te introduz ao conjunto de valores, crenças, comportamentos e costumes dos seres deste universo – os bitcoinheiros. Para encerrar com chave de bitcoin, nos brinda com a história de sua experiência pessoal e detalha com precisão as etapas percorridas, o que provoca uma sensação de intimidade, inspiração e identificação entre as partes envolvidas nessa jornada.

Segundo o Leta, “Um bitcoinheiro é alguém que realmente entendeu a tese do bitcoin e as suas mais variadas implicações”. Na minha opinião, o trabalho realizado pelo autor demonstra que ele é um dos melhores exemplares que temos desta espécie. Se você chegou até aqui, existe uma grande chance de que também se descubra um ‘bitcoinheiro’ no decorrer da leitura; mas atenção: é importante alertar que este livro poderá prejudicar suas horas de sono, uma vez que a curiosidade e o interesse despertado pelo bitcoin não tem limites. A força gravitacional é tal que, assim como aconteceu conosco, há a possibilidade de que você se sinta compelido a colaborar de alguma forma a construir algo com o melhor das suas habilidades. Aproveite a leitura e boa viagem.

**Ivan, Cocriador e host dos Bitcoinheiros.**

# INTRODUÇÃO

Salve, salve bitcoinheiros e curiosos, tudo bem com vocês? Esse livro é a compilação de diversos textos autorais que escrevi ao longo do segundo semestre de 2021 e primeiro semestre de 2022, encadeados em uma estrutura lógica que permite ao leitor ter uma visão completa do bitcoin e da sua comunidade. Estes textos podem ser encontrados na internet no portal <https://livecoins.com.br/>. Para o livro, esses textos foram revisados e, quando necessário, atualizados. Alguns textos são inéditos.

A primeira parte do livro, composta de dois capítulos, é denominada O PROBLEMA e explica os problemas do mundo relacionados ao dinheiro, ou seja, o que o bitcoin conserta. Essa é a primeira parte do livro pois não faz sentido estudar uma solução sem entender o que ela está solucionando.

A segunda parte, composta de sete capítulos, é denominada A SOLUÇÃO e foca em apresentar o bitcoin para as pessoas. Essa apresentação não é técnica ou formal, mas apresenta modelos mentais e analogias para ajudar os interessados não técnicos a entender a moeda e porque as pessoas o conhecem como “magic internet money” (“dinheiro mágico da internet”, em português). Nesta parte de apresentação do bitcoin, será discutida a descoberta do bitcoin pelo programador anônimo Satoshi Nakamoto, além dos principais fundamentos do dinheiro mágico da internet. Também existem dois capítulos sobre o preço do bitcoin, um contextualizando a moeda com

diferentes modelos de precificação e o outro explicando a tendência que ela apresenta para o longo prazo. Um dos capítulos foca em apresentar a moeda laranja a partir de uma análise qualitativa, focando em explicar porque o bitcoin pode ser considerado a melhor empresa do mundo, caso aceitemos a definição de uma empresa descentralizada. Os últimos dois capítulos são dedicados a explicar um pouco melhor como funciona a mineração, um tema que gera diversas narrativas que desinformam aqueles que não entendem a tese energética do bitcoin.

A terceira parte, composta de três capítulos, é denominada A COMUNIDADE e foca em apresentar os bitcoinheiros. Quem são os pertencentes deste “culto de fanáticos” (como insistem em nos denominar), quais membros crenças, valores e características de personalidade? O que torna esse grupo particular de indivíduos tão confiantes em relação a um ativo que foi criado há menos de 15 anos e que sequer existe no mundo físico.

A quarta parte, composta de dois capítulos, é denominada MODELOS MENTAIS. Nela, o foco é apresentar dois modelos mentais que considero importantes que todo investidor tenha em mente. São dois conceitos que sigo como minha estratégia de investimento.

A quinta parte ou APÊNDICE, é composta por um capítulo, onde conto um pouco mais sobre mim e de como foi meu mergulho na toca do coelho, o processo de descoberta do bitcoin, quais materiais me ajudaram e o que estava pensando em cada época desse processo.

Começar a estudar o bitcoin pode parecer assustador. São tantos termos novos e diferentes que é normal a gente se sentir acuado e desistir por falta de conhecimento. Pensando em ajudar o novato, o livro começa com um mini dicionário de termos comuns no ecossistema do bitcoin, assim como uma explicação do significado dos conceitos do ponto de vista de um bitcoinheiro maximalista.

A ideia deste glossário não é que você leia tudo de uma vez. Isso não faz sentido já que em menos de uma semana iria esquecer tudo. A ideia é que você possa consultá-lo quando estiver nas outras partes do livro e não entender algum termo. As referências utilizadas para embasar o texto estão numeradas e são apresentadas no final do livro. Ao longo do texto, são utilizados diversos anglicismos, o que é praxe nesse ecossistema. Apesar das normas requererem que esses termos sejam escritos com *itálico* ou entre

aspas, esse não foi o padrão utilizado no livro. Assim como inicialmente internet necessitava estar entre aspas ou itálico e atualmente não requer mais.

Caso queira se aprofundar mais nos estudos além deste livro, existem canais de YouTube (Bitcoinheiros, Area Bitcoin), Instagram (@usecripto), livros (O Padrão Bitcoin, Bitcoin Red Pill: O Renascimento Moral, Material e Tecnológico, Bitcoin: A moeda na era digital), artigos (Explica Bitcoin, Livecoins) e podcasts (21 milhões e Sessões de Hopium e Temática) específicas sobre essa moeda.

## GLOSSÁRIO

**Altcoin** - são todas as criptomoedas que não são o bitcoin. Altcoin vem de "alternative coin", ou moeda alternativa em português. As altcoins são tokens digitais com bancos de dados centralizados com protocolos que diferem do bitcoin, e a maioria surgiu a partir de bifurcações (forks) do código desta moeda com parâmetros modificados. Os bitcoinheiros chamam elas de shitcoins devido ao seu valor tender à zero.

**Altista** - quem acredita na alta. Termo que tem origem entre os investidores de bolsa, onde quem acredita na alta é chamado de altista, além de otimista. Altista é o termo em português para bullish, e o seu oposto é o baixista, ou seja, quem acredita em um movimento de queda no mercado.

**ATH** - é o acrônimo de "All Time High", que significa a alta máxima histórica. Quando alguém diz que a ATH do bitcoin foi de 355 mil reais, o que essa pessoa está dizendo é que este é o valor mais alto que o bitcoin já atingiu em relação a determinada moeda fiduciária (moeda fiat).

**ASICs** - acrônimo de "Application Specific Integrated Circuit" (Circuito Integrado de Aplicação Específica), são chips especializados em cálculos computacionais específicos. Há uma grande variedade de ASICs especializados em mineração de diferentes criptomoedas.

**Baleia** - é o termo utilizado para os grandes detentores de bitcoin. Podem ser pessoas físicas, fundos de investimento, bancos, etc. O termo baleia



é conhecido porque como possuem mais de 1000 BTCs, o seu comportamento influencia o preço do mercado. O ranking completo inclui baleias (quem tem mais que 1000 BTCs), tubarões (entre 1000-500 BTCs), golfinhos (entre 500-100 BTCs), peixes (entre 50-100 BTCs), polvo (entre 50-10 BTCs), caranguejos (entre 10 e 1 BTCs) e camarões (menos que 1 BTC).

**Bear (bearish)** - o termo "bear market" é usado para mercados em queda e quando um investidor está com um sentimento negativo em relação ao mercado. Acreditando que a tendência é de queda, ele está "bearish".

**Blockchain** - ou “corrente de blocos” em português é o registro público descentralizado de todas as transações do bitcoin em ordem cronológica. A blockchain é uma tecnologia específica que resolve um problema específico, e não a solução para todos os problemas de armazenagem de dados. Hoje em dia usam o termo “blockchain” como o “quântico”, que vai ser a solução mágica para alguma situação burocrática. A verdade é que o armazenamento de dados via blockchain descentralizada é ineficiente e custoso, só fazendo sentido para uma situação em específico: estabelecer confiança entre entidades independentes a partir da prova de trabalho, sem a necessidade de uma terceira parte.

Origem	Destino	Quantidade	Hash Bloco Anterior
José	Maria	4	14a45fca2c194068abc173e3ab8b821e
Alice	Bob	3	
	TOTAL	7	

Ilustração do texto “Blockchain no Google Sheets” do João Grilo Bitcoinheiro, que explica de uma maneira simples o que é e como funciona uma blockchain.

**Bitcoin e bitcoin** - Existe o Bitcoin (BTC), com "B" maiúsculo, que é a rede descentralizada de computadores conectados rodando o mesmo protocolo e existe o bitcoin (btc), com "b" minúsculo, o ativo financeiro usado como unidade de medidas. Ou seja: você compra bitcoins (ou os "centavos" dele, chamados

satoshis) e utiliza a rede Bitcoin para fazer as transações financeiras. Atualmente existe um movimento, encabeçado pelo Saifedean Ammous e a equipe de tradução do livro “O Padrão Bitcoin” para simplificar a grafia e transformar tudo em “bitcoin”. O argumento é que se perde muito tempo em discussões inócuas e que sempre é possível compreender o contexto se a frase se refere ao ativo ou à rede e ao protocolo. Neste livro, adotaremos o padrão “bitcoin” para todos os casos, pois concordo com o Saifedean Ammous e acredito que, assim como foi com a internet, que inicialmente possuía a grafia “Internet” e que só depois foi atualizada para “internet”, o mesmo ocorrerá com a grafia do Bitcoin.

**Bitcoinheiro (ou bitcoiner)** - são os adeptos da tecnologia bitcoin. Existem algumas escalas de bitcoinheiros, desde os novatos que ainda estão começando a entrar na toca do coelho (termo que os bitcoinheiros usam em referência ao filme Matrix, onde Neo tem que “seguir o coelho branco”), até os maximalistas, como são conhecidos os bitcoiners que acreditam que a moeda será o protocolo vencedor em um jogo em que o vencedor leva tudo.

Também pode ser definido como aquele que já entendeu a descoberta do bitcoin e sua inevitabilidade. O bitcoinheiro sabe e entende com clareza a unicidade ou diferença do bitcoin em relação a todos os outros ativos existentes, moedas fiduciárias e tokens digitais centralizados. O bitcoinheiro também sabe porque o Satoshi Nakamoto ter desaparecido é algo positivo e não negativo.

**Bitcoin Cash (BCH)** - é uma shitcoin resultante do fork (veja mais abaixo) mais conhecido do bitcoin até o momento. Foi um ataque ao bitcoin por um grupo que tinha como objetivo o controle da rede por meio da falsa narrativa de facilitar a realização de pagamentos e oferecer maior capacidade de transações por segundo.

**Bull (bullish)** - o termo “bull market” é usado para mercados em alta (altistas) e quando um investidor está com um sentimento positivo em relação ao mercado e acredita que a tendência é de alta ele está “bullish”.

**Carteira (ou wallet)** - conhecida como wallet, pode existir no formato físico, ou 100% digital, através de programas e apps. Facilita o armazenamento das chaves privadas e o envio e recebimento de mensagens criptográficas. As carteiras não armazenam os bitcoins, os bitcoins não estão em nenhum lugar específico, eles vivem na rede (ou mais especificamente, na blockchain. O que temos é a posse da chave que controla aqueles bitcoins.

**CBDCs** - É uma forma ainda mais centralizada de moedas fiats. A China

já lançou o seu Yuan Digital, a Europa, o Brasil e os EUA também já mostraram interesse na criação da sua moeda digital, e a criação do Euro Digital, Real Digital e Dólar Digital é questão de tempo. Com essas moedas digitais, os governos terão o poder de determinar como seus cidadãos irão utilizar seu dinheiro, um exercício de engenharia social e totalitarismo orwelliano.

**Chave Privada** - uma das chaves de um par de chaves criptográficas (a outra é uma chave pública) em um sistema de criptografia assimétrica. Deve ser mantida secreta pelo seu dono e pode ser usada para criar assinaturas digitais e para decifrar mensagens ou arquivos cifrados com a chave pública correspondente.

**Chave pública** - a outra das chaves de um par de chaves criptográficas em um sistema de criptografia assimétrica. É aquela que deriva os endereços públicos que podem ser utilizados para receber bitcoins.

**Cold Wallet** - é o método utilizado para gerar e armazenar chaves privadas sem conexão com a internet. Pode ser um pendrive, um hardware específico e dedicado (como Ledger, Trezor e Coldcard), uma folha de papel com um código QR ou mesmo um conjunto de palavras que a pessoa memorizou.

**Criptografia** - é uma técnica de construção e análise de protocolos usada para proteger dados e impedir que terceiros não autorizados tenham acesso a informações privadas.

**Custódia** - é a ação de ter a posse exclusiva ou compartilhada (multi assinatura) das suas chaves privadas para assegurar sua proteção e segurança. A custódia pode ser feita tanto por empresas quanto por pessoas. Um dos lemas principais para todo bitcoinheiro é o "not your keys, not your coins", que incentiva todos os usuários da rede bitcoin a fazer sua própria custódia a fim de serem independentes de terceiros.

**Cypherpunks** - é um grupo informal de pessoas interessadas em criptografia. Seu objetivo é assegurar a conformidade com privacidade a partir do uso da criptografia. Esse movimento teve origem nos anos 1990 e foi criado por um grupo de matemáticos, cripto anarquistas e hackers. Os membros originais não tinham ideologia social, eram mais preocupados com a matemática complexa da criptografia e com a filosofia mais ampla de anonimidade, privacidade e liberdade individual.

Os cypherpunks foram instrumentais no movimento em defesa da privacidade e anonimidade online. Eles usavam a criptografia como forma

de proteger a individualidade inibindo o controle dos dados trafegados pelos agentes governamentais, institucionais ou do setor comercial.

**DCA** - é o acrônimo de "dollar cost averaging", uma estratégia de investimento que consiste em realizar aportes diários, semanais ou mensais. Ao fazer isso, o investidor suaviza a volatilidade do seu investimento e simplifica sua estratégia. Existe todo um movimento entre os bitcoiners que valorizam este método, que é seguro e confiável no longo prazo. Se quiser entender mais do DCA procure o projeto "HOLD BTC 100" e também pesquise sobre o chavão "preço não importa" que os investidores de bolsa utilizam, baseada na hipótese do Mercado Eficiente<sup>2</sup>.

**Ethereum** - é a altcoin mais conhecida. O Ethereum é uma rede de código aberto fundada por Vitalik Buterin para supostamente desenvolver aplicativos descentralizados. Supostamente, porque não faz sentido acreditar que algo é descentralizado se este algo foi construído em cima de uma base centralizada, como é o caso deste projeto. Cerca de 70% dos tokens do ETH são pré-minerados, o que significa que os fundadores emitiram tokens para si e seus amigos, tornando o Ethereum efetivamente um scam.

**estado** - O estado corresponde ao conjunto de instituições no campo político e administrativo que organiza o espaço de um povo ou nação. Para o estado existir, é necessário que ele possua o seu próprio território e que exerça sobre este a sua cidadania, ou seja, o estado deve ser a autoridade máxima na área a ele correspondente. O autor deste livro concorda com o racional do Instituto Ludwig von Mises Brasil, que diz "se povo, sociedade, indivíduo, pessoa, liberdade, instituições, democracia, justiça são escritas com minúscula, não há razão para escrever estado com maiúscula".

**Exchange** - é o nome usado para as corretoras que vendem criptomoedas. Diferentemente das corretoras, a exchange também é uma bolsa, e existe uma formação de preço independente em cada uma delas.

**Fees** - é o valor que o usuário oferece à rede para que os mineradores insiram sua mensagem (transação) num bloco que será minerado.

**FOMO** - é o acrônimo de "Fear Of Missing Out", em português seria o "medo de ficar de fora". O FOMO é o termo utilizado para descrever o sentimento de ganância e medo de ficar de fora de um investimento com altos ganhos possíveis.

**Fork** - é uma bifurcação em que uma blockchain alternativa é gerada

a partir da blockchain original, de forma que passam a existir duas blockchains coexistindo a partir do momento do fork. Um exemplo de fork são o bitcoin e o bitcoin cash.

**Fiat** - ou moeda fiduciária, é qualquer título não-conversível, ou seja, não é lastreado a nenhum metal (ouro, prata). Seu valor é baseado na confiança que as pessoas têm em quem emitiu o título. A moeda fiduciária pode ser uma ordem de pagamento (cheques, por exemplo), títulos de crédito, dinheiro de papel, entre outros.

**FUD** - é o acrônimo de "Fear, Uncertainty and Doubt", ou em português "Medo, Incerteza e Dúvida". Termo usado para definir o estado de espírito causado por notícias negativas (verdadeiras ou baseadas em rumores). Os bitcoinheiros usam o termo FUD para se referir a notícias mal intencionadas ou simplesmente ignorantes que são superficiais e causam medo nos novatos.

**Gasto Duplo** - é uma possível falha no sistema das criptomoedas. O gasto duplo ocorre quando um usuário consegue gastar as mesmas moedas mais de uma vez.

**Hot Wallet** - é a carteira online utilizada para gerar e armazenar suas chaves privadas. As chaves armazenadas nela podem ser utilizadas para trocar bitcoins rapidamente com outros membros da rede. As hot wallets são consideradas menos seguras que as cold wallets, pois elas ficam hospedadas em celulares ou computadores que possuem acesso à internet e podem ser invadidos.

**Halving** - é o evento que reduz pela metade a recompensa dos mineradores pelos blocos minerados. No bitcoin, o halving ocorre a cada 210.000 blocos, aproximadamente uma vez a cada quatro anos. Os halvings causam os ciclos que foram observados no preço do bitcoin.

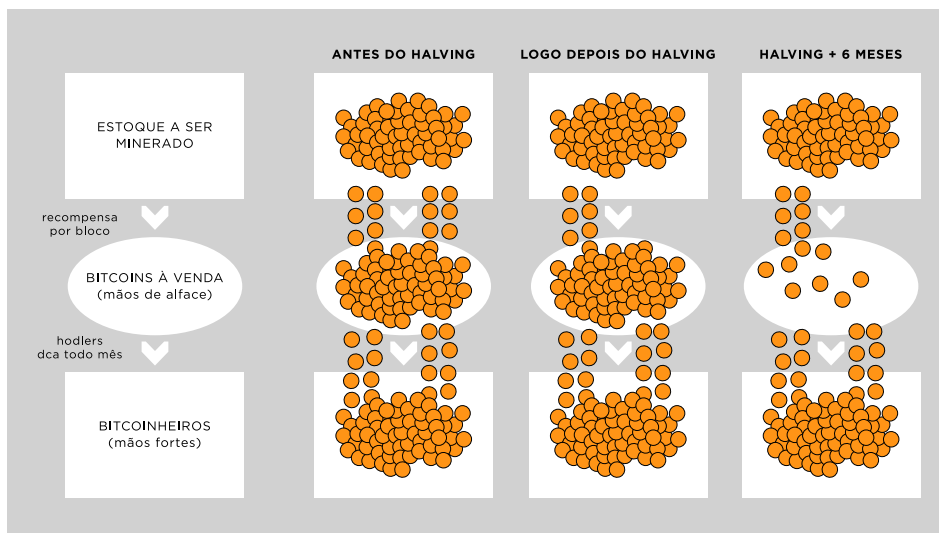


Imagem original concebida pelo @IIICapital<sup>3</sup>.

**Hard Fork** - é uma alteração no protocolo que o torna incompatível com as versões anteriores. Os nodes que não forem atualizados não processam as transações posteriores a este fork. Um famoso exemplo de hard fork do bitcoin é o bitcoin Cash.

**Hash** - é o termo técnico que descreve o código de saída (exclusivo e alfanumérico) obtido na aplicação de um algoritmo (função hash) em uma sequência de entrada (um texto, imagem, etc.) que permite saber se a sequência foi alterada ou permanece intacta.

**Hashrate** - ou taxa de hash, é a unidade de medida de processamento da rede, ou seja, é a velocidade com a qual a soma dos processadores que fazem parte da rede geram valores de hash por um intervalo de tempo. A unidade de medida usual é hashes/segundos (h/s).

**HODL** - é o termo utilizado no mundo das criptomoedas para o "buy and hold", uma estratégia popular para quem investe na bolsa de valores. HODL surgiu de um erro de digitação da palavra "hold", "segurar" em português, de um usuário do fórum bitcointalk em 2013. No mundo das criptomoedas, quem segue a estratégia de HODL é conhecido como HODLer.

**KYC** - é o acrônimo de "Know Your Customer", ou em português "conheça o seu cliente". Exchanges KYC são as exchanges que exigem que o usuário apresente documentação e valide a sua identidade para poder comprar e vender

seus bitcoins.

**Ledger** - é uma das principais fabricantes de cold wallets. Os bitcoinheiros consideram ela muito controversa e não a recomendam pois é focada em shitcoins. Seu código é fechado e já vazou informações privadas de clientes.

**Lightning Network** - é o sistema descentralizado de micropagamentos que roda em uma camada secundária acima da rede bitcoin. Graças à Lightning Network, hoje em dia é possível comprar até um café com bitcoin com taxas de transação muito baixas.

**Mecanismo de Consenso** - também conhecido como algoritmo de consenso, é um procedimento onde todos os participantes da rede chegam a um acordo comum sobre o livro contábil distribuído.

**Mempool** - é a abreviação de "Memory Pool", é o conjunto de transações que ainda não foram confirmadas na Timechain. Toda transação feita é direcionada para o mempool e lá os mineradores ordenam as transações para construir os blocos.

**Mineração** - é o nome dado ao processo de adicionar registros de transações no livro razão público do bitcoin (a Timechain) a partir da adivinhação de números aleatórios. É a partir da mineração que as transações do bitcoin são validadas e que novos bitcoins são emitidos.

**NFT** - é o acrônimo de "Not Fungible Tokens", ou em português "tokens não fungíveis". Os tokens NFT são como certificados (que podem ser criados em qualquer "blockchain") para supostamente representarem uma relação direta com algo digital que está hospedado em um servidor centralizado. Uma coisa fungível é algo passível de ser substituído por outra coisa de mesma espécie, qualidade, quantidade e valor.

Para ser mais direto, NFTs são scams.

**Nocoiner** - quem ainda não possui nenhum satoshi. Geralmente o termo nocoiner é usado de forma pejorativa, uma vez que os nocoiners comentam algo negativo sobre o bitcoin com grande convicção, sem perceber o tamanho de sua ignorância em relação a este tema.

**Normie** - quem ainda se pauta nos meios tradicionais para se informar. Os normies não são maldosos, só se baseiam em premissas erradas (só se informam pelos veículos tradicionais de notícias) e do senso comum para embasar praticamente todos os seus argumentos.

**NGU Tech (ou tecnologia NGU)** - NGU é o acrônimo de Number Go Up,

ou “o número sobe”. É uma brincadeira entre os bitcoinheiros, que dizem que o bitcoin possui uma tecnologia que faz o número subir. A NGU Tech é explicada em detalhes no capítulo 7.

**Nodes ou Full Nodes (nós completos)** - são todos os nós que verificam as regras do bitcoin e propagam transações válidas pela rede. Os full nodes (também conhecidos como full archive nodes) são computadores que rodam o software do bitcoin constantemente e mantêm uma cópia completa de todo o histórico de transações da rede enquanto os nodes prunados (que são nodes que mantêm apenas uma versão resumida com os blocos mais recentes). Em resumo, o full node registra e valida toda a informação que transita na rede bitcoin. Nesse sentido, a informação que não está de acordo com as regras é rejeitada.

**Plebs (plebe ou plebeu)** - é a designação de um bitcoinheiro padrão. Entre os bitcoinheiros, status ou certificações fiats são pouco valorizadas e o pensamento “você sabe quem eu sou?” é abominado. Em oposição, diversos bitcoinheiros se autodenominam plebs, buscando marcar a diferença entre a arrogância e o ego fiat em contraste com a busca pela verdade e humildade comum entre os bitcoinheiros. Ser só mais um pleb é o maior status que um bitcoinheiro pode almejar.

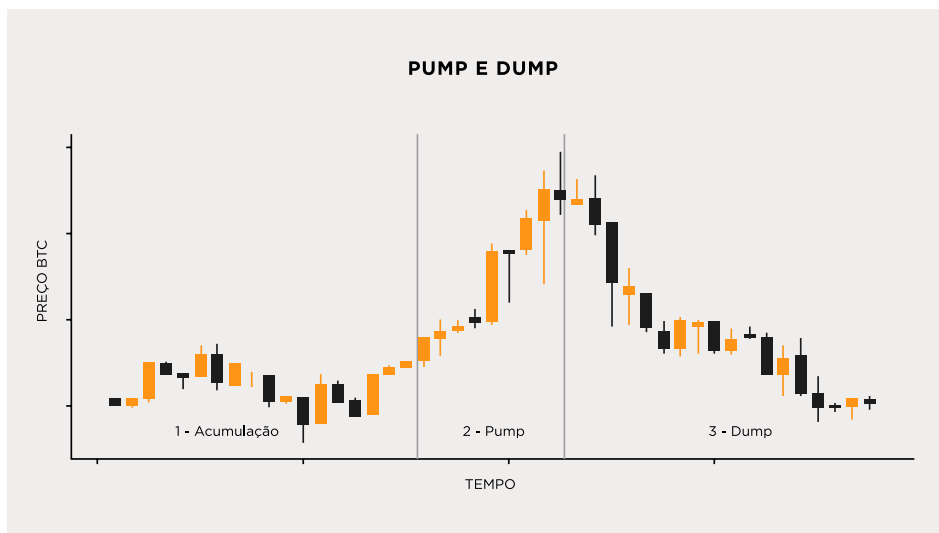
**Proof of Work (PoW)** - em português significa “prova de trabalho”. É o sistema utilizado para a validação de transações na rede bitcoin. Ela é difícil de ser produzida mas facilmente verificada. A prova de trabalho cria uma conexão entre os mundos físico e digital que não pode ser falsificada. Essa conexão é feita através do uso de energia para a mineração de bitcoins.

**Proof of Stake (PoS)** - em português significa “prova de participação”. É o sistema de validação de transações em uma rede que é baseado em uma série de masternodes. No PoS, quem tem mais moedas, manda mais.

Então, mesmo se uma criptomoeda baseada em PoS se tornar reserva global, nada mudaria. Ainda existiria uma elite de mandatários com poderes superiores ao restante da população que sempre continuariam no topo. Por isso que o bitcoin é PoW, pois é um sistema que acredita em regras e não em mandatários (rules, not rulers).

**Pump and Dump** - em português “inflar e descartar” é uma fraude que consiste em inflar artificialmente o preço de um ativo através de declarações positivas falsas e enganosas, com o objetivo de vender as ações compradas a baixo custo por um preço mais alto.





**REKT** - é a gíria americana utilizada para dizer que alguém foi totalmente destruído. Ela tem origem no mundo dos videogames de tiro em primeira pessoa. No mercado, tanto o tradicional quanto o do bitcoin e criptomoedas, esse termo é aplicado quando alguém é liquidado por um movimento inesperado.

**Satoshi Nakamoto** - é o pseudônimo da pessoa (ou grupo de pessoas) que descobriu o bitcoin. Ele atuou ativamente por dois anos após a publicação do whitepaper e depois desapareceu, permitindo que a rede crescesse por meio dos seus próprios incentivos criados no código, fazendo emergir a propriedade de descentralização. Existem diversas teorias, mas a verdade é que ninguém sabe realmente quem foi Satoshi Nakamoto, e talvez isso seja a sua principal contribuição para o bitcoin.

**satoshis** - são os "centavos" do bitcoin. Cada bitcoin é formado por 100 milhões de sats (ou sats, como a comunidade utiliza).

**Shitcoin** - em português "moeda de merda", é o termo utilizado pelos bitcoinheiros para descrever as altcoins. Na visão destes investidores, as altcoins não são verdadeiramente descentralizadas e geralmente os seus fundadores receberam tokens pré-minerados, o que compromete a integridade e o alinhamento de incentivos dessas altcoins.

**Smart Contracts** - em português "contratos inteligentes", é o termo usado para os contratos digitais programados e auto-executáveis entre duas ou mais partes para bens, serviços ou outros. As transações bitcoin são um exemplo

de smart contract que permite desintermediar, ou seja, cortar intermediários de diversos processos financeiros e jurídicos.

**Soft Fork** - é uma mudança simples no protocolo de uma criptomoeda que se mantém compatível com versões anteriores. Geralmente essa categoria de fork não traz problemas de validação para a rede já que ela continua funcionando mesmo com nodes desatualizados.

**Stablecoin** - é uma criptomoeda criada para que o seu valor permaneça estável. Exemplos de stablecoins são: I) USDT (Tether, uma criptomoeda lastreada no dólar americano em 1 USDT = 1 USD) e II) PAXG (uma stablecoin lastreada na onça do ouro).

**Token** - é a representação digital do valor de um ativo (físico ou não) no mundo das criptomoedas. Os tokens representam o direito de usar um produto ou serviço que terá uma função específica no ecossistema de um projeto.

**Transações P2P** - são transações entre duas entidades que negociam diretamente entre si, sem a intermediação de uma exchange, modelo no qual o bitcoin foi pensado em ser utilizado.

**Trezor** - Foi a primeira fabricante a popularizar o uso de cold wallets.

**Timechain** - como Satoshi se referiu originalmente e como os bitcoinheiros chamam a blockchain do bitcoin. Ou seja, outras criptomoedas podem ter uma blockchain, mas somente o bitcoin tem a Timechain.

**VC (Venture Capital)** - são os fundos de investimento. A função de todo fundo de investimento é ganhar dinheiro para os seus cotistas e uma maneira muito simples e eficiente de gerar lucros altos é via esquemas de pump and dump. Justamente por isso os VCs são muito ativos no mercado de cryptoativos. Os demais mercados são mais regulados e geralmente possuem mais liquidez, então nesses mercados é mais complicado executar um esquema de pump and dump. Isso explica parte da atividade especulativa associada ao mercado de NFTs, metaverso e shitcoins em geral. Nestes mercados, é possível executar wash trading sem consequências.

**Wash trading** - é uma forma de manipulação de mercado em que um investidor vende e compra simultaneamente os mesmos ativos financeiros para criar uma demanda artificial no mercado. No caso das NFTs, nada impede que quem produziu a NFT inicialmente não execute diversas operações de wash trading e eleve o valor de zero para muitos milhares de dólares somente com transações entre si. Inclusive, às vezes os investidores deslizam e são pegos

fazendo isso, como no caso da ex-primeira dama Melania Trump<sup>4</sup>.

**Whitepaper** - é o documento técnico que descreve as principais propriedades de um projeto baseado na tecnologia blockchain e sua criptomoeda correspondente. O whitepaper do bitcoin<sup>5</sup> foi publicado na lista de e-mails dos cypherpunks por Satoshi Nakamoto no dia 31 de outubro de 2008.

## **Bitcoin: Um Sistema de Dinheiro Eletrônico Peer-to-Peer**

Satoshi Nakamoto  
satoshin@gmx.com  
www.bitcoin.org

Traduzido para Português de [bitcoin.org/bitcoin.pdf](http://bitcoin.org/bitcoin.pdf)  
por Rodrigo Silva Pinto - <http://linkedin.com/in/rodrigossilvap>

**Resumo.** Uma versão puramente peer-to-peer de dinheiro eletrônico permitiria que pagamentos on-line fossem enviados diretamente de uma parte para outra, sem passar por uma instituição financeira. As assinaturas digitais fornecem parte da solução, mas os principais benefícios são perdidos se um terceiro confiável ainda é necessário para evitar o gasto duplo. Nós propomos uma solução para o problema de gasto duplo usando uma rede peer-to-peer. A rede insere data e hora nas transações através de um hash em uma cadeia contínua de prova-de-trabalho à base de hash, formando um registro que não pode ser alterado sem refazer a prova-de-trabalho. A cadeia mais longa não só serve como prova da sequência de eventos testemunhados, mas prova de que ela veio do maior pool de CPUs. Enquanto a maioria do poder das CPUs é controlado por nós que não estão cooperando para atacar a rede, eles irão gerar a cadeia mais longa e superar os atacantes. A própria rede requer estrutura mínima. As mensagens são espalhadas em regime de melhor esforço, e nós podem sair e regressar a rede à vontade, aceitando a cadeia mais longa de prova-de-trabalho, como prova de que aconteceu enquanto eles estavam fora.

Trecho do whitepaper.

## PARTE 1 - O PROBLEMA

*No coração da ciência existe um equilíbrio essencial entre duas atitudes aparentemente contraditórias - uma abertura para novas ideias, por mais bizarras ou contrárias à intuição, e o exame cético mais implacável de todas as ideias, antigas e novas.*

*É dessa forma que as verdades profundas são separadas de profundos disparates. O empreendimento coletivo do pensamento criativo e do pensamento cético, atuando em conjunto, mantém a ciência em andamento.*

Carl Sagan

## CAPÍTULO 1

# O QUE O BITCOIN CONSERTA?

Um dos lemas mais comumente usados na comunidade dos bitcoinheiros é o “fix the money, fix the world”, algo como “conserte o dinheiro, conserte o mundo”. Mas para consertar algo, o pressuposto básico é reconhecer que este algo está quebrado em primeiro lugar. Ou seja, quem não consegue diagnosticar o que existe de errado no mundo atual, não consegue visualizar o porquê esse mundo precisa de algo que o conserte.

### O bitcoin e a neosaldina

O bitcoin é uma solução, então para entendê-lo é necessário compreender qual o problema que ele soluciona. Um exemplo que sempre utilizo é o da neosaldina e a enxaqueca. Para quem não está com enxaqueca, uma neosaldina não possui valor algum e, provavelmente, seria recusada mesmo se oferecida de graça. Em compensação, para uma pessoa que está com uma crise de enxaqueca, essa mesma neosaldina vale muito. Ou seja, para quem conhece o problema e o está sentindo na pele, a solução faz muito mais sentido do que para quem não tem consciência do problema.



E qual o problema que o bitcoin conserta? O objetivo deste texto é responder melhor essa pergunta, mas basicamente: o bitcoin representa a separação entre o dinheiro e o estado.

## **Separação entre o dinheiro e o estado**

Todos estudamos a importância da separação entre a igreja e o estado em nossas aulas de história. De acordo com o Wikipédia, “a separação igreja-estado é uma doutrina política e legal que estabelece que o governo e as instituições religiosas devem ser mantidos separados e independentes uns dos outros. A expressão se refere mais frequentemente à combinação de dois princípios: secularismo do governo e liberdade religiosa”.

Em poucas palavras, foi a separação entre a igreja e o estado que permitiu a humanidade criar os estados modernos e a sociedade como nós os conhecemos hoje. Foi a separação entre a igreja e o estado que permitiu a construção do mundo em que vivemos. Antes, a religião era controlada por poucos e utilizada como ferramenta de poder e controle sobre os indivíduos, e pessoas podiam ser punidas por não concordar com estes dogmas e possuir uma visão de mundo diferente, sendo denominados hereges.



Um exemplo de punição utilizada por religiosos e pela igreja para defender seus dogmas.

Nosso mundo foi construído graças à negação dessa posição de autoridade da religião. Foi a possibilidade de geração de um tipo de conhecimento baseado em evidências e lógica (o chamado método científico, fruto da Revolução Científica) e não em dogmas impostos por doutrinas religiosas que fez a humanidade avançar. Você consegue imaginar viver em um mundo sem antibióticos, onde qualquer infecção pode ser fatal? Sem geladeira, onde a conservação de alimentos não é possível com a mesma eficiência? Até existem outras formas de preservação de alimento como a desidratação, a fermentação e o enlatamento, que permitem a conservação de alimentos sem utilização de eletricidade. Você consegue se imaginar sem motores a combustão ou a vapor, peças fundamentais para a Revolução Industrial e sem substituto até os dias de hoje? E um mundo sem eletricidade? Qualquer um desses avanços seria considerado bruxaria para um indivíduo da Idade Média. E sem essa separação, nada disso teria sido possível.

Da mesma forma, vivemos em um mundo que antecede a separação entre o dinheiro e o estado. Para entender o tamanho das implicações disso, o primeiro passo é se perguntar: o que é dinheiro?

Este é um tema profundamente explorado pelos bitcoinheiros, mas aqui vamos nos ater à definição simples de que o dinheiro é a tecnologia inventada pela humanidade que permite a transferência de trabalho e energia através do

tempo.

## O dinheiro na mão do estado

Mas, quais são os problemas do dinheiro estar na mão do estado? Ou, em outras palavras, qual o problema da nossa tecnologia de comunicação de valor entre indivíduos poder ser controlada por uma entidade centralizada e com interesses próprios?

Você deve se lembrar de quando era criança e seus pais te alertavam que “o dinheiro não cai do céu”, ou ainda que “dinheiro não nasce em árvore”. O que eles queriam dizer é que o dinheiro possui lastro na realidade, por isso ele tem valor.

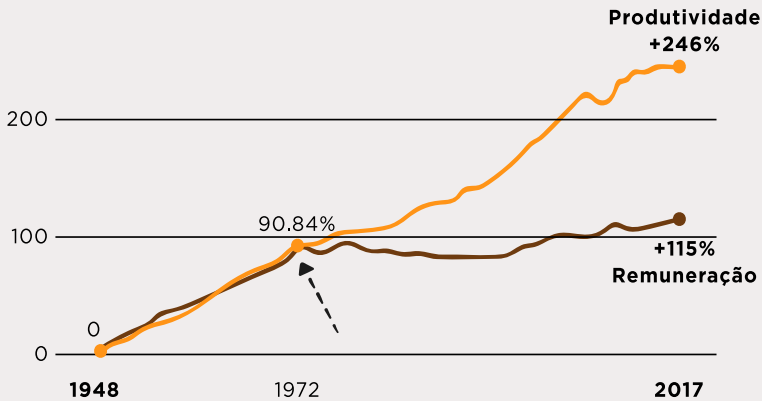
Mas os seus pais estavam enganados. Atualmente, pode-se dizer que o dinheiro não possui nenhum lastro real e efetivamente nasce em árvore. Ou seja, a tecnologia de comunicação de valor entre indivíduos está sendo manipulada em benefício de uma pequena elite que possui acesso às impressoras de dinheiro. Atualmente, todos os governos do mundo imprimem seu próprio dinheiro ao bel prazer, sem respeitar qualquer tipo de reservas em bens físicos.

Existem pessoas que acreditam que o governo é belo e moral e que, diferentemente do que acontece para indivíduos, o governo imprimir dinheiro não acarreta problemas. A história prova que este ponto de vista está errado. Um site que todo bitcoinheiro deve pesquisar e que comprova isso é o [wtfhappenedin1971.com](http://wtfhappenedin1971.com) (algo como “que porra aconteceu em 1971”.com), que compila diversos gráficos que ilustram o tamanho da mudança que o mundo passou a partir de 1971, quando o dinheiro passou a nascer em árvore. Este é o ano em que o presidente Richard Nixon rompe o lastro ouro/dólar, e com isso desassocia o mundo real do dólar. Isso fez com que a moeda americana virasse uma moeda fiat, ou seja, uma moeda que só tem valor por decreto e não pelo seu lastro.

Os três gráficos abaixo são do site [wtfhappenedin1971.com](http://wtfhappenedin1971.com) e ilustram bem o tamanho das mudanças associadas à Era Fiat:

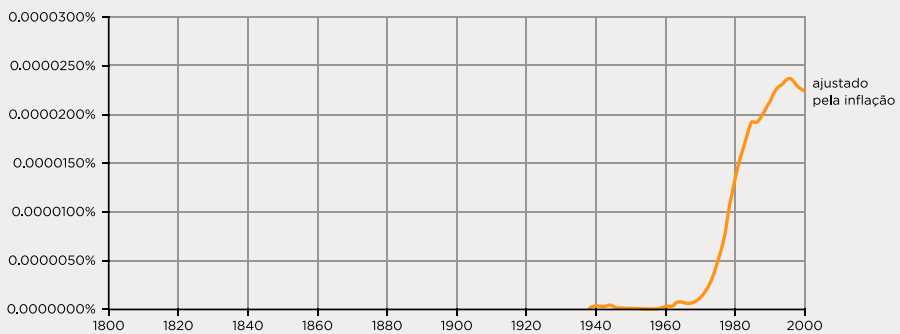


### CRESCIMENTO DA PRODUTIVIDADE E DA REMUNERAÇÃO POR HORA DESDE 1948



A produtividade real aumentou significativamente mais que a remuneração, que permaneceu praticamente estável desde a década de 1970.

### OCORRÊNCIA DO TERMO "AJUSTADO PELA INFLAÇÃO" NO GOOGLE BOOKS



A inflação passou a ser um fenômeno mais comum e recorrente, o que é comprovado pela ocorrência do termo "ajustado pela inflação" no Google Books (um serviço da Google que procura textos completos de livros, os escaneia e os converte utilizando o reconhecimento óptico de caracteres, para armazená-los em seu banco de dados digital).



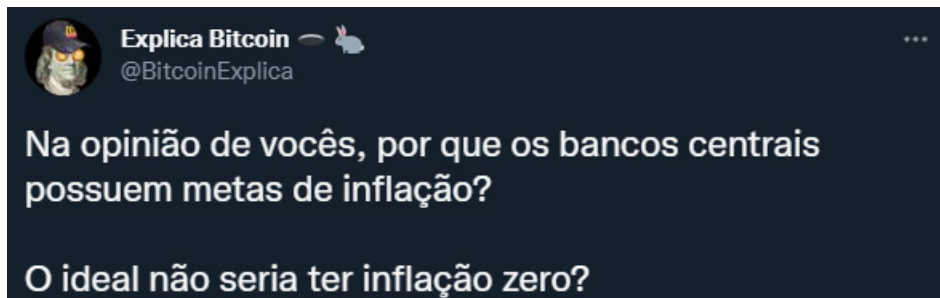
O processo de colapso de moedas nacionais se tornou algo comum após 1971.

## Os problemas do dinheiro na mão do estado

A seguir, são apresentados, de forma sucinta, alguns dos principais problemas associados ao dinheiro no mundo atual.

### Inflação planejada

Atualmente, os bancos centrais dos países do mundo possuem metas de inflação. Em outras palavras, eles miram e tentam fazer com que exista inflação. Os economistas keynesianos dizem que isso é positivo pois estimula o consumo e o crescimento. Para ver como a nossa comunidade de plebs bitcoinheiros enxerga essa inflação planejada, lancei a pergunta da imagem abaixo no Twitter<sup>6</sup>.





**Dino** @dino\_br21 · Apr 18

Replying to @BitcoinExplica

**Porque nos modelos de economia keynesianos tem umas groselhas lá sobre inflação incentivar atividade econômica, emprego blá blá blá**

Essa inflação planejada vem ocorrendo há décadas, uma vez que ela é uma das únicas maneira que os estados possuem para gastar mais do que arrecadam (a outra é o endividamento estatal via títulos de dívida), o que eles já fazem há décadas. Basicamente, eles pegam dinheiro emprestado do futuro e das próximas gerações para usar esse dinheiro no presente. Essa é a única razão que justifica o sistema econômico keynesiano ainda estar em pé: ele rouba das próximas gerações. Uma verdadeira pirâmide em que as gerações passadas acumularam um padrão de vida elevado e em troca sabotaram os millennials e a geração Z.

Os economistas keynesianos têm medo de deflação, pois na visão deles uma hipotética deflação estimula o poupador a reter o seu dinheiro, o que desaceleraria o consumo e geraria uma espiral recessiva. Para os governos um poupador é alguém que está desacelerando a economia ao reter seu capital, o que é perigoso, pois uma desaceleração tornaria as suas dívidas mais impagáveis do que a atual realidade.

Devido a essa visão capenga sobre inflação e deflação e o incentivo à emissão de moeda para pagar mais programas sociais, que são usados para comprar apoio político, atualmente os governos possuem dívidas impagáveis e, no ponto de vista deles, quanto maior for a inflação, melhor. Isso porque a inflação torna essa dívida mais viável, visto que o poder de compra do dinheiro diminui devido ao aumento da base monetária.

Desse ponto de vista, as metas de inflação simplesmente auxiliam o governo a não perder o controle dessa inflação proposital. Perder o controle dela significa entrar em uma hiperinflação, o que gera inquietação na sociedade e, possivelmente, revoltas e saques. A hiperinflação, a partir de um certo ponto, causa um fenômeno de repúdio à moeda nacional (onde as pessoas começam a se recusar a transacionar naquela moeda), culminando na perda de função de unidade de conta (como pode ser observado na Venezuela e Argentina). Então, no ponto de vista dos governos, o ideal é manter a inflação o mais alta possível sem que haja convulsão popular.



**agora chega** @apenascodorna · Apr 18

...

Replying to @BitcoinExplica

**Como bem disse Rothbard no seu livro, inflação é bom para o governo, mas mais do que isso, ele precisa ter o controle (não os bancos ou sem controle centralizado). A meta de inflação é apenas uma maneira de evitar a hiperinflação, onde eles perderiam o controle.**


Ou seja, os poupadores e os governos estão inerentemente em campos opostos: os poupadores são beneficiários da deflação, pois isso aumenta o seu poder de compra no futuro, já os governos se beneficiam da inflação, pois ela faz com que o poder de compra do dinheiro no futuro seja menor, tornando suas dívidas viáveis.

Em outras palavras, os incentivos do governo e dos poupadores são diametralmente opostos.

Mas o que isso significa? De uma maneira bem simplificada, as economias de todos os poupadores perdem seu poder de compra. Ou seja, quando o governo estabelece metas de inflação, na realidade ele está estabelecendo metas de roubo do tempo dos poupadores.

Em poucas palavras: o governo está roubando o nosso tempo de vida.

Isso porque, quando um indivíduo se dedica a trabalhar e a economizar dinheiro, ele está convertendo o seu trabalho em uma reserva de valor para o longo prazo chamada dinheiro. Quando o governo ativamente possui metas para diluir o poder de compra dessa reserva de valor, efetivamente ele está roubando o tempo que este indivíduo se dedicou para acumulá-la. Então, quando você ler sobre "meta de inflação", saiba que isso quer dizer "roubo do poder de compra do fruto do seu trabalho".



[INGRESSO.COM](#) [BATE-PAPO](#) [MEU NEGÓCIO](#) [PASSEI DIRETO](#) [PAGSEGURO](#) [UOL PLAY](#)

[SAC](#) [EMAIL](#) [ENTRE](#)

[ASSINE UOL](#)

[PRODUTOS](#) [NOTÍCIAS](#) [CARROS](#) [ECONOMIA](#) [FOLHA](#) [ESPORTE](#) [SPLASH](#) [UNIVERSA](#) [VIVABEM](#) [TILT](#) [EOCA](#) [CANAL UOL](#) [MOV](#) [NOSSA](#) [TAB](#) [START](#)

DÓLAR COM.

+0,43%

R\$ 4,668

PESO

+0,97%

R\$ 0,041

EURO

+0,40%

R\$ 5,035

BITCOIN

+2,53%

R\$ 195.171,25

BOVESPA

-0,55%

115.056,66 pts

IPCA

+1,62%

Mar. 2022

SELIC

+11,75%

16 Mar. 2022

**VERSÃO OFICIAL:**

## ECONOMIA

Para ajudar economia, meta de inflação deve ficar em 3%, dizem analistas

**TRADUÇÃO:**

**o governo a  
pagar suas dívidas**

**roubo do poder  
de compra**

Para ajudar ~~economia~~, meta de ~~inflação~~ deve ficar em 3%, dizem analistas

Um exemplo de como os governos fazem para enganar a população. A inflação "ajuda a economia" e não "a inflação dilui o poder de compra dos indivíduos".

O pleb bitcoinheiro Diego Kolling fez uma boa síntese dessa questão de inflação planejada ser o oposto do que ocorreria em um livre mercado, onde a tendência natural seria a deflação devido ao aumento de produtividade natural que o livre mercado gera:



**Diego Kolling** @diegokolling · Apr 18

Replying to @BitcoinExplica

Se a quantidade de moedas em circulação é fixa (inflação zero), ela tende a apreciar com o tempo pois, para a mesma quantidade de moeda, haverá mais coisas no mundo.

Logo, as moedas valerão mais coisas.

E se valerão mais coisas com o tempo - e não menos, como hoje - eu pouparei



1



6



**Diego Kolling** @diegokolling · Apr 18

E se eu pouparei, eu não investirei em qualquer coisa nem muito menos consumirei qualquer porcaria, porque agora meu dinheiro em cash tem um retorno ano a ano

Mas se eu fizer isso, partindo de onde estamos agora, viveremos uma deflação bizarra e a economia pode entrar em colapso



8



3



**Diego Kolling** @diegokolling · Apr 18

Por isso o BC estabelece a meta de inflação: para garantir que todos continuem a consumir e investir facilmente pois a moeda está pegando fogo.

Está pegando fogo porque ele não para de imprimir.

Imprimir como? Via inflação.

Isso nos torna ratos na matrix do BC.



**Diego Kolling**

@diegokolling

Replying to @diegokolling and @BitcoinExplica

**A deflação é o “livre mercado”.**

A inflação é a função centralizadora contra ele (transferência de riqueza/poder injustamente para proteger a dívida do calote).

É necessário um caminho de transição de um sistema destinado a falhar. #Bitcoin 

## Alta preferência temporal

Uma hipótese bastante conhecida entre quem estudou economia austríaca é que a preferência temporal das pessoas, ou seja, a capacidade delas de se planejarem para o longo prazo, é diretamente afetada pela qualidade do dinheiro que elas têm acesso. Por exemplo: o hábito do brasileiro de fazer a “compra do mês” tem origem no nosso período de hiperinflação no final dos anos 1980 e início dos anos 1990. Isso ocorre pois em períodos inflacionários o poder de compra do dinheiro se torna “um cubo de gelo derretendo”, nas palavras do Michael Saylor. Ou seja, os indivíduos são incentivados a trazerem o consumo do futuro para o presente.



Um dinheiro que é programado para se desvalorizar torna as pessoas mais imediatistas, uma vez que torna mais difícil o planejamento de longo prazo. Isso estimula as pessoas a consumirem o quanto antes, visto que no futuro esse

dinheiro em suas mãos terá um poder de compra menor. Ou seja, um dinheiro que se desvaloriza estimula as pessoas a gastarem no presente ao invés de poupar para o futuro. Essa questão de como a qualidade do dinheiro afeta os padrões de pensamento das pessoas será aprofundada em um capítulo mais adiante, onde é feita a comparação do perfil de personalidade dos bitcoinheiros do exterior com os bitcoinheiros brasileiros onde observamos que, em média, são mais imediatistas que os bitcoinheiros gringos.

Os efeitos deletérios da mudança de preferência temporal em uma sociedade com metas de inflação afetam todas as tomadas de decisão dos seus indivíduos.

O que quero dizer com isso? Que em uma sociedade que incentiva a gratificação instantânea e não escolhas que foquem o longo prazo, todas as escolhas serão baseadas nessa lógica. Então, as escolhas alimentares, por exemplo, não levarão em conta os efeitos deletérios do açúcar e dos óleos vegetais na saúde, mas no prazer imediato que uma bela pizza de pepperoni pode proporcionar.

Em outras palavras, estamos sacrificando o longo prazo pelo curto prazo. Assim como os hábitos alimentares, podemos inferir que os hábitos de consumo também serão extremamente imediatistas. Não é coincidência que na sociedade atual existe o conceito de “fast fashion”<sup>7</sup>, onde o foco são produtos fabricados para serem consumidos e descartados rapidamente.

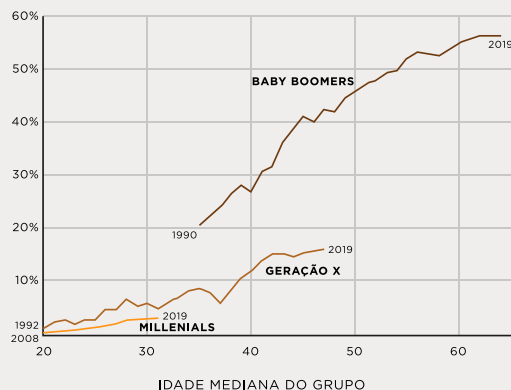
### **Sociedade fiat**

Essa mudança nos nossos padrões de consumo ocorre em todos os ramos da atividade humana. Uma consequência direta do dinheiro ter cada vez menos poder de compra é que precisamos trabalhar cada vez mais para atingir os mesmos objetivos. Por isso, hoje em dia é muito mais difícil para um millennial sonhar em comprar sua própria casa do que era no passado. E isso não é uma teoria da conspiração ou um discurso de uma geração acomodada, é fato observado nos dados. Ou, como o Michael Saylor diz, citando Hayek: o caminho da servidão consiste em você trabalhar cada vez mais para ganhar um dinheiro que vale cada vez menos.



## RIQUEZA INTERGERACIONAL

Porção da riqueza nacional que cada geração possui, separado pela idade mediana do grupo



Com cada vez menos tempo para qualquer coisa que não seja trabalho, uma vez que os frutos deste trabalho são cada vez menores e sendo constantemente erodidos propositalmente, a alimentação piora e comemos mais comida congelada e pedimos mais delivery ao invés de cozinhar. Com menos tempo, nosso prazer passa a ser assistir uma série no Netflix ou comprar alguma tralha na Amazon ou no Shopee, e não passear no parque ou fazer uma atividade física gratuita por duas horas no parque. Numa sociedade com cada vez menos tempo, o lazer precisa ser consumido em alta intensidade. Isso é a essência da sociedade fiat atual, um mundo em que ninguém tem tempo para si. Mas poucos percebem a razão desta falta de tempo: ele está sendo roubado pelos governos, quando estes desvalorizam o poder de compra do dinheiro.

A sociedade fiat também pode ser sintetizada nas palavras do personagem Tyler Durden de Clube da Luta:

*"Trabalhamos em empregos que odiamos, para comprar porcarias que não precisamos, com dinheiro que não temos, para impressionar pessoas que não gostamos".*

Essa necessidade de impressionar o outro vem de uma falta de tempo para buscar o autoconhecimento. Na sociedade fiat, a falta de tempo e a quantidade de ruído gera indivíduos não pensantes, conhecidos como NPCs

(non-player character, ou personagem não jogável) na comunidade bitcoinheira do Twitter. Quem não tem tempo para respirar fundo e pensar, não tem tempo para fugir da sociedade fiat e buscar entender as coisas por conta própria.



Dois memes sobre os NPCs que circulam na internet com a frase “eu apoio o ponto de vista atual”, fazendo referência às pessoas que tem a opinião facilmente moldável pela mídia e redes sociais. Poderia ser “eu apoio a causa atual também”.

### Dinheiro censurável

O dinheiro fiat é um dinheiro censurável por definição, uma vez que o seu controle é dos governos, que possuem o poder de definir se determinada moeda fiduciária ainda é válida ou não. No Brasil, todo o dinheiro poupado pela população já foi confiscado. Isso aconteceu em março de 1990, quando o então presidente Fernando Collor decretou o confisco das poupanças como medida para combater a inflação galopante que afetava o país. Nessa época, a poupança era a principal forma de investimento da grande maioria dos brasileiros que tinham algum dinheiro guardado, então, na prática, o estado se apropriou do fruto do trabalho da maioria dos brasileiros.



**O GLOBO**

**Impressão**

As notícias contidas nesta edição são de autoria dos redatores do jornal e não representam necessariamente a opinião do jornal.

## Collor bloqueia o dinheiro



João Carlos de Sá, João Antônio Rangel, Secretário de Planejamento, e Antonio Rios, Presidente do BC, apóiam a greve em andamento contra o Collor.

No plano econômico mais radical já decretado no Brasil, o presidente Collor ordena que, a partir de amanhã, o Banco Central detenha a circulação de notas e moedas em circulação de 100 mil e 50 mil. O Banco Central também vai detê-lo em 10 mil e 5 mil. O plano também prevê a suspensão de todas as operações de crédito e de depósito em nome de pessoas físicas e jurídicas, e de todas as operações de crédito e de depósito em nome de empresas e de pessoas físicas e jurídicas. O plano também prevê a suspensão de todas as operações de crédito e de depósito em nome de empresas e de pessoas físicas e jurídicas.

### Congresso reage com perplexidade

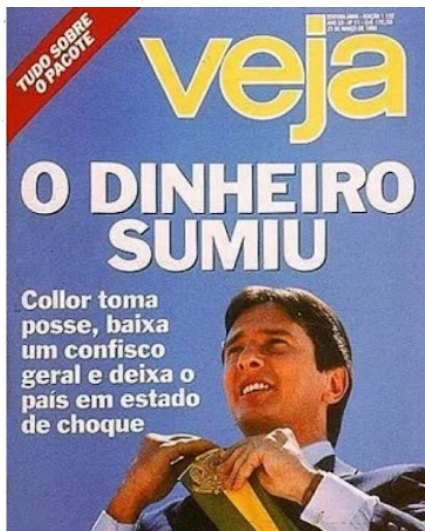
O Legislativo reagiu com perplexidade diante da decisão do presidente Collor de decretar o bloqueio do dinheiro. O Congresso Nacional está reunido em sessão ordinária e os deputados e senadores estão expressando sua surpresa e preocupação com a medida.

### PRINCIPAIS MEDIDAS DO PLANO CONTRA A INFLAÇÃO

<b>POUPANÇA</b> Aumento de 10% no prazo de 12 meses para o Tesouro Nacional e 5% para o Tesouro Estadual e Municipal.	<b>REAJUSTE SALARIAL</b> Limitação de 10% no reajuste salarial para o setor privado e 5% para o setor público.
<b>CONTROLE DE PREÇOS</b> Limitação de 10% no aumento de preços para o setor privado e 5% para o setor público.	<b>CONTROLE DE CÂMBIO</b> Limitação de 10% no aumento de preços para o setor privado e 5% para o setor público.
<b>CONTROLE DE CÂMBIO</b> Limitação de 10% no aumento de preços para o setor privado e 5% para o setor público.	<b>CONTROLE DE CÂMBIO</b> Limitação de 10% no aumento de preços para o setor privado e 5% para o setor público.

### Remarcações de preços dão até 5 anos de prisão

As infrações de preços são, de agora em diante, consideradas crimes. O artigo 312 do Código Penal prevê a pena de prisão de 1 a 5 anos para quem cometer infrações de preços. O artigo 313 do Código Penal prevê a pena de prisão de 1 a 5 anos para quem cometer infrações de preços.



Confiscos de bens monetários são recorrentes na história, então, para não me estender muito, vou citar só um exemplo clássico e outro contemporâneo de como, quando necessário, mesmo os governos dos países ditos “mais civilizados” também não respeitam a propriedade privada dos seus cidadãos:

Estados Unidos, 1933 - todo o ouro dos cidadãos foi confiscado em 1933 em consequência da crise de 1929. Isso aconteceu quando a Ordem Executiva 6102 foi assinada em 5 de abril de 1933 pelo presidente dos EUA, Franklin D. Roosevelt, “proibindo o acúmulo de moedas de ouro, barras de ouro e certificados de ouro dentro dos Estados Unidos continentais”.

Canadá, 2022 - O mesmo aconteceu recentemente nos protestos dos caminhoneiros canadenses, onde o governo do Canadá decretou o congelamento dos fundos do financiamento coletivo dos protestos. Além disso, indivíduos também foram perseguidos e tiveram suas contas congeladas, efetivamente perdendo acesso ao seu próprio dinheiro do dia para a noite por ter opiniões diferentes das que os políticos no poder possuem, graças a decisão de algum burocrata e alguns apertados de botão.

Exemplos não faltam e o fato é que enquanto o dinheiro continuar censurável, indivíduos ainda sofrerão as consequências das barbeiragens econômicas dos estados e terão o seu dinheiro confiscado por estes mesmos estados em tentativas de auto salvação. Mesmo o ouro é facilmente identificável e por conta disso o seu transporte é de alto risco. Fugir de uma situação de crise

ou de um regime tirânico levando ouro simplesmente não é uma opção plausível. Não é viável esconder o patrimônio familiar acumulado numa maleta ou em outros lugares<sup>8</sup> ao tentar cruzar as fronteiras e fugir dessas situações.

Nos dias de hoje, o dinheiro fiat está, em sua maioria, sob controle dos estados e essa tendência só tende a piorar, uma vez que a digitalização do mundo é um processo que segue e seguirá ocorrendo. Conforme formos utilizando mais o dinheiro digital e menos as notas, será cada vez mais fácil para o governo controlar a totalidade das moedas fiduciárias. Hoje, o acesso ao dinheiro fiduciário está sujeito ao cancelamento com alguns simples toques de botão e por alguma decisão monocrática judicial.

### O caso das ex-colônias africanas

O fato do dinheiro ser controlado não afeta somente a população local de determinado país. Atualmente, ainda existe colonialismo, na forma de colonialismo monetário, ocorrendo no mundo. Um exemplo é o caso da França e a utilização do Franco CFA<sup>9</sup> ("Community For África", ou "comunidade para a África" em português) como forma de controle e poder sob um vasto território africano.



Cerca de metade da população<sup>10</sup> da República Centro-Africana precisa de ajuda humanitária.

Atualmente, 16 ex-colônias francesas na África possuem como moeda o Franco CFA. Somadas, essas nações possuem uma população de cerca de 185 milhões de pessoas e ocupam uma área de cerca de 80% do tamanho da Índia. São elas: Senegal, Mali, Costa do Marfim, Guiné-Bissau, Togo, Benim, Burkina Fasso, Níger, Camarões, Chade, Gabão, Guiné Equatorial, República do Congo, República Centro-Africana e Comores. Vale ressaltar que dentre estas ex-colônias, 10 estão entre os países mais pobres da África.

O modelo de controle via dominação monetária foi inventado pelos nazistas, quando eles assumiram o controle das colônias francesas durante a segunda guerra mundial. Ao final da guerra, a França decidiu manter esse modelo, uma vez que ele era efetivo na dominação das colônias. Atualmente, 100% do comércio internacional destas nações passa pelo tesouro da França. A França também faz a custódia de 90% das reservas de ouro e 50% das reservas internacionais desses países. E como "as reservas" de um país não significa nada mais que o dinheiro do povo desse país, isso significa que a poupança de cerca de 185 milhões de africanos é controlada até hoje pela França.

A França também possui prioridade de acesso às exportações desses países, além de receberem preços melhores. Estes países também só podem realizar importações a partir da conversão do Franco CFA em Euro, aumentando o controle da França e da Europa. E o Franco CFA não pode ser convertido em nenhuma outra moeda do mundo, só no Euro.

Desde a criação do Franco CFA, em 1945, até a adoção do Euro no final da década de 90, a desvalorização foi de 99,5%. Neste período, ocorreram episódios em que o Franco CFA foi desvalorizado artificialmente em 50% da noite para o dia, como em 1994<sup>11</sup>.

A justificativa oficial para essa desvalorização, medida oficial adotada pela França, é que com isso as exportações se tornariam mais baratas e os países africanos conseguiriam produzir a preços mais competitivos. Um ponto de vista mais cético mostra que quem pôde comprar estes produtos a preços mais "competitivos" (baratos) foi a própria França. Detalhe: a França pode imprimir o Franco CFA virtualmente de graça, o que significa dizer que eles possuem acesso a tudo que esses países produzem a um custo zero. Esquema que lembra muito a descrição do início de empobrecimento da África graças as miçangas de vidro no texto "Mestres e Escravos do Dinheiro"<sup>12</sup> do Robert Breedlove, processo que facilitou significativamente toda a questão da escravidão e do comércio do

atlântico nos séculos seguintes.

## **Desbancarizados**

Apesar de todas as críticas que são dirigidas constantemente aos bancos, os serviços bancários também apresentam vantagens óbvias, como não ter que esconder dinheiro pela casa e com isso se tornar um ótimo alvo para roubos e furtos ou conectar-se com a rede financeira global e realizar pagamentos em tempo real. Estamos tão acostumados com os benefícios de um sistema bancário relativamente sólido, com conta poupança (que às vezes é confiscada) e meios de pagamento como cheques e cartões, que não pensamos muito em como seria a nossa vida se esse sistema bancário não existisse.

Entretanto, isso ocorre somente porque somos privilegiados. Atualmente, existem cerca de 1,7 bilhões de pessoas<sup>13</sup> no mundo que não possuem acesso a esse sistema. Essas pessoas são conhecidas como “desbancarizadas”. No Brasil, mesmo após a pandemia acelerar a digitalização e a bancarização por conta dos auxílios, ainda existem 34 milhões de brasileiros<sup>14</sup> que utilizam muito pouco ou nem possuem conta em bancos. Em levantamento de janeiro de 2021, estimou-se que 10% dos brasileiros não possuem conta em banco (16,3 milhões) e outros 11% (17,7 milhões) não usaram a conta no mês anterior, totalizando 21% da população.

Pessoas desbancarizadas são marginalizadas da nossa sociedade. Elas não conseguem fazer planos de médio ou longo prazo e são forçadas a pensar sempre no dia a dia. Isso significa, entre outras coisas, que elas não conseguem se aposentar e tendem a continuar em trabalhos mal qualificados e mal remunerados ao longo de toda a sua velhice ou, pelo menos enquanto seu corpo permitir.

Geralmente pessoas são desbancarizadas por diversos motivos, como falta de instrução e residência em regiões menos desenvolvidas, nos rincões que o mundo moderno ainda mal chegou. Um desses diversos motivos é porque essas pessoas não são economicamente viáveis como clientes para os bancos. Elas representam um risco, não uma oportunidade, e não vale a pena para os bancos terem elas como clientes.

## **O exemplo de El Salvador**

É natural que existam muito mais pessoas desbancarizadas em países

pobres, como é o caso de El Salvador. Até 2020, cerca de 70% da população<sup>15</sup> (cerca de 4.5 milhões de pessoas) era desbancarizada.

Além disso, cerca de 20% do PIB de El Salvador é proveniente de remessas internacionais que salvadorenhos que imigraram para os Estados Unidos e Europa enviam para seus parentes. Essas remessas eram alvo de taxas elevadas cobradas pelos intermediários (Western Union principalmente), o que significava que a população já pobre de El Salvador ainda perdia uma parte considerável do seu dinheiro.

Levando estes dois fatores em conta, El Salvador se tornou o primeiro país do mundo a adotar o bitcoin como moeda legal. Com isso, os intermediários são cortados e hoje salvadorenhos que moram no exterior podem mandar dinheiro sem custos para seus familiares. Isso já era possível antes, mas a adoção como moeda legal incentivou a população a aprender mais sobre o bitcoin.

Mas o principal dessa adoção de El Salvador é a bancarização dos desbancarizados. Em menos de um ano, mais de 60% da população, ou um total superior a 4 milhões de pessoas já são usuários da carteira estatal Chivo. Ou seja, ainda existem cerca de 2.5 milhões de pessoas sem acesso a essa carteira. Nesse número, além dos desbancarizados, também estão incluídas as crianças. Ou seja, graças à adoção do bitcoin, do dia para a noite, mais de 2 milhões de pessoas se tornaram bancarizadas e hoje possuem acesso a uma rede monetária que as permite armazenar sua riqueza ao longo do tempo.

## **Ou seja...**

Existem diversos problemas atrelados ao fato do dinheiro estar na mão do estado. Seja o fato dos estados possuírem metas de inflação que efetivamente roubam o tempo de vida e o trabalho acumulado dos seus cidadãos, seja o fato do dinheiro ser censurável e poder ser confiscado, além de ser utilizado até hoje como forma de colonialismo. Existem também cerca de 1.7 bilhões de pessoas que nem possuem acesso ao sistema bancário e com isso não conseguem armazenar o fruto do seu trabalho para o longo prazo.

Também existem as consequências de segunda ordem que essas questões relacionadas ao dinheiro geram, como uma sociedade fiat baseada numa alta preferência temporal onde ninguém tem tempo e a alimentação e os cuidados com a saúde são menosprezados em detrimento de gratificações imediatas.

O objetivo deste texto era justamente ilustrar quais são os problemas atuais relacionados ao dinheiro, pois sem um diagnóstico claro do problema, a solução não faz sentido. Esse texto propositalmente não lidou com o tema da desigualdade porque esse tema será mais profundamente discutido no próximo capítulo sobre o chamado Efeito Cantillon. E, como dito acima, o bitcoin conserta isso.



## CAPÍTULO 2

# EFEITO CANTILLON

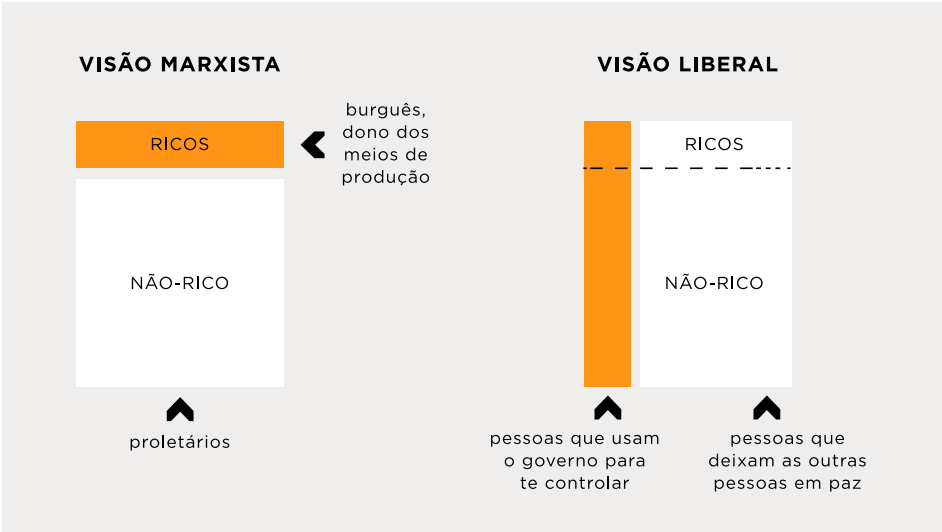
*Analisando essa cadeia hereditária, quero me livrar dessa situação precária. Onde o rico cada vez fica mais rico, e o pobre cada vez fica mais pobre. E o motivo todo mundo já conhece, é que o de cima sobe e o de baixo desce!*

**Xibom Bombom<sup>16</sup> – As Meninas**

Você também já deve ter escutado falar de Karl Marx, e ter uma noção geral da visão comunista<sup>17</sup> de mundo. Algo como “os meios de produção não podem ser de uma só pessoa (burguês) e sim de todos os trabalhadores (proletariado), assim o lucro é repartido por igual” em uma hipersimplificação. Esse pensamento é uma das diversas tentativas de se explicar o fenômeno de “o de cima sobe, e o de baixo desce”. Nele, existe uma luta de classes entre o “proletário” e o “burguês” e seus interesses sempre serão conflitantes.

O ponto de vista liberal (também chamado de liberalismo clássico<sup>18</sup>, bem diferente do “liberalismo” que existe no Brasil) difere do ponto de vista marxista. Em outra hipersimplificação, liberais tendem a enxergar a sociedade a partir de dois pilares centrais: I) liberdades individuais, direito à propriedade privada e economia baseada em livre iniciativa e livre mercado e II) o estado deve ter um papel pouco atuante na economia, pode redistribuir renda para as camadas menos favorecidas da população e deve incentivar certos padrões e normas sociais e culturais. O ponto de vista I

é mais unânime, enquanto que o II gera conflitos mesmo entre os liberais mais clássicos (vários liberais defendem que o estado não deveria intervir em nada na redistribuição de renda enquanto outros acreditam que o estado pode atuar onde a iniciativa privada não tem penetração para combater distorções do sistema, mas em uma forma mais semelhante a ONGs e não como competidor no livre mercado).



Exemplo esquemático das visões marxistas e liberais de mundo.

Tanto o comunismo como o liberalismo são duas correntes de pensamento consagradas e frequentemente usadas como forma de interpretar a sociedade. Também existem outras tentativas de explicar o fenômeno de “por que a sociedade é estratificada?” que não geraram correntes de pensamento próprias, mas que continuam interessantes como conceitos. Um desses conceitos é o Efeito Cantillon, que lida com o processo de geração de inflação relativa e como ele afeta em graus diferentes estratos sociais distintos.

O Efeito Cantillon

Richard Cantillon, um banqueiro e filósofo francês do século 18, reparou que o tempo que um indivíduo leva para ter acesso ao capital também está envolvido na estratificação da sociedade. Sua teoria básica é que quem se

beneficia mais da emissão de moedas (impressão de dinheiro, em linguagem coloquial) é quem está mais próximo da fonte de emissão da mesma. Ou, de uma maneira mais formal: a emissão de nova moeda tem efeito seletivo na inflação e quanto mais próximo o indivíduo/empresa estiver da emissão, menos efeito será sentido. E o resultado desta distribuição assimétrica é uma inflação também assimétrica.

Em sua época, isso significava que quem estava mais próximo do rei colhia mais benefícios e que quanto mais distante do rei, maiores os riscos de ruína. Em outras palavras: o dinheiro não é neutro e os amigos do rei sempre colhem vantagens de suas posições privilegiadas.

Em sua obra, Cantillon discute a forma com que o dinheiro flui pela sociedade. No seu estudo de caso, ele observa como o valor, que na sua época era extraído na forma de ouro em uma mina, flui pela sociedade. Basicamente, as pessoas ricas mais próximas da mina gastam o ouro com luxos e serviços, promovendo uma alta localizada nos preços. Este consumo faz o dinheiro circular na economia. Quando o dinheiro chega ao restante da população, ele chega acompanhado de um aumento de preços. Ou seja, efetivamente a população em geral não teve nenhum ganho de poder de compra, apesar de ter recebido mais dinheiro. Somente quem teve acesso no início da circulação desse ouro que colheu frutos reais.

Em outras palavras, quando dinheiro novo é colocado no sistema pelos Bancos Centrais, somente quem está “próximo do dinheiro” e recebe ele primeiro é realmente beneficiado. É o caso de grandes corporações e bancos, por exemplo, que conseguem empréstimos com taxas vantajosas e realizam investimentos. Esses investimentos fazem o dinheiro circular na economia, mas também geram aumento de preços, fazendo com que os outros membros da sociedade não colhem nenhum benefício real desse dinheiro novo colocado em circulação pelos Bancos Centrais. Ou em uma linguagem mais formal, o Efeito Cantillon pode ser descrito como a mudança relativa entre os preços causada pela mudança na base monetária. O resultado direto do Efeito Cantillon é uma redistribuição de riqueza e poder de compra do pobre para o rico, uma espécie de Robin Hood às avessas. Como a oferta monetária aumentou sem um aumento proporcional de produtividade na economia, o rico, mais próximo à fonte, viu seu poder de compra relativo aumentar às custas do pobre. Este teve seu poder de compra diluído, já que por possuir

poucos ou nenhum bem com preço atrelado à expansão da base monetária (e conseqüentemente, atrelado à inflação de ativos), como imóveis ou ações, viu o seu proverbial “pedaço da torta” diminuir.



Representação esquemática do Efeito Cantillon adaptando a imagem que mostra as diferentes visões de mundo (Marxista X Liberal) que circula pela internet com adaptação do Explica Bitcoin para ilustrar o Efeito Cantillon e os Cantillonários.

Quando os Bancos Centrais tornam o dinheiro mais acessível, isso não significa que a demanda por tudo irá subir ao mesmo tempo. Na realidade, a história mostra que certas classes de ativos são favorecidas em detrimento de outras, o que faz com que os preços subam em certas áreas enquanto em outras o preço cai.

Richard Cantillon descreveu este processo no século 18, quando a economia inteira ainda era lastreada no ouro e na prata. Isso significa que o efeito descrito por ele, apesar de já exacerbado, ainda era lastreado em algo físico, ou seja, no mundo real.

Mas o dinheiro mudou em 1971, quando o presidente americano Richard Nixon fez com que o dólar deixasse de ser lastreado em ouro. Um site (já citado anteriormente) que ilustra com diversos gráficos toda a magnitude que esta quebra de lastro trouxe para sociedade é o WTF Happened in 1971<sup>19</sup>, mas para os fins deste livro podemos dizer que quando o dinheiro deixou de estar vinculado à realidade o jogo mudou. Como? Em outra hipersimplificação:

basicamente o dinheiro começou a nascer em árvore. Ou seja, os EUA passaram a imprimir dinheiro sem lastro para comprar petróleo da Arabia Saudita, criando o sistema petro-dólar<sup>20</sup>. Ou, colocando de outra forma: os EUA entraram em acordo com a Arábia Saudita para que esta só aceitasse dólares em troca do petróleo. Após o fim do acordo de Bretton Woods, o lastro do dinheiro se tornou subjetivo e baseado na força da economia interna dos EUA: consumo, aumento do PIB e produção. Isso é um contra senso, visto que a definição de lastro não permitiria que algo subjetivo fosse usado para lastrear nada. Seria algo como: “eu posso ir ao banco tomar mais dívidas pois hoje meu cargo é melhor, meu salário é melhor e eles ainda irão aumentar conforme for promovido”.



Três notas de 10 dólares de anos diferentes. Note que a nota de cima é conversível por ouro (“Ten Dollars in gold coin payable to the bearer on demand” significa que essa nota de 10 dólares podia ser convertida em moeda de ouro) e que as outras duas não.

E como o Efeito Cantillon se manifesta no mundo atual? Ele não implica necessariamente que a criação de dinheiro sempre beneficiará os mais ricos, mas sim o fato de que como o dinheiro circula na sociedade importa. Não existe neutralidade no dinheiro e nem em sua circulação. Teoricamente, se os Bancos Centrais quisessem distribuir dinheiro diretamente para cada cidadão através de depósitos direto em wallets, não ocorreria o Efeito Cantillon, pois todos receberiam o dinheiro simultaneamente. O Efeito

Cantillon não diferencia aumento de preço entre ativos (como ações, fundos imobiliários, imóveis) e passivos (como alimentos, vestuário, lazer). Logo, se todos recebessem o dinheiro ao mesmo tempo, a primeira pessoa a usar ele teria um nível de preços  $X$ , e a segunda  $X+i$  (onde  $i$  é a inflação até este momento) e a terceira teria preços de  $X+i*n$  (onde  $n$  representa o aumento de preços em relação ao tempo), e assim por diante. O problema está na criação de nova renda sem vínculo à produção, o que gera um desequilíbrio natural na relação oferta x demanda. A impressão causaria inflação generalizada, seja na forma de inflação de consumo (representada pelo IPCA) ou na inflação de ativos, como vimos nos dois anos de pandemia (2020-2021).



Meme satirizando as políticas do FED de expansão da base monetária.

Em uma economia sem lastro a impressão tende ao infinito.

A partir da crise do Covid-19, estamos vendo uma impressão de dinheiro generalizada, processo carinhosamente apelidado pelos bitcoinheiros de “money printer go brrr” (algo como “a impressora tá on”). Este processo também é conhecido como expansão da base monetária e está diretamente relacionado com a inflação.

Se uma economia é lastreada na sua capacidade produtiva, aumentar a sua base monetária sem aumentar a sua capacidade produtiva é fazer dinheiro nascer em árvore, ou seja, é um dinheiro sem lastro no mundo concreto. Pareceu complicado né? Então vamos simplificar com um exemplo:

se o total de produtos e serviços da economia for cotado em cãezinhos e o seu país possuir 4 cãezinhos iguais e 10 dinheiros como base monetária, cada cãozinho vale 2.5 dinheiros. Se este país expandir a sua base monetária em mais 10 dinheiros (20 dinheiros no total) e não aumentar o número de cãezinhos, cada cãozinho passará a valer 5 dinheiros.

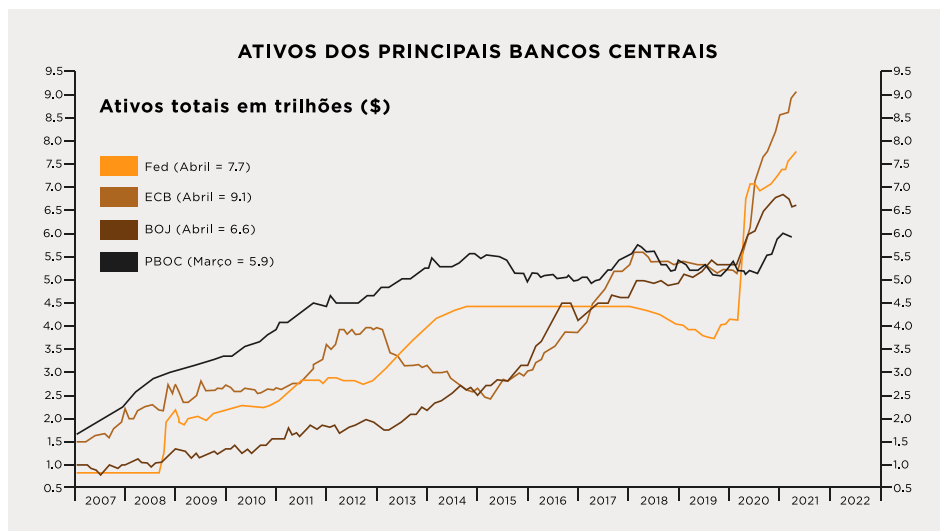
$$\frac{\$ 10}{\text{Imagem de 4 cãezinhos}} = 2.5 \text{ \$/cão}$$

$$\frac{\$ 20}{\text{Imagem de 4 cãezinhos}} = 5 \text{ \$/cão}$$

Nada como cãezinhos para o leitor não dormir.

Assim como no exemplo dos cãezinhos, o mundo está sofrendo um grande processo de expansão da sua base monetária. Essa expansão monetária gera inflação, assim como no exemplo o preço dos cãezinhos subiu. Da mesma forma, qualquer bem escasso tende a se valorizar conforme a base monetária é expandida, pois se o numerador (o número de cima na divisão) aumenta e o denominador (o número debaixo) se mantém constante, o resultado será sempre maior.

A imagem abaixo mostra o balanço dos principais Bancos Centrais mundiais (FED = EUA; ECD = União Européia, BOJ = Japão e PBOC = China). Em média, esses balanços triplicaram na última década. Ou seja, deveríamos ter multiplicado por três o numerador na década que passou e manter o denominador aproximadamente constante para acomodar esta expansão de base monetária. Isso implicaria em um grande aumento do preço dos cãezinhos e, no mundo real, implica em inflação generalizada em todos (ou quase todos) os aspectos da nossa vida.



Evolução da quantidade de ativos que os principais Bancos Centrais do mundo possuem nos seus balanços entre 2007 e 2021.

E como todo esse dinheiro não chega ao mesmo tempo para todos os indivíduos, esta impressão sem precedentes gera também um Efeito Cantillon sem precedentes.

### Efeito Cantillon e a recuperação em K

Desde o choque que o Covid-19 causou nos mercados em março de 2020, uma das principais discussões entre os economistas foi como seria a forma da recuperação. Seria uma recuperação em V, com uma queda rápida e uma recuperação igualmente rápida? Seria uma recuperação em Nike, com uma queda abrupta e uma recuperação mais lenta? Diversos tipos de recuperação foram discutidos ao longo de 2020.

A recuperação que foi observada foi denominada pelos especialistas como uma recuperação em K. Mas e o que uma recuperação em K significa?

Ela significa que existe uma acentuada divisão entre os vencedores e os perdedores, entre setores que apresentaram uma vigorosa recuperação e setores que enfrentaram grandes dificuldades.

Os especialistas que analisaram essa recuperação interpretam que os vencedores são as empresas com estrutura enxuta e margens altas, geralmente empresas do mundo digital. Estas empresas conseguiram migrar



para o trabalho remoto sem perda de eficiência e continuaram conseguindo entregar os produtos para seus clientes via internet.

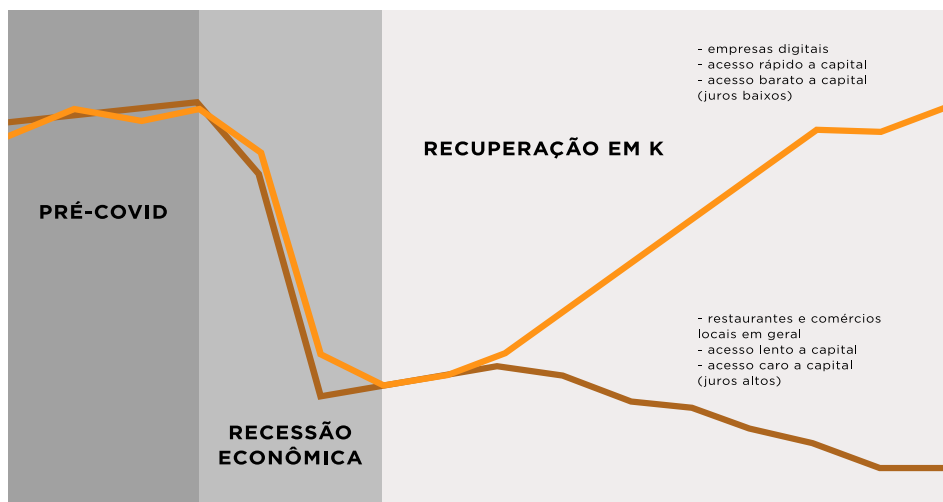
Já os perdedores são modelos de negócio da velha economia em que o funcionário precisa trabalhar presencialmente e o cliente também precisa consumir presencialmente. Ou seja, restaurantes, comércios locais, hotelaria e turismo de uma forma geral.

Basicamente, para os vencedores os negócios nunca estiveram melhores, enquanto que para os perdedores a situação foi e segue sendo desesperadora.

Essa é a narrativa padrão sobre a recuperação em K e explica porque as ações das empresas de tecnologia subiram significativamente entre 2020-2021, enquanto que as ações de empresas da velha economia não apresentaram os mesmos sinais de recuperação. As vantagens que as vencedoras possuem são consideráveis, mas não são as únicas vantagens competitivas dessas empresas. Essa recuperação em K também ilustra o Efeito Cantillon, já que essas empresas possuem acesso diferenciado ao capital, tanto na forma de juros mais baixos como na velocidade de obtenção de novo capital via empréstimo ou aporte de mais capital dos investidores que já investiram antes na empresa.

O Airbnb, por exemplo, conseguiu levantar cerca de \$2 bilhões<sup>21</sup> em 1 mês após a eclosão da pandemia de Covid no início de 2020. Ao mesmo tempo, todos os comerciantes, donos de restaurantes e outros trabalhadores da economia real eram obrigados a fechar suas portas e a ficar trancado em casa esperando o auxílio emergencial (que tanto nos EUA como no Brasil foram insuficientes para compensar o tempo de portas fechadas e ineficientes em sua distribuição).

Ou seja, além de todas as vantagens competitivas associadas aos diferentes modelos de negócio, as vencedoras geralmente também se beneficiam diretamente do Efeito Cantillon.



## PARTE 2 - A SOLUÇÃO

*Emancipate yourselves from mental slavery. None but ourselves can free our minds.*

*Emancipem-se da escravidão mental. Ninguém a não ser nós mesmos pode libertar as nossas mentes.*

**Redemption Song - Bob Marley**

## CAPÍTULO 3

# O QUE É O BITCOIN?

Essa é a pergunta que todos os iniciantes fazem: mas afinal de contas, o que é o bitcoin? Pode parecer uma pergunta simples, mas o oposto é verdade. Para entender o que é o bitcoin, diversos conceitos precisam ser amarrados em conjunto.

Como dito anteriormente, o bitcoin é a solução do problema do dinheiro estar na mão do estado, então, de maneira simplista: o bitcoin é uma forma de dinheiro. Mas as especificidades desse dinheiro são confusas para os iniciantes e o objetivo deste texto é tentar desfazer um pouco essa confusão.

O primeiro passo para desmistificar o bitcoin é definir melhor os termos, uma vez que existe a rede de computadores rodando o mesmo protocolo denominado como bitcoin e o ativo bitcoin, que circula nessa rede de computadores rodando o mesmo protocolo.

### **Diferenças entre a rede e o ativo**

Atualmente, a grafia adotada pela maioria dos bitcoinheiros separa o “Bitcoin” e o “bitcoin” para diferenciar entre a rede e a moeda.

Entretanto, o autor optou por seguir um padrão diferente, seguindo o autor dos livros “O Padrão Bitcoin” e “O Padrão Fiat”, Saifedean Ammous. O Saifedean prefere utilizar tudo como “bitcoin” por achar que a diferenciação

confunde mais do que ajuda na compreensão dos leitores. Ele também cita que, no início a internet, também recebia a grafia de “Internet” e que com o tempo essa grafia foi sendo trocada para “internet” no uso cotidiano das pessoas. Apesar de me causar estranheza escrever tudo com “b”, concordo racionalmente com os argumentos do Saifedean e adotei este padrão, referindo-me tanto ao protocolo como às moedas como bitcoin., levando os leitores a entenderem qual dos conceitos (rede ou ativo) está sendo abordado pelo contexto.

**Bitcoin** - o “B” é utilizado para se referir ao protocolo e a rede.

**bitcoin** - o “b” é utilizado para o ativo. Quando nos referimos ao ativo, o bitcoin pode ganhar o plural e ser os bitcoins.

Ou seja, existe a mineração de bitcoin. Os bitcoins minerados são transferidos de um usuário ao outro através da rede Bitcoin. Esses usuários podem fazer essas transações de maneira peer-to-peer pois rodam o Bitcoin em seus nodes.

Ok, com a nomenclatura esclarecida, é hora de entender as especificidades do dinheiro bitcoin. Para isso, o primeiro passo é entender a dificuldade de se criar confiança em sistemas descentralizados.

## **O Problema dos Generais Bizantinos**

O Problema dos Generais Bizantinos é um problema de teoria dos jogos, que descreve a dificuldade que entidades descentralizadas possuem para chegar a um consenso sem depender de um ponto central de confiança. Em uma rede onde nenhum membro pode verificar a identidade de outros membros, como os membros podem concordar coletivamente sobre uma certa verdade?

A analogia da teoria dos jogos por trás do chamado Problema dos Generais Bizantinos é a de que vários generais estão sitiando a cidade de Bizâncio. Eles cercaram a cidade, mas devem decidir coletivamente quando atacar. Se todos os generais atacarem ao mesmo tempo, eles vencerão e a cidade será tomada. Entretanto, se atacarem em momentos diferentes, a cidade conseguirá repelir os ataques e eles serão derrotados.

Os generais não têm canais de comunicação seguros uns com os outros porque quaisquer mensagens que enviarem e receberem podem ter sido interceptadas ou enganosamente enviadas pelos defensores de Bizâncio.

Como os generais podem se organizar para atacar ao mesmo tempo?

Apenas os sistemas descentralizados enfrentam o Problema dos Generais Bizantinos, uma vez que não possuem uma fonte confiável de informações e nenhuma forma de verificar as informações que recebem de outros membros da rede. Em sistemas centralizados, por outro lado, o problema não ocorre, visto que uma autoridade é confiável para publicar informações verdadeiras e evitar que informações falsas ou fraudulentas se espalhem pela rede.

Ou seja, o sistema financeiro tradicional não se faz necessário lidar com essa questão, pois nele existe a confiança nas instituições financeiras. E o bitcoin é a única solução já encontrada para esse problema de teoria dos jogos.

Pela primeira vez na história, a humanidade descobriu uma forma de se estabelecer confiança em um sistema descentralizado. Como? Utilizando 1) o mecanismo conhecido como prova de trabalho (proof of work, PoW) e 2) a Timechain (nome dado a blockchain do bitcoin especificamente).

O conjunto de regras do bitcoin é objetivo e não há discordância sobre quais blocos ou transações são válidos, permitindo que todos os membros concordem com uma única verdade.

## **A prova de trabalho e o gasto duplo**

A prova de trabalho é um protocolo utilizado para a prevenção de ataques que surgiu como tentativa de reduzir os spams. Neste tipo de protocolo, para que um usuário realize uma ação, este deve ser capaz de provar que realizou alguma tarefa, considerada como a prova de que o usuário gastou recursos para gerar uma resposta que satisfaça algum requisito do avaliador. Para esse sistema funcionar, porém, a criação da tal prova deve ser trabalhosa, enquanto sua verificação pelo avaliador deve ser simples e direta, como um quebra cabeças: difícil de ser montado e simples de ser verificado.

Para o protocolo de PoW funcionar, a tarefa deve ser difícil e trabalhosa, mas não impossível. Já a verificação dessa prova, por outro lado, deve ser muito rápida e simples de ser realizada, como no exemplo do quebra-cabeças ou como em uma cartela de bingo.

## Gasto duplo

Talvez você já tenha escutado que o bitcoin é a invenção da escassez digital. Mas o que isso significa? Em poucas palavras, significa que o bitcoin é o primeiro ativo digital que é resistente ao famoso “control + C → control + V”.

A capacidade de copiar e colar um arquivo digital, quando aplicado a formas digitais de moedas, é conhecida como gasto duplo. O gasto duplo acontece quando um usuário consegue gastar as mesmas moedas digitais mais de uma vez. Diferentemente de moedas físicas, arquivos digitais podem ser duplicados, logo, o ato de gastar uma moeda digital não implica uma transferência de posse de uma pessoa para a outra. Portanto, é necessário que outros meios sejam utilizados para prevenção contra o gasto duplo.

Como o bitcoin consegue evitar o gasto duplo? Pelo mesmo mecanismo que gera confiança nesse sistema monetário descentralizado, a prova de trabalho. Apenas um minerador pode validar as transações da rede. O mecanismo de prova de trabalho garante que o minerador troque energia por poder computacional, o que não pode ser falsificado. Para a prova de trabalho funcionar e evitar falsificações, ela precisa ser trabalhosa de ser executada e fácil de ser verificada.

## A criação do bitcoin: os primeiros cypherpunks e Satoshi Nakamoto

*“A privacidade é necessária para uma sociedade aberta na era eletrônica. Privacidade não é segredo. Um assunto privado é algo que não desejamos que o mundo inteiro saiba, mas um assunto secreto é algo que ninguém quer que ninguém saiba. Privacidade é o poder de se revelar seletivamente ao mundo.”*

**Eric Hughes, Manifesto Cypherpunk**

Apesar de parecer “novo”, a criação do bitcoin é fruto de mais de 30 anos de desenvolvimento de um grupo de pessoas que se interessavam por criptografia e privacidade, conhecidos como cypherpunks. Os cypherpunks surgiram em São Francisco e obtiveram alcance global quando passaram a se comunicar através de uma lista de e-mails ao invés de encontros presenciais.

O valor mais importante para os cypherpunks é a privacidade.

Embora o argumento de que “beleza, mas eu não sou um cypherpunk, não estou fazendo nada de errado. Eu não tenho nada a esconder” seja comum, este acaba estando completamente equivocado. Como é possível perceber, tal pensamento é baseado na premissa falsa de que a necessidade de privacidade significa querer esconder algo que está errado. Mas isso não é correto. Trata-se, entretanto, apenas do interesse de preservar a privacidade como ferramenta de defesa. Por exemplo, você provavelmente tem cortinas nas janelas para que as pessoas não possam ver dentro de sua casa. Não é porque alguém está conduzindo atividades ilegais ou imorais que possui cortinas nas janelas para que as pessoas não possam ver dentro de sua casa, mas simplesmente porque não deseja se preocupar com a possibilidade de outros estarem espionando.

Os cypherpunks produziram diversas invenções focadas em tentar resolver a questão da transmissão de valor com privacidade e sem a necessidade de um validador externo de confiança:

Em 1997, Adam Back criou o Hashcash, um mecanismo anti-spam que gerava um custo de tempo e poder computacional, portanto energia e dinheiro, para enviar um e-mail, tornando os spams economicamente inviáveis.

Em 2004, Hal Finney criou a prova de trabalho reutilizável (reusable proof of work, RPOW em inglês), baseado no Hashcash. RPOW eram tokens criptográficos que só podiam ser utilizados uma vez. A validação e proteção contra gastos duplos ainda era executada em um servidor central.

Em 2005, Nick Szabo publicou a proposta para o “bitgold”, um token digital baseado no RPOW. O bitgold não possuía um limite de tokens, mas imaginava que as unidades seriam precificadas de maneira diferente de acordo com a quantidade de processamento computacional utilizado na sua criação.

Em 2008, o pseudônimo Satoshi Nakamoto publicou o whitepaper do bitcoin, que cita diretamente tanto o bitgold como o Hashcash.

Portanto, o bitcoin pode ser entendido como uma máquina distribuída que automatiza a emissão de unidades monetárias escassas e a liquidação de transações financeiras através da conversão de energia em poder computacional. Devido a essa necessidade de poder computacional,



o que significa um custo, a prova de trabalho faz com que não sejam economicamente viáveis os ataques de hackers que buscam possibilitar os chamados "gastos duplos".

### Satoshi Nakamoto

Mas... quem foi Satoshi Nakamoto? Por mais surpreendente que seja, a verdade é que ninguém sabe. Existem várias hipóteses e esse é um dos temas que é discutido de tempos em tempos entre os bitcoinheiros. Mas a verdade é que, por mais que seja divertido esse exercício especulativo, a verdade é que não importa quem foi Satoshi Nakamoto.

E por que não importa?

Uma analogia interessante é a referente ao "grande filtro" do Paradoxo de Fermi, que basicamente questiona o porquê de nós não termos encontrado evidências de vida inteligente fora da Terra. Nesse contexto, o grande filtro seria uma possível solução desse paradoxo que postula que não encontramos vida inteligente fora da Terra pois existiria um filtro que não permitiria às civilizações evoluir além do estágio de viagens inter sistemas solares.

No contexto de um dinheiro descentralizado, o grande filtro é sobreviver aos ataques de governos. Se o propósito do bitcoin é separar o dinheiro do estado, nada mais natural que o estado lute contra e tente se defender. Então, caso o fundador do bitcoin fosse conhecido, ele e sua família seriam alvos de ataque e captura estatal.

Usando a expressão da comunidade, ninguém conhecer o Satoshi é uma feature, e não um bug. Ou seja, é de propósito que ninguém sabe quem foi Satoshi. Foi uma escolha consciente e necessária para a sobrevivência do projeto no longo prazo.

*"Muitas pessoas automaticamente descartam a moeda eletrônica como uma causa perdida por causa de todas as empresas que falharam desde a década de 1990. Espero que seja óbvio que foi apenas a natureza centralmente controlada desses sistemas que os condenou. Acho que esta é a primeira vez que estamos tentando um sistema descentralizado e não baseado em confiança."*

Satoshi Nakamoto<sup>22</sup>

## Hal Finney e os primeiros bitcoinheiros

Os cypherpunks estavam focados em construir um dinheiro digital anônimo por anos e construíram vários sistemas iniciais, todos sem sucesso. Até que, no dia 31 de outubro de 2008, Nakamoto apresentou o conceito do bitcoin na lista de email dos cypherpunks conhecida como The Cryptography Mailing List. O artigo original escrito por Satoshi é denominado "Bitcoin: Um Sistema de Dinheiro Eletrônico Peer-to-Peer" e possui apenas nove páginas.

Embora a ideia inicial do bitcoin tenha sido proposta pela primeira vez no final de 2008, foi somente em janeiro de 2009 que a rede bitcoin foi criada. Sendo mais específico, o Bloco Gênesis foi minerado no dia 03 de janeiro de 2009, às 18:15:05 UTC (Brasília é UTC-3).

O primeiro bitcoinheiro conhecido é Hal Finney, que, no início de janeiro, respondeu ao anúncio de Satoshi e, nas duas semanas seguintes, trabalhou com o fundador para depurar o sistema e fazê-lo funcionar sem bugs. Ele baixou a versão 0.1.0 - e ela travou, o que surpreendeu Satoshi, que estava testando o sistema e não teve nenhum travamento. Hal Finney e Satoshi Nakamoto também testaram as versões 0.1.2 e 0.1.3 do bitcoin. Houve mais travamentos, mais depuração, mais reescrita e reformulação do código repetidamente.



Primeira citação ao bitcoin no Twitter, em tweet do Hal Finney no dia 11 de janeiro de 2009<sup>23</sup>.

Hal Finney se tornou a primeira pessoa a executar o software bitcoin e o primeiro a receber uma transferência de bitcoin quando, em janeiro de 2009, recebeu 10 bitcoins como recompensa pela mineração do bloco 70. Outro fato interessante sobre o Hal Finney é que ele foi um dos primeiros

indivíduos a fazer uma previsão de preço do bitcoin. Ele estimou, em um e-mail para Satoshi em 2009, que extrapolou a riqueza total das famílias em todo o mundo - considerando algo em torno de US \$ 100-300 trilhões - com a oferta de 21 milhões de bitcoin, o que significa que cada moeda teria um valor potencial de US \$ 10 milhões.

A primeira transação utilizando bitcoin ocorreu no dia 22 de maio de 2010, data que agora é conhecida como Bitcoin Pizza Day e é comemorada pela comunidade. A transação ocorreu quando Laszlo Hanyecs concordou em pagar 10.000 bitcoins por duas pizzas da pizzeria Papa John's. Outro marco relevante ocorreu no dia 9 de fevereiro de 2011, quando o preço do bitcoin atingiu US\$ 1 pela primeira vez.

Ou seja, o bitcoin não nasceu como dinheiro. No sentido mais literal, o bitcoin é um programa de computador que é executado simultaneamente por milhões de pessoas ao redor do mundo. Esse programa de computador funciona utilizando tokens (as moedas bitcoin), que estão sendo monetizados desde a primeira transação. Com isso, o programa de computador passou a ser dinheiro.

### **O desaparecimento de Satoshi**

Satoshi continuou a contribuir com o lançamento do protocolo, em conjunto com outros desenvolvedores, até meados de 2010, quando o contato com a comunidade começou a gradualmente diminuir. Foi nessa época que ele entregou o controle do repositório de código fonte e funções-chave de alerta do software para Gavin Andresen, um desenvolvedor que estava envolvido na comunidade e havia conquistado a confiança de Satoshi. Ele também entregou o controle do domínio bitcoin.org e vários outros domínios para membros com reputação na comunidade do bitcoin.

As estimativas mostram que os endereços relacionados a Satoshi Nakamoto possuem uma fortuna de aproximadamente um milhão de bitcoins. O fato dessas moedas nunca terem sido movimentadas leva os bitcoinheiros a chamar a criação do bitcoin como uma concepção imaculada. Isto é, não existe um criador que lucrou com a criação do bitcoin, diferentemente de todas as outras criptomoedas.

## Adoção pelo culto de fanáticos

Com o tempo, o bitcoin caiu no gosto de um grupo de nerds que amam tecnologia e foi se tornando cada vez mais alvo de interesse e pesquisa. Um dos primeiros locais em que ele foi debatido foi no Reddit, mais especificamente no r/Bitcoin. Desde essa época, o protocolo já era conhecido como “magic internet money” (ou “dinheiro mágico da internet”). A capa utilizada por esse fórum do Reddit brinca com essa definição inclusive.

A bela imagem do mago do dinheiro mágico da internet (abaixo) foi submetida pelo usuário /u/mavensbot. A influência que esse desenho tosco teve era impossível de ser imaginada na época. O desenho simplista feito no programa Paint chamou a atenção dos usuários do Reddit que visitavam a primeira página da internet e despertou sua curiosidade. O tráfego para a página do subreddit cresceu exponencialmente e deu bastante exposição ao bitcoin, tanto que nessa época o desenho tosco foi até mesmo referenciado pelo desenho South Park nos capítulos que fazem referência a série Guerra dos Tronos. Essa cultura memética associada ao bitcoin é mal interpretada pelos outsiders, que não entendem a cultura da internet em geral e do bitcoin em específico e preferem chamar os bitcoinheiros de “culto de fanáticos” ao invés de estudar e tentar entender o ecossistema.



## E a tal mineração de bitcoin?

O primeiro passo para explicar a mineração de bitcoin é entender para que ela serve. O principal objetivo da rede bitcoin é permitir que transações sejam efetuadas sem a necessidade de uma terceira entidade de confiança (um banco, empresa, governo, etc), o que torna a rede incensurável. É justamente a estrutura da mineração, baseada em prova de trabalho, que

permite que isso seja possível. Basicamente, a mineração de bitcoin serve para validar as transações sem a necessidade desse terceiro de confiança, bem como para garantir que a emissão de novos bitcoins ocorra de maneira justa. Como? É justamente isso que esta seção te explicará.

A mineração do bitcoin é um processo complexo que possui linguagem técnica. Neste texto, eu vou tentar simplificar o máximo possível, tentando não reduzir demais a ponto de descaracterizar o que é a mineração. Mas, como este texto não é técnico, o objetivo desta seção é dar uma visão geral, sem entrar nos detalhes de como a mineração do bitcoin funciona.

Da mesma forma, vale ressaltar que, quando alguém quer aprender a dirigir, essa pessoa não precisa aprender como funciona um motor a combustão, praticamente nenhum usuário de dinheiro fiduciário (governamental) entende como funciona realmente o sistema financeiro atual. Ou seja, não é necessário compreender a parte técnica do bitcoin para conseguir utilizá-lo com sucesso, da mesma forma que não é necessário entender a equação química da combustão para saber dirigir um carro.

Então, começando de uma forma simples, se a mineração de bitcoin pudesse ser reduzida a uma fórmula matemática, ela seria:

$$\text{energia} + \text{poder computacional} = \text{bitcoins}$$

Mas, diferente do que ocorre com outras commodities, onde quanto mais energia colocada na equação, mais commodity é produzida, mais energia não significa que mais bitcoins serão emitidos. No caso do bitcoin, mais energia significa que mais poder computacional está protegendo a rede.

A taxa de emissão de bitcoins é constante e predeterminada, ou seja, não é afetada pela quantidade de energia adicionada à rede. A variação de poder computacional supostamente poderia acelerar a emissão de bitcoins, caso não existisse o ajuste de dificuldade, que controla a dificuldade da mineração. Quando mais poder computacional é aplicado na rede, a dificuldade aumenta, para manter a emissão de blocos de transação estável, sendo estes produzidos a cada 10 minutos, aproximadamente.

Também é o ajuste de dificuldade que permite que a rede se readapte quando atacada, como foi o caso da "grande migração chinesa de hashrate"

de 2021, quando a China banizou a indústria de mineração de bitcoin do país e cerca de 50% da hashrate do bitcoin foi desligada de uma hora para a outra. Mesmo perdendo 50% da sua capacidade computacional, graças ao mecanismo de ajuste de dificuldade, a rede bitcoin se ajustou e em pouco tempo já estava funcionando normalmente, emitindo um novo bloco a cada 10 minutos em média.

A emissão de bitcoins é constante e ocorre como remuneração para cada bloco minerado. Essa emissão não pode variar por ser controlada pelo código. A cada quatro anos, a quantidade de bitcoins minerados por bloco é reduzida pela metade, evento este conhecido como halving. Em outros termos, a cada 4 anos, a remuneração que o minerador recebe a cada bloco minerado cai pela metade. Inicialmente, a remuneração era de 50 bitcoins, que depois caiu para 25, 12.5 e hoje se encontra em 6.25 bitcoins por bloco minerado.

Os equipamentos de mineração de bitcoin são móveis, e os mineradores os alocam onde energia barata está disponível. Estes equipamentos consomem energia tentando adivinhar a solução de uma equação, o que significa que mais energia utilizada aumenta a chance probabilística de um determinado minerador encontrar a solução correta. O minerador que encontra a solução descobre um novo bloco, ganhando as taxas de transação e taxa de subsídio do bloco como recompensa.

Vale mencionar que o termo mineração é emprestado do ouro. Isto porque, para a produção do ouro, é preciso muito trabalho para sua descoberta e extração de dentro da terra. Milhares de dólares são investidos em pesquisa e equipamentos para ser possível sua extração de forma eficiente. O ouro é escasso e difícil de ser produzido. De maneira análoga, a mineração de bitcoins pode ser vista como uma versão digital desse processo, onde mais energia empregada resulta em maior probabilidade de sucesso na obtenção da commodity.

Para entender como funciona a mineração do bitcoin e o porquê do seu uso de energia não ser um problema, é necessário entender o conceito de proof of work (prova de trabalho) aplicado à mineração de bitcoin.

## **A prova de trabalho no bitcoin**

Sistemas descentralizados não possuem um único ponto de

confiança. A grande inovação do Satoshi foi conseguir construir um sistema que permite a todos os seus participantes verificar a veracidade de um fato de maneira independente. E o que permite isso é justamente o protocolo de proof of work (prova de trabalho). O objetivo da prova de trabalho é criar um registro irrefutável. Se dois registros competirem entre si, no caso de uma tentativa de gasto duplo, por exemplo, é o registro com mais trabalho embutido nele que é o verdadeiro, por definição, o que é conhecido como Consenso de Nakamoto<sup>24</sup>.

O protocolo de proof of work tem duas principais funções: ele permite validar as transações sem uma entidade intermediária atuando no processo, o que é conhecido como “sem um terceiro de confiança”, além de permitir que novas moedas sejam emitidas de maneira justa, sem favorecimento aos “amigos do rei”.

**Validação de transações** - essa definição de “mais trabalho = verdade” funciona justamente porque trabalho requer energia. O trabalho executado é algo que você não consegue mentir, discutir ou fingir. A prova de que você fez o seu trabalho é auto-evidente no resultado do seu trabalho. Trazendo para o cotidiano, podemos dizer que qualquer mérito físico é prova de trabalho. Por exemplo: é auto-evidente que tanto o escalador que consegue realizar subidas sem corda como a bailarina dançando o Lago dos Cisnes realizaram muito trabalho para chegar neste nível técnico. Este trabalho também é auto-evidente nos resultados físicos, como nas mãos dos escaladores e nos pés das bailarinas. A matéria da faculdade que você estudou sozinho, fez a prova sem colar e passou, também é prova de trabalho, assim como um quarto limpo e organizado.



O alto desempenho físico, bem como seus efeitos no corpo, são provas de trabalho irrefutáveis.

No bitcoin, trabalho significa poder computacional (hashrate) das máquinas usadas na mineração. E não é qualquer tipo de computação que o bitcoin usa, mas sim um tipo de computação muito específico que impede qualquer forma de atalho ou nova descoberta que melhore a eficiência dos processos: a adivinhação. Isso acontece porque em um processo de adivinhação, os resultados são probabilísticos, o que significa que o minerador que quiser ter uma probabilidade maior de adivinhar a solução do bloco precisa executar mais trabalho (leia-se, utilizar mais energia).

A prova de trabalho é a ponte entre o universo da informação digital e o mundo físico. A computação precisa de energia e existe a relação direta de + energia = + hashrate = + chance probabilística de minerar o bloco e ganhar a recompensa do bloco. A mineração de bitcoins via prova de trabalho foi a forma idealizada por Satoshi Nakamoto para garantir a segurança da rede. Na prática, a mineração de bitcoin é uma competição para resolver problemas matemáticos, onde o ganhador tem a habilidade de escrever no livro contábil do bitcoin. As transações são registradas publicamente nos blocos, que são encadeados entre si formando a sequência de blocos conhecida como timechain (a blockchain do bitcoin em específico é conhecida como timechain). E, como registrar essas transações nos blocos demanda altas quantidades de eletricidade, tentativas de golpe são desincentivadas porque demandariam muito capital e acesso às máquinas de mineração.



**Distribuição de moedas** - uma das principais questões relacionadas aos criptoativos de maneira geral é como ocorreu a distribuição dos tokens inicialmente. Você poderia reivindicar a maioria dos tokens para si mesmo ou então enviar eles para amigos e parentes, mas isso só recriaria o sistema atual em que algumas elites são privilegiadas em detrimento do resto da população, comprometendo a credibilidade do sistema. No mundo dos criptoativos, existem diversas moedas que possuem tokens pré-minerados, ou seja, tokens que foram distribuídos pelos seus criadores para si mesmo ou para seus amigos.

Mas então, como distribuir esses tokens de uma maneira justa? Sem que uma elite de amigos do rei seja criada como consequência da criação dessa nova moeda? A solução utilizada por Satoshi para o bitcoin foi distribuir as moedas criando um jogo de adivinhação aleatório entre os mineradores, onde estes são obrigados a entregar algo valioso (a energia) em troca do direito de reivindicá-las. Ou seja, quanto mais energia os mineradores utilizarem, maior a chance deles adivinharem a resposta nesse jogo de adivinhação aleatório e maior a chance deles receberem bitcoins pela energia aplicada.

Satoshi não tinha outra maneira de conseguir emitir unidades de valor digital para o mundo físico de maneira justa e descentralizada. Por se tratar de um sorteio, todos aqueles dispostos a contribuir à proteção da rede têm iguais chances de competir pela recompensa dos blocos, o que evita que os “amigos do rei” tenham vantagens em relação aos demais participantes. A prova de trabalho garante que as chances de um minerador são proporcionais à quantidade de eletricidade que ele utilizou, mantendo justa a distribuição das novas moedas emitidas. Além disso, o minerador, quando valida uma transação, recebe as taxas pagas pelos usuários.

## **Mas afinal, que raios é minerar um bloco?**

Como a mineração de bitcoin é um assunto complexo, eu perguntei para o meu amigo @nor\_b3rt se poderia adicionar seu texto sobre a mineração de bitcoin para complementar essa seção. A visão dele é mais técnica e descritiva que a minha, e o processo de mineração é descrito numa visão complementar.

Com a palavra, Norbert:

Para explicar o que ocorre na mineração, preciso explicar brevemente alguns conceitos envolvidos, mas prometo ser bem breve em cada um deles.

## **Mineradores**

No início do bitcoin, qualquer um com um computador e uma conexão à internet poderia minerar bitcoin. Atualmente, devido aos custos energéticos e à grande concorrência pela mineração, essa atividade demanda um tipo de computador específico (ASIC), construído desde o projeto somente para esta finalidade. Um computador pessoal é bastante generalista, precisa resolver diversos tipos de atividades. Uma máquina mineradora de bitcoin não faz nada além de processar os cálculos que você conhecerá a seguir.

## **Pools de mineração**

Hoje em dia, as pessoas que querem ganhar dinheiro minerando blocos precisam adquirir uma ou mais destas máquinas dedicadas. Estas máquinas não são baratas (as mais modernas custam mais de R\$ 20 mil cada). Com isso, minerar um bloco com poucas máquinas dedicadas seria economicamente ruim, demandaria muito tempo e muita energia para obter êxito. A probabilidade de encontrar um bloco atuando assim é como tentar encontrar uma pepita de ouro no seu próprio quintal. O melhor seria você ingressar em um pool de mineração. Mas o que são pools?

Um pool é uma associação de várias máquinas de mineração que podem estar em qualquer lugar do mundo. O pool coordena a mineração entre todas essas máquinas e soma o poder de processamento de cada uma ao conjunto. As chances de um pool conseguir minerar um bloco são bem maiores. Cada participante do pool será remunerado na proporção do poder de processamento que agrega ao conjunto.

## **Algoritmo SHA-256**

Antes de chegar na mineração de um bloco em si, eu preciso explicar basicamente o que é o tal algoritmo SHA-256, utilizado no processo de mineração. A sigla SHA vem de Secure Hash Algorithm (Algoritmos de Hash Seguro).

Um algoritmo é meramente uma sequência determinada de passos. Uma receita de bolo é um algoritmo. Execute os passos na mesma ordem e você sempre terá o mesmo bolo.

Pense no SHA-256 como uma caixa preta. Entra qualquer coisa de um lado (um número, um texto ou até um arquivo) e do outro lado sai um valor, o resultado: o tal hash. Existem diversas implementações de cálculos de hash, sendo o SHA-256 uma delas.

Ok, não é bem uma caixa preta. O cálculo é bastante complexo<sup>25</sup> e não convém explicar aqui, mas a implementação é pública, existem diversas bibliotecas de código aberto implementando o SHA-256.

No caso do SHA-256, sempre teremos um resultado cujo valor pode ser representado em 64 caracteres, não importando o tamanho da entrada. Um mero caractere ou um arquivo de 10 GB produzem valores diferentes, mas todos os hashes sempre serão alguma coisa semelhante a isto:

**e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855**

Uma característica fundamental do cálculo de um hash é que trata-se de um cálculo de mão única. Qualquer informação pode ter seu hash calculado, mas é impossível fazer o caminho inverso: extrair qual informação gerou um determinado hash. Se eu não disser aqui no texto o que produziu tal hash, você jamais saberia.

Outra característica do sha-256 é o “efeito avalanche”. Um mísero caractere diferente provoca um hash completamente diferente. A letra “a” (minúscula) gera o seguinte hash:

**ca978112ca1bbdcafacc231b39a23dc4da786eff8147c4e72b9807785afee48bb**

Já a letra “A” (maiúscula) produz um hash completamente diferente:

**559aead08264d5795d3909718cdd05abd49572e84fe55590eef31a88a08fdffd**

Don’t trust, verify: teste você mesmo. Há diversas ferramentas para calcular o hash SHA-256 de qualquer coisa, sejam bibliotecas prontas nas linguagens de programação, sejam sites com as referências 26 e 27.

Veja se eu estou te enganando com os valores citados acima!

## Transações

Resumindo grosseiramente, uma transação bitcoin é o envio de uma quantia do endereço A para o endereço B. Além disso, há também uma quantia paga aos mineradores. O minerador fica com as taxas das transações que ele conseguir colocar dentro de um bloco.

A taxa a ser paga é variável. Quem tem urgência na confirmação de suas transações paga uma taxa mais alta. Quem não tem pressa paga as taxas mais baixas e sua transação pode levar horas ou até dias para ser confirmada dependendo da quantidade de transações pendentes na rede.

As transações que foram criadas e propagadas recentemente pela rede ficam aguardando serem validadas, no que chamamos de mempool.

## Os blocos

Entenda um bloco como um conjunto de transações (limitados a aproximadamente 1 MB de informação) e um cabeçalho (ou header), com metadados (informações referentes ao bloco em si).

Cada novo bloco minerado é adicionado à cadeia de blocos existentes.

Esta cadeia de blocos por sua vez está armazenada em cada um dos milhares de nós validadores espalhados pelo mundo. Um nó de validação nada mais é do que um software que qualquer pessoa pode baixar e rodar por conta própria para colaborar com a rede. O nó validador é o elemento da rede bitcoin que confere o quebra-cabeças montado. Refaz o cálculo do minerador já com o nonce descoberto e valida o hash obtido. Este processo, diferentemente da mineração, requer muito pouca energia para ser realizado.

Dentre todas as informações contidas no bloco, vamos nos concentrar nas mais básicas para a compreensão da mineração:

- 1 - Timestamp (o instante em que o bloco está sendo minerado com precisão de segundos)
- 2 - Lista das transações que o minerador colocou no bloco, limitada a 1 MB de dados\*

\*Originalmente, o fork SegWit implementou um bloco adicional de 3MB para este tipo de transação, totalizando um tamanho máximo teórico de 4MB (na prática poderia chegar a uns 2.5MB). Basta abrir o mempool.space para acompanhar o tamanho dos blocos minerados e atualmente quase todos excedem 1MB.

3 - Hash do bloco anterior

4 - Nonce (explico em breve)

Pelo fato do bloco conter o hash do bloco minerado anteriormente cria-se uma trava de segurança perfeita. Se fosse possível alterar qualquer bloco já minerado, haveria uma quebra do hash de todos os blocos subsequentes. É isso que traz a confiabilidade da blockchain.

A principal qualidade da blockchain é que só existe um único caminho possível na sequência dos blocos, saindo do bloco atual e indo até o bloco gênese (o primeiro bloco minerado). Assim, todos os participantes (nós e mineradores) concordam com a ordem das transações.

## Halvings

O mecanismo de halving é a política monetária do bitcoin. Ele controla a velocidade da expansão da base monetária, a inflação do bitcoin. A cada 210.000 blocos, a recompensa recebida a cada bloco minerado cai pela metade (daí o termo halving). Os primeiros 210.000 blocos pagavam 50 BTCs, os 210.000 seguintes pagavam 25 BTCs e assim por diante, até o momento em que todos os quase 21 milhões de bitcoins terão sido minerados.

## Mineração

Chegamos, finalmente. A blockchain, timechain ou livro-razão é onde todas as transações ficam registradas, desde a primeira, em 03/01/2009, até hoje. Ela é composta pela sequência dos blocos, na ordem em que foram minerados.

O processo consiste em criar o próximo bloco a ser adicionado à blockchain. O minerador que conseguir incluir o próximo bloco recebe a quantidade de bitcoins determinada pelo ciclo de halvings, acrescida de todas as taxas das transações incluídas no bloco.

O software de mineração irá selecionar a maior quantidade possível de transações que cabem dentro de um bloco, priorizando aquelas que possuem as maiores taxas.

Junto dessa lista de transações, o software precisa juntar todas as informações no bloco e calcular o hash obtido utilizando, entre outros elementos, o hash do bloco anterior e o timestamp.

Até aí, pode aparecer qualquer hash, correto? Agora as coisas

começam a esquentar (literalmente).

### **Dificuldade da mineração**

Para o bloco ser considerado como válido, é necessário que o hash obtido tenha um valor inferior ao definido pela dificuldade vigente na rede.

Vamos colocar uma regra arbitrária para fins didáticos. Só iremos aceitar blocos cujo hash calculado se inicie por "00". O minerador precisa comprovar que, por tentativa e erro, conseguiu encontrar um hash que atenda a dificuldade vigente. É desta forma que exigimos uma prova de trabalho.

Esta é uma das regras vigentes na rede cujos nós de validação (nodes) irão verificar quando receberem um novo bloco. Caso o hash do bloco propagado por um minerador seja superior à dificuldade programada, o bloco é rejeitado por todos eles.

Para termos uma ideia do poder de processamento da rede bitcoin, vamos comparar o poder de processamento de uma CPU moderna de um computador pessoal com uma máquina de mineração dedicada:

Hoje em dia, uma CPU para desktop consegue calcular algo próximo de 15.000.000 hashes por segundo, ou então 15MH/s (megahashes).

Uma única máquina de mineração dedicada, como a Antminer S19 consegue calcular 110.000.000.000.000 hashes por segundo, ou então 110TH/s (terahashes). 7,3 milhões de vezes mais rápida que uma CPU de desktop comum.

Todas as máquinas mineradoras somadas na rede bitcoin atualmente calculam aproximadamente 195.339.327.381.705.800.000 hashes por segundo, ou então 195EH/s (exahashes).

Ou seja, a rede tem um poder de processamento equivalente a 13 trilhões de CPUs comuns.

Todo este poder computacional prova que a rede é segura. Para atacar efetivamente a rede bitcoin, gerando qualquer tipo de impacto, seria necessário controlar mais da metade dessas máquinas mineradoras ao mesmo tempo. A quantidade de equipamentos, energia e dinheiro necessário para executar tal ataque inviabiliza o mesmo (fica muito caro e inviável). Pela teoria dos jogos, faz muito mais sentido se juntar à rede e receber suas recompensas em bitcoin do que atacar a rede.

## Ajuste na dificuldade

A rede bitcoin foi projetada para que um novo bloco seja minerado a cada 10 minutos. A cada 2016 blocos minerados, a dificuldade é ajustada, seja para aumentar a dificuldade (um aumento de computadores na rede está fazendo novos blocos serem calculados mais rapidamente), seja para reduzi-la (queda na quantidade de mineradores, um país que bane a mineração, blackouts etc).

O incremento ou decremento na dificuldade é realizado na proporção calculada para que a média de intervalo entre os blocos fique sempre em 10 minutos. Isso é fantástico, pois torna a mineração do bitcoin constante. Pense no ouro. Se o preço disparar no mercado, haverá um incentivo para que a mineração de ouro aumente no mundo. Consequentemente, a oferta de ouro aumentará numa velocidade maior, ajustando também o seu preço. Já o bitcoin possui uma oferta inelástica: O aumento no número de mineradores não interfere na velocidade da criação de novos bitcoins devido ao ajuste.

## Nonce

Se o minerador precisa encontrar um hash que atenda a dificuldade desejada, o que ele pode fazer para calcular novos hashes uma vez que ele não pode fazer nada além de juntar as transações, o hash do bloco anterior e o timestamp? Aí que entra o nonce.

Nonce vem de “number used only once”. É um número inteiro que pode ir de 0 até aproximadamente 4 bilhões.

O nonce é o valor que minerador precisa descobrir para produzir um hash iniciado em “00” no nosso exemplo. O processo se dá por força bruta, tentativa e erro. É isso que irá demandar energia e todo o poder de processamento dos processadores das ASICs, assim como está fritando seu cérebro agora.

Então, ao iniciar o cálculo, o nonce vale 0:

1 - Calcula o hash do bloco

2 - Hash calculado atende a dificuldade? Se sim, sucesso, propaga o bloco e ganha a recompensa. Caso contrário, incrementa o nonce em 1 e tenta de novo.

Então é isso? Não, tem mais!

O nonce pode ir de 0 ao valor máximo 4.294.967.296 sem que se

obtenha um hash válido de acordo com a dificuldade. Isso mesmo, não é nada fácil. O que fazer então?

Notou que um dos fatores do cálculo é o timestamp? Notou também que o timestamp possui uma precisão de segundos? A capacidade de processamento atual da rede é tão absurda que os valores do nonce são esgotados em menos de 1 segundo. Sim, você leu direito, é rápido mesmo. Aguardar o próximo segundo seria um grande desperdício.

O software minerador pode efetuar diversas alterações no bloco que está tentando minerar, como por exemplo trocar alguma das transações, ele pode descartar uma delas e utilizar outra, reiniciando o nonce em 0 e tentando descobri-lo novamente.

Assim que algum dos mineradores consegue encontrar um nonce que produza um hash válido para o bloco que está sendo minerado no momento (bingo!), ele propaga o bloco encontrado na rede. Todos os mineradores, ao receberem as informações do novo bloco e a mempool atualizada, partem então para a mineração do próximo bloco.

À medida que a dificuldade de mineração foi aumentando com o ingresso de mais mineradores, criou-se um outro atributo, o extra nonce. É um outro valor que pode ser ajustado da mesma forma que o nonce citado acima, na tentativa de produzir um hash válido.

Veja um exemplo prático e divirta-se com a ferramenta na referência 28.



## CAPÍTULO 4

# A DESCOBERTA DO BITCOIN

Uma conversa recorrente na comunidade dos bitcoinheiros é a pergunta: “O bitcoin foi inventado ou descoberto?”. Inicialmente essa pergunta parece simples. Obviamente o bitcoin foi inventado, não?

Não. Na minha opinião, o bitcoin, assim como as outras “invenções” científicas e tecnológicas, foi descoberto e não inventado.

O objetivo deste texto é te explicar as premissas dessa visão e te ajudar a entender porque, caso Satoshi não tivesse existido, o bitcoin teria sido descoberto por qualquer outra pessoa.

### O Possível Adjacente

Existe uma figura no nosso inconsciente coletivo que é o gênio solitário na sua garagem. Esse cientista brilhante e incompreendido está desvendando algum grande mistério da natureza sozinho.

Essa imagem é totalmente equivocada. Mesmo gênios como Isaac Newton reconhecem que “se eu vi mais longe, foi por estar sobre ombros de gigantes” e não é à toa que esta é a citação escolhida na página inicial do Google Acadêmico. A ciência, e o conhecimento como um todo, não é um esforço individual, mas sim coletivo.

Esse conceito inicialmente parece contraintuitivo, mas as evidências históricas comprovam esta visão. Existem diversas descobertas científicas,

como o Cálculo e a Teoria da Seleção Natural, que ocorreram repetidamente de maneira independente.

A Teoria da Seleção Natural é corretamente atribuída a Charles Darwin. Sua história é bem conhecida: a volta ao mundo no Beagle, o estudo dos tentilhões nas Ilhas Galápagos, o terremoto no Chile e assim por diante. O que pouca gente sabe é que hoje em dia a Teoria da Seleção Natural é conhecida como teoria de autoria de Darwin-Wallace.

Isso porque Darwin demorou mais de 20 anos para publicar sua descoberta, e nesse meio tempo um jovem naturalista chamado Alfred Russell Wallace chegou às mesmas conclusões que Darwin havia chegado ao estudar a floresta amazônica e o Arquipélago Malaio<sup>29</sup>. Será que foi pura coincidência os dois raios terem caído no mesmo lugar?

Não, não foi mero acaso. Na realidade, esses dois brilhantes cientistas possuíam acesso às mesmas referências. Ambos citam o trabalho de James Hutton e de Charles Lyell, dois geólogos que discutiam como as mudanças topográficas ocorriam gradualmente ao longo de um grande espaço de tempo, conhecido como tempo geológico ou tempo profundo. Essa visão é conhecida como Uniformitarismo e se opõe ao Catastrofismo, que na época era associado ao Dilúvio e à ideia de que a idade da Terra era de apenas 10 mil anos. Graças a esses autores, o conceito de tempo profundo começou a existir na comunidade científica. Tanto Darwin como Wallace leram esses trabalhos.

O mesmo vale para o trabalho de Thomas R. Malthus. Malthus discutiu a questão de recursos finitos e chegou a esboçar ideias de “luta pela vida” e “sobrevivência dos mais aptos”. Mas ele focou seu trabalho na geografia populacional, não na natureza de uma maneira mais ampla. Tanto Darwin como Wallace citam o trabalho de Malthus como peça chave no quebra-cabeça da evolução.

A descoberta do Cálculo por Newton e Leibniz também ocorreu de maneira independente. Os dois matemáticos passaram o resto da vida brigando<sup>30</sup> para estabelecer quem havia sido o real inventor do Cálculo ao invés de supor que ele poderia ter sido desenvolvido duas vezes em um curto espaço de tempo.

O termo “possível adjacente” foi cunhado em 1996 por Stuart Kauffman, um biólogo evolutivo. Para ele, sistemas biológicos são capazes de

se transformar em sistemas complexos a partir de mudanças incrementais. Isso ajuda a explicar como sistemas complexos tem origem: um passo de cada vez.

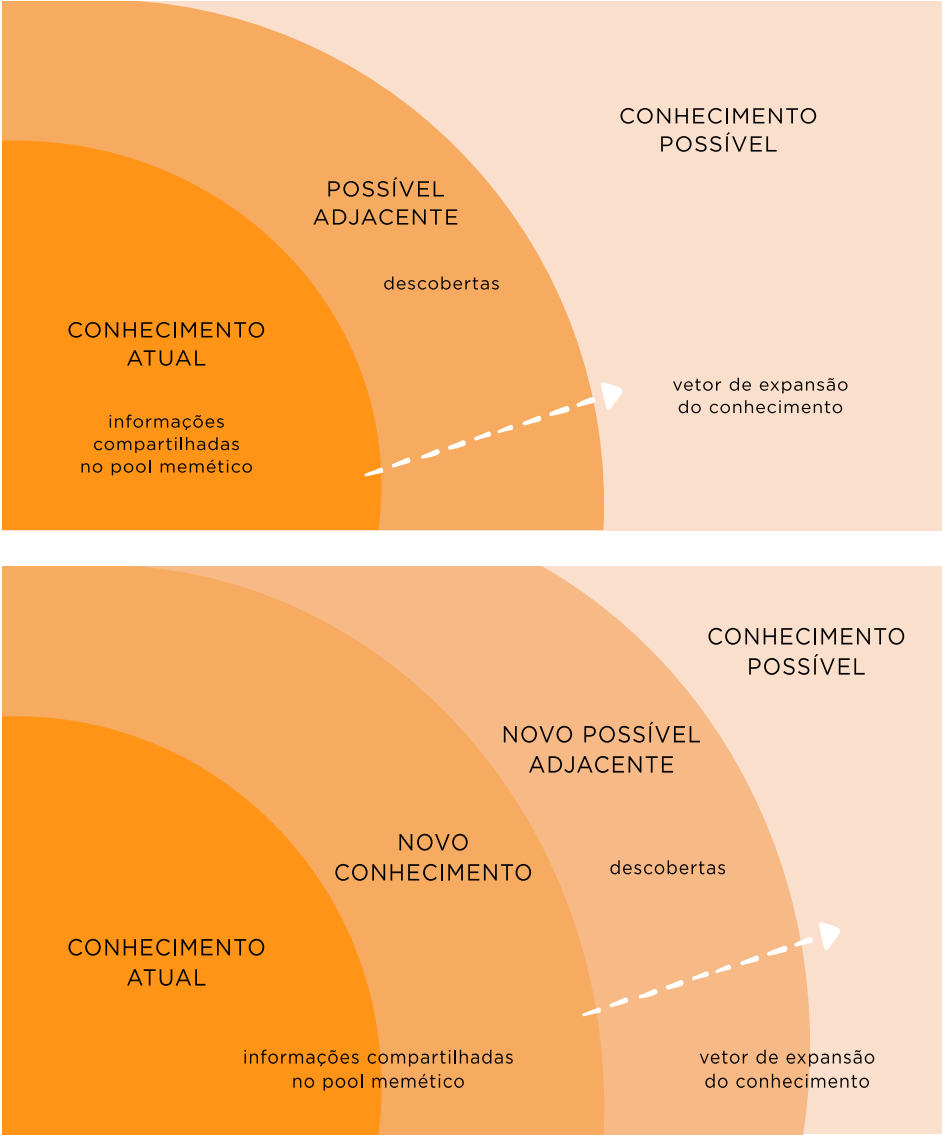
Exemplificando: a origem da vida ocorreu em um ambiente primitivo conhecido como “sopa primordial”<sup>31</sup>. A atmosfera não possuía oxigênio, e era rica em hidrogênio, amônia, metano e água. Algo fez com que essas moléculas se juntassem e se tornassem aminoácidos. Estes são capazes de se combinar formando proteínas e criando material orgânico. Este material orgânico eventualmente poderia ter dado origem à vida biológica como conhecemos hoje. Cada passo dessa cadeia não poderia ter existido antes do passo anterior. O hidrogênio, o metano, a água e o amônio não se ligariam sozinhos para formar proteínas, mas a forma recombinada deles chamada aminoácidos sim.

O possível adjacente é a essência do processo científico, quando novos conhecimentos são descobertos a partir dos conhecimentos adjacentes disponíveis, sejam livros ou artigos científicos. Basicamente, o conhecimento científico já existente representa as peças de um quebra-cabeça que já está montado na frente de todos. O cientista que faz uma descoberta simplesmente encontra o encaixe disponível na peça mais recentemente encaixada.

O conceito original de “meme” foi definido pelo biológico Richard Dawkins no livro “Gene Egoísta”. Este livro é um estudo de como os genes são a unidade de seleção da evolução, e não a espécie, grupo ou mesmo o indivíduo, contrário ao consenso científico na época. No livro, o autor propõe que os genes estão para a biologia como os memes estão para as informações culturais; e a menor unidade de seleção cultural é um meme. Ou seja, tanto uma história, como uma canção e mesmo uma imagem com texto em cima são memes. Analogamente ao “pool genético”<sup>32</sup>, existe um “pool memético”<sup>33</sup>, onde todos os memes disputam espaço; ou eles têm êxito, se fixam e são propagados pela sociedade, ou são esquecidos. Essas unidades culturais estão em um pool memético, onde todos os cientistas podem consultar essas informações.

Esse pool memético é compartilhado e torna o espaço para evolução cultural científica limitada ao possível adjacente que essas unidades de informação cultural permitem. Ou seja, não seria possível existir uma Teoria

de Seleção Natural sem que existisse o Malthusianismo ou o Uniformitarismo.



O conceito de psico-história, pensando por Isaac Asimov, ilustra bem esse conceito. Na psico-história, mesmo que as ações de um indivíduo em particular não possam ser previstas, os eventos futuros podem ser previstos com a utilização de estatística aplicada a grandes populações. As ações de

um único indivíduo não podem ser previstas, mas o comportamento de um grupo suficientemente grande pode.

Tanto a psico-história, conceito de ficção científica, como o possível adjacente, da biologia, possuem uma característica em comum: as ações de indivíduos específicos não importam para a tendência macro.

Nós gostamos de nos achar floquinhos de neve especiais, mas na verdade somos banais. Com variações básicas limitadas e alguns poucos arquétipos de personalidade possíveis, como as poucas categorias de qualquer teste de personalidade como o RIASEC ou Myers Briggs demonstram.

O que levanta a pergunta: um ser humano consegue inventar algo realmente novo?

## A descoberta do bitcoin

*"A privacidade é necessária para uma sociedade aberta na era eletrônica."*

**Eric Hughes, Manifesto Cypherpunk, 1993**

Assim como a imagem do cientista solitário, nós também tendemos a imaginar o Satoshi Nakamoto dessa maneira. Mas na realidade ele também estava em cima do ombro de gigantes quando concebeu o bitcoin.

O bitcoin pode parecer "novo", mas na realidade ele é a culminação de um processo de mais de 30 anos de um grupo de pessoas interessadas por criptografia e privacidade. São os chamados "cypherpunks". O Manifesto Cypherpunk data de 1993, quando diversas tentativas de solucionar a questão da transmissão de valor de forma privada sem um terceiro confiável já haviam sido realizadas e falharam. De maneira resumida, podemos simplificar algumas das peças de quebra-cabeça do "pool memético" dos cypherpunks utilizadas por Satoshi em:

- Hashcash, criado em 1997 por Adam Back.
- A prova de trabalho reutilizável (reusable proof of work, RPoW em inglês), baseado no Hashcash, criada em 2004 pelo, Hal Finney.
- A proposta para o "bitgold", um token digital baseado no RPoW, publicada em 2005 por Nick Szabo.

Até que em 2008, o pseudônimo Satoshi Nakamoto publicou o

whitepaper do bitcoin, "Bitcoin: A Peer-to-Peer Electronic Cash System".

Também existiu toda uma pré-história<sup>24</sup> de desenvolvimento anterior a 1997. Foi o aprendizado gerado por todas estas tentativas que permitiu que Satoshi conseguisse alcançar esse possível adjacente mágico chamado bitcoin. Por mais brilhante que Satoshi tenha sido, a verdade é que se ele não tivesse descoberto o bitcoin em 2008, alguém provavelmente o teria descoberto pouco depois.

## CAPÍTULO 5

# FUNDAMENTOS DO BITCOIN

O final de 2021 e o início de 2022 pegaram a maioria dos bitcoinheiros de surpresa. Todos os analistas que tentaram prever o preço no último ano acreditavam que, no início de 2022, nós estaríamos em patamares muito superiores aos atuais, provavelmente acima até dos 100 mil dólares por bitcoin. Contudo, ao invés disso, despencamos dos 69 mil dólares para os 33 mil dólares nos últimos meses, uma queda superior a 50%.

Vários bitcoinheiros, especialmente os iniciantes, se assustaram com este movimento inesperado. Outros, no entanto, não perderam a tranquilidade e viram a queda como uma oportunidade para comprar mais satoshis a preços que eles achavam que não veriam de novo. Enquanto uns vendiam em pânico, outros aproveitavam a promoção.

O que diferencia estes dois grupos de investidores?

Pra mim, a resposta é simples: os investidores que se assustaram estão focando sua atenção na variação do preço, enquanto os bitcoinheiros que permaneceram em paz focam sua atenção nos fundamentos do bitcoin. No capítulo 14, escrevo sobre a diferença entre o ruído e o sinal em maiores detalhes. Mas, adiantando, basicamente ruído são as informações irrelevantes, que servem somente para distrair os investidores, enquanto sinal são as informações relevantes, as quais de fato ajudam os investidores a embasar sua tese de longo prazo.

O objetivo deste capítulo sobre os fundamentos do bitcoin é se aprofundar no sinal, ou seja, olhar de perto os fundamentos do bitcoin. Quais as características do protocolo que levam os bitcoinheiros a acreditar que a variação de preço de curto prazo é irrelevante, uma vez que o objetivo é surfar a curva de adoção desta tecnologia no longo prazo?

A ideia deste capítulo também é mostrar o que poderia fazer um bitcoinheiro mudar de ideia em relação ao bitcoin. O que diferencia a religião ou a pseudociência da ciência bem feita é que, na ciência, não existem dogmas, mas apenas hipóteses, que nada mais são que chutes educados. Não precisa existir confiança, e sim dados abertos e hipóteses sendo testadas. Ou seja, tudo pode ser falseado. E como essa digressão se aplica ao bitcoin? Simples, o capítulo busca entender quais os fundamentos do bitcoin que, caso alterados, poderiam afetar e até mesmo falsear a tese do bitcoin. Fiz essa pergunta no Twitter<sup>35</sup>.



**Explica Bitcoin** 🗨️  
@BitcoinExplica

...

Na sua opinião, quais são as características mais importantes do **#Bitcoin** ₿ ?

Ou seja, quais são os pilares da tese que se fossem alterados a sua convicção se abalaria?

[Translate Tweet](#)

8:51 PM · Dec 16, 2021 · Twitter Web App



**Victor Stabile** @vmstabile · Dec 17, 2021

...

Replying to @BitcoinExplica

**#Bitcoin** ₿ é escassez digital descentralizada, o resto é consequência ou meio.

Foram muitas respostas boas e parecidas, o que mostra o alinhamento que os bitcoinheiros possuem. Apesar de sermos uma tribo descentralizada, ainda mantemos uma coesão forte devido ao nosso ethos (que será tratado no capítulo 11). De acordo com o Victor Stabile, da Refúgio Bitcoin, o “bitcoin é escassez digital descentralizada”, sendo o resto consequência disso ou o



meio para se alcançar essa tal escassez digital descentralizada. Achei essa uma síntese ótima, que organiza os conceitos e consegue explicar em uma frase simples as principais características do bitcoin.

Mas, considerando que o objetivo deste capítulo é ajudar os novatos a entender melhor o que significa essa tal “escassez digital descentralizada”, escolhi uma forma um pouco diferente de apresentar os fundamentos do bitcoin. Neste capítulo, escolhi adotar uma separação entre os fundamentos técnicos e os fundamentos sociais do bitcoin, apesar de que na realidade eles se retroalimentam em um loop de feedback positivo, o que os torna praticamente indissociáveis.

## Fundamentos técnicos

### 21 milhões

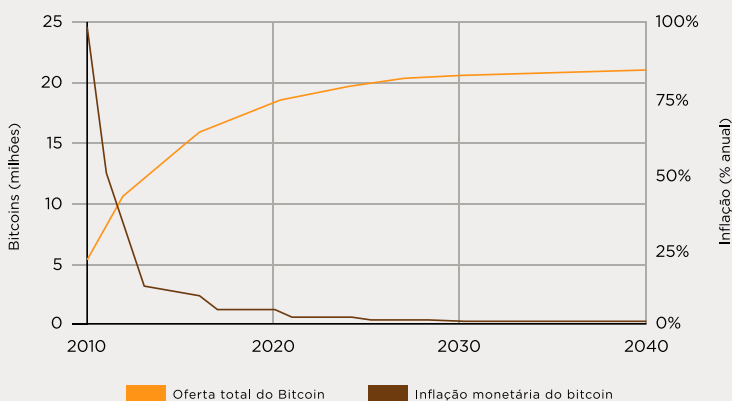
O bitcoin tem uma oferta limitada de 21 milhões de bitcoins (lembrando que “o bitcoin” pode ser tanto a rede e o protocolo como as moedas). Atualmente, cerca de 90% destes 21 milhões já foram emitidos, o que significa que mais de 18,9 milhões de bitcoins já estão em circulação. E os últimos 2,1 milhões serão emitidos nos próximos 120 anos, aproximadamente.

Ter um estoque auditável é um dos principais pontos fortes do bitcoin, pois nenhuma moeda fiat ou mesmo o ethereum, supostamente seu principal concorrente, podem dizer o mesmo.

Além disso, essa oferta de 21 milhões de bitcoins é inelástica, isto é, não importa quanto o preço do bitcoin suba, novos bitcoins sempre serão emitidos de acordo com o que determina o protocolo. Isso significa que bitcoins “extras” não serão emitidos. Ou seja, o bitcoin é a única commodity conhecida pelo homem que possui uma demanda inelástica.

Enquanto o número máximo de 21 milhões de bitcoins for mantido, o bitcoin segue tendo uma escassez irreplicável. Abrir qualquer exceção a este limite de 21 milhões é violar um dos fundamentos básicos do bitcoin e diluir o poder de compra de todas as moedas que já estão em circulação.

### OFERTA E INFLAÇÃO MONETÁRIA DO BITCOIN (2009-2040)



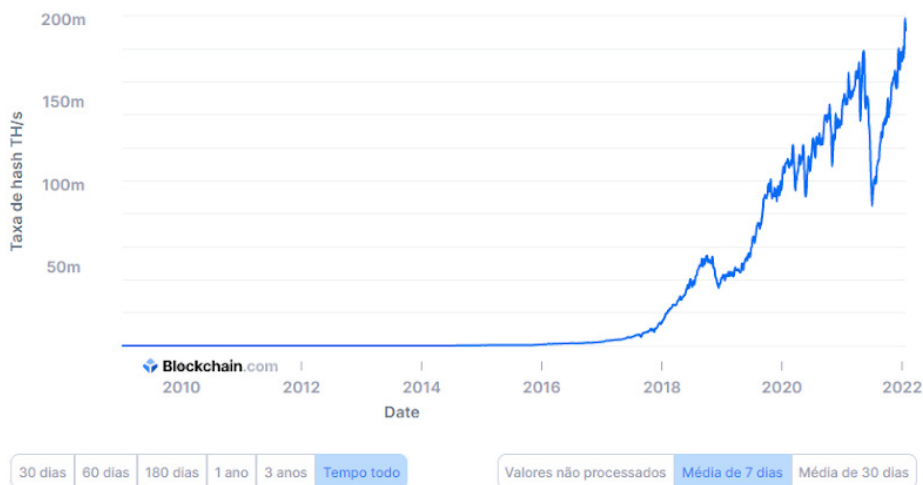
### Hashrate

O bitcoin é um protocolo que uma rede de computadores está rodando simultaneamente. Alguns desses computadores são os nodes, que validam os mineradores, e os outros são os mineradores, que validam as transações e a emissão de novas moedas. A mineração de bitcoin é um processo que demanda muito poder computacional dos seus participantes, uma vez que, quanto mais poder computacional utilizado, maior a chance do minerador encontrar o próximo bloco de transações do bitcoin (somente o minerador que encontra o bloco é remunerado).

Para os propósitos deste texto, não é importante entrar em uma explicação detalhada da mineração, mas apenas saber que o nome dado a esse poder computacional é hashrate, ou taxa de hash. O hashrate mostra quanto poder computacional os mineradores estão alocando na rede a cada segundo. O gráfico abaixo mostra a evolução da hashrate desde a criação do bitcoin.

## Taxa de hash total (TH/s)

O número estimado de terahashes por segundo que a rede de bitcoin está a realizar nas últimas 24 horas.



É possível notar o quanto o poder computacional da rede vem aumentando nos últimos anos. Também é visível a recuperação em V da rede após a China banir a mineração de bitcoin, no final do primeiro semestre de 2021. Em menos de um ano, a hashrate se recuperou de uma queda de cerca de 50%, tendo inclusive atingido novas máximas históricas posteriormente.

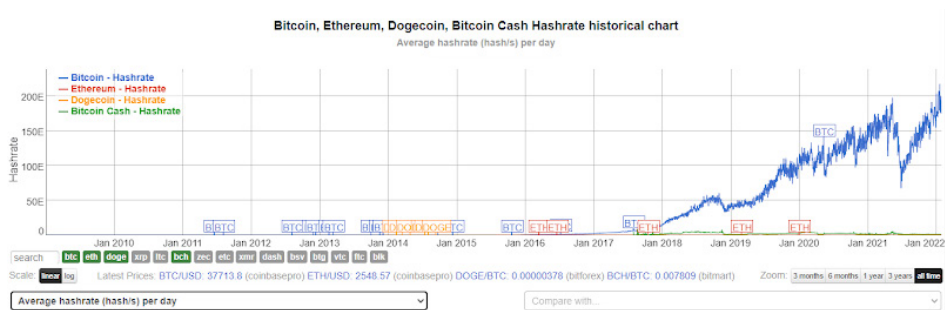
E por que a hashrate é importante? É esse poder computacional elevado que evita ataques à rede e garante a imutabilidade do histórico de transações do bitcoin. Se algum único player conseguisse centralizar mais de 50% do poder computacional da rede ele poderia, em teoria, alterar e deletar transações, além de efetuar gastos duplos. Esse vetor de ataque é conhecido como o "ataque dos 51%". Quanto maior for a hashrate da rede, maior o número de computadores que são alocados exclusivamente para a mineração de bitcoin, o que torna esses computadores seguradores da rede automaticamente.

Isso significa que, quanto maior a hashrate, maior o custo para se atacar o bitcoin. O atacante precisaria, no cenário mais barato, comprar 51% dos computadores utilizados na mineração, que são máquinas extremamente específicas e sofisticadas conhecidas como ASICs. No pior dos cenários, este atacante precisaria encomendar máquinas novas e comprar ASICs o

suficiente para dobrar a hashrate da rede.

Esse racional do custo para se atacar o bitcoin também mostra por que é importante que o processo de mineração do bitcoin utilize grandes quantidades de energia. Essa alta quantidade de energia significa que, para atacar a rede do bitcoin, o atacante precisaria não apenas de uma quantidade caríssima de computadores, mas também de uma quantidade significativa (e caríssima) de energia. Em qualquer desses cenários, valeria mais a pena, economicamente, para o atacante simplesmente ser remunerado por tanto hashrate empregado na rede.

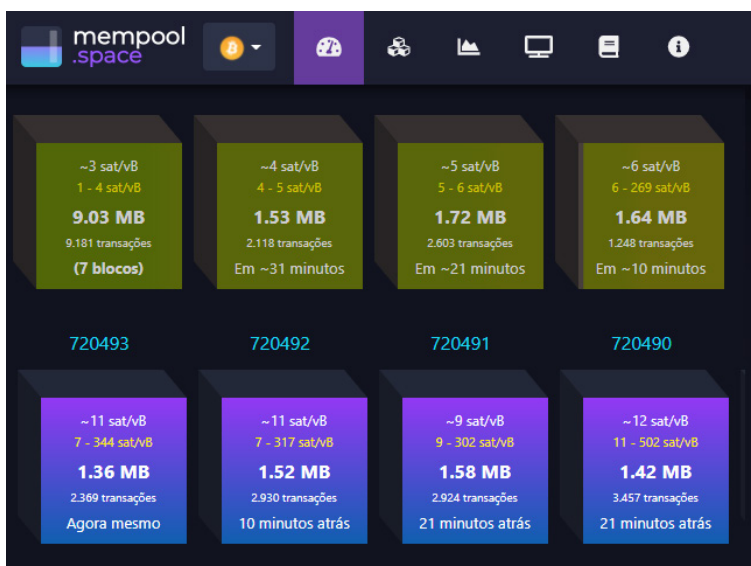
É possível perceber, portanto, que a hashrate é a medida de proteção da rede bitcoin porque é ela quem revela o grau de segurança da rede. Uma comparação da hashrate do bitcoin com a de outras criptomoedas ilustra bem o quão superior é o bitcoin, como a imagem abaixo mostra:



Sim, as hashrates do ethereum, do bcash e da dogecoin estão plotadas no gráfico também, porém, como se percebe, elas tendem a zero em comparação à do bitcoin. Se você quiser conferir por conta própria, consulte as referências 36 e 37 ao final do livro.

### Um bloco a cada ~10 minutos

O protocolo do bitcoin determina que novos blocos sejam minerados, em média, a cada 10 minutos. Se olharmos abaixo (nessa tela copiada do mempool.space<sup>38</sup>, que expõe dados sobre o funcionamento da Timechain), é possível notar que o tempo entre cada bloco não é sempre de 10 minutos, mas que os intervalos médios acabam sendo em torno deste tempo.



Eventualmente, blocos acabam sendo minerados em intervalos menores ou maiores que 10 minutos, e está tudo bem. Entretanto, caso o tempo médio de cada bloco se afaste muito dessa média de 10 minutos por um longo período (alguns ajustes de dificuldade), é provável que a rede esteja com graves problemas.

Isso é tão verdade que muitos bitcoinheiros pensam nessa emissão constante de blocos como os batimentos cardíacos do bitcoin. Uma modificação dos batimentos cardíacos pode significar uma arritmia, caso os blocos sejam emitidos, em média, em períodos menores que os 10 minutos, ou um estado de coma e até mesmo a morte, caso os blocos parem de ser emitidos. Não à toa, uma expressão comum no vocabulário dos bitcoinheiros é “tick tick next block” (“tick, tock, próximo bloco”). Essa expressão é usada para mostrar que variações de preço não possuem importância e que o coração da rede segue batendo no seu ritmo estável.

Como a hashrate é variável e pode tanto crescer como sofrer quedas bruscas com o passar do tempo, caso não existisse um mecanismo de regulação, a tendência seria que a emissão do bitcoin se desviasse da média de um bloco a cada 10 minutos. Esse mecanismo de regulação é conhecido como “ajuste de dificuldade”.

O ajuste de dificuldade ocorre a cada 2016 blocos, ou a cada duas

semanas, aproximadamente. O nome “ajuste de dificuldade” significa que a dificuldade do processo de mineração aumenta com o aumento da hashrate e diminui em caso de queda na hashrate. O que faz o resultado geral destes movimentos ser a estabilidade do tempo de emissão de novos blocos.



O exemplo extremo do funcionamento do ajuste de dificuldade ocorreu quando a China, no ano passado, proibiu a mineração de bitcoin. Inicialmente, a rede ficou mais lenta, pois menos poder computacional estava sendo empregado enquanto a dificuldade ainda estava elevada. Nas semanas seguintes, graças ao ajuste de dificuldade, a rede encontrou um novo equilíbrio. Nos meses posteriores, conforme as máquinas chinesas eram realocadas, a hashrate voltou a subir (uma recuperação em V), assim como a dificuldade, de maneira proporcional. A imagem abaixo mostra como a dificuldade da rede varia de acordo com o hashrate.



## Descentralização

Descentralização é um conceito chave para entender o bitcoin e como os bitcoinheiros enxergam o mundo. Idealmente, a descentralização deveria ocorrer em todas as diferentes partes do bitcoin. Seja no desenvolvimento de atualizações no GitHub (uma plataforma de hospedagem de código-fonte e arquivos. Ele permite que programadores contribuam em projetos privados e/ou Open Source de qualquer lugar do mundo), seja na mineração, a descentralização é e sempre será vital para o bitcoin ser bem sucedido.

Abaixo, temos uma lista das diferentes formas de descentralização as quais são consideradas chave pelos bitcoinheiros:

**Tamanho dos blocos** - o bitcoin já passou por uma guerra civil (conhecida como “Guerra do Tamanho dos Blocos”) e perdeu um grupo de apoiadores que estavam envolvidos desde os primórdios quando este grupo propôs aumentar o tamanho dos blocos. Teoricamente, esse aumento do tamanho dos blocos faria com que o bitcoin pudesse ser utilizado como moeda mais facilmente, pois as transações seriam consolidadas de maneira mais rápida. Entretanto, aumentar o tamanho dos blocos também acabaria significando um maior grau de centralização da rede. Isso porque seria mais difícil para os pequenos usuários rodarem seus nodes validadores a partir de equipamentos simples e baratos. Os usuários foram intransigentes e, ao final, saíram vencedores desta questão, mantendo a validação do bitcoin o mais descentralizada possível, com os blocos em seu tamanho original.

**Número de nodes validadores** - como dito acima, o número de pequenos usuários (eu e você), conhecidos como “plebs” pela comunidade, rodando os nodes validadores, também é considerado um fator de descentralização. Quanto mais simples e barato for rodar um node validador, mais saudável a rede do bitcoin estará.

**Mercados p2p fortes** - muitos de nós ainda compramos bitcoin nas exchanges como o Mercado bitcoin ou a Bipa. Mas essas exchanges precisam seguir normas do governo e identificar seus usuários. Uma prática que é mais aconselhável é comprar bitcoin direto de outra pessoa. O bitcoin foi criado para isso, está até no título do whitepaper: bitcoin: A Peer-to-Peer Electronic Cash System. Isso permite que, caso os governos tentem proibir a utilização do bitcoin, essa medida seja inócua e o bitcoin continue sendo utilizado. Pode-se dizer que quanto mais trocas ocorrerem sem nenhum terceiro, mais

forte estará o bitcoin.

**Quem foi Satoshi Nakamoto?** - talvez uma das questões mais intrigantes sobre o bitcoin e que todo bitcoinheiro já conversou com amigos sobre quem foi Satoshi Nakamoto. Essa talvez seja uma das principais perguntas que mostram se alguém entendeu o bitcoin ou não. Por quê? Porque o fato do Satoshi Nakamoto ser desconhecido é uma das principais características positivas do bitcoin. E isso é algo que só se torna claro depois de algum estudo e reflexão. Mas pense: como o estado consegue perseguir alguém que ele não conhece? Se o estado quiser interferir no ethereum ou no Facebook (agora Meta), todos sabem quem precisa ser influenciado/coagido. No caso do bitcoin, ninguém tem controle e nem mesmo influência real sobre as decisões da rede, o que não pode ser dito de nenhuma outra criptomoeda ou outra forma de investimento. O bitcoin é o único ativo descentralizado do mundo.

**Mineração PoW** - a mineração do bitcoin é feita a partir da chamada “prova-de-trabalho” (PoW, sigla de proof-of-work), que é justamente o que faz com que a mineração utilize tanta energia. A PoW foi a forma escolhida para estruturar o bitcoin pois, pelo menos até o momento, essa foi a única solução encontrada pelos humanos para o “problema dos generais bizantinos”<sup>39</sup>. Tal problema é relacionado à teoria dos jogos e descreve a dificuldade que entidades descentralizadas possuem para chegar em um consenso sem depender de um ponto central de confiança. Sem uma solução para esse problema, seria impossível a invenção de um dinheiro da internet descentralizado. Diversas altcoins tentam solucionar esse mesmo problema teórico utilizando a validação via “prova de participação”, mas essa solução é essencialmente centralizadora, uma vez que, nela, quem tem mais (moedas), manda mais.

**Descentralização geográfica da mineração** - também é importante que a mineração do bitcoin ocorra em diferentes jurisdições. Isso significa que banimentos futuros de jurisdições específicas possuirão apenas poder moderado de influência na rede. Por exemplo, antes do banimento da China, um risco real era a apreensão de todo o equipamento de mineração que estava lá e totalizava cerca de 50% do poder computacional da rede. Teria sido a maneira mais simples e barata de se efetuar um ataque dos 51%. Mas a China não fez isso, e agora a rede está mais descentralizada e segura. Mas



a premissa se mantém: quanto mais descentralizada geograficamente for a mineração, mais resiliente ela será.

## Imutabilidade

*"A natureza do bitcoin é tal que, uma vez que a versão 0.1 foi lançada, o design principal foi gravado em pedra para o resto de sua vida."*

**Satoshi Nakamoto**

O principal fundamento do bitcoin, na opinião de muitos, é a imutabilidade. Isso porque o fato da parte técnica do bitcoin ser praticamente imutável é o que gera confiança no protocolo e faz com que os fundamentos sociais ocorram.

Mas o que significa imutabilidade<sup>40</sup>?

Existem, basicamente, duas linhas de respostas: uma que foca na imutabilidade das regras que foram originalmente criadas por Satoshi Nakamoto e outra que foca na imutabilidade do histórico da Timechain (a cadeia de blocos do bitcoin).



**Narcélio Filho** @narcelio · Jan 24

...

Replying to @BitcoinExplica

1) Imutabilidade nas regras criadas pelo Satoshi em 2009.

2) Provável imutabilidade no histórico da blockchain. Quanto mais antiga a informação, mais provavelmente imutável ela é.



26



**Jaraguá** @JaraguaBTC · Jan 24

...

Replying to @BitcoinExplica

Duas vertentes. Uma rígida e outra incremental.

Rígida: Intransigência com hardforks

Incremental: Incapacidade de se desfazer transações a medida que blocos são adicionados após.



7



A imutabilidade das regras colocadas por Satoshi em 2009 vem, principalmente, da intransigência dos bitcoinheiros que rodam seus próprios nodes e não aceitam nenhuma mudança proposta.

Como o bitcoin é um protocolo de código aberto, qualquer pessoa que quiser pode copiá-lo, modificar algumas normas e lançar como uma outra moeda. Hipoteticamente, caso tal pessoa conseguisse convencer os nodes a rodarem a sua versão do código, o bitcoin teria sido modificado. Parece simples, né?

Foi o que o pessoal do bitcoin Cash (um fork do bitcoin) pensou. Eles queriam atualizar uma única questão do protocolo original: aumentar o tamanho dos blocos minerados de 1MB para 2MB. Apesar desta mudança ter sido defendida por alguns dos principais nomes do bitcoin da época, além de mineradores e exchanges, ela não foi aceita pela comunidade. Um grupo de usuários espalhados pelo mundo entendeu que, se os blocos aumentassem de tamanho, a rede perderia em descentralização, pois seria necessário mais espaço no disco do computador para armazenar a Timechain inteira.

Para que ocorra qualquer mudança no protocolo original, é necessário que uma gama muito grande de usuários diferentes, com interesses diferentes, entre em acordo. Caso isso não ocorra, os nodes continuarão protegendo e se organizando na rede original. E eles são avessos a mudanças.



**Bruno ∞/21M @Bruno\_Nardi** · Jan 24

...

Replying to [@BitcoinExplica](#)

Meu node, meu software, minhas regras, quem quiser fazer diferente pode forkar mas não interfere em nada com meu node.



6



Doar



**BTC DOOM Guy @BitcoioD00mMano** · Jan 24

...

Replying to [@BitcoinExplica](#)

Quem quiser mudar alguma regra vai ter que vir aqui em casa e alterar as regras do meu node



1



25



Doar

A imutabilidade da Timechain significa que as transações são finais e irreversíveis. Uma vez que uma transação é confirmada e colocada em um bloco da Timechain, é extremamente improvável que essa transação

seja tirada de lá. Essa transação estará lá enquanto o bitcoin existir. E essa certeza aumenta a cada bloco minerado de tal forma que, após apenas 6 blocos minerados, já podemos afirmar que essa transação está validada enquanto existir a Timechain.



**Fiduma** @FidumaHODL · Jan 24

...

Replying to @BitcoinExplica

Após alguns blocos de uma transferência confirmada, o custo para alterar/desfazer essa transferência inviabiliza alguém querer fazê-la, portanto consideramos que é imutável.



**BitMorpheus** @BitMorpheus · Jan 25

...

Replying to @BitcoinExplica

A imutabilidade deriva da consolidação da maior cadeia de hashes. A partir de 6 blocos a transação se torna imutável;



1



1



**Anderson Lara** @AndersonJLara · 23h

...

Por que 6 e não 5 ou 7?



1



**BitMorpheus** @BitMorpheus · 20h

...

É probabilisticamente imutável, 6 é um número ao qual a probabilidade de reversão da rede é praticamente nula. Cada bloco de diferença entre o consenso e o atacante aumenta a dificuldade e diminui a probabilidade exponencialmente como descrito no capítulo Cálculos do white paper.



1



Pareceu meio complexo ainda né? Tudo bem, um desenho que estava circulando no Twitter ano passado explica bem essa questão:

## PORQUE VOCÊ NÃO CONSEGUE TRAPACEAR NO BITCOIN



Para um atacante modificar uma transação no bloco laranja, ele não teria somente que utilizar a energia para solucionar um bloco, mas sim energia para solucionar todos os blocos até o bloco laranja. E esse atacante teria que solucionar todos os blocos antes que qualquer outro minerador solucionasse apenas um bloco, o que é matematicamente bastante improvável.

### Fundamentos Sociais

Os fundamentos técnicos do bitcoin são extremamente importantes e servem de base sólida para os fundamentos sociais. Mas são os fundamentos sociais que realmente dão valor para o bitcoin, uma vez que valor é uma questão intersubjetiva. Ou seja, o que dá valor ao bitcoin (ou a qualquer outra coisa do mundo) são as pessoas compartilharem a crença subjetiva que ele é valioso. Essa crença tem origem em suas características técnicas, mas, caso essas características existissem e não fossem reconhecidas, elas existiriam em vão. Por este motivo, não adianta o bitcoin ter os fundamentos técnicos perfeitos caso não esteja ocorrendo adoção significativa deste protocolo.



**Você não está  
fazendo errado  
se ninguém souber  
o que você  
está fazendo.**

“Você não está errado se ninguém souber o que você está fazendo”. Ou seja, as coisas só podem ser percebidas quando as pessoas sabem o que é para ser percebido.

A forma que o autor do texto utiliza para acompanhar a evolução dos fundamentos sociais do bitcoin é acompanhar a evolução da sua adoção e o comportamento dos HODLers que usam a estratégia da compra recorrente.

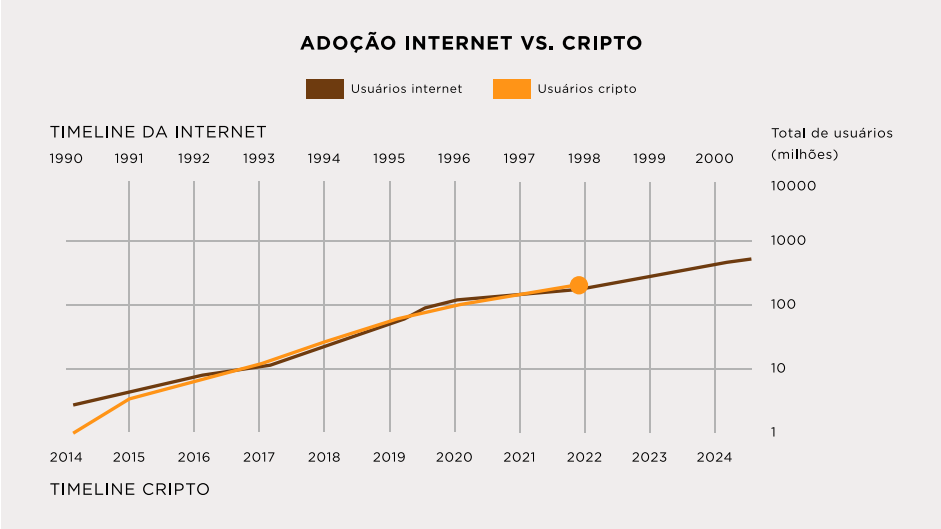
## Adoção

A taxa de adoção do bitcoin é o seu principal fundamento social. Ela que ilustra os efeitos de rede sendo criados em torno do protocolo, ou, em palavras mais simples, mostram se a ideia está “pegando”.

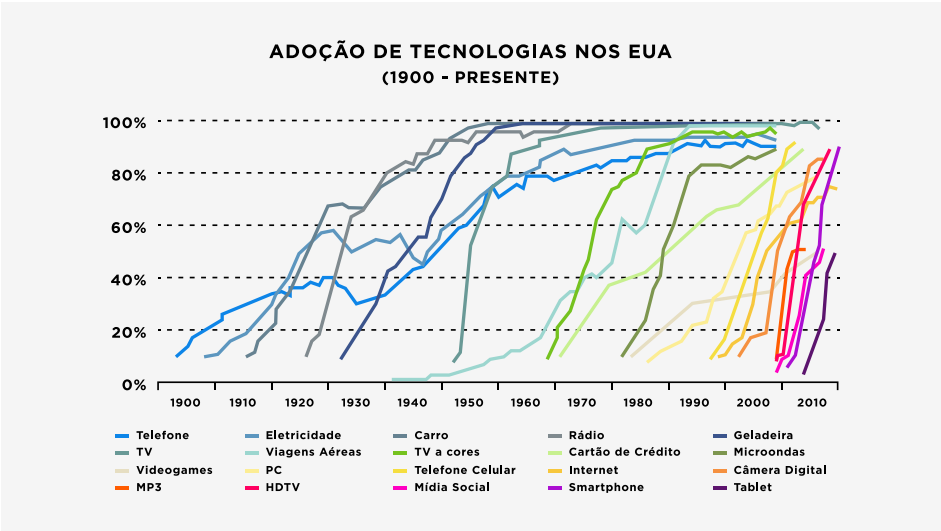
Ideias ou “pegam” ou “não pegam”, não existe um meio termo. Ou apresentam uma taxa de adoção suficiente para fazê-las superarem o “abismo” (que será bastante comentado no capítulo 12), atingindo um ponto de não retorno, ou acabam sendo aquelas tendências abortadas, como as paletas mexicanas e os tablets.

Atualmente, a adoção do bitcoin e do ecossistema das criptomoedas como um todo vem ocorrendo em alta velocidade. Essa adoção é comparada constantemente com a taxa de adoção da internet no final dos anos 90, como a imagem abaixo ilustra. Nessa comparação de curvas de adoção, o bitcoin está, aproximadamente, no mesmo estágio em que a internet estava em 1998, com cerca de 200 milhões de usuários. Já a velocidade de adoção mostra como o bitcoin é útil e resolve um problema real para muitas pessoas

em todo o mundo, tal qual a internet. Se não fosse esse o caso, a adoção não estaria ocorrendo nesta velocidade. Que problema é esse? A falta de uma reserva de valor acessível e confiável.



O gráfico abaixo ajuda a esclarecer a adoção do bitcoin em taxas equivalentes à taxa de adoção da internet. Basicamente, os dados demonstram que a adoção do bitcoin vem seguindo os passos de uma das tecnologias que foram adotadas mais rapidamente na história humana.



Essa adoção também garante que, no longo prazo, a teoria dos jogos se desenvolverá de uma maneira favorável ao bitcoin. É através da referida teoria que se justifica o recrutamento de políticos e empresários para a causa do bitcoin, fato que torna qualquer ataque à rede mais difícil.

O exemplo mais conhecido desse tipo de teoria dos jogos em ação é a Uber, que tinha como estratégia desenvolver uma base de clientes nas cidades antes das prefeituras terem tempo de legislar e proibir seus serviços. Dita base de clientes tornava politicamente custoso tentar proibir a Uber. O mesmo está acontecendo com o bitcoin, mas em escala global.

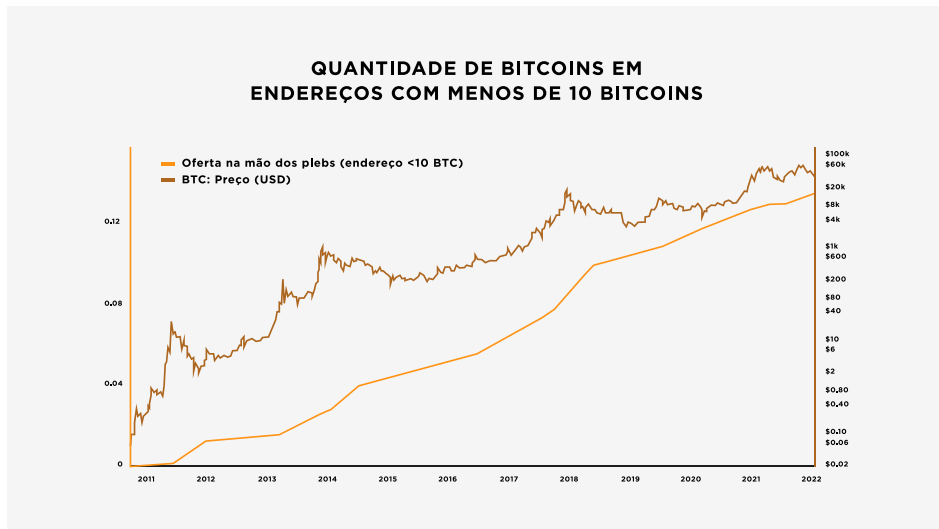
### **HODLers absorvendo oferta constantemente**

Existem diferentes tipos de usuários do bitcoin. Desde traders, que não se importam minimamente com qualquer característica filosófica por trás de seu investimento, até libertários, que comprariam bitcoin mesmo se o preço não se valorizasse em relação às moedas fiduciárias. Um dos tipos de usuários são os HODLers, aqueles que compram bitcoin sem intenção de vender e o seguram por longos períodos de tempo. Tais usuários escolheram usar o bitcoin em vez de outros tipos de investimento como a sua reserva de valor.

Geralmente, os HODLers utilizam a estratégia da compra recorrente (conhecida como “preço não importa”<sup>41</sup> para os investidores de bolsa), também denominada DCA (dollar cost averaging). Isso significa que esses HODLers compram o bitcoin a cada dia, semana ou mês, independentemente do preço. São pessoas que veem o bitcoin como reserva de valor e, em sua visão, todo dinheiro fiduciário por eles recebido como pagamento preserva melhor o seu valor se convertido imediatamente para moeda forte.

Ou seja, eles representam uma fonte de demanda constante, que vai enxugando a liquidez do mercado e tirando moedas de circulação. A imagem abaixo ilustra esse comportamento e mostra que a quantidade de carteiras com menos de 10 bitcoins aumentou constantemente ao longo de toda a história do bitcoin. Esse número (10 bitcoins) é utilizado como parâmetro por mostrar o movimento dos HODLers plebs, isto é, dos trabalhadores que utilizam o bitcoin como poupança e que, todo mês, convertem uma parte do seu salário para satoshis. Como a quantidade de HODLers é influenciada pela adoção, quanto maior a adoção, maior o número de pessoas executando

essa estratégia e mais bitcoins sendo retirados de circulação por um longo período de tempo.



Essa dinâmica, por si só, já significaria que, no longo prazo, haveria menos bitcoins em circulação e, por consequência, o preço aumentaria. Mas o halving ainda precisa ser levado em conta, o que torna essa combinação mais explosiva. Halving é o evento responsável por, a cada quatro anos aproximadamente, cortar pela metade a remuneração dos blocos minerados. Isso significa que, a cada quatro anos, a taxa de emissão de novos bitcoins cai pela metade.

Ou seja, como o bitcoin é um ativo cuja demanda é cada vez maior (por conta da curva de adoção acelerada - o que é visível através do comportamento dos HODLers), e cuja oferta não é repostada na mesma velocidade que antes, mas sim 2x mais devagar devido aos halvings, a elevação do preço, no longo prazo, é certa. Justamente em razão do desequilíbrio entre oferta e demanda verifica-se a tendência de reprecificação do bitcoin, onde um novo ponto de equilíbrio, em um valor mais elevado, é encontrado para solucionar o desequilíbrio entre oferta e demanda.

Um modelo mental que eu gosto de utilizar para entender o efeito dos HODLers de longo prazo absorvendo a oferta de bitcoins é o da caçada de persistência dos caçadores coletores.

**A caçada de persistência** - a ação dos HODLers que utilizam a



estratégia do DCA, grupo de investidores que também é conhecido como “exército do DCA”<sup>42</sup>, pode ser comparada também à estratégia de caça mais primitiva praticada pela humanidade, conhecida como “caçada de persistência”<sup>43</sup>.

Além da capacidade de comunicação e inteligência, o ser humano ainda possui duas outras grandes vantagens evolutivas em relação aos outros mamíferos da África: I) ele é bípede, o que significa que ele é mais eficiente correndo longas distâncias, além de poder utilizar os braços para levar ou arremessar coisas; e II) ele consegue se regular termicamente de uma maneira muito mais eficiente por não ter pelos e conseguir suar.

A caçada de persistência é a técnica de caça que consiste na perseguição a um outro animal em que os humanos vencem pela exaustão e pelo superaquecimento do alvo<sup>44</sup>. Nesta espécie de caça, os humanos perseguem os animais por horas. Os animais sempre são mais rápidos em pequenas distâncias, porém eles não conseguem se recuperar plenamente antes dos humanos os alcançarem e continuar a perseguição. Isso leva estes animais a exaustão, fazendo com que eles não consigam mais fugir, se tornando presas fáceis.

A ação dos HODLers fazendo o DCA é equivalente à ação do caçador que está perseguindo e pressionando a presa. Os HODLers fizeram a lição de casa e possuem mais convicção do que os traders e outros especuladores que deixam seus bitcoins em exchanges. Desta maneira, os HODLers surfam a curva de valorização do bitcoin conforme a liquidez vai sendo extraída paciente e persistentemente pelo exército do DCA. Uma hora, o antílope (no caso, a pressão vendedora) vai cansar e a recompensa pela persistência será um belo banquete de carne (a valorização do ativo pela baixa liquidez no estoque, com poucos bitcoins a venda).

## **Ou seja...**

Muitos se assustam com a volatilidade do bitcoin e vendem em pânico em movimentos de queda acentuados.

“Será que a bolha finalmente estorou?”, “Eu sabia, eram tulipas!”, eles pensam, enquanto suas mãos de alface executam a venda.

Enquanto isso, outros aproveitam para aumentar o saldo de bitcoins em suas wallets. Essa diferença de comportamento existe por conta de uma

enorme e persistente assimetria de educação em relação ao bitcoin. Apesar de ser o dinheiro mágico da internet, o bitcoin tem fundamentos sólidos e verificáveis. São eles:

- Escassez de uma oferta limitada em 21 milhões de bitcoins,
- Hashrate;
- Emissão de um novo bloco a cada 10 minutos em média;
- Descentralização em todos os aspectos;
- Imutabilidade dos aspectos técnicos;
- Adoção;
- Absorção da oferta pelos HODLers que usam o bitcoin como reserva de valor de longo prazo.

São esses os fundamentos que fazem do bitcoin a “escassez digital descentralizada”, como dito no início do texto.

Quando a volatilidade vem associada a uma deterioração dos fundamentos, existe sim motivo para atenção e um olhar mais atento. No entanto, caso a volatilidade não esteja relacionada a qualquer alteração negativa nesses fundamentos, existe apenas um significado para os bitcoinheiros: promoção.

Ou, na linguagem dos bitcoinheiros: “buy the dip!” (compre na queda).

## CAPÍTULO 6

# PRECIFICANDO O BITCOIN

Existem diversas maneiras de se precificar o bitcoin, inclusive precificando-o com o valor de R\$ 0. Neste capítulo, são abordados alguns dos modelos de preço que existem no mercado, apresentando-se uma breve reflexão sobre cada um deles.

Vale lembrar, também, que tudo que está aqui descrito ignora os movimentos de curto prazo e foca somente nos fundamentos de longo prazo. Se você é trader e pretende entender qual será o preço do bitcoin daqui a uma semana ou a um mês, sinto muito, mas não entendo nada desse assunto. Aqui, o foco é o jogo de soma não-zero, isto é, o jogo de longo prazo baseado em fundamentos, e não o jogo de soma zero, equivalente ao trade do dia-a-dia.

### O bitcoin vai a zero

Vamos começar esse capítulo lidando com o principal medo da maioria dos novatos no bitcoin: e se um dia o bitcoin for a zero? E se a "bolha" realmente estourar? Existem duas abordagens para responder esta questão: a baseada em dados e a baseada no poder das narrativas.

### Análise baseada em fundamentos

Uma crítica bastante comum (e superficial) ao bitcoin é a referente

à crença na possibilidade de surgimento futuro de outras criptomoedas melhores. Os adeptos desta crítica frequentemente argumentam que “ninguém garante que o bitcoin não será o MySpace ou Orkut do futuro”. Apesar desta crítica até parecer inteligente em um primeiro momento, ela não resiste a uma análise mais aprofundada.

Um dos fatores mais relevantes do bitcoin é o de que ele já alcançou o efeito de rede, algo que o MySpace nunca chegou a realmente atingir. Como conferir isso? Simples: o market cap máximo que o MySpace chegou foi de \$12 bilhões<sup>45</sup>, um valor relativamente elevado, mas que é 83.3x menor do que o market cap de \$1 trilhão que o bitcoin atingiu em períodos distintos de 2021. Um market cap deste tamanho ilustra bem a quantidade de interações que esta rede possui. Nunca existiu uma companhia de tecnologia com efeitos de rede e market cap superior a \$100 bilhões que foi a zero. E o bitcoin, no auge de 2021, atingiu 10x este valor de \$100 bilhões.

Outro fundamento importante é a hashrate da rede (a capacidade de processamento computacional da rede). Comparando a hashrate do bitcoin com a de outros criptoativos a diferença é óbvia e ilustra a diferença entre a Timechain do bitcoin e de outras redes.

O principal fundamento do bitcoin é a sua comunidade e o efeito de rede a ela associado. Por esta razão, quando alguém argumentar que “essa shitcoin é o próximo bitcoin”, se pergunte: “qual a sua capacidade de processamento?”. “Já foi gerado algum tipo de efeito de rede para essa comparação fazer sentido?”.

Além da hashrate, também é interessante ressaltar a rede de full nodes, que são computadores que rodam o software do bitcoin constantemente e que se sincronizam entre si em tempo real. Em resumo, o full node registra e valida toda a informação que transita na rede bitcoin, de modo que a informação que não está de acordo com as regras é rejeitada.

Esqueça as manchetes sensacionalistas. Enquanto o bitcoin possuir uma rede estável ou em crescimento de full nodes, bem como uma hashrate estável ou em crescimento, a tese segue inabalada.

### **Análise baseada no poder das narrativas**

Grande parte dos críticos do bitcoin se apoiam no conceito de “valor intrínseco” e afirmam que o bitcoin não possui este valor.

Muito já foi escrito sobre esse assunto, com vários autores de várias correntes de pensamento econômico distintas defendendo o porquê do dinheiro não precisar ter valor intrínseco. Ou faz sentido pensar que um pedaço de papel colorido possui valor intrínseco?

Mas, no âmbito do bitcoin, preferimos uma abordagem mais prática.

Você já parou para pensar que uma obra de arte não passa de um pedaço de pano com tinta? O que atribui o seu valor não é o custo da tinta nem o custo do pano, pois o valor intrínseco combinado destes materiais é irrisório. O que realmente dá valor a uma obra de arte é a convenção social estabelecida entre os apreciadores de artes. A abstração compartilhada entre eles sustenta esse valor. É uma pura questão de oferta e demanda, da narrativa que um determinado grupo de indivíduos decide aceitar.

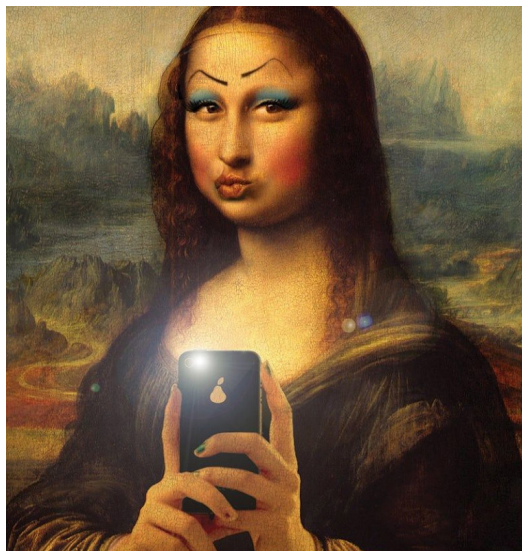
O autor deste texto, por exemplo, não vê valor em panos pintados e não gastaria suas economias neles, mas esta é uma opinião subjetiva. Basicamente, minha opinião não importa desde que existam pessoas o suficiente que enxergam valor nestes panos pintados. O mesmo vale para cartas de RPG. Ainda que para a maioria das pessoas do mundo elas não possuam valor, esses pedaços de papel podem ser vendidos por um valor significativo enquanto houver uma minoria disposta a comprá-los. É, na prática, o funcionamento da lei da oferta e da demanda.

Não à toa, existem cartas de Magic que custam até R\$2,8 milhões<sup>46</sup> e cartas de Pokémon chegam a valer R\$1,9 milhões<sup>47</sup>. O mercado é sempre soberano e uma opinião subjetiva sobre se um ativo tem valor ou não é só isso, uma opinião. Se não existisse demanda, não existiria valor, e ambos tenderiam a zero com o tempo.



Esta é a Black Lotus, a carta mais valiosa do Magic e que possivelmente vale mais que a sua casa. O valor intrínseco dela, ainda assim, é a tinta da impressão e o papel.

“Mas a arte original é única e escassa e existem milhares de outras shitcoins no mercado, então o bitcoin não é escasso”. Este argumento, utilizado por muitos, simplesmente não considera que existe uma infinidade de gravuras da Monalisa que não afetam a escassez e, portanto, o valor da Monalisa original. A mesma relação se aplica ao bitcoin e as shitcoins e uma breve comparação dos seus fundamentos (feita no capítulo 15) deixa isso claro.



Esta sátira da Monalisa altera de alguma forma o valor da Monalisa original?

## Como enxergamos o mundo?

Você já deve ter escutado a respeito do livro “Sapiens”, do historiador Yuval Harari. Um dos conceitos apresentados no livro é o poder das narrativas para a mobilização de grupos humanos. O ser humano compreende o mundo, de acordo com Harari, em três esferas distintas: a realidade objetiva, a realidade intrassubjetiva e a realidade intersubjetiva.

A **realidade objetiva** é o mundo concreto descrito pelas leis da física e da química. Por exemplo: se eu soltar um copo no ar ele vai cair por conta da gravidade. Isto é uma realidade objetiva. Não importa as origens culturais, o gênero e nem a idade da pessoa, o copo cairá, pois, a lei da gravidade funciona de maneira igual para todos.

A **realidade intrassubjetiva** é o mundo do meu eu interno. Onde minha interpretação subjetiva do mundo é o fator mais importante. Minhas sensações, emoções e sentimentos. Esta realidade é impossível de ser comunicada, pois mesmo as palavras já distorcem o seu real significado. Entre o pensamento e a formulação em palavras já existe um abismo, entre as palavras ditas por uma pessoa e a compreensão destas mesmas palavras por outra pessoa, outro.

A **realidade intersubjetiva** representa as nossas abstrações compartilhadas, ou seja, as histórias que compartilhamos com os outros. Estas histórias ganham força de verdade conforme mais e mais pessoas passam a acreditar nelas. Por exemplo: não existem direitos humanos universais ou fronteiras. Eles são uma convenção social, uma espécie de abstração compartilhada e não uma realidade objetiva. Um leão não respeitará os seus direitos humanos caso você passe desavisadamente em sua frente na savana africana.

A vibração de uma torcida ao ver o seu time fazer um gol é outro ótimo exemplo de realidade intersubjetiva. Objetivamente falando, os homens chutarem a bola dentro do gol não deveria afetar em nada a realidade de um grupo de pessoas. Mas, como fomos ensinados, desde o nascimento, a gostar de futebol, o gol do time provoca um evento de catarse coletiva. E pessoas que usam cores diferentes (as cores de outros times) incomodam profundamente grupos de torcedores, pois elas são o equivalente à pintura de guerra, apesar de serem só cores.



Aqui temos a imagem do símbolo do Internacional em azul, as cores do seu maior rival, o Grêmio. Isso causa incômodo em qualquer pessoa que acompanha o futebol e esse incômodo é significativamente maior para os torcedores do Internacional. Por que isso ocorre? São só cores.

Da mesma forma, existirem dias certos para trabalhar e dias certos para descansar é um acordo coletivo, uma realidade intersubjetiva. Não existe diferença real entre um domingo e uma segunda-feira além da convenção social.

Ou seja, algo se torna real simplesmente por ser uma narrativa compartilhada entre muitos indivíduos. As realidades intersubjetivas são as convenções sociais que adotamos sem nem perceber que elas são opcionais. Elas são o caldo cultural de um determinado povo, seus costumes e suas tradições.

Religiões são ótimos exemplos de realidades intersubjetivas. Elas não existem de fato na natureza, mas elas existem na mente dos humanos e isso gera resultados concretos no mundo real.

### **Religiões não são zeradas**

Uma comparação que muitos críticos costumam fazer aos bitcoinheiros é que nos comportamos como uma religião. O autor deste texto discorda em partes desta visão, pois considerando que, geralmente, seguir uma religião implica respeitar diretrizes dogmáticas, abdicando-se da independência de pensamento, nada poderia ser mais contrário ao ethos dos



bitcoinheiros do que isso. Ethos significa o “conjunto dos costumes e hábitos fundamentais, no âmbito do comportamento (instituições, afazeres etc.) e da cultura (valores, ideias ou crenças), característicos de uma determinada coletividade, época ou região”. E podemos afirmar que sim, os bitcoinheiros, possuem costumes e hábitos fundamentais que os caracterizam. É justamente por conta do ethos dos bitcoinheiros ser tão coeso que existe esta impressão de comportamento religioso, como será discutido no capítulo 10. Para fins argumentativos, entretanto, vamos considerar que o bitcoin é sim uma religião e os bitcoinheiros seus discípulos.

Então a questão que fica é: é possível zerar uma religião?

Se você se recordar das aulas de religião e de história do Império Romano, a resposta é auto evidente. O Império Romano foi um dos impérios mais poderosos que o mundo já conheceu. Foi no coração deste império que Jesus Cristo nasceu, viveu e foi crucificado. Desde a sua criação, o Império Romano tentou acabar com o cristianismo. Mesmo com milhares de cristãos sendo literalmente jogados aos leões no Coliseu para entretenimento da população pagã, o número de cristãos só crescia. Até que o Imperador Flávio Aurélio Constantino (272 d.C. - 337 d.C.) se converteu ao cristianismo.



“Pai, perdoa-lhes; porque não sabem o que fazem.”

A história do cristianismo pode ser utilizada como um exemplo perfeito para a hipótese de que “o mais teimoso ganha”, que o autor Nassim Taleb apresenta no livro “Arriscando a própria pele”. Basicamente, uma minoria teimosa o suficiente, que possua convicção por tempo suficiente, acaba influenciando todos os outros ao seu redor a adotarem o seu pensamento. A figura esquemática abaixo ilustra o raciocínio do Taleb, em que uma pequena minoria teimosa e convicta consegue influenciar o seu núcleo próximo, que influenciará mais pessoas.

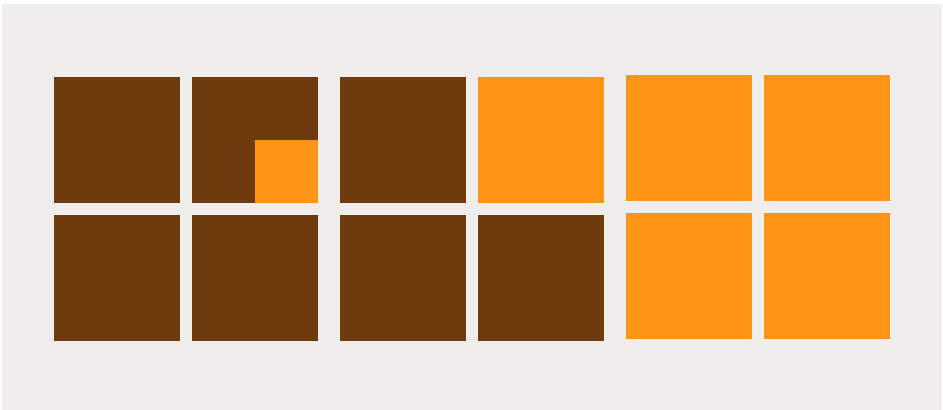


Imagem do livro Arriscando a própria pele exemplificando o conceito da minoria teimosa e a sua capacidade de dispersão de influência.

Ou, nas palavras de Taleb: “Renormalização dos grupos: os quatro quadrados contém quatro quadrados menores dentro deles e apenas um dos quadrados está de uma cor diferente. Aplicando a regra de que a minoria que impõe sua visão na sua pequena esfera de influência em cada um dos três passos nós entendemos a regra da minoria teimosa”.

Todos estes conceitos abstratos e lições de história nos ajudam a ver que não, o bitcoin não vai a zero. Para isso acontecer seria necessário perseguir e eliminar todos seguidores dessa “religião”. Mesmo se a rede for comprometida, ainda existem seguidores religiosos que a reergueriam.

Como o bitcoin não vai a zero, a próxima pergunta é “então como precificá-lo?”. É sobre isso que as próximas páginas irão tratar.

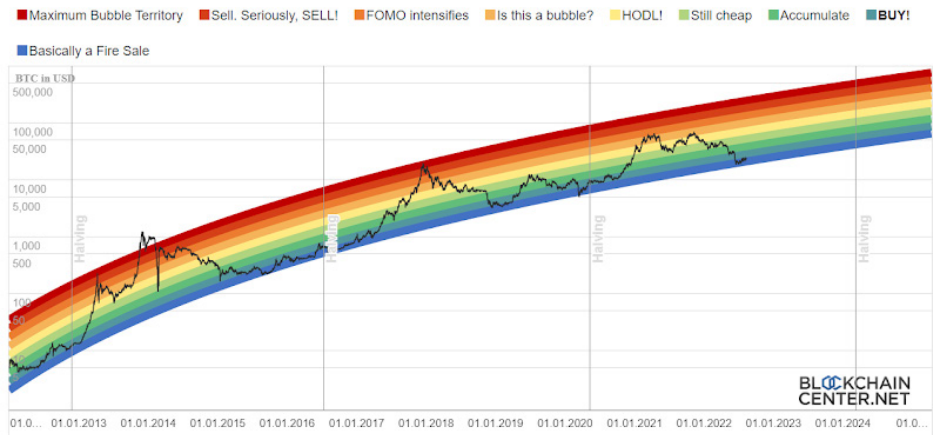
**Gráfico de Arco Íris**

O Gráfico de Arco Íris é uma proposta mais leve de se olhar para

os movimentos de longo prazo do bitcoin, ignorando os ruídos gerados pela volatilidade do dia a dia. As faixas das cores seguem uma regressão logarítmica (introduzida inicialmente no bitcointalk pelo avatar trolololo<sup>48</sup> em 2014). Esta previsão de preço é completamente arbitrária e sem nenhuma base além da progressão logarítmica, ou, em outras palavras: esse modelo é válido até o dia que deixar de ser (assim como todos os outros modelos).

É interessante notar, porém, que esta regressão foi feita em 2014 e conseguiu prever, com exatidão, o comportamento do preço no ciclo de alta de 2017-2018 e o ciclo de baixa de 2018-2019. De acordo com esse modelo, o movimento de 2020-2021 não teve um pico de bolha, e nem mesmo chegou a ter um grande período de FOMO. Também é interessante notar que esse gráfico colorido acertou o fundo do mercado de maio-julho de 2022.

Bitcoin Rainbow Price Chart  
(Log Scale)



### Valuation comparado

Uma outra alternativa de precificação para o bitcoin é comparar o seu market cap (valor total de mercado) atual com o market cap de outras reservas de valor. Mas, para fazer esta avaliação, é necessário, primeiro, entender melhor o conceito de reserva de valor.

A principal função de uma reserva de valor é, como o nome diz, a manutenção do poder de compra com o decorrer do tempo. Existem diversas opções de reservas de valor e, historicamente, o ouro foi considerado como a melhor alternativa.

As reservas de valor mais utilizadas no mundo atualmente são:

**Ouro:** reserva de valor mais tradicional, também possui utilização como joalheria e aplicações industriais. O ouro, entretanto, possui alguns pontos negativos como reserva de valor que são pouco comentados. 1) a custódia do ouro é arriscada, razão pela qual, geralmente, acaba sendo feita por bancos. Isso significa dizer que ele é facilmente confiável. 2) sua verificação é um processo altamente custoso e depende de alguns poucos especialistas e de seus equipamentos especializados. 3) como qualquer outra commodity, quando o preço aumenta, seus respectivos produtores são incentivados a utilizar sua capacidade produtiva ociosa para aumentar a produção. Ou seja, o próprio movimento de alta no preço dele gera, como consequência, um processo que, no futuro, resultará em um valor real menor para o próprio ativo, uma vez que ele se torna menos escasso.

**Imóveis:** quando o imóvel é visto como investimento e está sendo comprado para ser alugado ou revendido posteriormente. Ou seja, no cenário em que o imóvel não é visto como uma opção de moradia ou lazer. Todo brasileiro é traumatizado ou foi educado e aconselhado financeiramente por alguém que é traumatizado com a hiperinflação e o confisco do Collor. Todos já escutaram, por diversas vezes, que um imóvel é um ótimo investimento porque, além de preservar valor em um cenário de inflação, ninguém pode confiscá-lo. Contudo, além de gerarem obrigações tributárias (IPTU), contas e todo tipo de manutenção, os imóveis, quando alugados, podem ser fonte de verdadeiras dores de cabeça. Ou seja, imóveis são reservas de valor com custos fixos e incômodos constantes com a manutenção. Todos estes imóveis vistos como investimento tendem a ser substituídos pelo bitcoin como forma reserva de valor, uma vez que o bitcoin preserva melhor o seu capital (por não possuir custos e gastos fixos associados). Também vale ressaltar que o mercado imobiliário também é incentivado a construir mais imóveis quando os preços estão em alta, aumentando o estoque de imóveis.

**Ações:** idealmente, o mercado acionário reflete o crescimento das melhores empresas de determinado país. Com a mudança de paradigma que ocorreu no mundo nos últimos anos (juros reais negativos), cada vez mais as ações são vistas como reserva de valor em detrimento dos títulos de renda fixa. Prova disso é o desempenho das ações de Facebook, Amazon, Amazon, Netflix e Google em comparação ao resto do mercado acionário (a famosa

recuperação em K<sup>49</sup>). Ações de empresas deveriam, supostamente, servir para que os seus sócios e funcionários, que acreditam no projeto, tenham exposição aos lucros caso tal projeto se concretize. A maioria dos investidores não se aprofunda tanto nas empresas, e muitos inclusive preferem utilizar fundos passivos (conhecidos como ETFs) do que escolher empresas específicas. Estes são investimentos feitos pensando em conservar o poder de compra ao longo do tempo, ou seja, são investimentos em reservas de valor.

**Renda Fixa:** até pouquíssimo tempo, a renda fixa era vista como uma reserva segura e confiável. Porém, com a diminuição das taxas de juros em todo o mundo, o investimento deixou de preservar valor no tempo, visto que sua rentabilidade real passou a ser negativa, perdendo da inflação (isto ainda considerando a inflação oficial, que é um dado totalmente poluído). Basicamente, entramos em um mundo com juros reais negativos. Se considerarmos a inflação de ativos ao invés da inflação oficial, o poder de preservação de valor da renda fixa no tempo piorou significativamente mais. Hoje, a renda fixa poderia ser chamada de perda fixa.

**Fundos:** Existem tanto fundos que são focados exclusivamente em ações (FIAs), fundos multimercados (FIM) que focam nas melhores oportunidades do momento, fundos imobiliários (FII) que focam em administração de imóveis e geração de renda passiva, fundos passivos (ETFs), fundos de recebíveis ou direitos creditórios para investidores profissionais, aporte inicial de 1mi (FIDCs), e também existem os fundos que investem em outros fundos (FICs). Todos estes fundos são, no lato sensus, reservas de valor também. Isso significa que quem investe nesses fundos não investe necessariamente por acreditar nas teses, e sim como uma maneira de preservar o seu valor de compra no futuro. Ou seja, caso surja uma maneira mais eficiente de preservar valor de compra e transmitir este valor de compra para o futuro, estes fundos (e todas as outras classes de reserva de valor menos eficientes) serão parcialmente desmonetizados.

Se o ouro é historicamente a melhor reserva de valor, o bitcoin é o ouro digital, ou ouro 2.0 caso você prefira (mesmo bancos como o JP Morgan<sup>50</sup> já vem reconhecendo o bitcoin como o ouro digital). Ele apresenta quase todas as características positivas do ouro (não é possível fazer joias com o bitcoin), mas o bitcoin também melhora diversas características do ouro, sendo inconfiscável, incensurável e descentralizado. O que significa

que o bitcoin não pode ser atacado com sucesso por governos, diferente do ouro que se encontra todo apreendido pelos governos.

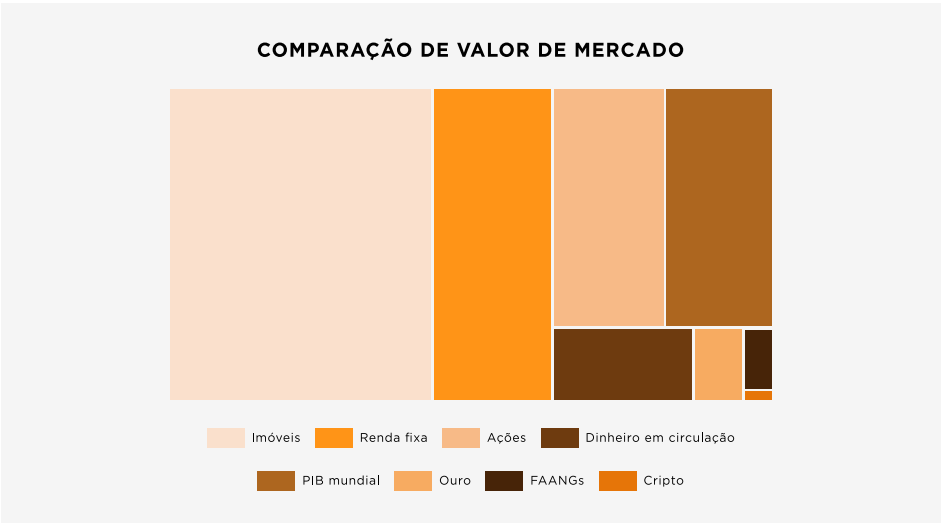
### Comparando os market caps

Pensando que o bitcoin é, no mínimo, igual ao ouro na qualidade de reserva de valor, o market cap destes dois ativos teria que ser igual.

Atualmente, o market cap do ouro está em \$12 trilhões e o market cap do bitcoin está em \$726 bilhões. Isso significa que o market cap do bitcoin teria que multiplicar por ~16.5x para se equiparar ao market cap do ouro. Se a cotação do bitcoin de hoje (21/02/2022) é de ~\$38.300, então a cotação do bitcoin quando os market caps estiverem iguais será de ~\$632.000.

Como o bitcoin é uma reserva de valor muito superior ao ouro, este seria só o valor mínimo para o bitcoin. Considerando ainda que o bitcoin tende também a desmonetizar as demais reservas de valor (imóveis, investimentos nos mercados acionários e até mesmo a renda fixa), essa previsão de cotação em \$632.000 ainda é uma previsão extremamente conservadora.

O mercado imobiliário global possui um valor total estimado em \$280 trilhões, enquanto que o mercado de renda fixa possui cerca de \$130 trilhões alocado e o mercado acionário global cerca de \$90 trilhões. Se considerarmos que parte destes mercados será desmonetizada por uma reserva de valor superior, a conclusão é óbvia: o valor de mercado do bitcoin ainda está muito abaixo do seu potencial.



## Bitcoin como um paraíso fiscal

Primeiro vamos explicar o que é um paraíso fiscal. Os países que são conhecidos como paraísos fiscais são aqueles que oferecem tributação baixa para estrangeiros, atraindo capital de todas as partes do mundo. Regras rígidas de sigilo bancário são uma característica comum nestes países, fazendo com que os paraísos fiscais sejam constantemente relacionados a lavagem de dinheiro e a crimes financeiros. De forma resumida, paraísos fiscais são regiões com regras fiscais flexíveis, sobretudo quando comparadas às normas do direito internacional para combater crimes, como sonegação de impostos e lavagem de dinheiro. A Receita Federal considera como paraísos fiscais estados ou regiões com tributação de renda menor que 20% ou que não tenham regras de transparência a respeito de titularidade ou composição societária de empresas.

Todas estas características que descrevem os paraísos fiscais podem ser utilizadas também para descrever o bitcoin. O capital alocado em bitcoins jamais será taxado dentro do sistema bitcoin, o que significa dizer que as taxas associadas a preservar o seu capital na reserva de valor chamada bitcoin são nulas, enquanto que o dinheiro aplicado em outros paraísos fiscais são taxados anualmente pelos bancos desses países.

O bitcoin também não se importa com titularidade e todo usuário da rede é conhecido pelo conjunto de letras e números que compõem seu endereço, e não pelo seu nome e CPF. O bitcoin é a rede mais inclusiva do mundo justamente pela sua incapacidade de discriminar qualquer indivíduo que a esteja utilizando.

Como a própria função dos paraísos fiscais é fugir de fiscalização e taxação, estimar o valor total neles mantido é uma tarefa difícil. Existem estimativas<sup>51</sup> que variam entre \$8,7 trilhões (Gabriel Zucman, Universidade de Berkeley) a \$36 trilhões (James. S. Henry, economista).

Vale frisar que o bitcoin não desmonetizará apenas o ouro, ou apenas o mercado imobiliário ou apenas os paraísos fiscais. Ele desmonetizará todos estes mercados ao mesmo tempo, conforme a sua hipótese de valor (de ser uma reserva de valor confiável, inconfiscável e sem erosão de capital via impostos ou taxas) ficar cada vez mais clara.

O valor total que o bitcoin desmonetizar de cada uma dessas classes de ativos somados, portanto, determinará o preço final do bitcoin. Qualquer

modelo de valuation comparado que não leva isto em conta estará com premissas falhas.

De acordo com o Institute for International Finance, o tamanho global dos ativos financeiros era de \$900 trilhões. Se o bitcoin capturar 5% deste mercado, o valor do bitcoin equivale a esses 5% (\$45 trilhões) dividido pelo número de moedas (21 milhões). Ou seja, um valor estimado de \$2.14 milhões de dólares por bitcoin. Se o bitcoin capturar 10% do mercado de ativos globais, o valor estimado é superior a \$4 milhões por bitcoin.

O processo de escolha de reserva de valor é um processo de seleção natural, e o Superpredador (o predador que reina sobre uma cadeia alimentar inteira) deste mercado é o bitcoin. Parece bom demais para ser verdade né? Muita torcida e pouco fundamento? Vamos aos próximos modelos de precificação.

### **Custo energético como valor justo**

A mineração do bitcoin é um processo que demanda alta quantidade de energia. Isso, inclusive, torna este processo alvo de muitas críticas infundadas. Ignorando as críticas e pensando na relação entre o custo energético e o valor do bitcoin, uma pergunta surge: "será que o valor justo de um bitcoin pode ser calculado com base na energia utilizada na sua mineração?

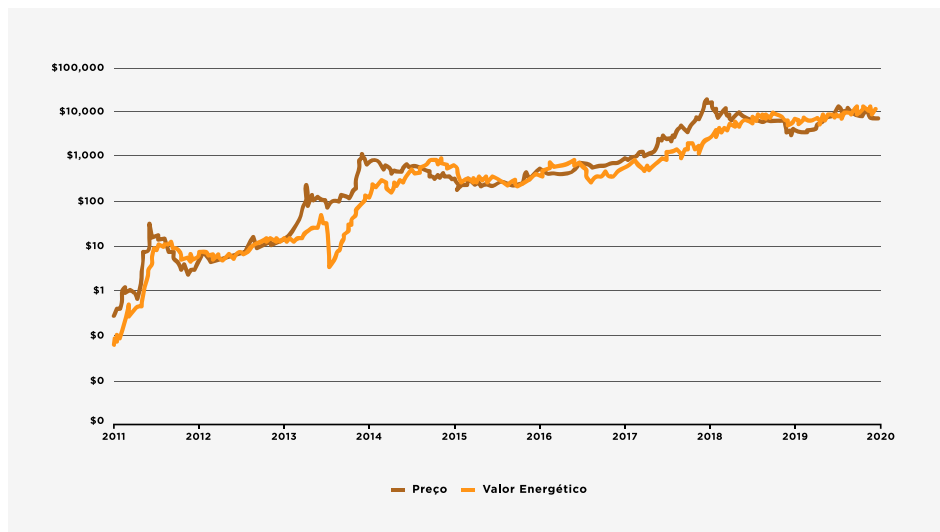
A hipótese apresentada por Charles Edwards<sup>52</sup> é a de que o valor do bitcoin pode ser expresso em função das seguintes variáveis: energia utilizada para a sua mineração, taxa de crescimento do estoque de bitcoins e valor em dólares da energia, expresso por uma constante (f). Estas variáveis levam à fórmula do Valor Energético do bitcoin (V) abaixo:

$$V = \frac{\text{Energia Utilizada}}{\text{Taxa de crescimento do estoque}} \times f$$

Essa fórmula também pode ser alterada para representar o Valor Energético do bitcoin (V) em função da Energia Utilizada no processo. Este modelo é profundamente trabalhado no artigo original, se alguém quiser se aprofundar no tema, a leitura é recomendada. O resultado obtido pelo modelo



pode ser observado na imagem abaixo e demonstra como a correlação entre o Valor Energético do bitcoin e o seu preço é alta.



O valor energético varia de acordo com a oferta de bitcoins e da quantidade de processamento computacional, e portanto energia, que está sendo alocada na rede.

Uma conclusão que pode ser extraída deste modelo é a de que a saúde do ecossistema de mineração está diretamente ligada ao valor do bitcoin. Isso significa dizer que a utilização de mais energia pelos mineradores aumenta o valor intrínseco do bitcoin, e que o contrário é verdadeiro também, isto é, uma diminuição no uso de eletricidade pela rede gerará uma diminuição do valor do bitcoin.

Como este modelo utiliza dados reais do consumo energético, ele não pode ser usado de maneira preditiva para o preço futuro do bitcoin, uma vez que não se sabe o quanto de energia a rede continuará usando.

## S2F e S2FX

Os modelos de stock-to-flow (S2F) e stock-to-flow utilizando classes de ativos para balizar o modelo (S2FX) são dois modelos bastante comentados pois se baseiam puramente na escassez e na oferta para estimar o preço justo do bitcoin.

Originalmente, os modelos de stock-to-flow foram desenvolvidos para commodities, como ouro, prata e pedras preciosas em geral. A ideia básica

por trás destes modelos é analisar a escassez de determinado ativo e, com isso, determinar um “valor justo” para o mesmo. Este “valor justo” aumenta conforme a dificuldade de obtenção de determinado ativo aumenta, ou seja, conforme a dificuldade de se obter mais de determinada commodity aumenta. Assim, o S2F modela o preço a partir da variação da oferta de determinado ativo.

De acordo com o PlanB<sup>53</sup>, a escassez consegue ser quantificada pela relação stock/flow, onde “stock” é o tamanho da oferta atual e o “flow” é a produção anual de determinada commodity. A relação inversão (flow/stock) também é conhecida como taxa de crescimento da oferta. A hipótese principal deste modelo é que a escassez (medida em termos de stock/flow) gera valor por si só.

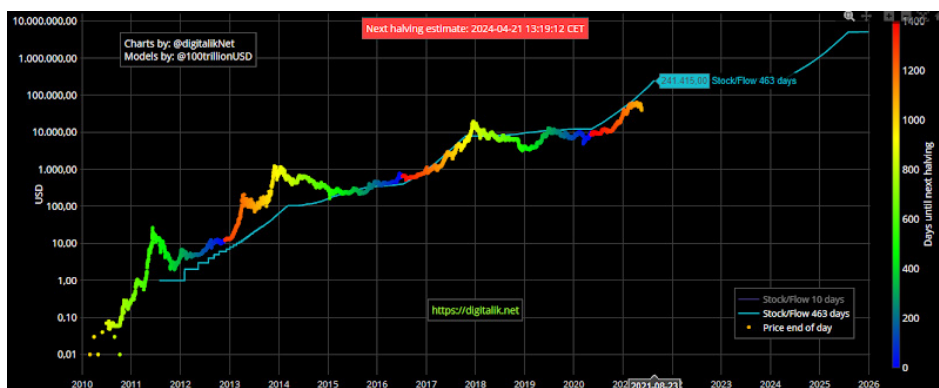
O PlanB propôs dois modelos diferentes de stock-to-flow para o bitcoin:

1) o modelo de S2F, que leva em conta a equação de oferta e demanda e o tempo;

2) e segundo modelo associa o bitcoin com outras classes de ativos (prata e ouro) e deixa de considerar o tempo como um fator importante. Este modelo é conhecido como S2F com outros ativos (S2F cross assets), ou simplesmente S2FX

### **OK, mas quais preços esses modelos preveem?**

O modelo S2F mostra que o preço médio do bitcoin em um ciclo de quatro anos (entre maio de 2020 e início de 2024) estará entre \$100.000 e \$120.000. No próximo ciclo de halving (2025-2029), o preço médio do ciclo de quatro anos deve variar entre \$1.000.000 - \$1.200.000. Já o modelo S2FX mostra que o preço médio do bitcoin neste ciclo de halving estará entre \$240.000 e \$310.000. No próximo ciclo de halving (2025-2029) o preço chegaria até \$5.000.000.



Modelo S2FX do PlanB<sup>54</sup>.

Originalmente, o modelo S2F foi publicado em março de 2019, com o bitcoin valendo ~\$4.000 e com market cap de \$70 bilhões. No artigo original, o preço do bitcoin chegaria a \$55.000 após o halving de 2020, com um market cap de \$1 trilhão. O que de fato ocorreu ao longo de 2021. Ou seja, em 2019, no auge do ciclo de baixa, o modelo foi capaz de prever o comportamento do preço futuro com grande precisão. E previu este preço futuro prevendo uma multiplicação de 13.75x.

Se você quiser se aprofundar mais nesses dois modelos, os artigos originais do PlanB sobre o S2F<sup>55</sup> e S2FX<sup>56</sup> são boas fontes de pesquisa. Hoje em dia, estes modelos talvez sejam os mais reconhecidos, além de serem citados com confiança por investidores institucionais e por revistas de investimento como a Forbes<sup>57</sup>.

Mas estes modelos de stock-to-flow não levam em conta as emoções humanas, então ele é só uma ilustração do aumento de escassez de acordo com os halvings, não um modelo preditivo.

## Modelo Composto da Fidelity

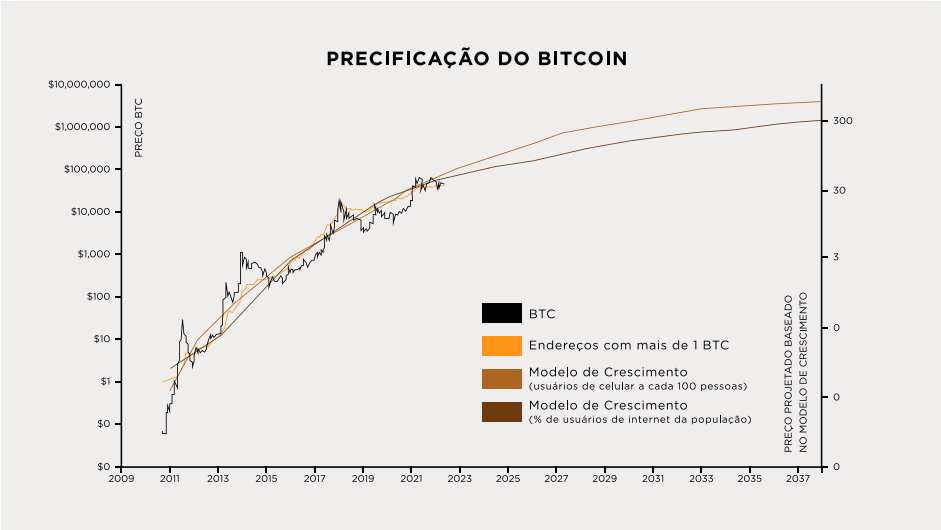
A Fidelity Investments, uma das maiores gestoras de ativos do mundo, utiliza um modelo misto para precificar o bitcoin em relatório sobre o ativo. Este modelo misto leva em conta:

a) o modelo de S2F do Planb para representar a oferta

b) a demanda é modelada com base no modelo de curva em S de adoção de tecnologia. A Fidelity usou como premissa que a curva S de adoção de novos usuários do bitcoin é semelhante a curva de adoção dos telefones

celulares.

O gráfico obtido pela sobreposição destas duas curvas pode ser observado abaixo. Este gráfico mostra que os modelos de oferta e demanda estão bem alinhados e ambos prevêem um aumento contínuo dos preços.



Modelo composto da Fidelity.

Vale notar que, no futuro, os modelos começam a divergir. Isto ocorre porque a curva S de adoção de novas tecnologias costuma atingir um platô, enquanto que no modelo S2F a tendência se mantém exponencial. A conclusão final do relatório da Fidelity é que o modelo S2F provavelmente é otimista e que, possivelmente, a curva representada pela demanda é mais plausível.

Tenho uma leitura ligeiramente diferente do modelo da Fidelity: acredito que o preço do bitcoin vem seguindo as duas linhas de tendência. A curva de adoção em S tem marcado o preço nos ciclos de baixa e o S2F está marcando os ciclos de alta. A tendência que o gráfico da Fidelity mostra é que este padrão se mantenha pelos próximos dois ciclos pelo menos. Depois, no futuro mais distante (talvez a partir de 2030), o platô representado pela curva S de adoção faz sentido como cenário base de um mundo já hiperbitcoinizado (quando as coisas forem cotadas em satoshis e a reserva de valor mundial for o bitcoin, e não o dólar), o que pode acontecer num futuro não tão distante. De acordo com diversos gestores renomados como

Ray Dalio<sup>58</sup>, Bill Miller<sup>59</sup>, Paul Tudor Jones<sup>60</sup> e Stanley Druckenmiller<sup>61</sup>, o dólar perderá o status de moeda forte mundial nos próximos 15 anos).

Este pensamento é interessante pois o modelo S2F não leva em conta a variação das emoções do ser humano. E estas variações emocionais sempre são fatores determinantes para o comportamento do preço dos ativos no mercado. Por isso que o preço do bitcoin ultrapassa o modelo S2F nos ciclos de alta e cai abaixo dele nos ciclos de baixa.



Ciclo de emoções humanas de acordo com a variação do preço de um determinado ativo.

Claro que é sempre legal ver projeções futuras de preços. Ter pontos fixos para poder traçar projeções conforta o nosso psicológico e passa segurança. Mas modelos sempre são somente isso: modelos. Nenhum modelo nunca será capaz de realmente prever o futuro pois ele sempre será, por definição, reducionista em algum ou diversos aspectos.

Particularmente, sempre preferi pensar nas coisas a partir das suas premissas do que na derivação destas premissas, ou seja, entendendo os fundamentos das coisas ao invés de ficar tentando prever como o preço irá variar no próximo ano. Nesse sentido, os bitcoinheiros têm um meme que é a melhor precificação na minha opinião: o bitcoin possui NGU Tech. O que NGU quer dizer? Simples, Number Go UP ("o número sobe" em inglês), que será explicado mais a fundo no próximo capítulo. Entendendo os fundamentos centrais da tese do bitcoin, como a anti-fragilidade da rede baseada em uma

descentralização verdadeira e a política de expansão monetária previsível e imutável, a volatilidade do preço deixa de ser algo importante no curto prazo. No longo prazo só existe uma alternativa: Number Go Up.

Inicialmente, falar que o bitcoin possui tecnologia NGU parece uma brincadeira superficial, mas conforme você passa a entender mais sobre a oferta e a demanda do bitcoin, você entende que só existe uma opção para o preço: pra cima. Mas o NGU será tema do próximo capítulo, antes, no entanto, vamos pensar no aspecto geracional do bitcoin.

### Haters Go Down

Uma reflexão interessante também é que a grande maioria dos detratores do bitcoin são pessoas, em geral, mais velhas e menos abertas à tecnologia, enquanto a maioria dos bitcoinheiros são da geração millennial. Além disso, a maioria dos jovens da geração Z convive com o bitcoin desde que eles têm memória. Para eles, o bitcoin é só mais um ativo, tão válido como um fundo imobiliário ou uma ação da bolsa, e não um patinho feio disruptor, complexo e exótico.

O mesmo processo sempre ocorreu na adoção de qualquer nova tecnologia disruptiva e, com certeza, também existiram motoristas de carruagens e charretes, idosos ou não, que reclamavam da invenção do carro e nunca se adequaram ao mundo moderno do início do século passado. Quem escutou o seu conselho e investiu em carruagens não fez um bom negócio, como as imagens abaixo ilustram.

Trânsito na 5th Avenue de Nova Iorque  
Manhã de Páscoa de 1900



Source: US National Archives.

Trânsito repleto de charretes e com apenas um automóvel no início de 1900 em Nova Iorque.

Trânsito na 5th Avenue de Nova Iorque  
Manhã de Páscoa de 1913



Source: George Grantham Bain Collection.

Trânsito repleto de automóveis e com apenas uma charrete em <sup>1913</sup> em Nova Iorque, mostrando que em apenas treze anos houve uma transição completa de um modal de transporte para o outro.

Em seu livro “A Estrutura das Revoluções Científicas” (1962), Thomas Kuhn descreve o processo de mudança de paradigmas. Basicamente, existem mudanças de compreensão (paradigmas científicos, na linguagem deste filósofo) em determinados temas que ocorrem de tempos em tempos. Estas mudanças sempre enfrentam resistência de setores mais conservadores. Poucas coisas conseguem convencer estes setores conservadores, mas como estes ambientes são formados pelos pesquisadores mais velhos, a ciência tende a evoluir conforme os mais antigos vão sendo substituídos pelos mais novos, os quais já entendem o novo paradigma. Existe uma famosa frase do Max Planck, pai da física quântica, que faz alusão clara a essa questão: “A ciência avança de funeral em funeral” que faz alusão clara a essa questão.

Um processo semelhante ocorre no Cerrado, onde queimadas naturais estimulam o rebrotamento de diversas espécies vegetais. No Cerrado, o fogo gera regeneração no ecossistema<sup>62</sup>. Na evolução do conhecimento, a aposentadoria e morte dos conservadores e arcaicos gera avanços, pois críticas ultrapassadas deixam de ser relevantes. Por exemplo, o economista e ganhador do Nobel de economia Paul Krugman é um grande crítico do bitcoin. No primeiro momento, esse fato pode causar certa apreensão, mas depois que pesquisamos sua opinião sobre a internet<sup>63</sup> é possível notar um padrão: “Até 2005 mais ou menos, vai ficar claro que o impacto da Internet na economia não será maior que o impacto das máquinas de fax”. Mostre essa

frase para um millennial e se prepare para ver ele dando risada. Atualmente, uma resposta bastante comum a comentários deste economista é "Quem é Paul Krugman e o que é um fax?"

A mesma coisa ocorrerá com o bitcoin: conforme os mais velhos forem se aposentando e morrendo, serão os mais jovens que irão alocar o capital passado adiante. Então o importante não é somente a opinião dos mais velhos, que possuem o capital hoje em dia, mas sim o que será feito com este capital daqui a 5, 10 ou 20 anos.

Se pergunte: você conhece algum millennial que se importa com ouro?

Que queira comprar um imóvel? Que confia no governo e nas instituições?

Hoje em dia, e cada vez mais no futuro, os jovens não fazem distinção entre o virtual e o real. Para os millennials, o virtual é real e a palavra "analógico" possui uma conotação bastante negativa, quase uma ofensa.

Será mesmo que os jovens irão preferir reservas de valor analógicas como o ouro ou um imóvel?

Acredito que não. Então, pra mim, a precificação do bitcoin é bem simples: Number Go Up numa janela de tempo grande o suficiente.



## CAPÍTULO 7

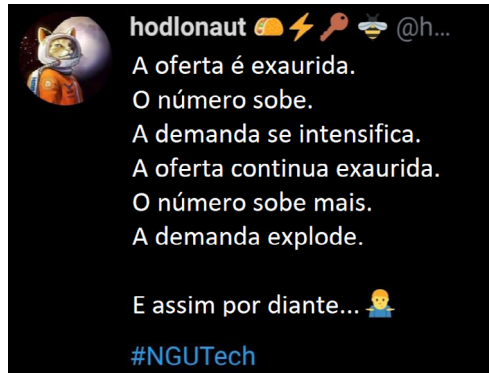
# A TECNOLOGIA NGU

Como falamos no capítulo anterior, o bitcoin possui a tecnologia NGU. Mas o que isso significa? É isso que este capítulo irá explicar.

Diferentemente das outras formas de bens monetários, o bitcoin ainda está no início do seu processo de adoção. O que significa que, além do grupo de características que impedem a expansão arbitrária e desenfreada da base monetária, ele também apresenta uma faceta extremamente benéfica para os usuários que adotarem esta nova forma de dinheiro: a tecnologia NGU.

O termo NGU vem do inglês “Number Go Up”, ou “o número sobe” em tradução literal, e é um meme bastante utilizado para descrever uma das principais características do bitcoin: os ciclos de alta do preço, em escala logarítmica, que ocorrem após os halvings.

Em linguagem memética, seria algo como “o foguete não tem ré!”. Inicialmente, a tecnologia NGU parece uma brincadeira superficial, mas conforme você passa a entender mais sobre a oferta e a demanda do bitcoin, você entende que só existe uma opção para o preço do bitcoin no longo prazo: foguete não tem ré!



Tweet do hodlonaut, um bitcoinheiro conhecido na comunidade internacional, descrevendo sucintamente como a tecnologia NGU funciona.

E por que o foguete não tem ré?

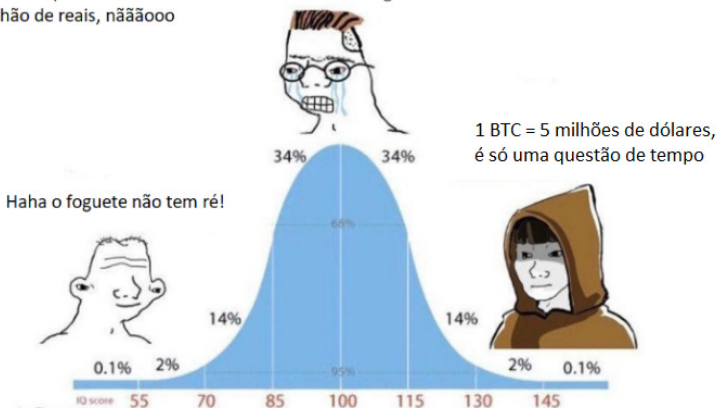
Resumidamente, nunca existiu uma reserva de valor digital, ou seja, nunca existiu uma reserva de valor teletransportável e imaterial, com efeito de rede, oferta inelástica e um “culto religioso” a divulgando e protegendo. O que isso tudo quer dizer? Entendendo os fundamentos centrais da tese do bitcoin, como a anti-fragilidade da rede baseada em uma descentralização verdadeira e a política de expansão monetária previsível e imutável, a volatilidade do preço no curto prazo deixa de ser algo importante.

No longo prazo só existe uma alternativa: Number Go Up.

Para explicar o porquê disso, vamos abordar 5 fatores que embasam a tecnologia NGU.

Nãããoo, o bitcoin é uma bolha, igual as tulipas!

Nãããoo, ele é dinheiro de criminoso. Você não consegue usar ele numa padaria. Nãããooo. 1 bitcoin nunca vai chegar a 1 milhão de reais, nãããooo



## 1. Curva de adoção do bitcoin

Compreender como a adoção desta nova tecnologia monetária está ocorrendo é o primeiro passo para entender a tecnologia NGU. Isso porque adoção significa aumento de demanda.

Todas as tecnologias apresentam um processo de adoção que segue o padrão de uma curva em S, como é representado na imagem com as curvas de adoção das tecnologias (apresentada no capítulo 5). Nela, a inclinação da curva representa a taxa de adoção de determinada tecnologia.

Repare na inclinação da curva de adoção dos telefones celulares (amarelo ouro). Em um período aproximado de uma década e meia a adoção dos celulares passou de incipiente, com menos de 10% da população possuindo um, para uma taxa de adoção superior a 90% dos americanos. O modelo divulgado pela Fidelity utiliza a adoção dos celulares como modelo de piso para o preço do bitcoin, enquanto o modelo do stock-to-flow marca as altas do preço.

A adoção do bitcoin e do ecossistema das criptomoedas como um todo vem ocorrendo em alta velocidade e os números dessa adoção, quando analisados, se assemelham com a taxa de adoção da internet. Nessa comparação, o bitcoin ainda está com o mesmo grau de adoção que a internet possuía no final dos anos 1990s, com cerca de 200 milhões de usuários.

De acordo com estes modelos, ainda é bastante cedo na curva de adoção e, seguindo o padrão atual, os próximos anos serão de NGU. Ou, em outras palavras, se pergunte: você gostaria de ter investido na Amazon no final dos anos 1990s? Agora você pode investir em um ativo que está passando por uma curva de adoção semelhante, com a diferença de que este ativo (o bitcoin) não possui nenhum concorrente competitivo.

## Cotação da ação da Amazon entre 1997 e 2022



## 2. Exército do DCA

Além disso, o bitcoin conta com um “exército de formigas” de bitcoinheiros (conhecido também como exército do DCA<sup>64</sup>) espalhado pelo mundo. Este exército de formigas já aderiu ao padrão bitcoin e que todo mês converte o seu dinheiro fiat em satoshis, independente do preço. A estratégia de comprar um pouco todo mês é bastante utilizada entre os bitcoinheiros que fazem HODL (quem compra bitcoin para o longo prazo e não se importa com as variações de curto prazo do preço). Soma-se a isso a dinâmica imposta pelos halvings e a diminuição gradual de emissão de bitcoins com o passar do tempo. A oferta de bitcoins disponíveis está diminuindo continuamente, fazendo com que o preço suba por uma simples questão de oferta e demanda.

A imagem do halving (no glossário) mostra o ciclo de vida de um bitcoin, que tem início quando ele é emitido como recompensa do bloco minerado. Esses bitcoins ficam disponíveis na oferta em circulação das exchanges, e são comprados e vendidos por traders e mãos de alface, que compram e vendem satoshis de acordo com as oscilações de curto prazo.

Até o momento em que um HODLER de longo prazo compra estes satoshis. A partir deste momento, estes sats estão efetivamente fora da oferta em circulação por, provavelmente, um longo período de tempo, visto que esses HODLers já entenderam que o bitcoin possui a tecnologia NGU como uma das suas vantagens e que guardar sua energia monetária em bitcoin é a melhor forma de preservação de capital.

### **O Modelo da Banheira Furada**

Um modelo mental que ajuda a ilustrar o efeito do exército de formigas que faz compras recorrentes é o modelo da banheira furada já comentado no capítulo 5 sobre os fundamentos do bitcoin.

Imagine que a quantidade de água que sai da torneira para encher a banheira são os novos bitcoins que são emitidos como recompensa do bloco no processo de mineração e que a água já acumulada na banheira são os bitcoins à venda nas exchanges (a oferta líquida). O exército de formigas representa diversos furos nessa banheira e seu comportamento de compras recorrentes sem a intenção de venda vai drenando a liquidez da banheira. Conforme a adoção do bitcoin vai aumentando e mais HODLers passam a utilizar a estratégia de compras recorrentes, maior a quantidade de furos nessa banheira.

No início, a vazão de água na torneira é muito maior que a vazão dos furos, o que significa que a banheira está acumulando mais água. Neste exemplo, isso significa que o preço do bitcoin tende a diminuir, pois mais bitcoins estão em circulação nas exchanges.

Conforme o tempo passa e a vazão da torneira é diminuída pelos halvings, e, ao mesmo tempo, a vazão dos furos vai aumentando graças à adoção de novos HODLers, a tendência é que a banheira vá esvaziando. Nesse exemplo, isso significa que o preço tende a subir até achar um novo ponto de equilíbrio; isso porque existe mais demanda pelos bitcoins do que bitcoins disponíveis nas exchanges. O resultado disso é que o preço sobe (NGU), fazendo que alguns HODLER vendam seus bitcoins, o que nesse modelo significa que o furo passa a agir como uma torneira e passa a colocar água na banheira novamente.

Vale ressaltar, entretanto, que um HODLER é alguém que estudou e construiu uma grande convicção em relação à tese do bitcoin, então faz

sentido supor que ele venderá o mínimo de satoshis possível. E conforme o preço do bitcoin sobe, estes HODLers que precisam vender seus bitcoins, precisarão vender cada vez menos satoshis a cada mês para pagar o seu custo de vida, uma vez que o preço do bitcoin subiu e esses satoshis estão conseguindo comprar mais moeda fiat. Então, o fato do preço subir também diminui a quantidade de satoshis que os HODLers terão que vender eventualmente.

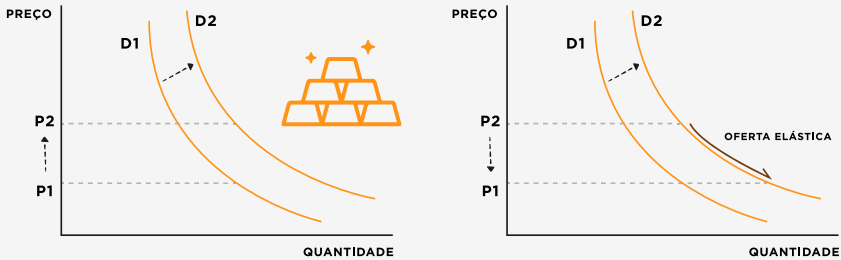
### 3. Oferta Inelástica

As imagens a seguir são um modelo visual simples que ilustra como o preço, a demanda e a oferta geralmente variam. São utilizados os exemplos do ouro, mas na verdade qualquer outro bem que não possui a tecnologia NGU poderia ser utilizado como exemplo, e do bitcoin, que possui a tecnologia NGU.

O modelo do ouro mostra dois momentos de demanda distintos, representados pelas curvas D1 e D2. Quando a demanda D1 aumenta, se tornando D2, o preço P1 também aumenta, se tornando P2, pois a quantidade de ouro permaneceu constante. Contudo, como o preço P2 é maior que o preço inicial P1, o incentivo para os mineradores de ouro é aumentar a produção deste bem mineral. Isso acontece porque a oferta do ouro (e de qualquer outra coisa que não utilize a tecnologia NGU) é elástica. Com um preço mais elevado, novas jazidas de ouro se tornam viáveis economicamente e mais ouro é produzido, fazendo a quantidade de ouro em circulação aumentar.

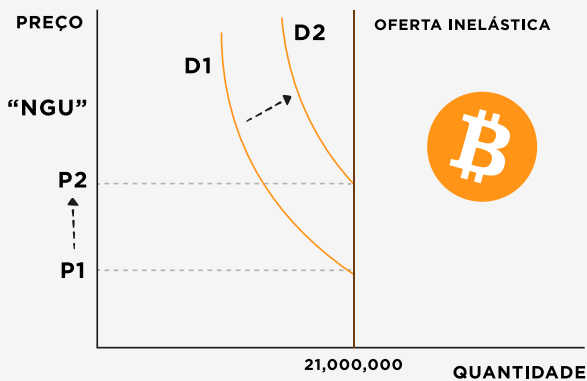
Ou seja, como a oferta do ouro é elástica, os produtores conseguem aumentar sua produção, aumentando a quantidade de ouro em circulação e levando o preço de P2 de volta para P1, mesmo que a demanda se mantenha superior ao momento inicial (D1).

### SEM TECNOLOGIA NGU



Quando o mesmo modelo é aplicado ao bitcoin, esta dinâmica não ocorre, uma vez que a oferta de bitcoins é inelástica. Isso significa que não serão produzidos mais bitcoins só porque a demanda por esses bitcoins aumentou. E se a demanda aumentou e a oferta não pode ser alterada, só resta uma alternativa para o preço: number go up!

### TECNOLOGIA NUMBER GO UP



O fato da oferta do bitcoin ser inelástica significa que, mesmo com o preço subindo exponencialmente, é impossível aumentar a produção de bitcoins. Isto ocorre, pois, a taxa de emissão de bitcoins é estabelecida por código e não pode ser alterada sem que a rede entre em consenso, o que vai

contra a estrutura de incentivos, já que não é benéfico para os HODLers diluir a quantidade de bitcoins criados. Ou seja, não serão minerados mais de 21 milhões de bitcoins e essa mineração seguirá o cronograma inicialmente delimitado no protocolo, diminuindo a remuneração por bloco minerado a cada halving.

#### 4. O valor nominal do bitcoin tem relação com a base monetária fiat

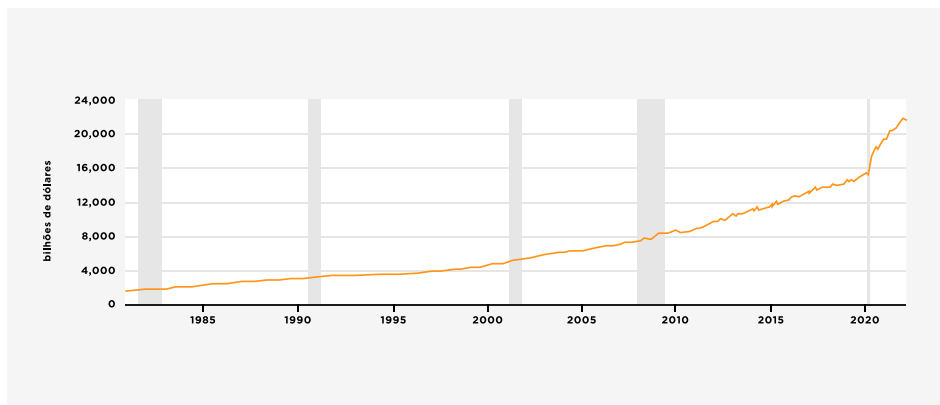
Para entender o movimento do preço do bitcoin, também faz sentido entender como as moedas fiat funcionam. De uma maneira muito simplificada, podemos dizer que a tendência natural de toda moeda fiat é a expansão da base monetária, o que é verdade universal para todas as moedas fiat que já existiram e existem hoje em dia. Ou seja, a oferta das moedas fiat, ao invés de serem limitadas como a do bitcoin, tendem ao infinito até que elas percam todo o seu valor e sejam substituídas por outra moeda fiat, que também perderá todo o seu valor.

E o que a oferta de um bem tender ao infinito significa na prática? Qualquer pessoa que lembre das aulas de matemática sabe que um valor qualquer (vamos usar X) dividido por 2 é o dobro desse valor X dividido por 4, que é o dobro desse valor X dividido por 8 e assim sucessivamente. Isso significa que se esse valor é dividido por infinito, não importa qual seja o valor inicial, ele tende a zero. E como a emissão de moedas fiat tende ao infinito, isso significa que elas não preservam valor no tempo.

$$\frac{X}{2} = ? \quad \frac{X}{4} = ?/2 \quad \frac{X}{\infty} = 0$$

Forma simples de ilustrar o conceito de que qualquer coisa dividida por infinito tende a zero.





O  $M^2$  reflete bem a impressão de dinheiro pelo FED (o banco central americano). Pode parecer que ela não está tendendo ao infinito, mas vamos sempre lembrar que quem citou que o FED tem dinheiro infinito foi um dos seus diretores, o Neel Kashkari, presidente do Banco Central de Minneapolis, que disse<sup>65</sup>: “existe uma quantidade infinita de dinheiro no FED”.

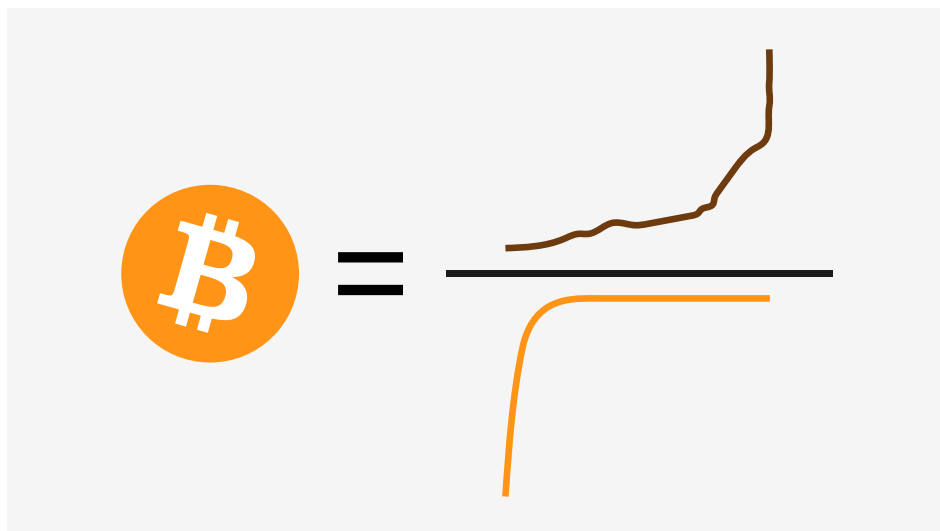


E o que aconteceu com o dólar devido a esse processo de expansão da base monetária (que é o nome bonito para “imprimir dinheiro a rodo”).

Como ficou implícito na discussão acima, o valor de qualquer coisa depende de dois fatores: a oscilação do seu próprio valor e a oscilação da moeda que você está usando como régua. Ou seja, mesmo que o bitcoin fique estável, o simples fato das moedas fiats estarem perdendo valor já significa que ele está ganhando valor em termos relativos. E, apesar de muitos

reclamarem sobre a volatilidade, a verdade é que o bitcoin é estável e possui uma emissão programada. O grosso da inflação do bitcoin já ficou para trás, e agora já estamos em 19 milhões de bitcoins emitidos dos 21 milhões totais que serão emitidos até 2140.

E o que isso significa? NGU em termos da moeda fiat. A imagem abaixo ilustra conceitualmente esse pensamento. Nela, a linha verde representa a quantidade de moeda fiat em circulação e a linha laranja a quantidade de bitcoins em circulação. O preço do bitcoin, assumindo que ele manterá seus fundamentos, refletirá essa equação esquemática.



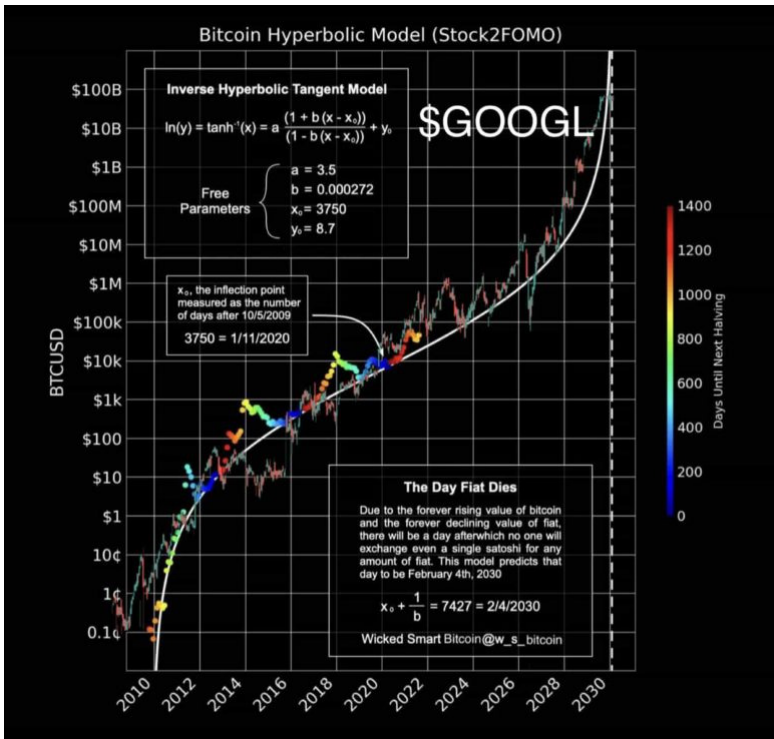
## 5. O Modelo Stock-to-FOMO

A questão apresentada no item 4 é, por si só, extremamente altista. Mas ela também é extremamente simplista e não leva em conta o aumento da demanda. O mesmo pode ser dito do modelo stock-to-flow. Mas como modelar a demanda crescente pelo bitcoin ao longo do tempo e o seu efeito dela no preço?

O modelo de precificação mais altista de todos, conhecido como stock-to-FOMO (uma brincadeira com o stock-to-flow) ou modinha-FOMO, faz justamente isso. FOMO é o acrônimo em inglês da expressão "Fear Of Missing Out", o que em português significa "medo de ficar de fora". É a famosa "dor de corno" de ver um amigo seu ganhando dinheiro e você não ganhar

nada. O FOMO é um sentimento bem comum no mercado de investimento e está associado aos ciclos de alta tanto do bitcoin como de qualquer outro ativo financeiro.

Para exemplificar como o FOMO atua, a imagem abaixo mostra o desempenho da ação do Google. Os últimos anos marcaram o FOMO do mercado institucional em relação a ações de tecnologia e o trade que mais rendeu no mercado foi justamente comprar as empresas digitais com efeitos de rede já estabelecidos, visto que elas estavam surfando a curva de adoção da tecnologia internet.



Como todo bitcoinheiro sabe, existe e sempre existirá uma teoria dos jogos de alta intensidade ocorrendo relacionada à adoção do bitcoin. Isso significa que grandes players e entidades tendem a entrar em um FOMO exacerbado conforme a adoção do bitcoin for avançando e eles forem entendendo as ramificações da oferta inelástica associada ao efeito dos halvings na oferta em circulação.

O bitcoin possui uma característica em termos de adoção que o

diferencia de todas as outras empresas com efeitos de rede associadas à internet. Nessas empresas, o life time value (LTV), que é uma métrica para estimar o quanto de dinheiro um usuário irá mobilizar ao longo de toda a vida nessa empresa. Vamos usar o exemplo da Amazon: digamos que o meu LTV nela seja de R\$50.000,00, ou seja, eu irei gastar cerca de cinquenta mil reais na Amazon ao longo da minha vida. Esses R\$50.000,00 não serão utilizados ao mesmo tempo, e sim disperso ao longo de décadas. Ou pensando no exemplo do Google: talvez você assine o Google Drive e gaste R\$10 reais por mês, além de navegar pela internet um tempo relativamente constante, o que gera receitas pequenas e constantes para o Google ao longo do tempo.

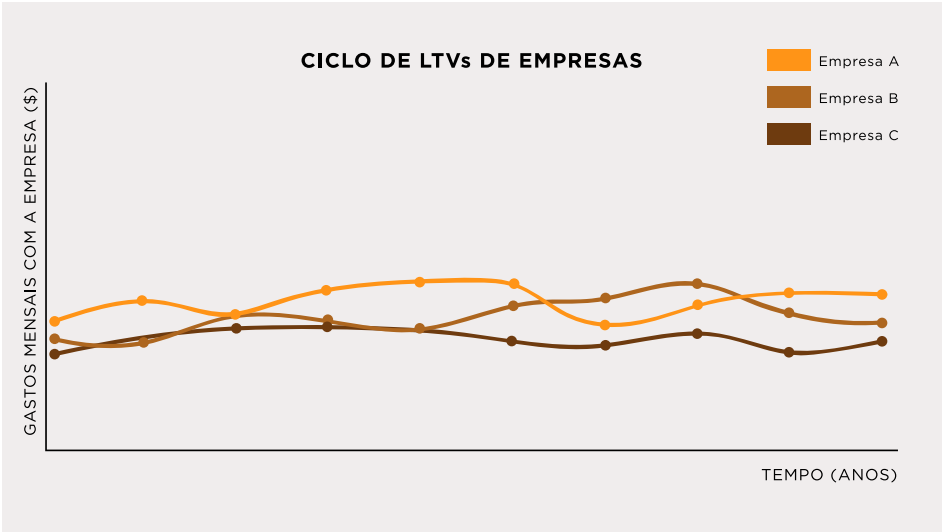


Figura esquemática que ilustra que diferentes empresas possuem diferentes LTVs, porém a tendência média é sempre um consumo disperso ao longo do tempo.

Com o bitcoin este padrão muda. Como o bitcoin é uma rede monetária baseada, entre outras coisas, em teoria dos jogos, faz sentido que todos os seus participantes tentem antecipar a sua entrada na rede. Ou seja, o LTV não será disperso ao longo de décadas, e sim de meses ou poucos anos. De fato, isso é observado no comportamento da maioria dos bitcoinheiros que geralmente seguem estes três passos na sua alocação de capital na rede monetária bitcoin:

- I) inicialmente eles investem somente um pouco do seu patrimônio;
- II) conforme eles ganham confiança e compreensão do bitcoin,

eles investem todo o seu patrimônio líquido (uns até mesmo vendem suas propriedades);

III) eles não têm mais dinheiro guardado para investir, mas seguem fazendo compras recorrentes mensais ou semanais, conforme eles vão recebendo seus salários em fiat.

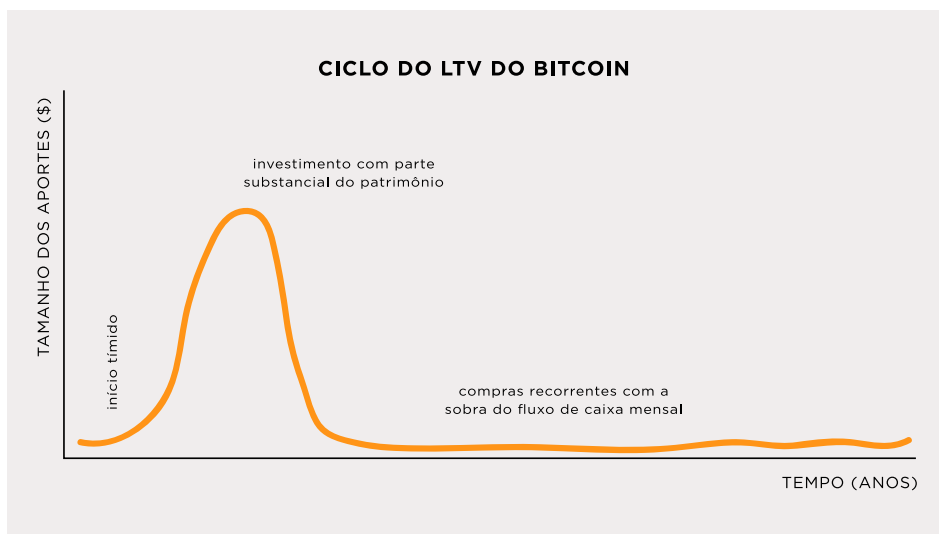


Figura esquemática que ilustra o comportamento típico de um bitcoinheiro e o padrão da sua realocação de capital do sistema fiat para a rede monetária bitcoin.

Ou seja, o LTV, que poderia demorar décadas para ser adicionado em outras empresas digitais com efeitos de rede, é adicionado significativamente mais rápido na rede de valor denominada bitcoin. O que significa dizer, portanto, que mesmo o padrão de arco tangente hiperbólica das empresas da Nasdaq talvez sejam enviesados para baixo quando o assunto é estimar o tamanho do sentimento de FOMO que o início da adoção por grandes players do mercado irá causar.

O modelo stock-to-FOMO considera quatro estágios de evolução desta curva de arco tangente hiperbólica:

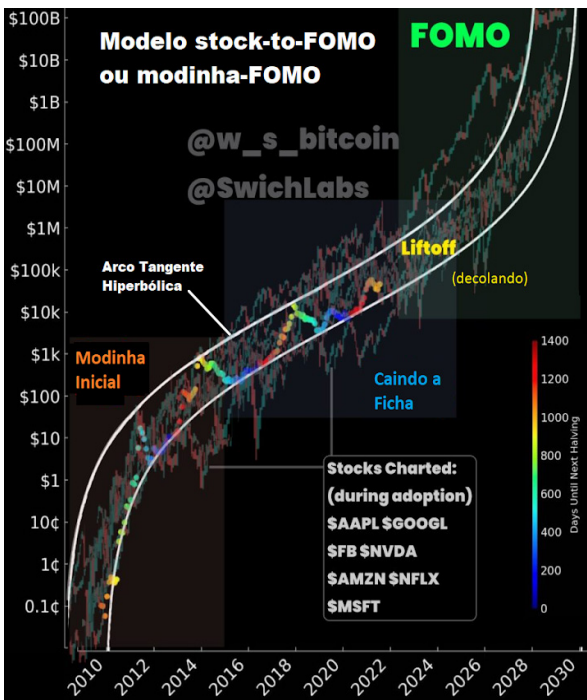
**I) Modinha inicial** - quando os inovadores e aficionados por tecnologia descobrem e investem nessas ações e no bitcoin. Nesse estágio ocorre o primeiro ciclo de apreciação intensa de capital, que no bitcoin ocorreu até por volta de 2014.

**II) Caindo a ficha** - quando o resto do mundo vai acordando e percebendo o que está ocorrendo debaixo dos seus narizes.

III) **Decolando** - é o início do segundo ciclo de apreciação intensa de capital, quando o restante do mundo começa a tomar medidas de acordo com o novo conhecimento adquirido conforme a ficha caia.

IV) **FOMO** - os players institucionais e estados soberanos perceberão finalmente que eles estão em uma competição para ver quem conseguirá acumular mais satoshis antes dos seus rivais. O FOMO associado a essa fase futura tende a ser intenso.

O modelo do stock-to-FOMO utiliza as ações do Google (\$GOOGL), Facebook (\$FB), Netflix (\$NFLX), Microsoft (\$MSFT), Apple (\$AAPL) e Nvidia (\$NVDA) para ilustrar justamente essa adoção de tecnologia e FOMO que ocorreu associado às ações dessas empresas nas últimas duas décadas. Todas essas ações apresentaram desempenho similar, seguindo uma curva arco tangente hiperbólica, e representam a adoção da internet e dos smartphones. O desempenho similar delas pode ser observado na imagem a seguir, onde o preço do bitcoin é plotado em conjunto com o histórico do movimento do preço dessas ações de tecnologia nas últimas décadas.



Modelo stock-to-FOMO (ou Modinha-FOMO) que compara a trajetória em arco tangente hiperbólica de diversas empresas de tecnologia da Nasdaq com a variação do preço do bitcoin.



Jason Lowery  
@JasonPLowery

...

Em outras palavras, o preço do BTC denominado em USD será infinito, como o modelo stock-to-FOMO do [@w\\_s\\_bitcoin](#) previu.

Existirá um ponto no futuro que nenhuma quantidade de USD (ou outra moeda) conseguirá comprar BTCs. Neste ponto, o BTC virou unidade de medida.



Caitlin Long 🔑⚡🟡🔵 @CaitlinLong\_ · Dec 3, 2021

Eu tenho conversado com ex-investidores de Wall Street que se tornaram bitcoinheiros há vários anos e um fez uma previsão que eu não consigo parar de pensar:

"Algum dia, não existirão bitcoins a venda. Será literalmente impossível comprar"

Eu concordo que isso pode acontecer. Impossível de prever.

12:34 PM · Dec 3, 2021 · Twitter Web App

## Ou seja...

Mesmo sem a tecnologia NGU, o bitcoin já seria a forma superior de bem monetário devido às suas características técnicas. Entretanto, como ainda estamos no estágio de descoberta de valor do bitcoin pelo restante do mundo, essa forma superior de bem monetário ainda conta com uma característica extremamente positiva: é a única forma de bem monetário que possui a tecnologia NGU. Ou seja, este bem monetário ainda te permite surfar a curva de adoção dele, o que é extremamente vantajoso do ponto de vista de quem já adotou o bitcoin.

## CAPÍTULO 8

# A MELHOR EMPRESA DO MUNDO

### O bitcoin NÃO é uma empresa

Primeiro vamos deixar claro que o bitcoin NÃO é uma empresa. Uma empresa é formada pelos seus fundadores, que são conhecidos e se tornam os chefes.

O bitcoin, por outro lado, é uma rede descentralizada que, por definição, não possui líderes ou chefes. Ele foi criado pelo pseudônimo Satoshi Nakamoto e até hoje não se sabe se foi criado por uma pessoa ou um grupo de pessoas. Não existe nenhuma forma de entidade que controla o bitcoin, e, portanto, ele não responde às ordens de um pequeno grupo de seres humanos. Essa é uma das suas principais características e mostra que o bitcoin definitivamente não é uma empresa.

Contudo, esse texto abordará o tema com uma visão mais criativa. Então, vamos começar perguntando "o que é uma empresa?"

De acordo com a definição do Google:





# empresa

/ê/

substantivo feminino

1. obra ou desígnio levada a efeito por uma ou mais pessoas; trabalho, tarefa para a realização de um objetivo; empreendimento.  
"as navegações portuguesas constituem e. notáveis"
2. organização econômica, civil ou comercial, constituída para explorar um ramo de negócio e oferecer ao mercado bens e/ou serviços.  
"e. de telecomunicações"
3. **POR EXTENSÃO**  
empresa como entidade jurídica; firma.  
"a e. não pagou os impostos"

Então empresas são organizações econômicas, constituídas por uma ou mais pessoas para executar obras ou desígnios e empreendimentos. As empresas são entidades constituídas juridicamente.

## Avaliando empresas e commodities

Empresas são entidades jurídicas que visam o lucro, portanto, é possível avaliá-las de acordo com seu desempenho. O método mais utilizado para avaliar uma empresa é o Fluxo de Caixa Descontado (FCD)<sup>66</sup>, que permite analisar o valor estimado de uma empresa a partir das perspectivas de faturamento futuro, geralmente algo entre 5 e 10 anos, dependendo da maturidade da empresa (startups vs. empresas listadas na bolsa, por exemplo). Existem outras formas de avaliar uma empresa, como a partir do seu valor patrimonial ou o quanto custaria para um novo entrante construir uma infraestrutura equivalente, entre outros<sup>67</sup>.

A avaliação via FCD (Fluxo de Caixa Descontado) só pode ser efetuada em entidades que possuem entradas de caixa, ou seja, que vendem produtos ou prestam serviços. Ou seja, é possível fazer uma análise de FCD na barraquinha de suco de limão da minha sobrinha, mas não é possível fazer uma análise de FCD em moedas como o dólar e o real ou em commodities, como o milho e o minério de ferro. Um dos motivos citados pelos críticos para comentar sobre o bitcoin negativamente é algo na linha de "eu não sei nem como avaliar o bitcoin, ele não gera caixa, então não gera valor". Esses críticos "geniais" não percebem que o bitcoin não é uma empresa e que, portanto, não faz sentido pensar em termos de FCD.



Exemplo da metodologia do FCD para avaliação de empresas<sup>68</sup>.

As moedas são comparadas entre si em um processo darwiniano para a definição da reserva global de valor onde a tendência é que a melhor predomine sobre as piores. Além disso, elas também refletem as políticas monetárias de seus países. Contudo, a realidade é que as moedas nunca são muito analisadas, pois geralmente só existe uma moeda oficial obrigatória em cada país. O que faz com que as qualidades dessa moeda não sejam realmente debatidas e analisadas. Exemplificando: quantas vezes vocês viram o debate sobre a expansão da base monetária em meios de comunicação não-bitcoinheiros? Então...



Bolívares venezuelanos e sua equivalência em produtos básicos (uma galinha depenada e um rolo de papel higiênico). O Bolívar venezuelano é um exemplo de moeda que perdeu o processo darwiniano e entrou em hiperinflação.

Já as commodities, como o ouro, soja, milho e o minério de ferro, possuem uma metodologia própria de avaliação chamada Stock-to-Flow (S2F). O S2F é um método relativamente novo que basicamente tenta modelar as forças de oferta e demanda e entender como elas geram escassez, que é a base do valor de qualquer commodity nesta visão.

## Por que o bitcoin é a melhor empresa do mundo?

### O que são empresas?

Ou seja, sintetizando a sessão anterior, o bitcoin não deve ser avaliado como uma empresa pois ele não gera lucro, não vende produtos, não possui um CEO. E portanto, não faz sentido nenhum pensar no bitcoin como uma empresa, certo?

É aqui que eu gostaria de propor uma discussão mais heterodoxa e criativa. Em uma análise em sentido amplo<sup>69</sup>, ou seja, abstraindo certas características e focando em outras arbitrariamente para observar um padrão, o bitcoin pode ser visto simplesmente como a melhor empresa do mundo.

Se a rede bitcoin for analisada de maneira específica<sup>70</sup> como uma

empresa como entidade jurídica, de fato, o bitcoin não é uma empresa. Mas se nós adotarmos uma visão mais ampla, é possível ver relações entre empresas e a rede do bitcoin.

Lembrando das definições de uma empresa do Google citadas no início do texto, o bitcoin é uma obra levada a efeito por uma ou mais pessoas que possuem um objetivo em comum. Apesar de ser uma rede descentralizada, a comunidade de bitcoinheiros age como uma tribo coesa e apresenta diversas características em comum (como será discutido no capítulo 11), assim como os funcionários de uma empresa que possui uma cultura forte (como o Google<sup>71</sup> ou a Ambev<sup>72</sup>, por exemplo).



Cena do filme "Os Estagiários"<sup>73</sup>, uma comédia de 2013 sobre a cultura do Google e seus funcionários (conhecidos como googlers).

Levando isso em conta, o exercício que este capítulo propõe é avaliar o bitcoin como uma empresa. Ou seja, vamos analisar diversos itens qualitativos que são extremamente desejáveis para uma empresa de sucesso e ver como esses atributos se aplicam ao bitcoin.

Nesta seção, serão citadas diversas características desejáveis de uma empresa, tanto do ponto de vista de um investidor na bolsa, como no ponto de vista do empreendedor que fundou e administra a empresa no dia a dia. Esta é a análise qualitativa dos fundamentos da empresa bitcoin e seus "funcionários".

## Branding

Branding é a estratégia de gestão da marca que visa torná-la mais reconhecida pelo seu público e aumentar a sua presença no mercado e no imaginário popular. A estratégia busca a admiração e desejo pelos valores que a marca cria em torno de si mesma. Seu objetivo principal é despertar sensações e criar conexões fortes, que serão fatores relevantes para a escolha do cliente pela marca no momento de decisão de compra.

Basicamente, o branding é a estratégia que busca tornar a marca forte e reconhecida.

Por exemplo, qual a diferença entre um celular da marca A e da marca B? A diferença é que se a marca B for a Apple, você pagará o dobro por um celular dela, mesmo que possua as mesmas especificações técnicas do celular da marca A. Isso acontece porque a Apple sempre soube trabalhar muito bem o branding da sua marca, e hoje é considerada uma marca sexy e inovadora por seus clientes.



Campanha de marketing da Apple. Desde a sua criação a Apple buscou se diferenciar das outras empresas de tecnologia.

Isso faz com que eles tenham seguidores fiéis, que só aceitam ter produtos da Apple, independentemente do preço. A Apple sempre buscou se diferenciar como uma empresa feita para quem pensa diferente, gente criativa e líderes inovadores. Suas campanhas de marketing são consistentes neste sentido desde a sua criação e conseguiram colocá-la em um lugar de destaque no imaginário popular.



Depois de mais de 40 anos a Apple segue reforçando o seu mesmo posicionamento de marca.

Apesar de o bitcoin não possuir uma equipe de marketing e nem um logo oficial, sua marca é extremamente popular e reconhecida. De fato, a marca do bitcoin é tão reconhecida que é utilizada como metonímia para todo o mercado de “criptomoedas”. Ou seja, hoje, diversas pessoas utilizam a palavra “bitcoin” querendo se referir ao mercado de criptomoedas como um todo, da mesma maneira que utilizam “Bombril” ao invés de “palha de aço” ou “Band-Aid” no lugar de “curativo”.

Hoje o B com dois riscos cruzados é universalmente conhecido como símbolo do bitcoin e tanto a cor laranja quanto o símbolo são utilizados como referências a ele em diversos lugares da cultura popular.



A marca “oficial” do bitcoin, com o B com os dois riscos cruzados e a cor laranja.

## Cultura Forte

As principais empresas do mundo também prezam bastante por manter uma cultura forte. Mas o que isso quer dizer? Uma cultura forte significa que tudo e todos da empresa se comportam seguindo determinados códigos de conduta. Pode-se dizer que a cultura de uma empresa é a sua constituição.

As empresas buscam ter uma cultura forte, onde os funcionários se identificam e acreditam na maneira com que a empresa faz negócios, (o ethos da empresa, por assim dizer). No mundo das empresas de tecnologia todos já escutaram a respeito dos googlers e da cultura do Google. Outro exemplo são os PicPay Lovers, a maneira com que a empresa PicPay recruta e incentiva os seus funcionários a se auto denominarem.



Anúncio de vagas de emprego da PicPay, focando na qualidade da cultura da empresa.

A ideia é que uma cultura forte gera coesão grupal, uma espécie de senso de tribo, entre os funcionários de uma empresa. Um grupo coeso tende a ter desempenho melhor, perder menos tempo com atritos e desavenças e trabalhar uns pelos outros. No mundo dos esportes isso é conhecido como “vestir a camisa”, o que faz com que os atletas joguem com mais raça e entrega, mesmo correndo o risco de se lesionar.

Apesar de ser uma rede descentralizada, a comunidade dos bitcoinheiros age como uma tribo coesa e apresenta diversas características em comum, assim como os funcionários de uma empresa que possui cultura. São diversos os rituais compartilhados pelos bitcoinheiros de todo mundo. A cultura bitcoinheira é tão forte, que diversas pessoas se referem a ela como

um culto<sup>74</sup> ou religião<sup>75</sup>.

As empresas esperam que seus funcionários desenvolvam “senso de dono”, ou seja, que eles tomem decisões como se eles fossem realmente os donos dela. Para conseguir alinhar os interesses com funcionários estratégicos, as empresas até chegam a oferecer uma pequena parte da sociedade na forma de ações. De maneira análoga, os bitcoinheiros possuem seus satoshis, fazendo com que efetivamente eles sejam donos de uma pequena parcela do bitcoin. O senso de dono é tão forte entre os bitcoinheiros que é bastante comum que estes, quando alcançam sua independência financeira, passem a se dedicar a trabalhos voluntários em prol da difusão do bitcoin. Eles fazem isso com um enorme senso de compromisso e propósito, e realmente acreditam que assim eles estão mudando o mundo para melhor. A missão é espalhar a palavra de Satoshi.



Um membro do “culto” do bitcoin buscando sinalizar o seu pertencimento ao grupo e a sua visão de mundo, mesmo que isso cause com possível dor de cabeça associada por ele estar sinalizando no meio de uma audiência no congresso americano<sup>76</sup>.

## Propósito

O tema “propósito” também é bastante comentado no mundo do empreendedorismo. O propósito da empresa é o que motiva a empresa e seus colaboradores a se dedicarem; é o que as empresas fazem para transformar o mundo em um lugar melhor. O propósito é a principal razão para que uma empresa exista no mercado, mesmo que muitas vezes ele esteja esquecido



devido à quantidade de tarefas e rotinas do cotidiano.

Da mesma forma, a comunidade dos bitcoinheiros é uma comunidade ligada por um propósito extremamente forte: consertar o dinheiro. Um dos lemas dessa comunidade é “conserte o dinheiro, conserte o mundo”, e mostra bem o propósito do bitcoin: consertar o mundo. Todo o ethos da comunidade bitcoinheira deriva do ethos dos cypherpunks<sup>77</sup>, como a comunidade de matemáticos, de hackers e de criptoanarquistas se autodenominou nos anos 1990.



*fix the money,  
fix the world.*

Conserte o dinheiro, conserte o mundo (em inglês “fix the money, fix the world”), um dos lemas da comunidade dos bitcoinheiros.

Os cypherpunks foram essenciais no movimento em defesa da privacidade e da anonimidade online. Eles usavam a criptografia como forma de proteger a individualidade ao inibir o controle dos seus dados de navegação pelos agentes governamentais, institucionais ou do setor comercial.

O senso de propósito dos bitcoinheiros fica claro quando você percebe que na comunidade existem pouquíssimos vendedores e muitos educadores. O que mostra claramente que a maioria da comunidade é missionária com a causa do bitcoin, e não mercenária.

Empresas com propósito nobre conseguem negociar com seus funcionários salários menores, pois elas vendem também o sonho de “trabalhar por um mundo melhor”. Os funcionários estarão “contribuindo de verdade para a sociedade”. Isso é ainda mais verdade com o bitcoin, onde muitos convertidos trabalham de graça pela missão e pelo propósito de consertar o dinheiro e, assim, mudar o mundo.

## Atração e retenção de talentos

Um dos lugares comuns nas palestras que os coaches dão para empresas é como uma empresa não é nada mais do que as pessoas que a compõem. Uma empresa não existe na vida real, ela é uma ficção que faz com que várias pessoas se unam e trabalhem em prol de um objetivo comum, um propósito compartilhado. Ou, em outras palavras, um CNPJ é a somatória dos CPFs envolvidos na sua criação e na sua operação do seu dia a dia.

O capital intelectual de uma empresa determina a capacidade desta de se adaptar a mudanças e lidar com novas situações. Assim, o Google sempre foi considerado uma empresa muito forte e com um futuro promissor, pois todos os jovens talentos queriam trabalhar lá entre os anos 2010 e 2020. Da mesma forma, diversas outras empresas como o Meta, Airbnb, LinkedIn, PicPay, Ambev e diversas outras conseguem se destacar da concorrência devido à capacidade de atrair talentos para compor sua equipe.

Contudo, atrair os talentos é somente uma parte da equação. Na realidade, a empresa precisa conseguir também reter os talentos atraídos. Ou seja, não adianta nada conseguir contratar ótimos funcionários que perdem o interesse em pouco tempo de empresa e se demitem para procurar novas oportunidades. O tempo de treinamento de novos funcionários e a perda de cultura e processos relacionada à saída de funcionários antigos são dois custos altos que uma empresa paga caso não consiga reter os seus talentos<sup>78</sup> (o que é conhecido como turnover no jargão do meio das empresas de tecnologia).

Os bitcoinheiros comparam a capacidade de atração do bitcoin com a de um buraco negro.

Diversos talentos das ciências da computação, engenharia, filosofia, marketing, ciências da natureza e demais áreas do conhecimento são "recrutados" pelo bitcoin todos os dias. Para quem não conhece a comunidade deve até soar meio estranho, mas a realidade é que uma vez que a pessoa realmente entende o bitcoin e todas as suas consequências indiretas, dificilmente conseguirá escapar da gravidade do buraco negro.

Essa gravidade de buraco negro não só atrai para o bitcoin como retém talentos. A independência financeira que vem como resultado da valorização do bitcoin permite que os bitcoinheiros se dediquem às suas preferências.

## Setor Perene

Quando um investidor da bolsa estuda empresas para investir ou um empreendedor estuda um mercado para criar uma empresa, uma das características que eles devem observar é se o setor é perene. Ou seja, esse setor vai continuar existindo pelos próximos 10, 20 ou 50 anos? Ou a empresa irá se tornar as novas paletas mexicanas?

Assim, um dos itens que existem na lista de características de uma empresa é entender se o setor da empresa que você quer investir faz sentido no longo prazo. No longo prazo, você apostaria que qual destes serviços deixarão de ser relevantes: a transmissão de energia ou o consumo de paletas mexicanas? Então você preferiria investir em uma paleteria mexicana ou em ações de uma transmissora de energia na bolsa?



Diferentes setores da economia apresentam diferentes graus de necessidade real da população, e portanto só alguns deles são perenes no longo prazo.

O bitcoin nada mais é que uma nova tecnologia de dinheiro. Com uma tecnologia melhor que o dinheiro atual, que transforma o dinheiro em uma rede social monetária, mas basicamente o bitcoin continua sendo dinheiro.

E o dinheiro é uma das principais tecnologias inventadas pelo homem. Ele permite comunicar valor no tempo e no espaço.

Ou seja, graças ao dinheiro é possível realizar trocas entre pessoas. Antes da invenção do dinheiro só era possível realizar trocas entre pessoas que **a)** se conheciam (e uma delas eventualmente pagava "fiado") ou **b)** entre pessoas que possuíam o que trocar entre si.

Ou seja, se eu fosse um produtor de cabras e eu tentasse realizar uma troca com o produtor de trigo, só conseguiria realizar a troca caso este produtor me conhecesse e quisesse ter um crédito comigo ou caso ele quisesse uma cabra. Com a invenção do dinheiro, trocas entre pessoas que

não possuem o que trocar entre si se tornaram viáveis, o que permitiu que a economia das sociedades humanas mudasse em ordens de grandeza. Com essa invenção, o ser humano passou a conseguir armazenar a sua energia de trabalho (outra forma de falar “o seu tempo”) de forma transportável, e assim ele conseguiu trocar ela pela energia de trabalho de outros seres humanos.

O dinheiro é uma tecnologia de milhares de anos. Inicialmente conchas e outros objetos colecionáveis eram utilizados como moeda. Papel que foi assumido pelo ouro e pelas moedas de metal. Porém tanto o ouro como as moedas de metal são pesados, o que atrapalha o seu transporte, e são mais difíceis de se emitir, uma vez que você precisa extrair os materiais para confeccionar esta forma de dinheiro. Também é mais difícil proteger esses metais, e a tendência foi sua concentração nos cofres dos bancos.

Nos últimos séculos as moedas de metal foram gradativamente substituídas pelo dinheiro de papel, o que foi potencializado em 1971 quando o presidente dos EUA, Richard Nixon, acabou com a conversibilidade entre o dólar e o ouro.

A evolução do dinheiro continuou na era da informação e o dinheiro de papel foi substituído por dinheiro digital que pode ser manipulado através de cartões de plástico. Com a evolução constante da tecnologia da informação, o dinheiro se tornou eletrônico e deixou de precisar ter necessariamente um equivalente no mundo físico.



Evolução do dinheiro utilizado pela humanidade, desde trocas e escambos até o dinheiro eletrônico e o bitcoin.

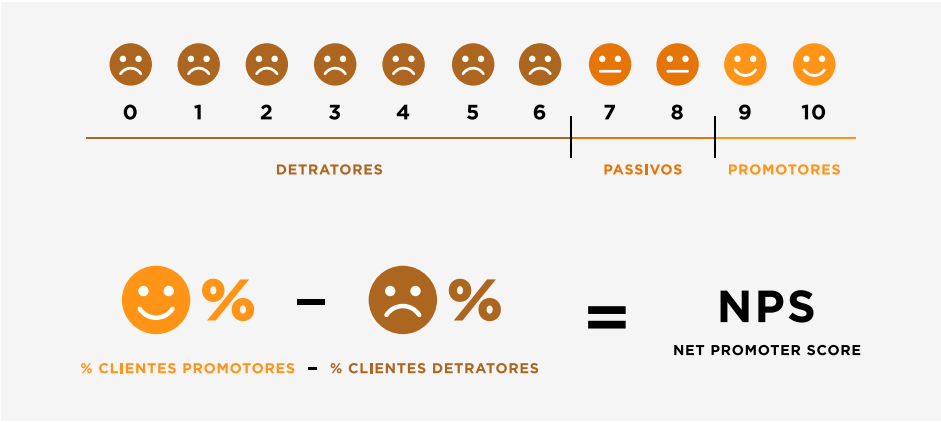
O dinheiro eletrônico nada mais é que a evolução do dinheiro de papel. Ou seja, ele também não possui lastro e milhões de novos dólares (ou outras moedas fiat) podem ser “produzidos” com alguns cliques de botão em um computador dos bancos centrais do mundo, gerando uma infinidade de problemas.

Porém, o dinheiro continuou com o seu processo de evolução. Em 2009, o pseudônimo Satoshi Nakamoto publicou o white paper do bitcoin, que nada mais é que a evolução do ouro e das moedas de metal. Assim como o ouro e as moedas de metal, o bitcoin é lastreado no mundo físico. Basicamente, o bitcoin representa a invenção da escassez no meio digital.

### NPS

As empresas utilizam diversas métricas para tentar quantificar o sentimento dos seus clientes em relação à qualidade do seu produto, do seu atendimento etc. Uma das métricas mais utilizadas nos dias de hoje é o Net Promoter Score (NPS)<sup>9</sup>. O NPS tem como objetivo medir o grau de lealdade dos clientes das empresas de qualquer segmento, trazendo reflexos da experiência e satisfação dos clientes.

Para executar uma avaliação de NPS, as empresas pedem que seus clientes classifiquem a probabilidade (na escala de 0 a 10) de que eles indiquem seus amigos. Clientes que avaliam a empresa com notas entre 0 e 6 são vistos como detratores, com notas entre 7 e 8 são clientes neutros e clientes que classificam a empresa entre 9 ou 10 são promotores.



Representação em imagem da metodologia NPS.

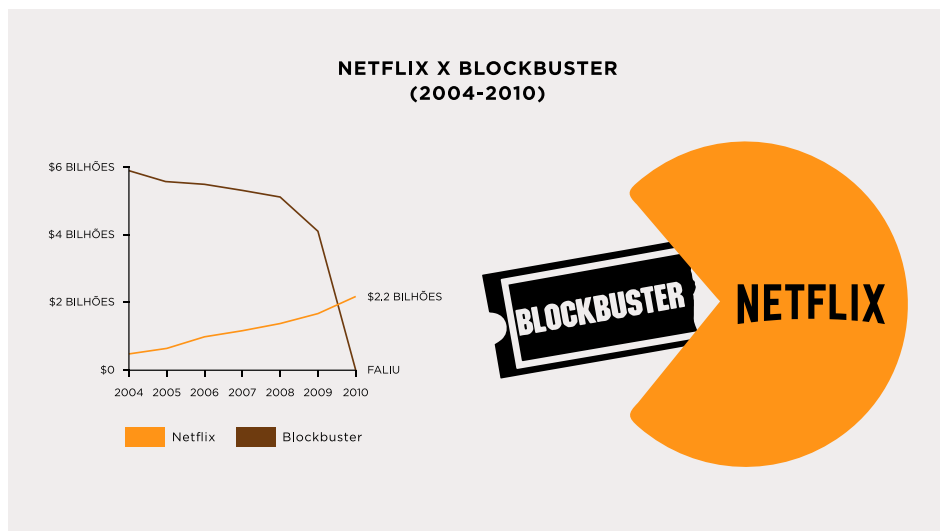
As empresas almejam que a maioria dos seus clientes sejam promotores de seus produtos. Isto é uma vantagem competitiva enorme, pois uma avaliação boca a boca<sup>80</sup> é muito mais efetiva do que uma campanha de marketing para atrair clientes (ou para perder clientes no caso de críticas). Isso acontece porque o ser humano confia muito mais em outro ser humano que em campanhas de marketing e, se alguém de sua confiança te indicar algo, as chances de você escutar esta pessoa são bem maiores.

Como já comentamos acima, o Buraco Negro do bitcoin atrai e retém diversos talentos, muitos deles inclusive trabalham de forma voluntária por acreditar no propósito por trás do bitcoin. Em outras palavras, o marketing boca a boca do bitcoin é fortíssimo, tanto que diversas vezes é considerado uma religião ou um culto de fanáticos pelos não-iniciados. Ou seja, o bitcoin possui um NPS altíssimo, com diversos promotores, que se dedicam a espalhar a palavra de Satoshi.

## Inovação

Todo mundo sabe que vivemos numa época de intensa transformação. Uma época em que o velho e analógico é rapidamente substituído pelo novo e digital. Atualmente, as empresas precisam inovar para se manterem competitivas, e o lema “innovate or die” (inove ou morra)<sup>81</sup> se tornou uma sabedoria popular no meio empresarial (e as empresas que não absorveram essa sabedoria estão sendo disruptadas neste exato momento).

Exemplos disso são abundantes, e podemos citar rapidamente alguns casos como Blockbuster vs. Netflix; Nokia vs. Blackberry vs. Iphone; Kodak vs. câmeras digitais vs. câmera digital no celular; e assim por diante.



Duas maneiras de representar o que ocorreu na competição entre a Blockbuster e a Netflix.

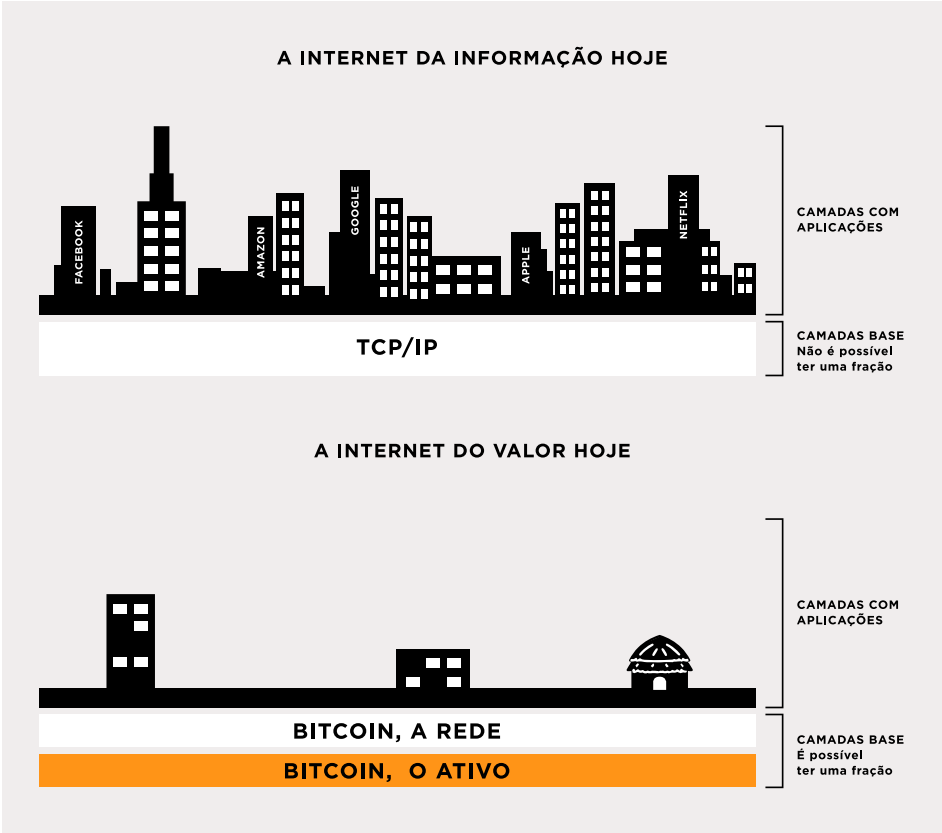
Uma crítica que alguns nerds apaixonados por tecnologia costumam fazer sobre o bitcoin é que ele é uma tecnologia velha e que as transações são lentas e ineficientes. Eles gostariam que o bitcoin seguisse os moldes do Vale do Silício de “move fast and break things” (mova-se rápido e quebre as coisas)<sup>82</sup> que funciona muito bem para startups, mas que não faz sentido para um sistema monetário. Para um sistema monetário, o ideal é “move slow and make everything work without a bug” (mova-se devagar e faça tudo funcionar sem nenhum bug).

Este tipo de crítica está errado em vários aspectos chaves e só mostra que esses nerds entendem de tecnologia e só, como um cavalo com cabresto e antolhos acreditando que só existe o seu campo de visão. Ou seja, eles não possuem uma visão de mundo abrangente.

Mesmo se a tecnologia por si só não fosse a melhor, esta é somente uma das características importantes do bitcoin, e não a sua principal característica. A descentralização real, que gera a incensurabilidade e a inconfiscabilidade, assim como os efeitos de rede gerados e a comunidade, são as principais características do bitcoin (como o capítulo 5 aprofundou).

Mas também é interessante ressaltar que o bitcoin é somente a camada base que permitirá que diversas outras camadas sejam construídas em cima. O mais importante para a camada base é que seja robusta e

confiável, e não que seja rápida e maleável, como diversos entusiastas em outras criptomoedas tentam argumentar. A imagem abaixo, uma tradução de uma imagem de um bitcoinheiro do Twitter chamado Croesus<sup>83</sup>, ilustra bem esta questão de camada base e camada secundária e como as aplicações do bitcoin serão construídas na camada secundária.



Como a Internet da Informação está constituída nos dias de hoje, com todas suas aplicações (Meta, Amazon, Google, Netflix, Apple, Airbnb etc) construídas como camadas secundárias enquanto que o protocolo é a camada base imutável. Da mesma maneira, na Internet do Valor (o bitcoin), as aplicações (Lightning Network, Liquid, entre outras) estão sendo construídas em camadas secundárias.

Assim como foi o caso com a Internet, é em cima da camada base do bitcoin que serão construídas as camadas com aplicações. Ou seja,



assim como na engenharia civil que constrói prédios, é importante ter uma fundação sólida para que estruturas sejam construídas em cima.

O principal exemplo de construção na segunda camada do bitcoin é a Lightning Network<sup>84</sup>, uma aplicação que permite que bitcoins sejam utilizados como ferramenta de micropagamentos. Assim dizendo, aquele argumento de que “não dá para usar bitcoin na padaria para comprar um café” mostra que a pessoa não conhece a Lightning Network. Outro exemplo de construção utilizando a camada base é a Liquid Network, uma sidechain, ou seja, uma camada paralela.

Essas aplicações permitem escalar o bitcoin sem alterar o seu protocolo base. Isto é, a partir da utilização destas camadas secundárias, é possível ampliar sua capacidade de processamento de transações do bitcoin (o que mata o discurso de venda da maioria das outras criptomoedas, que se propõem a “alcançar o que o bitcoin não alcançou” ou a “escalar o bitcoin”).

Em outras palavras, a empresa bitcoin é aberta à inovação mas, diferente do que ocorre com as outras criptomoedas, a inovação precisa ser feita sobre uma fundação sólida, estável e segura.



Nodes da Lightning Network, mostrando que mesmo essa camada secundária do bitcoin já está em pleno processo de adoção.

## A Lightning Network em El Salvador

O exemplo da adoção do bitcoin por El Salvador merece ser aprofundado. El Salvador é um país pobre na América Central onde cerca de 70% da população não possui contas em bancos tradicionais. Nos últimos

anos ocorreu uma grande adoção do bitcoin como dinheiro do dia a dia. Isso só é possível porque a população utiliza em grande medida a Lightning Network, que permite transações de bitcoin sem as taxas de transferência da camada base.

Por conta dessa adoção maciça da população, o presidente do país tomou a iniciativa e tornou El Salvador o 1º país em que o bitcoin é oficialmente uma moeda<sup>85</sup>.



oto de perfil do Presidente Nayib Bukele no twitter após o anúncio oficial de que El Salvador passaria a aceitar o bitcoin como meio oficial de pagamento.

Estima-se que cerca de 22% do PIB de El Salvador (algo como US\$ 4 bilhões, ou aproximadamente R\$ 20 bilhões) seja proveniente de remessas internacionais de dinheiro que os cerca de 2 milhões de salvadorenhos que migraram para os EUA remetem para o seu país. Mas, serviços de remessas internacionais são extremamente caros (algo entre 20% até 50% do valor original) e lentos, além de que só podem ser sacados na capital São Salvador.

Com a Lightning Network, o cenário é diferente e agora os salvadorenhos conseguem realizar remessas internacionais instantâneas, de graça e que podem ser acessadas e utilizadas diretamente pelo aplicativo, sem a necessidade da viagem até São Salvador.



Meme baseado no filme Borat<sup>86</sup> e espalhado pela comunidade bitcoinheira como reação ao anúncio da adoção do bitcoin por El Salvador.

### Governança perfeita

A governança é uma das características qualitativas mais importantes para um investidor quando está avaliando uma empresa para investir. O IBGC, a principal referência do Brasil sobre o tema, estabelece quatro princípios da governança corporativa. São eles: transparência, equidade, prestação de contas (accountability) e responsabilidade corporativa.

**Transparência** significa que os dados de desempenho econômico-financeiro, além de outros fatores tangíveis e intangíveis que direcionam a gestão da empresa devem ser disponibilizados para todos os interessados no negócio.

**Equidade** significa que todos os interessados na gestão da empresa ou dos projetos devem ter acesso às informações sobre os negócios. Mas não é só isso, é necessário também que todos esses participantes sejam tratados de maneira igualitária e justa.

**Prestação de contas** significa que a empresa se esforçará em transmitir as informações de maneira compreensível. A prestação de contas tem como intuito passar as informações da empresa para os interessados de forma clara, além de assumir totalmente as consequências dos seus atos. Os objetivos do princípio da prestação de contas são reduzir a desconfiança e reduzir as possibilidades de abuso por parte dos sócios e administradores.

**Responsabilidade corporativa** significa que a empresa deve buscar

trazer sempre resultados positivos para seus acionistas e investidores e, ao mesmo tempo, zelar pela manutenção de seus capitais, incluindo o capital humano, social, ambiental, intelectual e financeiro.

Em um sentido mais amplo, a governança corporativa é basicamente o conjunto de medidas tomadas pelas empresas para tentar garantir que todos os funcionários, clientes e investidores de determinada empresa estejam alinhados.

Nesse sentido mais amplo, pode-se dizer que o fato do bitcoin ser descentralizado, não possuir nenhum funcionário contratado e nenhum diretor mandando na empresa significa que possui a melhor governança possível.

Como o bitcoin é um protocolo open source (código aberto), todos os usuários da rede (que entendem de programação) têm acesso a todas as informações sobre o funcionamento dela. Os interesses dos usuários também estão alinhados financeiramente, de modo que todos os atores do ecossistema têm interesse de que o bitcoin seja bem sucedido.

O conhecido investidor Warren Buffet tem uma citação famosa que diz: “você deve investir em um negócio que até um idiota poderia dirigir, porque algum dia um idiota o dirigirá”. No caso do bitcoin, idiota algum jamais o dirigirá, tampouco gênio algum. O que dirige o bitcoin é o seu código. Como os bitcoinheiros costumam falar, o bitcoin é um sistema de regras, e não de regentes (“rules and not rulers”). Quer governança melhor do que saber que não haverá mudanças no time que está ganhando?

Você já se perguntou o que aconteceria com a Tesla caso o Elon Musk desaparecesse? E o que aconteceria com o Meta se o Mark Zuckerberg desaparecesse? Pois bem, o criador do bitcoin desapareceu e deixou o projeto em 2011. Ou seja, não existe um líder no bitcoin, o que é a melhor maneira de garantir que a governança do código será mantida.

## **Crescimento Viral**

O sonho de toda empresa é não precisar gastar dinheiro com marketing e conseguir estruturar um produto “que se vende sozinho”. Mas “se vender sozinho” não existe na vida real, o que existe são produtos que alcançam um crescimento viral.

Para alcançar este crescimento viral é necessário que o produto

que determinada empresa desenvolveu seja bom o suficiente para que cada novo cliente indique este produto para mais de um novo cliente. É a mesma lógica da taxa  $R^{87}$  da pandemia, na qual, se cada pessoa contaminasse mais que uma outra pessoa, a pandemia estava acelerando e se cada pessoa contaminasse menos de uma outra pessoa (em média), a pandemia estava sendo contida.

Ou seja, cada cliente traz novos clientes em uma taxa que permite que a empresa não precise contratar vendedores.

E nada representa mais a comunidade bitcoinheira do que o seu crescimento viral. Não é à toa que os bitcoinheiros são comparados a membros de cultos. Isso acontece porque uma vez que você realmente entende o bitcoin e todas as suas implicações, você realmente muda a sua compreensão de mundo e passa a enxergar como imperativo moral ajudar outras pessoas a também se salvarem. Da mesma forma que os jesuítas queriam catequizar os índios para salvar as suas almas, os bitcoinheiros realmente acreditam que é seu dever “catequizar” os seus familiares e amigos que ainda são normies e com isso salvá-los do inferno fiduciário.

Um exemplo de marketing viral aconteceu nas 500 milhas de Indianápolis de 2021, onde um grupo de bitcoinheiros se uniu para patrocinar um dos carros<sup>88</sup>. Este fato fez com que a fórmula Indy tivesse uma alta na sua audiência e também expôs os amantes do automobilismo ao bitcoin.



O carro do bitcoin chegou a liderar as 500 milhas de Indianápolis por mais de 30 voltas, fazendo com que a campanha de marketing fosse extremamente bem sucedida.

Além disso, ainda existe uma grande comunidade de bitcoinheiros que passam o dia produzindo memes para ajudar a espalhar a visão de mundo de um bitcoinheiro. Você talvez tenha visto os raios lasers nas fotos de

perfil de diversos bitcoinheiros no Twitter? Pois bem, memes são campanhas de marketing poderosíssimas na divulgação e na proteção do bitcoin.

## **Vantagens Competitivas de Longo Prazo**

Todo value investor que se preze é discípulo do Warren Buffett e conhece a sua filosofia de só investir em empresas com fossos econômicos<sup>89</sup> consolidados. O termo refere-se à capacidade de uma empresa manter uma vantagem competitiva em relação aos seus rivais e assim proteger sua rentabilidade e participação de mercado no longo prazo. Qualquer empresa pode ter uma vantagem competitiva no curto prazo, mas somente as vantagens competitivas de longo prazo são consideradas fossos econômicos.

Analogamente aos fossos que cercavam castelos medievais como forma de proteção contra invasores, empresas com fossos econômicos criam barreiras de entrada contra a concorrência. Fossos econômicos são características que determinada empresa possui que são difíceis de copiar ou reproduzir. Ter uma marca bem conhecida, poder de preços, custos menores e uma grande parcela da demanda do mercado são exemplos de fossos econômicos que uma empresa pode possuir.

No caso da “empresa” bitcoin, os fossos econômicos são gigantescos. Então será apresentada aqui apenas uma breve síntese de cada um deles, pois uma explicação aprofundada requisitaria um texto para cada um desses fossos.

### **Hashrate**

Hashrate é o termo utilizado para a capacidade de processamento computacional da rede do bitcoin. Quanto maior for o hashrate de determinada rede, mais forte e segura ela é. Quando a gente compara o hashrate do bitcoin com a de qualquer outra criptomoeda só existe uma conclusão possível: somente o bitcoin existe de verdade, as outras criptomoedas são castelos de areia, ou seja, elas não possuem rede computacional robusta para dar suporte a estes projetos. A imagem do capítulo 5 que compara a hashrate do bitcoin com outras criptomoedas ilustra bem a diferença entre ambos.

### **Marca Forte**

Este tópico já foi abordado acima, então vou simplificar: pergunte

para um normie quais criptomoedas ele conhece.

Basicamente, o bitcoin se tornou o Bombril das criptomoedas. O que eu quero dizer com isso? É dizer que o nome do produto não é “Bombril”, e sim “palha de aço”, mas mesmo assim todos o conhecem como Bombril.



Qual é o nome deste produto? Bombril ou palha de aço?

### Efeitos de Rede

Em economia e negócios, efeito de rede<sup>90</sup> é o efeito que um usuário de um bem ou serviço tem sobre o valor do produto para outros usuários. Quando o efeito de rede estiver presente, o valor de um produto ou serviço depende do número de outras pessoas que também utilizam o produto. As empresas digitais como Meta (donos também do Whatsapp e do Instagram), Twitter e Airbnb, são os melhores exemplos de efeitos de rede.

Exemplificando: para eu falar com alguém que possui o Whatsapp eu preciso ter o Whatsapp também. Se eu e todos os meus amigos tivermos o Whatsapp é muito mais difícil para um novo membro do nosso grupo adotar o Telegram, uma vez que ele não vai conseguir se comunicar conosco. O mesmo acontece com os telefones: se só eu tivesse um telefone e mais ninguém no mundo tivesse, eu não conseguiria falar com ninguém pois eu não teria para quem ligar. Como outras pessoas também possuem telefones, eu consigo falar com elas a hora que eu quiser.

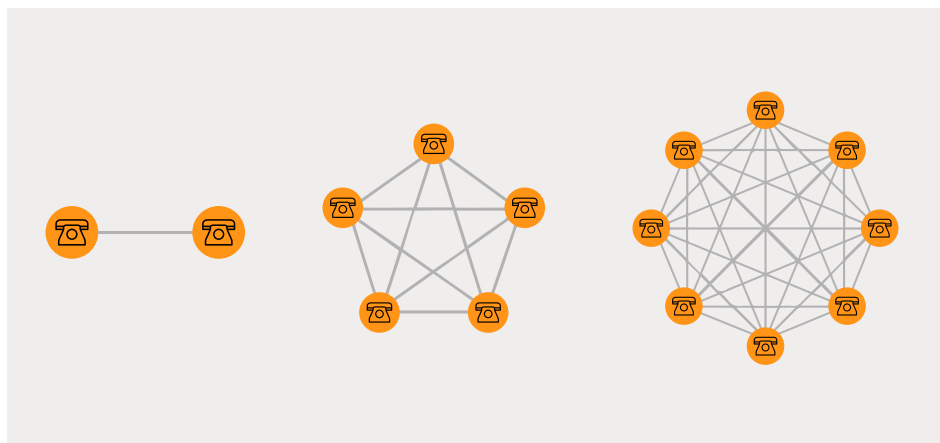


Diagrama clássico usado para exemplificar os efeitos de rede.

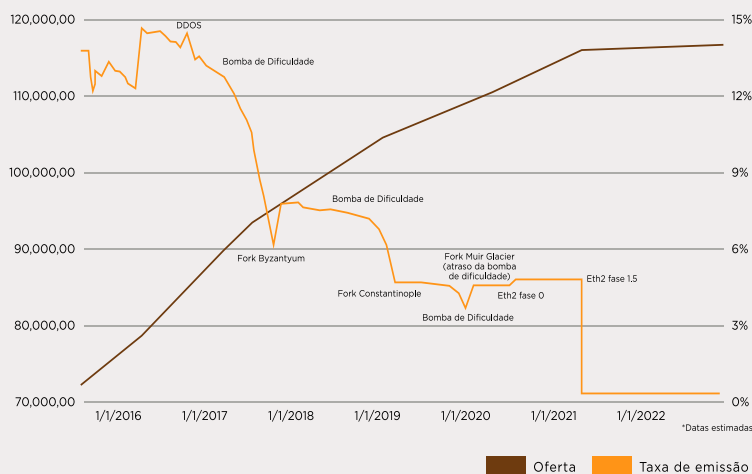
O efeito de rede do bitcoin pode ser observado tanto em casos reais como na Bitcoin Beach<sup>91</sup>, que fez com que El Salvador acabasse adotando o bitcoin como moeda oficial do país, como em modelos teóricos como os modelos de curva de adoção do Croesus<sup>92</sup> e do Michael Levin<sup>93</sup>.

### Teste do tempo

O bitcoin é a criptomoeda original e a única que está por aí há mais de 12 anos. O ethereum, segunda criptomoeda em tamanho de mercado, só existe há 6 anos e será atualizado em algum momento no futuro para o ethereum 2.0, o que significa efetivamente que o relógio é zerado novamente. O ethereum 2.0 terá acabado de nascer e, portanto, não dá para confiar que o seu algoritmo não possuirá bugs. Além do fato que não dá para confiar na governança de projetos que mudam de acordo com as vontades dos seus dirigentes. Diferentemente do bitcoin, o ethereum ainda é centralizado na mão do seu criador, que pode mandar e desmandar no projeto da maneira que ele bem entender. Isso fica claro quando a gente compara a política monetária errática do ethereum (sem levar em conta as moedas pré-mineradas) com a política monetária precisa do bitcoin:



## TAXA DE EMISSÃO HISTÓRICA E PROJETADA DO ETHEREUM



Taxa de emissão e oferta de ethereum. Reparem que o ethereum possui uma grande quantidade de tokens pré-minerados. Compare essa imagem com a da emissão histórica de bitcoin apresentada no capítulo 5, sobre os fundamentos do bitcoin.

## Testes contra ataques externos

O bitcoin também já mostrou resiliência e resistiu a diversos ataques externos. Diversos países já tentaram banir o bitcoin ou parte do seu ecossistema, mas nenhum desses países obteve êxito. O fato de o bitcoin ser descentralizado faz com que seja extremamente difícil fazer as leis valerem. Nesse sentido, é muito mais fácil regular uma empresa centralizada e com um CEO conhecido, como foi no caso da Microsoft, que sofreu medidas antitruste<sup>94</sup> por mais de uma década.

No primeiro semestre de 2021, o bitcoin sofreu um dos ataques mais graves, quando a China – país que detinha cerca de 40 a 50% da capacidade de processamento da rede – banizou a mineração de bitcoin. A rede demorou um tempo para se reorganizar, mas menos de um ano depois o poder de processamento computacional já ultrapassou em mais de 30% as altas históricas pré-banimento. Ou seja, mesmo quando até 50% da rede foi obrigada a ser desligada, o bitcoin aguentou bem. O resultado prático desse ataque foi que a mineração se tornou mais descentralizada, uma vez que os mineradores deixaram a China e se espalharam pelo mundo, principalmente

no Cazaquistão e nos Estados Unidos. Ou seja, a partir de um ataque à rede bitcoin, a mineração se tornou mais descentralizada.

## Bitcoin é banido na China; país proíbe todas as transações em criptomoedas

Gabriel Sérgio | 24/09/2021 14h55, atualizada em 24/09/2021 15h27

### Bitcoin se recupera após banimento na China e hashrate atinge novo recorde

Poder computacional da rede Bitcoin atinge maior valor em sua história e demonstra que o blockchain da principal criptomoeda do mundo está mais seguro do que nunca

Por CoinDesk

Publicado em: 03/01/2022 às 12h39

Tempo de leitura: 3 min



### China: Proibição faz mineradores de bitcoin buscarem refúgio no exterior

Governo de Sichuan, segundo maior centro de mineração de bitcoin da China depois de Xinjiang, publicou a ordem de proibição da atividade há uma semana

Por Samuel Shen e Andrew Galbraith, da Reuters

25/06/2021 às 16:08

Compartilhe:



### “Banimento do Bitcoin pela China foi inócuo”, destaca diretor da QR Capital



Cripto | 10.10.2021 12:33

Compilado de manchetes sobre o banimento do bitcoin pela China e a sua falta de efetividade.

#### REGULAÇÃO

### Índia pode reconhecer bitcoin como ativo financeiro, diz jornal local

Segundo a publicação, governo deve discutir em julho um projeto de lei que classifica o bitcoin e as criptomoedas como classe de ativos financeiros

Por Gabriel Rubinstein

Publicado em: 10/06/2021 às 16h40

Tempo de leitura: 2 min



Poucos meses depois de ameaçar banir o [bitcoin](#), a Índia pode seguir o caminho oposto. Segundo fontes do governo ouvidas pelo [jornal](#) local "New Indian Express", o país deve classificar a [criptomoeda](#) como uma classe de ativo financeiro em breve.

Exemplo da Índia onde tentaram banir o bitcoin, somente para poucos meses depois ser obrigado a reconhecer ele como uma classe de ativo. Os países não mudam de ideia dessa maneira por coerência e lógica, eles mudam de ideia porque são obrigados. E eles são obrigados pois é impossível banir o bitcoin.

O bitcoin também já foi atacado diversas vezes dentro do seu próprio ecossistema. Diversos programadores já tentaram criar alterações no código do bitcoin. Quando estas alterações são consideradas deletérias pela comunidade de bitcoinheiros, elas são ferozmente combatidas. Este foi o caso de uma mudança que propunha aumentar os blocos das transações, o que supostamente melhoraria a escalabilidade do bitcoin. Essa proposta foi vista como um ataque à descentralização, pois para validar blocos maiores os full nodes teriam que ser mais potentes e possuir mais espaço de armazenamento, o que tornaria mais caro rodar um full node, assim menos pessoas o fariam. Esta discussão ganhou ares de guerra civil e se estendeu por anos. Se você quiser se aprofundar neste tema, leia o livro “Blocksize War”<sup>95</sup>. E, no final desta guerra civil, o bitcoin descentralizado, da maneira que foi originalmente concebido por Satoshi, saiu vencedor.

### **Ou seja...**

Formalmente falando, o bitcoin de fato não é e nunca será uma empresa. Ele é um protocolo monetário descentralizado, inconfiscável e incensurável, qualidades que seriam impossíveis de se alcançar caso o bitcoin de fato fosse uma empresa e tivesse um CEO.

Mas se você avaliar de uma maneira mais ampla e analisar qualitativamente, você pode se surpreender e chegar a conclusão que o bitcoin é a 1ª empresa descentralizada do mundo. Essa empresa possui fundamentos qualitativos que são tão bons quanto – ou melhores – que os fundamentos das principais empresas do mundo.

## CAPÍTULO 9

# ALUMÍNIO, ENERGIA E MINERAÇÃO DE BITCOIN

*Não desperdice energia, torne-a útil.*

Wilhelm Ostwald, Prêmio Nobel de Química (1909)

Os próximos dois capítulos são sobre a fusão que ocorrerá entre a mineração de bitcoin e o mercado de geração de energia. O capítulo 8 explica como a Islândia, uma ilha isolada no meio do oceano, utiliza uma commodity para monetizar sua energia ociosa. Já o capítulo 9 é uma exercício de futurologia e imaginação, onde o autor deste livro tenta imaginar as derivações da humanidade ter inventado uma tecnologia de monetização de energia ociosa chamada mineração de bitcoin.

### A produção de alumínio

Muitos se referem ao alumínio como “eletricidade sólida”, devido à grande quantidade de energia que é necessária para transformar a alumina no metal puro alumínio. Cerca de um terço dos custos do processo de obtenção são gastos com energia.

A produção do alumínio começa com a mineração da matéria bruta, uma rocha chamada bauxita (fórmula química  $\text{Al}(\text{OH})_3$ ), que nada mais é que um conjunto de óxidos de alumínio hidratado de forma impura<sup>96</sup>. Quando a bauxita é refinada, o óxido de alumínio puro obtido é conhecido como

alumina ( $\text{Al}_2\text{O}_3$ ). Essa alumina passa por uma purificação, sendo dissolvida em soda cáustica, para depois ser filtrada. Um pó branco de alumina puro é obtido e usado para obter o alumínio através da eletrólise.

Na eletrólise, a corrente elétrica na célula eletrolítica promove a redução da alumina e decanta o alumínio metálico no fundo da célula. O oxigênio liberado reage com o carbono do ânodo e vira dióxido de carbono.

Ou seja, no caso do alumínio, podemos entender que **matéria prima + eletricidade → alumínio**.

## O alumínio na Islândia

A Islândia é uma ilha vulcânica no meio do oceânico Atlântico, com população pequena, com cerca de 370 mil habitantes<sup>97</sup>, e com potencial de geração de energia praticamente infinito. Isso porque a Islândia é uma ilha que está localizada em cima da divisão entre duas placas tectônicas e em cima de uma pluma mantélica<sup>98</sup>, o que faz ela possuir fontes abundantes de energia geotermal<sup>99</sup>. Adicionalmente, eles também possuem um grande potencial hidrotermal relacionado ao degelo da neve e geleiras.

Como a população islandesa é pequena, grande parte deste potencial energético é subaproveitado. Isso porque para que uma fonte energética seja utilizada, ela precisa estar próxima de um mercado consumidor, uma vez que o processo de transporte de energia não é um processo eficiente. Ou seja, a Islândia não possui um grande mercado consumidor para a sua energia, o que significa que não existe incentivo econômico para desenvolvê-la.

Mas a produção de energia abundante tem um valor e a maneira que a Islândia encontrou para explorar esse valor foi com a transformação de bauxita em alumínio. A energia é tão barata neste país que se torna economicamente viável transportar a bauxita extraída na Austrália e no Caribe para ser transformada em alumínio lá.

Atualmente, a Islândia é o 10º maior produtor de alumínio do mundo<sup>100</sup>, apesar de não possuir nenhuma reserva da sua matéria prima, a bauxita. Na prática, como eles não conseguem vender a energia diretamente, eles a transformam em uma commodity e assim conseguem monetizar essa energia excedente.

“Estamos localizados no meio do Oceano Atlântico Norte. Não estamos conectados à rede da Europa continental, então exportamos

energia na forma de alumínio.” disse Bjarni Mar Gylfason, economista-chefe da Federação das Indústrias da Islândia<sup>101</sup>.

A indústria do alumínio se aproveitou deste fato e hoje cerca de 70% da energia produzida na Islândia é utilizada por ela<sup>102</sup>. O que ajuda a explicar como a Islândia consegue ser o país com a 10ª maior produção de alumínio mesmo sem possuir essa matéria prima.

## **A mineração de bitcoin**

De uma forma bastante simplista, o bitcoin pode ser entendido como um protocolo distribuído que automatiza e valida a liquidação de transações financeiras, enquanto cria unidades monetárias escassas para incentivar a alocação de recursos computacionais e energéticos. A prova de trabalho cria uma conexão entre os mundos físico e digital que não pode ser falsificada. Essa conexão é feita através do uso de energia para a mineração de bitcoins.

O algoritmo de prova de trabalho requer energia. Permanece a relação diretamente proporcional entre energia utilizada e poder computacional. Quanto maior o consumo de energia, maior o poder computacional, e maior é a probabilidade de se minerar um bloco.

Se a mineração de bitcoin pudesse ser reduzida a uma fórmula matemática, ela seria:

$$\text{energia} + \text{poder computacional} = \text{bitcoins}$$

No caso do alumínio, quanto mais energia é colocada na equação, mais alumínio é produzido; enquanto que com o bitcoin mais energia não significa que mais bitcoins serão emitidos. Isso porque quando ocorre um aumento no hashrate, ou poder computacional da rede, a dificuldade para se minerar um bloco aumenta de forma proporcional, e o mesmo vale para o caso oposto: quando o poder computacional agregado diminui, se torna mais fácil minerar um bloco.

## **Mineração móvel e o mapa topográfico**

Para a instalação de uma operação de mineração de bitcoin só é necessária uma fonte energética e uma conexão com a rede bitcoin (seja pela internet, seja via satélite<sup>103</sup>). Isso significa que uma das principais

características da mineração de bitcoin é a sua alta mobilidade, o que possibilita que essa indústria arbitre o preço mundial da energia, buscando sempre as fontes mais baratas.

Um modelo útil para visualizar este conceito é o do mapa topográfico energético, um mapa em que o que determina os picos e vales é o preço da energia, não a altitude do terreno. Adicionar a mineração de bitcoin à matriz energética mundial é equivalente a colocar um copo de água sobre este mapa topográfico energético — a água vai preencher os vales e suavizar a topografia como um todo. A altitude mínima deste novo mapa topográfico será mais alta, o que significa que os produtores de energia podem vender essa energia produzida por um preço basal superior a zero em regiões em que antes essa energia não era aproveitada por não ter um mercado consumidor próximo.

Faz sentido para os mineradores buscarem os locais com energia muito barata, fazendo todo o mercado energético ganhar um “pisso”, um preço mínimo para a energia ser comercializada.

## CAPÍTULO 10

# AS IMPLICAÇÕES DA MINERAÇÃO DE BITCOIN PARA O SETOR DE ENERGIA

Muito se fala sobre a mineração de bitcoin. Os críticos acreditam que ela irá acelerar as mudanças climáticas devido ao seu alto consumo energético, enquanto os seus apoiadores acreditam que essa atividade será responsável por uma grande revitalização no setor de produção de energia em todo o mundo.

Mas qual dessas visões faz sentido? O objetivo deste texto é mostrar porque os críticos estão equivocados e como a mineração do bitcoin está revolucionando o setor de energia como um todo.

### O que é a mineração?

Vamos começar pelo básico: o que é a mineração de bitcoin?

Na verdade, não se mineram bitcoins, mas sim um bloco. Os bitcoins são um incentivo dado aos mineradores para que os mesmos aloquem recursos computacionais para que os blocos sejam minerados. Para se minerar um bloco válido, é necessário resolver um problema matemático por tentativa e erro, e então anexar a prova de trabalho ao bloco para que ele seja válido e possa ser verificado por todos os nós da rede. Solucionar esse problema demanda poder computacional, portanto energia. O minerador que achar primeiro a solução do problema transmite o seu bloco para a rede, sendo recompensado por isso com as taxas de todas as transações do



respectivo bloco, assim como a taxa de subsídio (6.25 BTC atualmente).

Como os mineradores competem entre si, quanto mais energia um minerador utilizar, maior será o seu poder computacional e maior as suas chances de minerar o próximo bloco. Ou seja, como dito no capítulo anterior, se a mineração de bitcoin pudesse ser reduzida a uma fórmula matemática, ela seria **energia + poder computacional = bitcoins**.

Os críticos não gostam dessa relação de que quanto mais energia um minerador utilizar, maior a sua chance de minerar bitcoins. Eles focam na fotografia ao invés de olhar o filme, ou seja, eles olham somente para o consumo atual de energia e observam que existem fontes que não são limpas na geração dessa energia.

Mas com uma análise mais profunda, é fácil ver que:

- A indústria da mineração de bitcoin utiliza proporcionalmente muito mais energia renovável que qualquer outra indústria.<sup>104</sup>

- Ninguém pensa se outros gastos de energia, por exemplo as luzes de natal, são um desperdício. Esse discurso moralista só é aplicado ao bitcoin. Mas desperdício é questão de opinião e se os mineradores de bitcoin estão comprando essa energia, ela é útil para eles. Na visão do minerador, consumidor dessa energia, ela está sendo bem utilizada, assim como as luzes de natal são um uso adequado de energia para os entusiastas dessa época do ano.

- A mineração de bitcoin gera incentivos para uma revolução no setor de energia.<sup>105</sup>

É conhecimento comum que a indústria da mineração utiliza bastantes fontes renováveis e existem inclusive mineradoras como a Arthur Mining<sup>106</sup> que utilizam somente fontes renováveis de energia. Por outro lado, entender como a mineração de bitcoin está revolucionando o setor de energia não é tão simples.

Pensando nisso, este capítulo explicará como a mineração de bitcoin já está afetando profundamente o setor de energia.

### **Monetização do gás natural desperdiçado**

O gás metano, que também é conhecido como gás natural, é bastante utilizado no nosso cotidiano. Ele é extraído da terra em lugares específicos e transportado via gasodutos até distribuidoras.

O que pouca gente sabe é que ele também é um subproduto da produção do petróleo. Contudo, ele não pode ser transportado pelos oleodutos do petróleo e muitas vezes é economicamente inviável construir um gasoduto só para a utilização deste gás. Isso significa que atualmente muitas vezes o gás metano encontrado junto com petróleo é queimado sem ser utilizado, pensando somente em mitigar os seus efeitos ambientais.

A indústria de mineração de bitcoin é altamente móvel e adaptável e atualmente diversas operações estão sendo montadas nos locais em que há extração de petróleo. Os mineradores compram o gás dos produtores de petróleo e o utilizam para gerar eletricidade, e com isso minerar bitcoin.

Ou seja, agora ao invés de ter gastos com a queima deste gás, os produtores de petróleo conseguem monetizá-lo. Em outras palavras, um recurso natural que estava sendo desperdiçado passou a ser monetizado graças à mineração de bitcoin. Essa monetização pode ser a diferença que faça um projeto de extração de petróleo se tornar economicamente viável e sair do papel.

### **Equilibrando a rede energética**

O bitcoin é um consumidor insaciável de eletricidade, uma vez que utilizar mais eletricidade aumenta as chances dos mineradores serem recompensados. O que pouco se fala é sobre as implicações disso para a rede de energia.

Para isso, o primeiro passo é entender como as redes energéticas funcionam hoje em dia. Atualmente, nós não conseguimos armazenar eletricidade de uma maneira eficiente, o que significa que toda a rede de energia precisa ser dimensionada de acordo com o momento de maior demanda de eletricidade.

Gracas amineraçãodebitcoin,agorasetornouviáveleconomicamente construir redes energéticas superdimensionadas. Ou, em outras palavras, não é preciso levar em conta somente a demanda da população local próxima da fonte de energia para decidir pela viabilidade financeira de um empreendimento de geração de eletricidade. Agora, toda a forma de energia barata pode ser monetizada através do bitcoin, um comprador insaciável de eletricidade barata.

Isso significa redes de energia maiores e mais robustas, ou seja,

redes de energia que estão protegidas de apagões, como os que ocorreram no Texas em 2021. Redes maiores e mais robustas também significam que o preço da eletricidade tende a ficar mais barato, uma vez que os usuários não precisarão pagar mais pela redundância da rede. Agora, existe uma tecnologia de monetização de energia ociosa que comprará essa fonte de energia ociosa. Isso é o oposto do que temos observado na Alemanha, por exemplo, onde menos energia vem sendo produzida devido ao fechamento das usinas nucleares e com isso o preço da eletricidade teve aumentos consideráveis nos últimos anos.

### **Destravando fontes remotas de energia**

Um efeito direto do fato da mineração de bitcoin ser móvel é que ela pode ser usada para subsidiar o início de qualquer projeto de eletricidade, na fase anterior à chegada das linhas de transmissão. Existem também lugares com energia abundante que não estão conectados à rede elétrica devido a sua distância do mercado consumidor.

A implicação deste racional é que diversas fontes de energia isoladas agora podem ser aproveitadas. Da mesma forma que a Islândia transforma sua energia em alumínio para conseguir explorá-la comercialmente, agora qualquer localidade do mundo com energia barata pode utilizar o bitcoin da mesma forma. Ou seja, uma comunidade isolada no interior do deserto do Saara pode monetizar a energia solar, abundante na região. Nestes locais, a mineração de bitcoin permite que essa energia seja convertida em bitcoin. Ou seja, graças à mineração de bitcoin, agora é possível monetizar fontes de energia que estavam sendo desperdiçadas devido a sua localização afastada do mercado consumidor.

Ou seja, antes do bitcoin, era impensável aproveitar e monetizar fontes de energias remotas, como ilhas vulcânicas, desertos com alta incidência solar ou cachoeiras e rios distantes de mercados consumidores. Agora essa lógica mudou e qualquer fonte de energia pode ser monetizada. Isso significa que agora existe uma base sólida para o desenvolvimento destas localidades remotas.

Então, agora cachoeiras distantes de cidades podem ter sua energia aproveitada, assim como a energia solar em diversos desertos do mundo e a energia da variação das marés em todos os oceanos do mundo, entre

tantos outros exemplos possíveis. O problema da humanidade nunca foi falta de energia, e sim falta de incentivo econômico para organizar e aproveitar as diferentes formas de energia disponíveis no planeta. Agora, graças à mineração de bitcoin, esse incentivo existe.

A capacidade que a mineração de bitcoin tem de transformar energia em dinheiro via prova de trabalho é ideal para a otimização na utilização de diversas fontes de energia que, sem o bitcoin, estavam sendo desperdiçadas pela sociedade. Assim, a energia deixa de ser um fenômeno essencialmente local, visto que agora existe uma forma de tornar a produção de qualquer fonte energética isolada economicamente viável.

O bitcoin pode ser visto como um comprador universal de energia que estabelece um preço mínimo maior que zero, tornando essas fontes energéticas isoladas possivelmente economicamente viáveis. Esses incentivos econômicos irão impulsionar a mineração de bitcoins e irão transformar completamente o setor de energia nas próximas décadas.

### **O setor de energia e de mineração de bitcoin irão se fundir**

A convergência gradual dos setores de mineração de bitcoin e energético vem ocorrendo e ocorrerá nas duas direções. Os produtores de energia utilizarão a mineração de bitcoin para transformar a energia excedente em dinheiro. As mineradoras de bitcoin passarão a gerar sua própria energia buscando melhorar suas margens. Esse processo terá continuidade e é provável que no futuro a maioria das empresas não seja de um ou de outro setor, mas sim dos dois. É possível que as principais empresas geradoras de energia também sejam mineradoras de bitcoin e que esses dois processos se tornem tão interconectados que passem a ser vistos como uma coisa só: você produz energia e vende ela para quem estiver pagando mais, a rede bitcoin ou a rede municipal.

### **Ou seja...**

A mineração de bitcoin já está trazendo benefícios enormes para o setor de produção de energia. Não é exagero dizer que estamos presenciando o início de uma revolução energética subsidiada pelo bitcoin.

Os frutos dessa revolução serão:

- As redes energéticas se tornarão mais estáveis e seguras, com

preços menores para o consumidor final.

- Acesso a novas fontes de energia remotas, fornecendo a base para regiões remotas se desenvolverem.

- A emissão de grande parte do metano de origem antrópica será enormemente diminuída, visto que esse gás é uma fonte de energia desperdiçada e a mineração de bitcoin é a tecnologia de monetização de energia desperdiçada.

## PARTE 3 – A COMUNIDADE

*He who knows not, and knows not that he knows not - he is a fool, shun him.*

*He who knows not, and knows that he knows not - he is simple, teach him.*

*He who knows, and knows not that he knows - he is asleep, wake him.*

*He who knows, and knows that he knows - he is insufferable, use him.*

*He who knows, and knows that he knows not – he is wise, follow him.*

*Aquele que não sabe e não sabe que não sabe - ele é um tolo, evite-o.*

*Aquele que não sabe e sabe que não sabe - ele é simples, ensine-o.*

*Aquele que sabe e não sabe que sabe - ele está dormindo, acorde-o.*

*Aquele que sabe e sabe que sabe - ele é insuportável, use-o.*

*Aquele que sabe e sabe que não sabe - ele é sábio, siga-o.*

Victor de Mello, modificado de provérbio árabe

## CAPÍTULO 11

# O ETHOS DE UM BITCOINHEIRO

Desde que caí na toca do coelho, algo sempre chamou minha atenção: como os bitcoinheiros possuem um ethos próprio bastante particular. Primeiro, deixe-me explicar rapidamente o que é “ethos”: em resumo, ethos é o conjunto de valores e crenças que uma comunidade segue e compartilha (se você quiser uma explicação detalhada, veja a explicação do Wikipédia<sup>107</sup>):

### éthos

/ˈɛθɒs/

*substantivo masculino de dois números*

1. conjunto dos costumes e hábitos fundamentais, no âmbito do comportamento (instituições, afazeres etc.) e da cultura (valores, ideias ou crenças), característicos de uma determinada coletividade, época ou região.  
"o é. da Antiguidade grega, do povo brasileiro, dos nordestinos"
2. RETÓRICA (ORATÓRIA)  
parte da retórica clássica voltada para o estudo dos costumes sociais.

Definições de Oxford Languages

Também faz sentido para o texto explicar o que eu considero um “bitcoinheiro”. Um bitcoinheiro é alguém que realmente entendeu a tese do bitcoin e as suas mais variadas implicações. É difícil achar uma definição simples para isso, mas digamos que é alguém que já dedicou mais de 100 horas aos estudos, que sabe explicar por que Satoshi Nakamoto ter desaparecido

é algo positivo e que possui a grande maioria do seu capital (pelo menos o líquido) em bitcoin. Outros termos utilizados para um bitcoinheiro é maximalista ou maximalista tóxico.

Para mim, foi incrível ir entendendo essa questão, referente ao ethos dos bitcoinheiros, pois eu já me identificava com a maior parte desse ethos, antes mesmo de conhecer o bitcoin. A coesão em torno desses valores e crenças só aumentou a convicção.

Muitas vezes, essa coesão de valores faz com que diversas pessoas descrevam os bitcoinheiros como um culto de religiosos fanáticos. O que faz sentido, visto que, se nós plotássemos o comportamento dos bitcoinheiros com o dos fanáticos religiosos em um diagrama de Venn (aqueles gráficos com bolas que se sobrepõem)<sup>108</sup>, a sobreposição seria de uns 90% tranquilamente.

Uma religião possui diversas características fundamentais:

- A crença em um Deus ou deuses (ou seja, um teísmo<sup>109</sup>);
- Um mito fundador (Adão e Eva, por exemplo);
- Rituais de pertencimento e tradições (batismo, missa de domingo, circuncisão, uso de véus, quipás e assim por diante);
- Valores éticos e morais bem definidos.

Tais características significam, por exemplo, que o Budismo é muito mais uma corrente filosófica do que uma religião propriamente dita. Isso porque Buda era um humano (e não o filho de Deus) que se relacionou com humanos. Ou seja, apesar de possuir um mito fundador, rituais de pertencimento, tradições e valores éticos e morais bem definidos, o Budismo não possui uma deidade central, de maneira que chamá-lo de religião não é totalmente correto.

O mesmo se aplica ao bitcoin. No sentido estrito, o bitcoin não pode ser considerado uma religião, uma vez que não existem deuses associados ao conjunto de crenças que os bitcoinheiros seguem. OK, mas então quais são as outras características dos bitcoinheiros que fazem com que essa tribo se pareça com uma religião? Ou, em outras palavras, qual o nosso ethos?

Provavelmente cada bitcoinheiro terá uma resposta ligeiramente diferente para essa pergunta, e todas são direcionalmente corretas, visto que uma das principais características do bitcoin é ser uma rede descentralizada que não possui um ponto único de verdade. Lancei essa pergunta no Twitter e, apesar das variações semânticas, a maioria das respostas apresentadas



possuía um grande sentido comum. Dito isso, vou tentar sintetizar abaixo qual o sentido em comum mencionado, ou seja, quais as crenças e valores que definem o nosso ethos.

### **“Don’t trust, verify”**

Ou, em português, “não confie, verifique”. Para um bitcoinheiro, todo mundo é um golpista até que se prove o contrário. Nós sabemos que não podemos confiar em ninguém além de nós mesmos e que as coisas não virão de mão beijada. Em outras palavras, não existe almoço grátis e se alguém está te oferecendo isso, provavelmente é algum tipo de golpe.

Nós, bitcoinheiros, aprendemos desde sempre a não confiar no sistema tradicional e incentivamos os novatos a assumir a responsabilidade pela custódia das suas moedas. Assim como o “don’t trust, verify”, esta é uma crença poderosíssima para ensinar as pessoas sobre responsabilidade individual.

Percebe-se, assim, que somos profundamente desconfiados do sistema e das pessoas. A cena do filme Matrix, em que o Morpheus está explicando para o Neo como a Matrix funciona<sup>110</sup>, ilustra claramente este conceito.

Dont trust, verify é um valor que gera uma profunda mudança em todos os bitcoinheiros, visto que sua consequência natural é o aumento de um forte senso de responsabilidade individual. Essa forma de enxergar o mundo te obriga a repensar todas as suas escolhas e todos os dados em que você se baseou para fazer essas escolhas. Por exemplo: você acha mesmo que o ideal é comer a cada 3h como os nutricionistas fiat tanto falam?

### **“Not your keys, not your coins”**

No bitcoin, caso você perca as suas chaves (a senha para acessar os seus satoshinhos), ninguém poderá te ajudar. Você terá perdido esse dinheiro para sempre. Isso é totalmente diferente do mundo fiat, onde você pode ligar para um gerente do banco caso você perca o seu cartão de crédito ou esqueça a sua senha. Não à toa, estima-se que cerca de 20% dos bitcoins estão perdidos<sup>111</sup> e nunca mais serão acessados. Notícias de pessoas revirando lixões pelo mundo em busca de HDs antigos são comuns<sup>112</sup> e servem de alerta para todos os bitcoinheiros mais responsáveis.

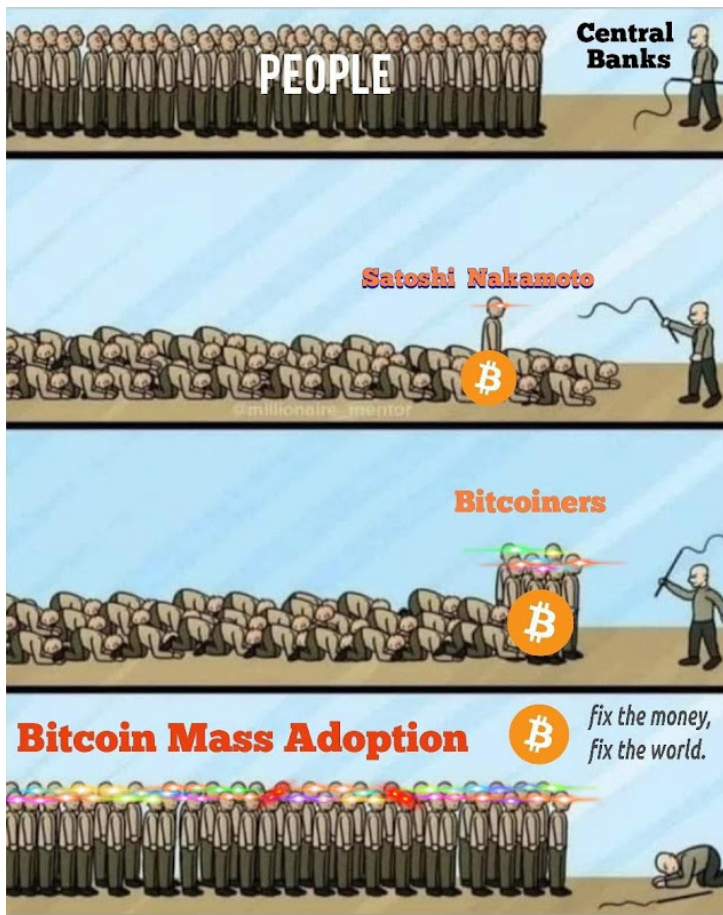
Isso pode soar assustador para muitos, mas se pergunte: como melhorar o mundo sem que os indivíduos desenvolvam responsabilidade individual?

### **Fix the Money, Fix the World**

“Conserte o dinheiro, conserte o mundo”. Ou, na sua versão mais completa: “Fix the Money, Fix the Individual, Fix the World”. Nós, brasileiros, temos uma péssima relação com dinheiro, dado que geralmente ele é fonte de angústia e apreensão. Somos ensinados, desde cedo, que “mais fácil é passar um camelo pelo fundo de uma agulha, do que entrar um rico no reino de Deus” ou, ainda, que “o amor ao dinheiro é a raiz de todos os males”. Esses conceitos moralistas são enganosos e nos fazem ter uma certa aversão natural ao dinheiro e aos ricos.

Ocorre que, na realidade, o dinheiro é a tecnologia, inventada pelo ser humano, que nos permite realizar trocas voluntárias com alguém de fora de nossa tribo. Se não fosse o dinheiro, a humanidade nunca teria ultrapassado o número de Dunbar<sup>113</sup> e estaria restrita a pequenas tribos de 100 a 230 pessoas, aproximadamente. O dinheiro é a camada base de comunicação de valor, uma vez que, sem ele, trocas não ocorreriam e pessoas com interesses diferentes não poderiam se conectar.

Como todo bitcoinheiro sabe, a grande maioria dos problemas do mundo está associada ao fato de que essa camada base de comunicação de valor (o dinheiro) está quebrada. Basicamente, o dinheiro foi usurpado da população e, agora, é controlado por uma pequena elite composta por banqueiros, banqueiros centrais e estados nacionais que manipulam essa camada base de acordo com os seus próprios interesses. É por conta dessa corrupção do dinheiro, também conhecida como Efeito Cantillon (tema do capítulo 2), que existe tanta desigualdade e injustiça no mundo.



Meme que ilustra bem a questão de “fix the money, fix the individual, fix the world”.

### Liberdade em 1º lugar

A liberdade é, com certeza, um dos valores supremos de todo bitcoinheiro. Não existe liberdade real sem liberdade financeira. Liberdade de um sistema opressor, que corrompeu a nossa camada base de comunicação e se apropriou dela. Nosso sistema financeiro atual (o sistema fiat) é lastreado em emissão de dívida, o que significa que o dinheiro fiat precisa ser inflacionário, pois a única forma de pagar essas dívidas é gerando inflação. Um sistema inflacionário baseado em dívidas é basicamente um sistema de escravidão por dívidas, onde você precisa trabalhar cada vez mais para receber um dinheiro que vale cada vez menos. Ou, como Michael Saylor<sup>114</sup> sintetizou esse pensamento de Hayek<sup>115</sup>: “A estrada para a servidão consiste

em trabalhar exponencialmente mais para ganhar um dinheiro que vale exponencialmente menos”.

Um dinheiro inflacionário, que vale cada vez menos, é uma maneira disfarçada de roubar o tempo das pessoas. O tempo utilizado por essas pessoas para gerar valor à sociedade é armazenado na forma de dinheiro, de maneira que, se esse dinheiro perde valor de maneira contínua, referido tempo é roubado, o que resulta na necessidade de uma quantidade de trabalho cada vez maior.

O bitcoin, por ser um dinheiro deflacionário, ou seja, um dinheiro que aumenta o seu poder de compra futuro ao invés de diminuí-lo, quebra no meio a lógica cruel descrita acima.

Nada torna um indivíduo mais livre e soberano do que um dinheiro que o empodera a falar “não”. Não, eu não vou trabalhar horas extras pois quero ficar com a minha família. Não, eu não vou me sujeitar a isso porque eu não preciso. E assim por diante.

Essa liberdade também permite que os bitcoinheiros escapem das armadilhas do coletivismo. Quando pessoas são incapazes de enxergar a saída para situações nas quais notam a diminuição constante de sua qualidade de vida, ou não entendem a razão pela qual tal diminuição ocorre, é muito fácil comprar discursos coletivistas de “bem comum” e de “taxar as grandes fortunas”. Em compensação, quando você entende o bitcoin e todas as suas derivações, você entende que você é o único responsável por si mesmo e que, na verdade, são esses mesmos políticos e banqueiros que usam tais discursos, coletivistas e vazios, que roubam o seu tempo.

### **Pensamento de longo prazo**

Outra grande ficha que cai quando alguém entende de verdade o bitcoin e se torna um bitcoinheiro é que o custo de oportunidade de tudo é o bitcoin. Esse pensamento é extremamente pesado, visto que todos nós compramos muitas coisas idiotas nos últimos anos, e esse dinheiro teria sido muito melhor investido se tivesse sido transformado em satoshis.

Uma consequência de se entender isso é a mudança de preferência temporal, ou seja, os bitcoinheiros deixam de valorizar as gratificações imediatas e passam a desenvolver um pensamento de longo prazo.

Tal pensamento de longo prazo, além de valer para decisões

financeiras como, por exemplo, a de comprar um carro novo ou continuar indo de bicicleta ou ônibus para o trabalho, influencia também em diversas outras partes de nossas vidas.

São comuns os relatos de bitcoinheiros que começaram a fazer mais atividade física ou a ler e estudar mais a partir do momento que eles realmente entenderam o bitcoin. E por que isso? Porque não adianta nada ficar rico e estar com a saúde debilitada ou não ter se desenvolvido intelectualmente.

As consequências do pensamento de curto prazo são vistas em todos os lugares da nossa sociedade, repleta de gordos reclamando de “gordofobia” em vez de começarem a se exercitar e de pessoas que preferem ver uma série no Netflix ou o Big Brother em vez de ler um livro. E o bitcoin conserta isso, ensinando as pessoas a adiarem as gratificações presentes e, com isso, irem bem no teste do marshmallow<sup>116</sup>.



Adiar as gratificações imediatas não é uma tarefa simples, como essa versão do teste mostra<sup>117</sup>.

### **Descentralização é superior**

A descentralização é uma característica fundamental da rede bitcoin. É ela que garante que as transações sejam incensuráveis, isto é, que as transações de bitcoin não possam ser interrompidas por governos corruptos ou mesmo por pessoas discriminando outras pessoas por cor, credo ou orientação sexual.

Além disso, sistemas descentralizados são muito mais eficientes em processar informações e lidar com incertezas quando comparados a

sistemas centralizados. Um belo exemplo disso é citado no livro *Antifrágil*, do Nassim. Um ministro da URSS foi visitar Londres para aprender e talvez importar lições positivas para a União Soviética. Depois de visitar e de ser apresentado a banqueiros e ministros, ele ainda tinha uma dúvida: como os ingleses faziam para distribuir o pão tão bem e nem ter filas?

Essa pergunta não fez sentido algum para os londrinos, uma vez que simplesmente não se fazia nada em relação ao pão. Eles simplesmente deixavam o livre mercado funcionar. Por outro lado, na URSS, existiam filas gigantes para a distribuição dos pães e os cálculos de quanto trigo produzir, quantos pães fazer por dia e como distribuir esses pães eram complicadíssimos.

Esse exemplo ilustra um grande problema de sistemas centralizados que é o intervencionismo ingênuo. Isto é, mesmo que você esteja muito bem-intencionado e acredite estar fazendo o bem, a capacidade de processamento de informação de um sistema centralizado sempre será inferior à capacidade de processamento de um sistema descentralizado.

Outro exemplo disso são os bandos de andorinha: não existe um agente central dizendo como cada uma delas deve voar. O que ocorre é que elas tomam decisões próprias, baseadas no comportamento das outras andorinhas em seu entorno. A somatória dessas pequenas decisões em um grupo grande de andorinhas é que gera o padrão final do seu voo coletivo. Em outras palavras, quando cada agente toma suas próprias decisões egoístas, as informações passam a ser processadas de uma maneira muito mais eficiente, o que jamais seria alcançado por um planejador central.



Nenhuma entidade centralizada controla o voo de um grupo de pássaros<sup>18</sup>, e nem deveria tentar controlar nenhum sistema complexo.

### **Código Aberto**

Um dos pilares fundamentais do ethos bitcoinheiro é o código aberto. Isso é válido no senso estrito dos programas de computador, visto que o fato de o código ser aberto é o que permite que ele seja verificado pela comunidade.

Os bitcoinheiros também valorizam o conceito de código aberto no sentido amplo, o que significa dizer que o conhecimento deve ser compartilhado. Nós, instintivamente, rejeitamos os gatekeepers (expressão em inglês que significa “porteiro”, no sentido de quem controla o fluxo do conhecimento) e acreditamos que a educação e o conhecimento devem ser livres.

Exemplos de gatekeepers são abundantes no mundo fiat, e os bitcoinheiros rejeitam todos eles. Um exemplo que para mim é bastante ilustrativo e próximo (visto que, antes do bitcoin, eu estava na academia perseguindo uma carreira universitária), é como as editoras de artigos científicos agem. As editoras cobram 35 dólares pelo acesso ao conhecimento e não pagam nada, nem para os revisores, nem para os autores desses artigos. Elas basicamente ganham bilhões de dólares (somente a Elsevier faturou mais de 9 bilhões de dólares em 2019) por serem as porteiras deste conhecimento. Entretanto, graças ao pensamento de código aberto e a

cazaquistanesa (e minha musa inspiradora) Alexandra Elbakyan, hoje em dia estudantes e pesquisadores têm acesso a todo o conhecimento acumulado pela humanidade de forma totalmente gratuita.

**Modelo aberto de acesso  
ao conhecimento**

**X**

**Modelo de acesso ao conhecimento  
dependente dos gatekeepers**



The image shows a comparison between two models of knowledge access. On the left, the Sci-Hub banner features a crow holding a red key, with the text "SCI-HUB" in large red letters, followed by "...to remove all barriers in the way of science" in a red arrow, and a search bar below. On the right, a screenshot of Elsevier's PDF purchase options shows a price of \$35.95 for academic use, with a "Purchase PDF" button at the bottom.

Sci-hub representa o pensamento de código aberto enquanto a Elsevier representa o pensamento dos gatekeepers.

## Proof of Work

O conceito de prova de trabalho (PoW, na sigla em inglês) é algo que foi esquecido na nossa sociedade fiat. Nós vivemos em uma sociedade que favorece os cantilionários, ou seja, quanto mais próximo a pessoa está da máquina de impressão de dinheiro, mais benefícios ela colhe. Assim, o seu talento e o seu esforço se tornaram coisas secundárias. Os valores foram distorcidos a tal ponto que, hoje em dia, "meritocracia" virou um palavrão e empresas precisam contratar de acordo com a "diversidade" (entre aspas, pois essa diversidade não abrange a diversidade de pensamento) e não com a competência.

Mas o bitcoin não se importa com nada disso. A rede bitcoin é apolítica, laica e não possui a capacidade de discriminar ninguém. No bitcoin, ninguém possui vantagens injustas.

Para se tornar um bitcoinheiro é necessário muito trabalho. Muito estudo e dedicação. Pessoas inteligentes começam a entender o bitcoin de verdade após aproximadamente 100 horas de estudos; já pessoas normais precisam de pelo menos 1000 horas. Se tornar um bitcoinheiro é PoW e, por isso, um dos mantras da nossa comunidade é que "cada um vai comprar



bitcoin no preço que merece”. Eu concordo com isso, e estou dentro da toca do coelho há menos de 2 anos. Eu poderia ficar ressentido e pensando no tamanho da oportunidade que eu deixei passar ao não comprar bitcoin antes, mas eu sou humilde o suficiente para entender que eu não mereci ter comprado antes por nunca ter me dedicado e estudado a fundo o assunto. Eu caí no conto das tulipas e isso não é culpa de ninguém, só minha.

A ideia de PoW também gera um grande respeito à propriedade privada e ao mérito de cada um. Penso nos bitcoinheiros mais antigos como gurus com os quais posso e devo aprender e não com inveja. Eles têm PoW de uma época em que as informações eram mais difíceis e esse mérito ninguém tira deles.

### **Pseudônimos**

Para muitos que ainda não se tornaram bitcoinheiros, nossa tribo pode parecer estranha. O fundador é desconhecido, as discussões no Twitter são feitas por um monte de avatares, e até mesmo o modelo de precificação que é mais levado a sério foi feito por um boné.

Para um bitcoinheiro, é assim que o mundo deve ser. Nós rejeitamos argumentos de autoridade e suspeitamos profundamente de qualquer pessoa que tente se validar com credenciais. Nós suspeitamos de contas verificadas no Twitter e suspeitamos de pessoas que exibem um MBA ou um PhD nas suas informações pessoais. Na nossa linguagem, essas são credenciais fiat e possuem pouquíssima relevância, ou até depõem contra a pessoa. Querer ser reconhecido por um título, no nosso ponto de vista, mostra insegurança no argumento e tentativa de vencer por carteirada, o famoso “você sabe com que você está falando?”

O mérito é das ideias, e nós julgamos e sempre julgaremos todas elas independente de qual for a fonte. Argumentos ad hominem<sup>119</sup> não nos representam e, na verdade, geram o efeito contrário. Nós rejeitamos argumentos ad hominem por achá-los desonestos e enviesados.



Estátua sem rosto construída em homenagem a Satoshi Nakamoto (utilizada como referência na capa deste livro) e o avatar de um boné utilizado pelo Plan B, quem primeiro propôs o modelo de stock-to-flow (S2F), o modelo de precificação do bitcoin mais respeitado.

## **Ou seja...**

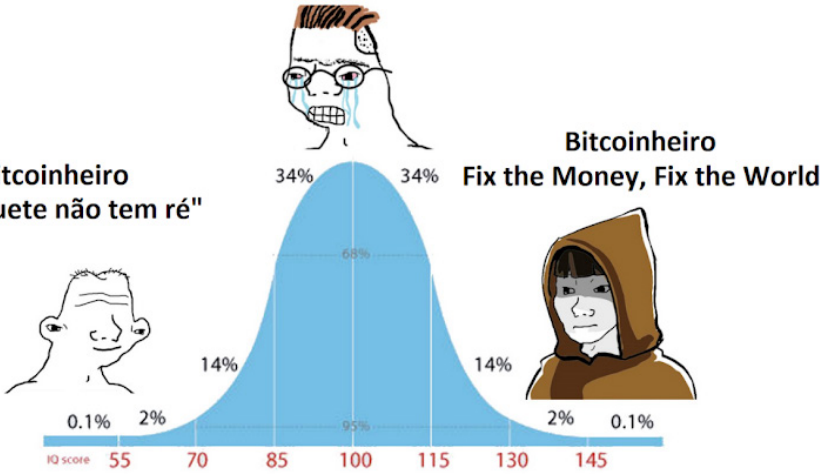
Você pode pensar que o bitcoin é um culto de fanáticos, uma religião ou uma corrente filosófica. Isso é uma questão semântica e depende da definição de religião que quisermos utilizar. Se uma religião não precisar de teísmos, somos sim uma religião. Temos o senso missionário de ter encontrado uma verdade tão verdadeira que queremos mostrá-la para todas as pessoas que amamos. Queremos espalhar o amor e a salvação ao próximo, tal qual a maioria das religiões.

Você pode ou não concordar com nossos valores, mas eles são inegociáveis para um bitcoinheiro.

E, se você acha que o bitcoin é uma religião ou corrente filosófica, você entende porque o bitcoin nunca irá a zero. Os romanos tentaram zerar o cristianismo por mais 300 anos até que o imperador Constantino liberasse esse “culto de fanáticos”. Menos de 100 anos depois, o império romano já estava convertido ao cristianismo. Ou, numa linguagem mais atual, “ideias são à prova de bala”, como já dizia o filme V de Vingança<sup>120</sup>.

## Cético/shitcoinheiro

Bitcoinheiro  
"Foguete não tem ré"



## CAPÍTULO 12

# A PERSONALIDADE DE UM BITCOINHEIRO

Uma coisa que sempre chamou a minha atenção desde que caí na toca do coelho foi como a personalidade dos bitcoinheiros tende a ser parecida. O bitcoin seleciona determinados padrões de comportamento, atraindo pessoas com determinadas características de personalidade e repelindo outras com características diferentes.

Eu sempre reparei isso no Bitcoin Twitter, a bolha dos bitcoinheiros no Twitter, mas nunca tinha pensado mais profundamente a respeito. Uma sequência de publicações do Brandon Quitten me elucidou a questão de “o que faz algumas pessoas entrarem na toca do coelho enquanto outras pessoas evitam a toca a todo custo? O que leva alguém a seguir o coelho branco (follow the white rabbit<sup>121</sup>)?”

### Teste de Myer Briggs

Todos nós já vimos diversos testes de personalidade em revistas e jornais. Existem uns mais sérios, outros menos. E com certeza eles são em parte pseudociência e se aproveitam do instinto humano de querer fazer parte de um “nós”, de pertencer a um grupo, de ter um bando.

Dois testes de personalidade conhecidos são os testes de Myer Briggs e o RIASEC. O RIASEC<sup>122 123</sup> é o teste que orientadores profissionais utilizam no seu dia a dia, mas o Myer Briggs<sup>124</sup> é o mais conhecido e comentado na

internet de modo geral. Então esse capítulo só focou no Myer Briggs, mas o pensamento com certeza é extrapolável e enquadra outros tipos de testes.

O teste de Myer Briggs fatia as nossas personalidades em 5 características<sup>125</sup> principais e a partir dela constrói os arquétipos de cada personalidade. Isso significa que, diferentemente de tarô, zodíaco e outros esoterismos que se baseiam em aleatoriedades externas às pessoas, ele nada mais é do que um teste descritivo, que forma grupos de acordo com as características de cada um.

Essas características que o Myers Briggs usa para agrupar as pessoas são:

**Mente** - mede como você se relaciona com seu ambiente: você é introvertido ou extrovertido?

**Energia** - mede como vê o mundo e processa informações: você é uma pessoa intuitiva ou observadora?

**Natureza** - mede como a gente toma decisões e lida com emoções: de forma racional ou sentimental?

**Táticas** - mede como a pessoa aborda o trabalho, se planeja e toma decisões: de uma forma julgadora ou exploradora?

**Identidade** - mede quão confiante a pessoa é enquanto ela vive a vida: ela é uma pessoa assertiva ou cautelosa?

Ou seja, dependendo de como a pessoa é nessas diferentes categorias ela é classificada de uma maneira diferente.

## Os meus resultados e a validade desses testes

Eu já fiz esse teste algumas vezes na vida e meus resultados sempre variaram entre INTJ, INTP ou ISTJ. São personalidades até que parecidas e pegando a "média" delas, vamos dizer pelo resto deste texto que eu sou INTJ, conhecida como "arquiteto"<sup>126</sup>.

Isso significa que eu sou introvertido (mente), intuitivo (energia), pensante (natureza), julgador (tática) e assertivo (identidade). Lendo mais sobre as características do "arquiteto", eu realmente me identifico com essa personalidade. Contudo, eu também me identifico com a INTP ("lógico"<sup>127</sup>) e com a ISTJ ("logístico"<sup>128</sup>), o que já me levanta uma pulga atrás da orelha: se eu me identifico com várias, será que esses testes não são só mais um tipo de zodíaco em que nós procuramos pertencimento e nos identificamos com

várias coisas sempre?

Outra pulga atrás da orelha que sempre aparece quando estou preenchendo esses testes é a seguinte: como eu devo responder eles? Com a minha visão sobre mim mesmo ou com a visão que as outras pessoas têm de mim (e que eu não necessariamente concordo)? Será que a minha visão de mim mesmo é imparcial? Ao mesmo tempo, será que os outros realmente me conhecem e sabem as minhas motivações? Parecem dúvidas bestas, mas isso com certeza coloca em xeque toda a validade destes testes e justificam que nós os enxergamos só como uma brincadeira e não como algo científico.

Imagine uma pessoa que preencha três testes desses de acordo com a) como ela acha que as pessoas a veem, b) como ela se vê e c) tentando ativamente ser "imparcial" e fazer um balanceamento entre a) e b). Essa pessoa vai ter três resultados diferentes, ou seja, três personalidades.

Ok, com essas ressalvas feitas, vamos para a parte mais divertida do capítulo.

## As personalidades mais comuns na comunidade

Bom, como eu disse acima, o que me levou a pensar nesse assunto foi este fio<sup>129</sup> do Brandon Quintten no Twitter. Ele fez uma enquete no seu perfil sobre qual personalidade de Myer Briggs seus seguidores eram e obteve mais de 500 respostas. Essa é uma amostragem pequena e enviesada, pois nem todos os bitcoinheiros usam o Twitter. Então é possível argumentar que essa amostragem representa bem mais os bitcoinheiros do Twitter do que todos os bitcoinheiros do mundo. Mas os dados são muito interessantes e acredito que são representativos da maioria dos bitcoinheiros que eu já conheci até hoje. E provavelmente uma amostragem significativa dos maximalistas utilizam o Twitter.

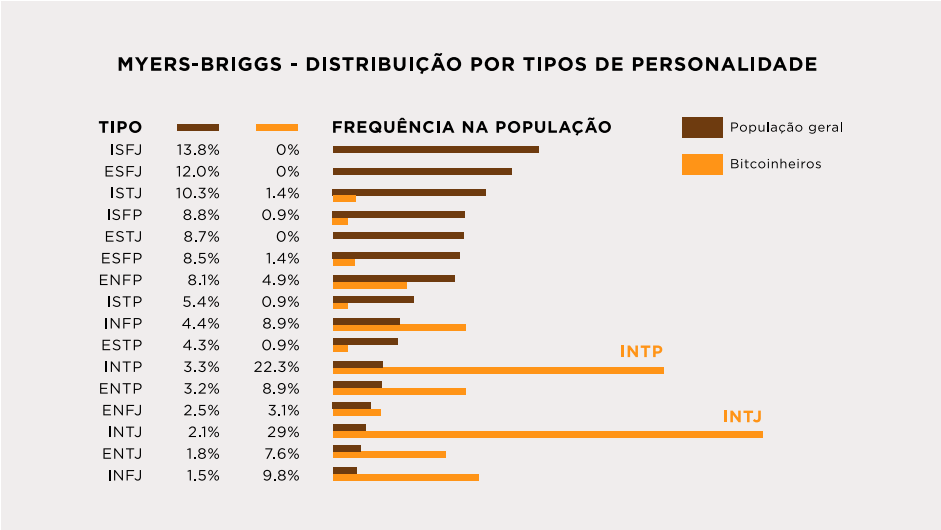
Vamos aos dados:

- 25% da população geral (normies + bitcoinheiros) é ISFJ ("defensor"<sup>130</sup>) ou ESFJ ("consul"<sup>131</sup>) e 0% dos bitcoinheiros se identificam com esse tipo de personalidade. Essas personalidades são "cordiais, responsáveis e reservadas" e realmente não se encaixam com a visão de mundo de um bitcoinheiro.

- A população geral está bem dividida entre introvertidos (50%) e extrovertidos (50%), enquanto que entre os bitcoinheiros do Twitter a maioria

é introvertida (73% contra 27% de extrovertidos).

- Existem duas personalidades que representam mais da metade dos bitcoinheiros (51%) e que são pouco representativas (5.4%) na população geral. São elas: 1) INTP (os lógicos), que representam 3.3% da população geral e 22.3% dos bitcoinheiros e 2) INTJ (os arquitetos), que representam 2.1% da população geral e 29% dos bitcoinheiros. Essas personalidades são “altamente analíticas, criativas, lógicas e valorizam o conhecimento” e são praticamente 10x mais comuns entre os bitcoinheiros do que entre a população normal (51% x 5.4%).



Como alguém que sempre oscila de resultados entre os INTP e INTJ, essa conclusão me pareceu interessante e fez bastante sentido. Isso explica porque eu me sinto tão à vontade no meio dos bitcoinheiros: a metade deles é realmente que nem eu! Temos as mesmas características básicas de personalidade, o que permite que nos conectemos melhor.

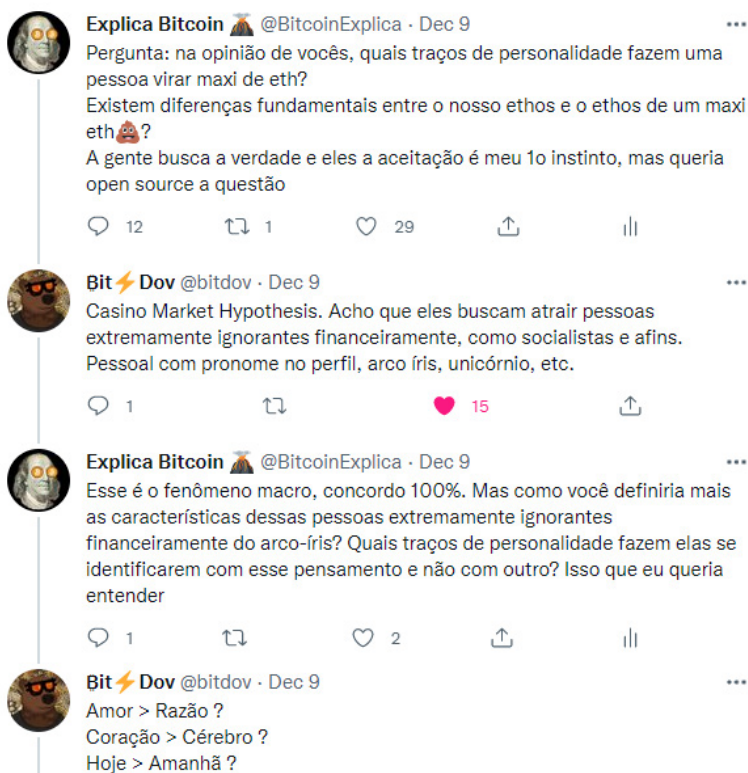
**Personalidade dos shitcoinheiros?**

O que me fez ficar curioso. Se os bitcoinheiros são tão parecidos (em média), será que essa mesma verdade vale para os shitcoinheiros? Será que eles possuem características fundamentais que os façam se identificar com determinado tipo de visão de mundo e comportamento?

Eu lancei essa pergunta no Twitter e tiveram respostas legais. A

melhor síntese pros propósitos deste texto foi essa do Dov<sup>132</sup>:

Amor > Razão ?  
Coração > Cérebro ?  
Hoje > Amanhã ?



Ele instintivamente acertou traços de pessoas “cordiais e responsáveis”, as personalidades ausentes entre os bitcoinheiros. São pessoas que têm dificuldade de falar verdades duras. Elas provavelmente preferem dourar a pílula ao invés de serem precisos na linguagem.

Eu fiquei pensando sobre isso também. Não encontrei nada de dados e o ideal seria conseguir fazer uma pesquisa com os “maxis de Ethereum” ou de DeFi e NFTs (eles existem?) e outros shitcoinheiros para ter uma visão mais completa. Mas minhas inferências (sem nenhum embasamento) são que o resto da comunidade “cripto” terá uma porcentagem maior das



personalidades que estão sub representadas entre os bitcoinheiros. A partir desta inferência e alguma observação, extrapolo que eles acreditam que a preservação dos sentimentos e o bem estar de todos é mais importante do que a busca pela verdade.

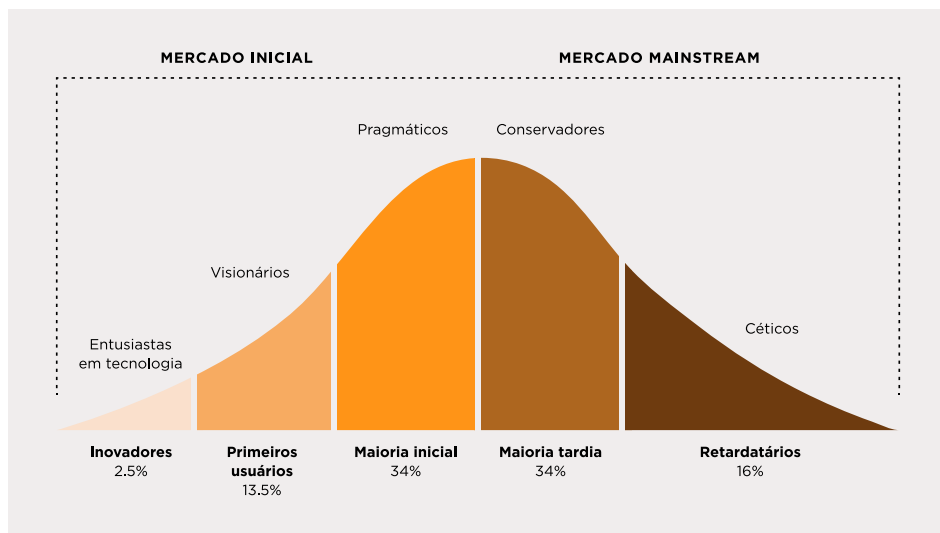
Pegando o vocabulário do LaserHodl<sup>133</sup> emprestado, são os “safe space maxis”, ou maximalistas de espaços seguros e protegidos. O mundo em plástico bolha. A aceitação e a empatia são os valores mais fortes. Algo como “a união faz a força”, “vamos todos nos abraçar” ou ainda “estamos todos juntos nessa”.

Mas isso são só extrapolações, o ideal seria conseguir fazer o mesmo teste de personalidade tanto com bitcoinheiros maximalistas e shitcoinheiros brasileiros para ver quais seriam os dados.

## Curva de adoção

Este pensamento de personalidades sub representadas entre os bitcoinheiros também gera outras reflexões.

Atualmente, ainda estamos em um estágio bem inicial da curva de adoção do bitcoin como tecnologia. Se a gente considerar o modelo padrão de adoção, ainda devemos estar entre os inovadores e os primeiros usuários. Ou seja, nem 15% da adoção do bitcoin já ocorreu. De fato, dependendo dos critérios usados para adoção, o número pode variar algo entre 200 milhões (dado que leva em conta os curiosos que compraram menos de 1% da sua carteira de investimento) até 250 mil (estimativa do Croesus para o número de bitcoinheiros maximalistas que existe no mundo<sup>134</sup>).



Esses 250 mil parece um número bem conservador, mas na minha opinião ele é o mais realista. Isso porque quem tem 1% ou mesmo 5% do patrimônio em bitcoin não deveria ser realmente considerado como “adoção”. Essa pessoa ainda está utilizando outro padrão monetário e utilizando o bitcoin como “hedge”, ou seja, ela ainda não entendeu e adotou o padrão bitcoin de fato.

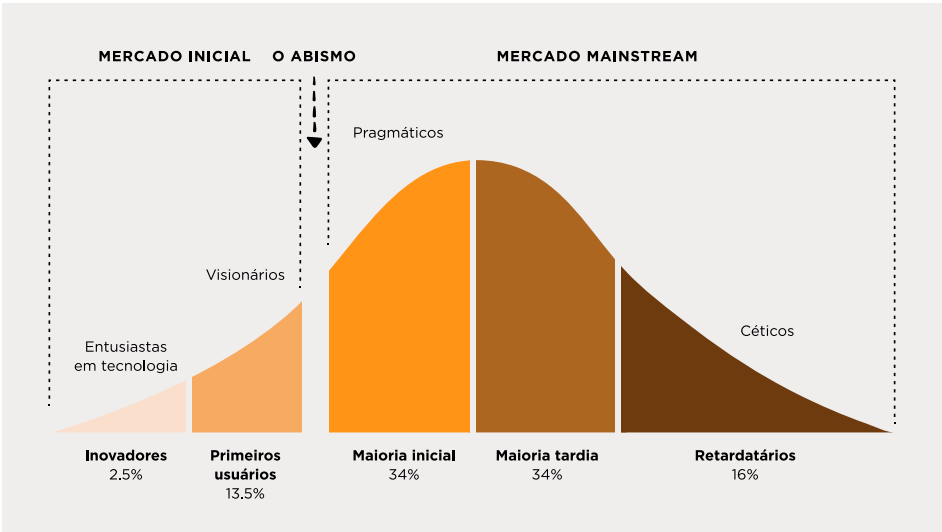
Faz sentido que a adoção do bitcoin esteja ocorrendo de forma seletiva e que os primeiros usuários (entusiastas em tecnologia e visionários) apresentem determinados perfis de personalidade (no caso do bitcoin, são INTP e INTJ). Estes grupos de entusiastas de tecnologia e visionários possuem características de personalidade bastante diferentes do restante da população.

## O Abismo

Um conceito relacionado à curva normal de adoção é o chamado “abismo”, que ocorre entre os primeiros usuários e o restante da população. Esse abismo é relacionado justamente às diferenças psicológicas e sociais entre estes dois grupos.

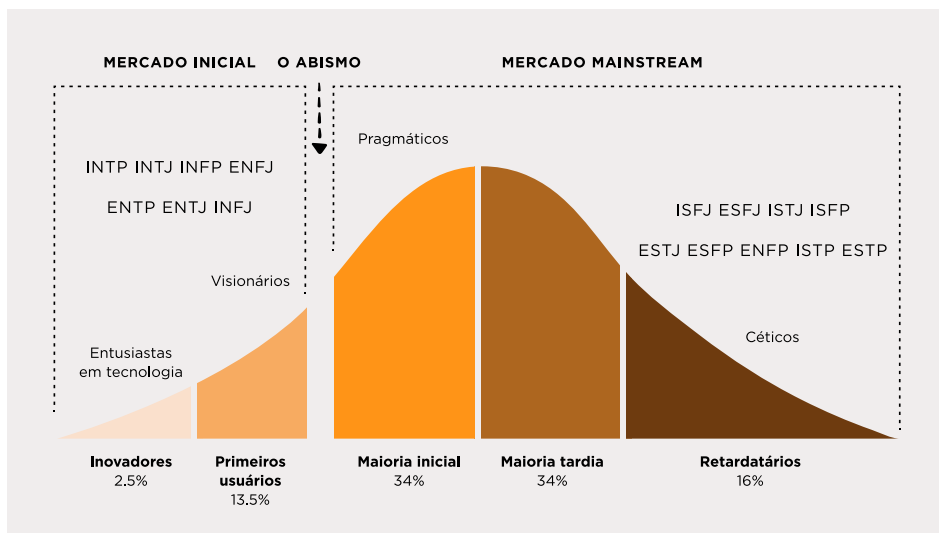
Os primeiros usuários são visionários em busca de mudanças revolucionárias. Eles veem um problema com o status quo e desejam ativamente adotar tecnologias que consertem isso. Eles estão dispostos a

assumir grandes riscos para impulsionar mudanças sociais de zero para um<sup>135 136</sup>. Por outro lado, os usuários da maioria inicial são pragmáticos e avessos ao risco. Eles estão procurando soluções incrementais e confiáveis. A maioria inicial não é influenciada pelos primeiros usuários, pois são de tribos fundamentalmente diferentes, o que gera o abismo.



Não parece uma extrapolação muito arriscada dizer que as pessoas do outro lado do abismo são justamente os grupos que estão menos representados na comunidade bitcoinheira. Essas outras personalidades, em média, não falam a nossa língua e não fazem parte da nossa tribo. Elas não possuem o nosso ethos e preferem uma comunicação sensível e harmoniosa em detrimento de uma comunicação que priorize a verdade, por mais áspera que ela seja. Às vezes a verdade é incômoda e existem aqueles que preferem mentiras suaves.

## Intuitivos X Observadores



É interessante notar que o traço mais comum entre os bitcoinheiros é o “N” na segunda letra, que significa que a nossa “energia” (ou seja, como a gente processa as informações do mundo) é intuitiva e não observadora.

Essas duas características são utilizadas para descrever o que as pessoas têm mais probabilidade de fazer com as informações coletadas do mundo ao seu redor. Os tipos de personalidade “Intuitiva” dependem da capacidade de extrapolar o que pode acontecer no futuro com base em fatos passados. Eles extrapolam cenários e hipóteses antes de conseguir chegar a uma decisão. Já as pessoas do estilo “Observador” estão mais interessadas em fatos observáveis e resultados mais diretos. Eles preferem evitar muitas camadas de interpretação sobre o que elas observam. Pessoas observadoras são mais pragmáticas e realistas.

**Intuitivos - “olhos no horizonte”** - as pessoas com o traço intuitivo preferem exercitar sua imaginação enquanto buscam novas idéias e possibilidades. Essas pessoas vivem suas vidas cotidianas como qualquer outro tipo de personalidade. Mas enquanto isso está acontecendo, suas mentes tendem a olhar para dentro e, ao mesmo tempo, focam suavemente em algum lugar além do horizonte. Suas vidas são de questionamento, investigação e conexão dos pontos no “quadro geral” das coisas. Intuitivos amam o teórico.

Eles costumam perguntar: "E se?" e ponderar as possibilidades que o futuro pode oferecer.

**Observadores - "faça o que funciona"** - os Observadores estão mais em contato com o que ocorre na frente deles e no presente. Isso não significa que os tipos de personalidade Observadores não se importam com o passado e o futuro. Mas eles veem ambos da perspectiva de como cada um influencia suas ações presentes. Isso os torna pessoas focadas e práticas. Eles enraízam seu pensamento principalmente no que é acionável, tangível e útil.

Em uma pesquisa da Practical Mind<sup>137</sup>, 91% daqueles com o traço intuitivo dizem que gostam de discutir diferentes visões e teorias sobre como o mundo poderia ser no futuro, em comparação com 55% daqueles com o traço observador.

Enfim, em média os bitcoinheiros atuais são intuitivos e os normies tendem a ser observadores. O que levanta diversas questões relacionadas à educação sobre o bitcoin e a adoção.

## O Ponto da Virada

No sentido "seleção darwiniana de um bem monetário, pautada na teoria dos jogos" o bitcoin provavelmente já ganhou. Uma mera comparação entre as suas características com as características de outros bens monetários como o ouro e o fiat ilustra isso. Esse fato faz com que muitos acreditem que o bitcoin é inevitável. Possivelmente ele até seja. Mas sempre existem vários caminhos possíveis para subir uma montanha, e nós ainda podemos tentar ajudar a determinar a forma com que essa adoção irá ocorrer.

O livro "Ponto da Virada", do escritor Malcolm Gladwell, fala sobre o que é necessário para fazer ideias viralizarem. O termo ponto de virada faz referência ao momento de não-retorno, quando as ideias pegam embalo e se propagam por conta própria. O autor cita três fatores que são responsáveis por fazer ideias se propagarem além desse "ponto da virada", que também pode ser visto como o "abismo" entre os primeiros 15% de usuários e os outros 85%. Esses fatores são:

**Regra dos Eleitos** - os eleitos são as pessoas necessárias para dar início a uma dispersão viral. Esses eleitos não precisam ser muitos, só alguns

poucos e bons já são o suficiente para criar um movimento. Existiriam 3 perfis entre os eleitos:

- Comunicadores: indivíduos com um networking extenso e que constroem pontes entre as pessoas da sua rede.

- Experts: indivíduos que consomem e distribuem informação no seu círculo social. Eles são o tipo de consumidor que compreendem os detalhes técnicos e sentem prazer em ajudar e instruir outras pessoas com o seu conhecimento.

- Vendedores: são indivíduos carismáticos capazes de persuadir outros em suas decisões de compra e comportamento.

**Fator de Fixação** - O fator da fixação é fundamental para que a mensagem seja fácil de compreender, memorizar e transmitir.

**Poder do Contexto** - Existe uma hora certa e um lugar certo para fazer as coisas. Sem o contexto adequado e o momento oportuno, a dispersão de uma ideia enfrenta ventos contrários e é dificultada. Uma frase que explica bem isso é que "texto sem contexto é pretexto".

## O Funil de Vendas

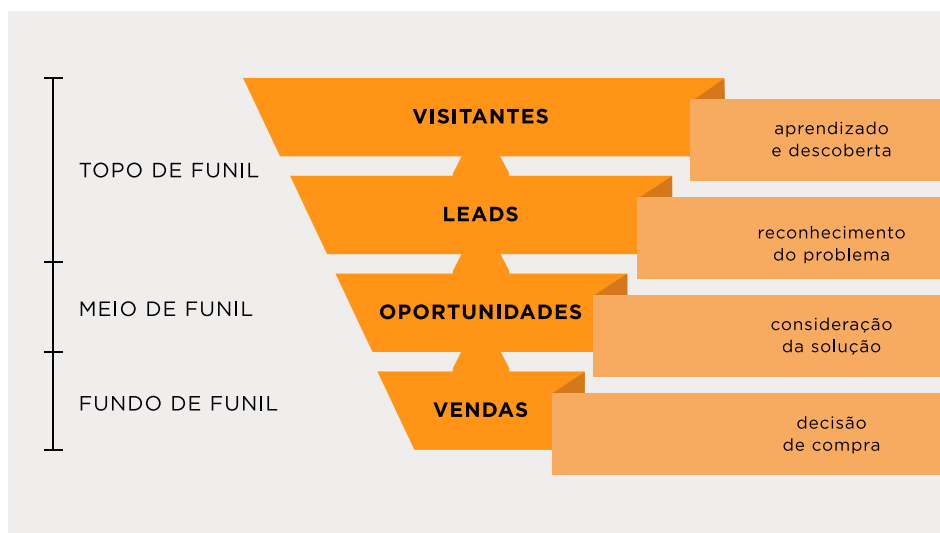
Entre os bitcoinheiros, existem muitos comunicadores e experts, porém existem poucos vendedores. Pensando nisso, essa seção fará uma breve explicação sobre um conceito básico de vendas, o "funil de vendas".

O funil de vendas pode ser visto como a "toca do coelho" do processo de vendas. Ele separa as fases que um potencial cliente passa até efetuar uma compra. Esse funil de vendas é segmentado conforme o cliente em potencial vai conhecendo mais um determinado produto: quanto mais fundo, maior a chance de fechar negócio.

**Topo de funil** - estágio de aprendizado e descoberta, quando o potencial cliente ainda está descobrindo que o seu produto existe. Neste momento o problema que o seu produto resolve é apresentado ao potencial cliente.

**Meio de funil** - estágio em que o cliente está prestando atenção e se educando, mas ainda não tomou nenhuma decisão. Ele está considerando qual a solução mais adequada para o problema em questão.

**Fundo de funil** - estágio de decisão de compra. É quando o cliente realmente efetua a compra.



Tanto os vendedores como as equipes de marketing desenvolvem estratégias de comunicação diferentes para cada estágio deste funil. Assim existem conteúdos mais simples para o topo do funil e conteúdo mais profundo e detalhado para quem já está mais próximo do fundo.

O estudo do bitcoin também segue (ou pelo menos deveria seguir) esse padrão. Ou seja, é importante que existam conteúdos direcionados para cada estágio do aprendizado de um normie que esteja na superfície da toca do coelho.

## Estabelecendo pontes

Juntando essas últimas seções, temos que: o grupo dos 15% iniciais é composto majoritariamente por pessoas intuitivas, enquanto o grupo dos 85% possui mais pessoas observadoras. Entre esses intuitivos, temos os comunicadores e os experts. Eu interpreto que entre esses 15% iniciais, os bitcoinheiros possuem pouquíssimas pessoas com perfil de vendedor. Em média, nós preferimos uma verdade áspera do que uma meia verdade, o que não poderia ser mais diferente da personalidade de um vendedor carismático que consegue vender algo para as personalidades "cordiais e responsáveis".

O poder do contexto atual é gritante, visto que os bancos centrais vêm imprimindo dinheiro como se não houvesse amanhã, ou, na linguagem memética bitcoinheira: "money printer go brrrr"<sup>138</sup>.

O fator de fixação, ou seja, a simplificação das narrativas e explicações para ajudar no início dos estudos dos normies, também já está bem amadurecido. Narrativas como “dinheiro incensurável” e “proteção contra a inflação” fazem um bom trabalho quando bem comunicadas, além, é claro, da tecnologia NGU (assunto do capítulo 7) que faz milagres.

Ou seja, juntando o pensamento do Malcom Gladwell com a curva de adoção, nós podemos pensar que:

- Os próximos grupos não adotarão o bitcoin pelas suas implicações filosóficas e sociais, eles adotarão o bitcoin pela facilidade de uso. São usuários pragmáticos e não ideológicos.

- Precisamos ter mais vendedores para atrair os outros tipos de personalidades e atravessar o abismo em direção aos 85% restantes. Ou pelo menos evoluir nossa narrativa, ou, na linguagem comercial, o nosso discurso de vendas.

Isso me leva à série de textos do Svetski<sup>139</sup> sobre os bitcoinheiros serem os remanescentes. A tese central dessa série de textos<sup>140 141 142</sup> é que a adoção ainda está no estágio seletivo, onde os bitcoinheiros ainda estão encontrando e acordando seus semelhantes. A tese pode ser simplificada na visão de que “não é o trabalho de um leão acordar todas as ovelhas, mas sim acordar os outros leões adormecidos.”

Isso faz sentido, visto que nós não estamos perto desses 15% iniciais de adoção antes do abismo. O fortalecimento do grupo de bitcoinheiros é importante e garantirá a preservação das qualidades do bitcoin no futuro. Entretanto, mesmo que as massas não importem, ainda existem leões adormecidos (mesmo que em menor grau) nos outros tipos de personalidade que são sub-representados entre os bitcoinheiros.

Nós precisamos pensar também que, se a adoção continuar seguindo a taxa de adoção atual, outras personalidades também entrarão no bitcoin. E se elas não entrarem, nós perdemos. Então é do nosso interesse que elas entrem e encontrem um ecossistema mais heterogêneo. Isto torna o bitcoin ainda mais antifrágil, pois novos conceitos e ideias são gerados, testados, incorporados ou descartados. Isso significa, na minha opinião, a necessidade de melhorar a nossa comunicação, de uma forma que os outros perfis de personalidade também consigam enxergar o valor do bitcoin.

O que me leva ao maximalismo tóxico: eu também sou culpado de



perder a paciência às vezes, todos somos. A toxicidade de fato já protegeu muito o bitcoin e seguirá protegendo. Mas nós precisamos entender que essa toxicidade se comunica melhor com os visionários e inovadores dos 15% iniciais, não com o restante da população. É importantíssimo que a nossa mensagem não seja diluída, pois ela implica diretamente na proteção da imutabilidade do bitcoin. Essa parte nós já estamos conseguindo fazer bem. Mas também é importante a criação de pontes para que as outras personalidades possam compreender o bitcoin.

Pessoas diferentes se identificam com partes diferentes da tese multifacetada que é o bitcoin. O bitcoin é extremamente complexo e faz sentido introduzir cada tipo de personalidade por vias diferentes. Certos textos e autores se comunicam melhor ou pior dependendo do tipo de personalidade da pessoa. Ou seja, eu não indico os textos do Svetski para um amigo coletivista/de esquerda, mas sim os textos do Alex Gladstein<sup>143</sup> <sup>144</sup>.

Aqui entra a reflexão sobre os “vendedores”. Os vendedores sabem que a sua mensagem precisa gerar um efeito específico nos seus possíveis clientes. Dependendo do estágio que esse possível cliente está no funil de vendas, o vendedor adequa seu discurso. Ele tem um incentivo financeiro a conseguir construir o melhor discurso de vendas possível para converter os curiosos em clientes.

Esse estudo sobre personalidades me faz pensar que a adequação da linguagem de acordo com o público é algo que, como comunidade, precisamos estar mais atentos.

Como as personalidades dos 15% iniciais é diferente das personalidades dos 85% restantes, nós não devemos criar conteúdo somente que nos agrade, e sim conteúdos que nos ajudem a vencer o abismo e nos conectar com os usuários observadores e pragmáticos.

Precisamos criar rotas para que todas essas outras personalidades possam encontrar o bitcoin caso elas desejem. Quais personalidades? Todas possíveis, mais é mais. Nós queremos converter o boomer que investe no mercado de ações, o esquerdista que quer acabar com as mazelas da desigualdade, pessoas não-técnicas que não entendem uma linha de código, o pescador tradicional em Jericoacoara e ou o garimpeiro de ouro na Amazônia. E eu não vejo isso como conflitante com o pensamento de adoção seletiva pois entender o bitcoin sempre requererá muita prova de trabalho.

Ou seja, mesmo em personalidades diferentes, ainda serão os remanescentes quem estarão se auto-selecionando. E nossa tarefa é sim acordar o máximo de remanescentes que estejam dormindo para conseguir fazer o bitcoin superar o abismo e se tornar realmente imparável como fenômeno social.

## **CAPÍTULO 13**

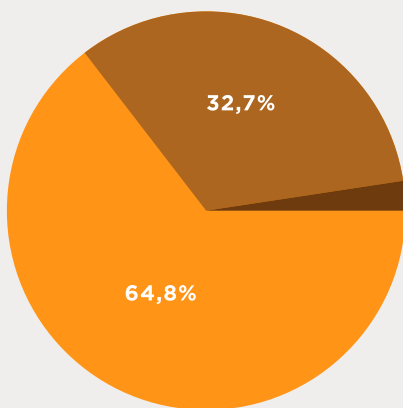
# **A PERSONALIDADE DE UM BITCOINHEIRO BRASILEIRO**

Para tentar replicar o experimento do Brandon Quintten, pedi para que as pessoas fizessem o teste e respondessem qual a sua personalidade Myer-Briggs em um formulário. Este pedido também foi replicado no Twitter.

Um total de 165 pessoas atenderam ao chamado até agora, um número bem superior ao que eu havia imaginado inicialmente. Ainda assim, esse número não é um número ideal e o formulário ainda está aberto para que mais pessoas o preencham ao longo do tempo, conforme este livro vai sendo lido. A base de dados inicial é enviesada pelo perfil dos usuários do Twitter e não necessariamente é representativa da personalidade dos bitcoinheiros brasileiros. Mas é o melhor possível até que, daqui alguns anos, os dados dos leitores sejam compilados em conjunto.

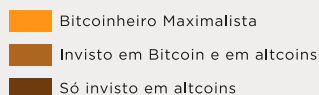
### **Analisando os dados nacionais**

Foram 165 respondentes. Destes, 107 pessoas (64,8%) se consideram bitcoinheiros maximalistas, 54 pessoas (32,7%) investem em bitcoin e em altcoins e 4 pessoas (2,4%) investem somente em altcoins.



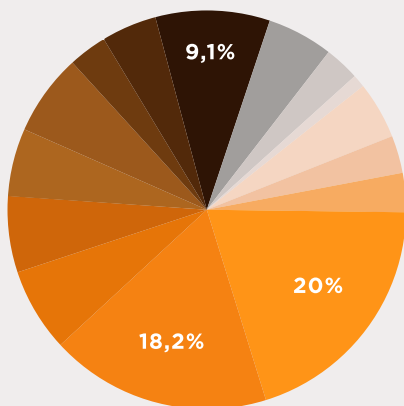
### COM QUAL ALTERNATIVA VOCÊ SE IDENTIFICA?

165 RESPOSTAS



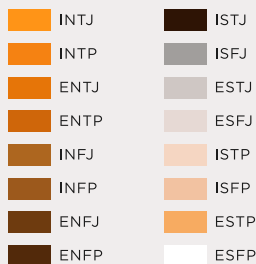
Entre os dados obtidos, merecem destaque:

- 38,2% destas pessoas (63) são INTJ (20% - 33 pessoas) e INTP (18% - 30 pessoas)
- 73% destas pessoas (120) são introvertidas (I na primeira letra).
- 71% das pessoas (117) são intuitivas (N na segunda letra), que significa que as pessoas processam as informações do mundo tecendo cenários e pensando em hipóteses abstratas.
- 71% destas pessoas (117) são pensadoras, pessoas que lidam com as emoções de maneira mais racional do que emocional (T na terceira letra).



### COM O SEU PERFIL DE PERSONALIDADE?

165 RESPOSTAS



## Analizando o conjunto geral de dados

O Brandon Quitten não publicou os dados originais, só as porcentagens. Então esses dados só permitem fazer comparação, e não juntar as duas bases de dados para ter uma amostragem maior. Abaixo é apresentada uma comparação entre as comunidades de bitcoinheiros nacionais e internacionais.

Existem semelhanças notáveis e diferenças consideráveis entre as duas populações analisadas.

Tipos de Personalidade	Tipo de personalidade	Número na pesquisa nacional	Taxa (%) na população bitcoinheira nacional	Taxa (%) na população bitcoinheira gringa	Taxa (%) na população geral	Diferença entre população nacional e população gringa de bitcoinheiros
INTJ / Arquiteto	Analistas	30	18,18%	29%	2,10%	11%
INTP / Lógico	Analistas	33	20,00%	22,30%	3,3%	2,30%
ENTJ / Comandante	Analistas	11	6,67%	7,60%	1,80%	0,93%
ENTP / Inovador	Analistas	10	6,06%	8,90%	3,20%	2,84%
TOTAL		84	50,91%	67,80%	7,10%	16,89%
INFJ / Advogado	Diplomatas	9	5,45%	9,80%	1,50%	4,35%
INFP / Mediador	Diplomatas	11	6,67%	8,90%	4,40%	2,23%
ENFJ / Protagonista	Diplomatas	5	3,03%	3,10%	2,50%	0,07%
ENFP / Ativista	Diplomatas	8	4,85%	4,90%	8,10%	0,05%
TOTAL		33	20,00%	26,70%	16,50%	6,70%
ISTJ / Logístico	Sentinelas	15	9,09%	1,40%	10,30%	-7,69%
ISFJ / Defensor	Sentinelas	9	5,45%	0%	13,80%	-5%
ESTJ / Executivo	Sentinelas	5	3,03%	0%	8,70%	-3%
ESFJ / Cônsul	Sentinelas	1	0,61%	0%	8,70%	-1%
TOTAL		30	18,18%	1,40%	41,50%	-16,78%
ISTP / Virtuoso	Exploradores	8	4,85%	0,90%	5,40%	-3,95%
ISFP / Aventureiro	Exploradores	5	3,03%	0,90%	8,80%	-2,13%
ESTP / Empresário	Exploradores	5	3,03%	0,90%	4,30%	-2,13%
ESFP / Animador	Exploradores	0	0,00%	1,40%	8,50%	1,40%
TOTAL		18	10,91%	4,10%	27,00%	-6,81%
TOTAL		165				

Esta planilha pode ser vista no link da referência 145.

Os perfis analistas (personalidades que são tanto N como Ts, ou seja, intuitivos e pensadores) são a maioria dos perfis nas duas comunidades. Entretanto, na comunidade nacional, eles representam "somente" 50.9%, enquanto na comunidade internacional eles são 67,8%.

Somando o número de diplomatas (Ns) aos analistas, temos todas as personalidades intuitivas. No Brasil todas as personalidades que são intuitivas representam 70.9% da população, enquanto na comunidade gringa essas personalidades representaram 94,5%.

A principal diferença entre as duas comunidades está justamente entre os INTJs (Logísticos) e os ISTJs (Arquitetos). Na comunidade internacional existem mais Arquitetos (29% contra 18,2%) enquanto que na comunidade nacional existem mais Logísticos (9,1% contra 1,4%); de resto os dados são bem semelhantes. O que talvez signifique que existe uma diferença cultural entre a comunidade internacional, com a cultura mais americanizada e globalizada gerando traços distintos de personalidade em relação à cultura nacional.

A principal diferença entre os INTJs e os ISTJs está na maneira de processar informação. Os Arquitetos são intuitivos (extrapoladores) e pensam em cenários hipotéticos, enquanto os Logísticos são observadores e preferem focar no presente e em coisas concretas.

### **Preferência temporal e dinheiro sólido**

Os bitcoinheiros brasileiros são, em média, menos intuitivos e extrapoladores que os bitcoinheiros da comunidade internacional. Os bitcoinheiros brasileiros, em média, pensam de uma forma mais concreta. Esse resultado me parece coerente. Faz sentido imaginar que por aqui as pessoas pensam menos no futuro e em cenários hipotéticos. Isso é um luxo e hábito de quem tem o presente mais resolvido que um brasileiro médio. De fato, nas 4 personalidades Sentinelas e em 3 de 4 personalidades Exploradores, que são personalidades Ss e não Ns (e, portanto, são observadores e não intuitivos), a comunidade nacional sempre teve números mais elevados.

Como o Saifedean Ammous escreve no livro O Padrão Bitcoin, a preferência temporal de um povo está diretamente relacionada com a força da moeda que ele utiliza. Ou seja, um dinheiro que não preserva o seu valor no tempo gera um incentivo para quem o utiliza para não armazenar seu valor nele. É interessante notar que a única diferença real observada entre a população nacional e a gringa é que os brasileiros não pensam tanto no longo prazo e estão mais focados no presente. Ou, nas palavras do Betinho, "Quem tem fome, tem pressa". Como o Brasil sempre teve moedas fracas, como os Cruzeiros, Cruzados e agora o Real (que comparativamente às moedas do passado até não é tão ruim assim), é natural que o brasileiro não tenha em média a tendência a pensar no longo prazo como indivíduos acostumados a utilizar o dólar.

### **Bitcoin e preferência temporal**

Uma das grandes fichas que caem quando alguém entende de verdade o bitcoin e se torna um bitcoinheiro é que o custo de oportunidade de tudo é o bitcoin. Esse pensamento é pesado e nos torna humildes, visto que todos compramos coisas idiotas nos últimos anos e esse dinheiro teria sido muito mais bem investido se tivesse sido convertido em satoshis.

Uma consequência dessa compreensão é a mudança de preferência

temporal do bitcoinheiro. Ou seja, os bitcoinheiros deixam de valorizar as gratificações imediatas e passam a desenvolver um pensamento de longo prazo, o que na escola austríaca de economia é conhecido como mudar de um pensamento de alta preferência temporal para um pensamento de baixa preferência temporal.

Já falamos sobre o teste do marshmellow, uma série de experimentos de psicologia do final dos anos 1960s e início dos anos 1970s, que testou a capacidade de autocontrole de crianças (nas palavras dos psicólogos “recompensa postergada”). Os psicólogos envolvidos nesses experimentos acompanharam as crianças pelas próximas décadas e constataram que as crianças que possuíam o autocontrole (baixa preferência temporal) conseguiram resultados melhores no vestibular (SAT, nos Estados Unidos), no desempenho escolar geral, além de possuírem um índice de massa corporal (IMC) mais saudável.

Ou seja, a característica de focar no longo prazo e abrir mão de gratificações instantâneas está diretamente relacionada a uma vida melhor. E atualmente, vivemos em uma sociedade que nos joga no sentido oposto e estimula o consumismo, o hedonismo e a falta de cuidado com o corpo e com a mente de maneira geral. Uma pessoa com baixa preferência temporal é um péssimo consumidor. Uma pessoa que cuida da alimentação e faz atividades físicas ao invés de ficar jogado no sofá vendo Netflix e pedindo delivery é um péssimo cliente para a indústria farmacêutica e hospitalar.

O bitcoin quebra essa lógica e conserta isso. Isso acontece porque toda a estrutura dos incentivos ensinam as pessoas a abrirem mão das gratificações instantâneas e, ao invés disso, adiarem as gratificações e com isso irem bem no teste do marshmallow.

## **Ou seja...**

Os dados obtidos na comunidade nacional são bastante similares aos dados obtidos na comunidade internacional. Os mesmos padrões macro podem ser atribuídos a um bitcoinheiro médio em ambas as comunidades. Bitcoinheiros são, em média, mais introvertidos, intuitivos e pensadores do que o restante da população, que apresenta uma taxa menor de pessoas com essas características.

A principal diferença observada entre a população internacional e

os brasileiros foi que os gringos são mais intuitivos que os brasileiros. Isso é observado tanto na diferença entre os Arquitetos e os Logísticos descrita acima, como no fato de que em todas as personalidades Sentinelas e praticamente todos os Exploradores; personalidades que são observadoras e não intuitivas, são mais comuns entre a comunidade nacional do que entre os gringos.



## **CAPÍTULO 14**

# **O MONOMITO E O BITCOIN**

### **A jornada de um bitcoinheiro**

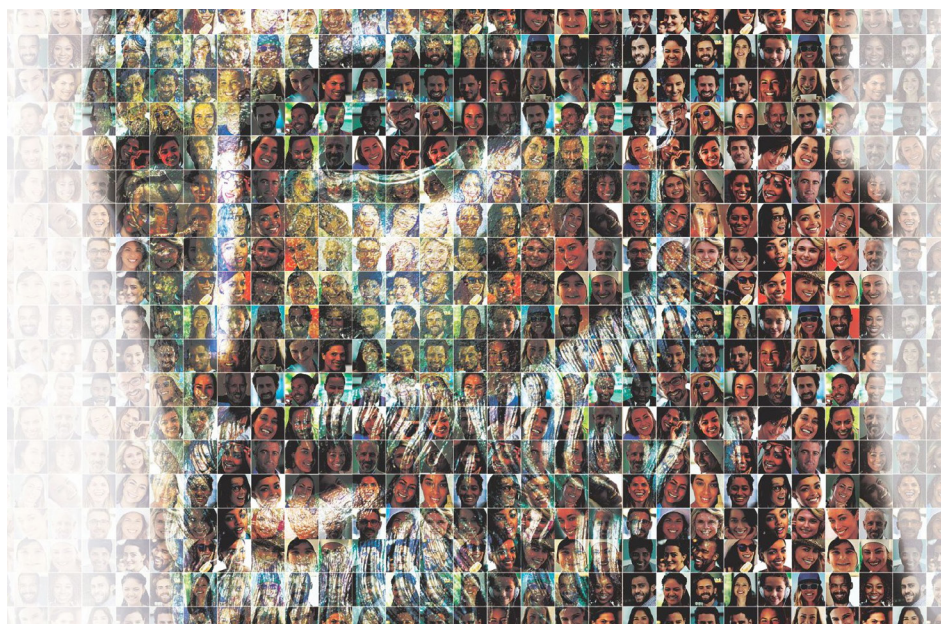
Todos temos nossas próprias histórias com o bitcoin, e no entanto elas são todas parecidas. Este texto é justamente sobre isso: histórias. Nós somos macacos sociais que por milhares de anos utilizaram as histórias como principal forma de passar conhecimento adiante. Antes da escrita ser inventada, os conhecimentos eram transmitidos via oral de geração em geração.

Por um processo de seleção (memética e natural), os macacos que conseguiam contar histórias que transmitiam informações de maneira mais eficiente e com maior resolução foram selecionados. Este processo de pressão seletiva memética gerou uma estrutura básica que é repetida constantemente em todas as nossas histórias.

### **A Jornada do Herói**

Talvez você já tenha escutado falar do “Monomito”, também conhecido como “a jornada do herói”. O Monomito é um arco narrativo (uma estrutura básica) bastante utilizado em histórias. Este arco narrativo é amplamente utilizado por todas as culturas e pode ser observado já nas primeiras histórias conhecidas pelo homem, como na Epopéia de Gilgamesh ou na história de Sidarta Gautama, o Buda. Essa estrutura base também está

presente na maioria dos clássicos de Hollywood, como Star Wars e Matrix. Nós também tendemos a contar a nossa própria história, para nós mesmos e para os outros, nos padrões desse arco narrativo.



A primeira vez que essa tal jornada do herói foi estudada e esquematizada foi em 1949, no livro *Herói de Mil Faces*, de Joseph Campbell. A partir do estudo e observação de obras antigas, Campbell estruturou uma espécie de roteiro que se repete em histórias contadas em diferentes períodos e civilizações. Ou seja, ele encontrou uma espécie de fórmula de sucesso amplamente utilizada por todos os contadores de história, que ele nomeou como “jornada de herói”. O termo “monomito” significa que na realidade todas as histórias que contamos são basicamente a mesma história, com a mesma estrutura. Um mito único compartilhado por toda a humanidade.



Luke Skywalker, o arquétipo clássico do herói e personagem principal da primeira trilogia de Star Wars (IV, V e VI).

A estrutura básica do monomito proposta por Campbell foi aprimorada ao longo do tempo e a versão mais difundida atualmente foi proposta em 2006 por Christopher Vogler com a publicação do livro *A Jornada do Escritor: Estrutura Mítica para Escritores*. O trabalho de Vogler basicamente condensou algumas ideias do seu antecessor.

A estrutura básica do monomito é dividida por Vogler em 12 etapas diferentes:

**1 – Mundo Comum.** Mundo do cotidiano do herói. Ele está vivendo a sua vida tranquilamente até que recebe o...

**2 – Chamado para a Aventura.** Este é o momento em que a jornada é oficialmente iniciada. Desse momento em diante o herói precisa cumprir determinada tarefa, ou alcançar determinado objetivo, e a partir desse objetivo ocorra a sua transformação. A partir desse ponto o herói não poderá mais retornar ao seu mundo comum que nós conhecemos no passo anterior da mesma maneira.

**3 – Recusa do Chamado.** O herói não aceita o chamado para a aventura de imediato. Isso acontece porque a temática da jornada do herói é o amadurecimento psicológico. E muitas vezes é muito mais cômodo a gente continuar na inércia do nosso dia a dia do que encarar uma mudança.

**4 – Encontro com o Mentor.** O herói geralmente é um iniciante e recebe ajuda de um personagem que é especialista no problema a ser resolvido. O mentor é a figura que ajudará o herói ao longo da sua transformação.

**5 – Travessia do Primeiro Limiar.** Nesse momento o herói já saiu do mundo comum e está adentrando o mundo extraordinário promovido pela aventura. A travessia do primeiro limiar é o período de treino e o amadurecimento necessário para que o herói possa enfrentar...

**6 – Provas, Inimigos e encontrar Aliados.** Este é o momento de tensão da história, onde o herói enfrenta os obstáculos que estão entre ele e seu objetivo. Ele é cada vez mais testado e desafiado, sendo forçado a se transformar. Para Vogler, é aqui que o herói aprende as regras desse mundo extraordinário.

**7 – Aproximação da Caverna Secreta.** É o momento de autoquestionamento do herói. Era necessário mesmo abandonar o mundo comum? Será que ele fez a escolha certa?

**8 – A Provação.** Momento em que o herói enfrenta grande dificuldade causada pelos questionamentos que ele teve no passo anterior. É aquele momento em que tudo dá errado e o herói corre risco real de falhar na sua missão.

**9 – A Recompensa.** Quando o herói vence aquela provação do passo anterior e evolui na sua transformação.

**10 – O Retorno.** O herói retorna do mundo extraordinário que promoveu sua transformação para o mundo comum do primeiro passo. Só que o herói ainda tem algum último obstáculo para resolver.

**11 – A Ressurreição.** Momento similar ao momento 8 da Provação. O herói passa por um grande desafio e, quando ele consegue solucioná-lo, ele consegue alcançar seu objetivo final. Dessa vez ele derrotou de vez o antagonista, ou se reconciliou com alguém, conseguiu o par romântico. A questão é que a transformação do herói está concluída.

**12 – O Retorno com o Elixir.** Na conclusão do monomito, o herói chega a sua comunidade, sua família, ao seu mundo familiar, porém desta vez ele está transformado, e esse é o Elixir. Esse elixir pode ser algo que vai ajudar sua comunidade, ou uma lição que ele aprendeu.

E por que eu estou falando tudo isso?

Simples, porque assim como o herói, o bitcoinheiro também tem a

sua jornada. E ter uma compreensão mais acurada do estágio em que nós (os bitcoinheiros, heróis das nossas próprias narrativas) estamos na nossa jornada, nos ajuda a nos situar e entender melhor o mundo à nossa volta.

## A Jornada de um Bitcoinheiro

Todos esses passos da jornada do herói podem ser identificados no caminho dos bitcoinheiros. É interessante notar que bitcoinheiros com mais de um ciclo provavelmente já concluíram a transformação da jornada do herói e já retornaram com o elixir. Já os bitcoinheiros das classes de 2020, 2021 e 2022 ainda estão em um estágio anterior, provavelmente entre o momento 6 a 8, e estão enfrentando as provas, os inimigos e as provações neste mercado de baixa. Essas classes (onde eu me incluo) estão tendo sua convicção testada.



A jornada do herói é uma estrutura arquetípica sobre a transformação do protagonista, então o primeiro passo é vencer a si mesmo. Nós somos nosso principal inimigo, o principal obstáculo a ser superado. É a nossa voz interior que pode abalar nossa confiança e nos fazer desistir do caminho de transformação.

Assim como em uma espada, a convicção é forjada a golpes duros.

Cada nova queda é uma martelada no nosso âmago. Essa é a diferença entre o saber teórico e a experiência prática e empírica de já ter vivido diversos ciclos, com multiplicações de 1000% e quedas de 80%.

**1 – Mundo Comum.** É o mundo normie. Onde todos vivíamos antes de cair na toca do coelho.

**2 – Chamado para a Aventura.** Praticamente todo bitcoinheiro recebeu diversos chamados para aventura na forma de diversos contatos iniciais com o bitcoin. Entretanto, para a tristeza e reflexão de todos,

geralmente antes de aceitar esse chamado, existiram diversas recusas.

**3 – Recusa do Chamado.** Todas as vezes que algum amigo ou conhecido tentou nos falar sobre bitcoin nós não escutamos. Estávamos distraídos pensando em qualquer outra coisa do Mundo Normie e não notamos a importância deste chamado. A sorte bateu na nossa porta e nós a ignoramos repetidas vezes.

**4 – Encontro com o Mentor.** É neste estágio inicial da aventura que os iniciantes encontram seus gurus. Dependendo dos gurus escolhidos, o normie se tornará um bitcoinheiro ou um shitcoinheiro. Então muito cuidado na escolha dos seus mentores. Lembre-se sempre: se a pessoa prefere riscar linhas imaginárias em gráficos ao invés de ensinar fundamentos, desconfie. Bitcoinheiros educam iniciantes a partir de fundamentos, enquanto shitcoinheiros/golpistas preferem confundir os iniciantes com informações irrelevantes para vender cursos.



Imagem sarcástica ilustrando o tipo de vídeo que você deve evitar no YouTube. Escutar mentores ruins é o caminho da ruína.

Todo o conhecimento necessário para se tornar um bitcoinheiro está disponível de forma gratuita na internet. Vale citar o canal dos Bitcoinheiros, do Korea, da Madu, das meninas da Uscripto, o Explica Bitcoin, o Planeta Bitcoin, o Imperativo Moral, o livro Bitcoin Red Pill, disponível também no YouTube também, o Diego Kolling, entre tantos outros.





Um dos meus mentores foi o Michael Saylor, The Bitcoin Bull Bull Bull (algo como o “Altista-mor” em tradução livre).



Outro dos meus mentores e um dos principais mentores da comunidade brasileira de bitcoinheiros, Bit Dov, o bitcoinheiro camarada.

**5 – Travessia do Primeiro Limiar.** Marca o início dos estudos indicados pelo mentor e o aprofundamento da compreensão de todas as derivações da tese do bitcoin. Bitcoinheiros que atravessam esse primeiro limiar começam a enxergar porque inflação é roubo de tempo, como a mineração do bitcoin

resultará na 3a Revolução Energética, a necessidade da separação entre o dinheiro e o estado, entra tantas outras epifanias.



A pílula laranja bate forte.



6 – Provas, Inimigos e Aliados. As primeiras grandes quedas enfrentadas pelos bitcoinheiros são as provas que ele precisa enfrentar para passar pela sua transformação de normie para bitcoinheiro. Os inimigos são os shitcoinheiros, economistas, gestores, faria limers e jornalistas que geram e amplificam FUDs. A cada queda do bitcoin eles saem das suas tocas para declarar o bitcoin “morto” e dançar em cima do seu caixão.



**Henrique Bredda** ✓  
@hbredda

...

Replying to @eiransimis @Vinicius1\_Bsb and @JamesGRickards

**Bitcoin?! Pra q complicar? Sai dessa.**

[Translate Tweet](#)

10:46 PM · Dec 9, 2018 · Twitter for Android

2 Retweets 13 Quote Tweets 12 Likes

Bitcoin realmente é muito complicado para quem não tem incentivos para compreendê-lo.



**Tiago Guitián Reis**  
@Tiagogreis

...

Replying to @BlueBalls\_Value

Eu julgo que eu entendo de bolhas.  
Talvez eu seja o brasileiro que mais  
leu livros a respeito. E com respeito a  
bitcoin eu vi todos os finais clássicos  
de bolha. Todos é mais alguns novos.  
Pra nós da Suno era claro que era  
bolha. Ficamos felizes de não ter  
indicado.

[Translate Tweet](#)

09:39 · 06/02/18 · Twitter for iPhone

A Suno acredita ter feito um favor aos seus assinantes ao protegê-los de investir no bitcoin quando ele estava custando por volta de 10.000 dólares.

**7 – Aproximação da Caverna Secreta.** É o momento de autoquestionamento que os bitcoinheiros de primeiro ciclo enfrentam. Era necessário mesmo abandonar o mundo normie? Será que fizemos a escolha certa? Será que não estou só ficando maluco? Afinal, todos da mídia tradicional e até mesmo economistas premiados com o Nobel são contra o bitcoin. Será mesmo que todos eles estão errados e um bando de malucos com avatares na foto de perfil do Twitter está certo? Não é muita arrogância da minha parte pensar isso?

**8 – A Provação.** Momento de dificuldades causadas pela insegurança e pelos questionamentos que ele teve no passo anterior. “Será que não vale a pena diversificar em outras criptomoedas?” “O Raoul Pal tem falado muito bem da Luna e seu ecossistema”. “Talvez eu devesse deixar meus bitcoins em um protocolo DeFi para ganhar um troco a mais”. “O influenciador recomendou um projeto do metaverso que é incrível e vai revolucionar as coisas”.

É aquele momento em que tudo pode dar errado e o herói corre risco real, pois ou é bitcoin, ou é golpe. E se o bitcoinheiro não fizer a custódia de seus satoshis, os bitcoins não são deles e tudo que ele tem é uma promessa que alguém lhe devolverá seus preciosos satoshis. O canto da sereia fala alto e cabe aos bitcoinheiros resistirem a ele.



**EARN UP TO 18% YIELD ON  
YOUR CRYPTO**



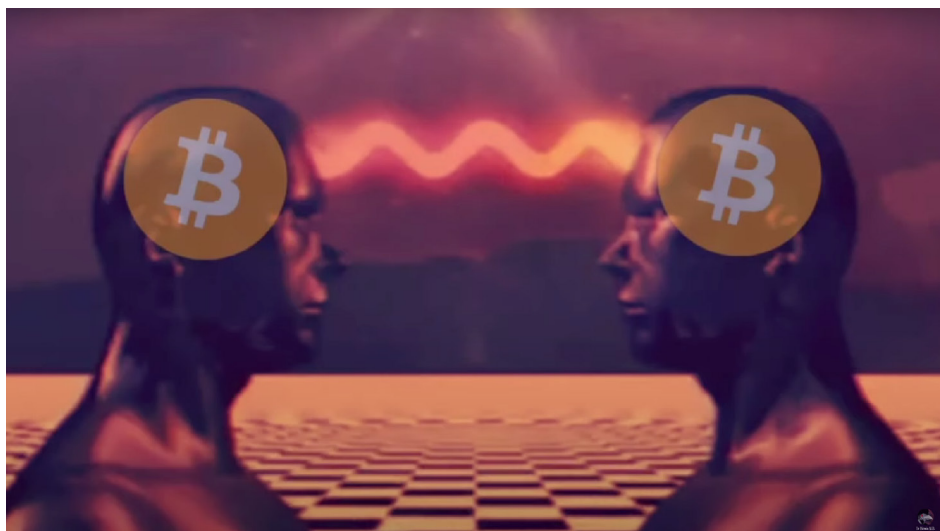
Ganhe até 18% de retorno com as suas criptos.

**9 - A Recompensa.** A convicção, quando mantida, permite atravessar as provações e se manter no caminho correto, acumulando satoshis e se mantendo humilde. Esse é o estágio em que o bitcoinheiro entende que a melhor estratégia é fazer o DCA, se manter humilde e acumulando sempre mais satoshis.

**10 – O Retorno.** Essa convicção faz com que o bitcoinheiro queira salvar seus amigos e familiares do colapso das moedas fiduciárias e do controle estatal. Entretanto, estes amigos e familiares ainda verão essa conversa sobre a “moeda mágica da internet” como um papo de maluco e não escutarão o chamado para a aventura. A maioria das pessoas não está pronta para sair do mundo normie.

**11 – A Ressurreição.** Quedas sempre ocorrerão em um ativo em fase de adoção, e com o bitcoin não é diferente. O bitcoinheiro terá que enfrentar as dúvidas e incertezas dos seus amigos e familiares que escutaram o chamado à aventura e agora estão no negativo e com medo.

**12 – O Retorno com o Elixir.** No próximo ciclo de alta, o bitcoinheiro concluiu a sua transformação e se torna mentor de uma nova geração de bitcoinheiros. Este papel cabe aos bitcoinheiros mais experientes e é primordial no esforço coletivo de educação em prol da continuidade da adoção seletiva.



## Ou seja...

A mente humana é limitada e busca padrões para interpretar e compreender a realidade. Ao longo de milênios, a única maneira que possuíamos de passar o conhecimento adiante era através das tradições orais. Ou seja, nós fomos selecionados para aprender via histórias e hoje aprendemos de maneira muito mais eficiente através delas do que por equações. É como o nosso cérebro foi programado para funcionar. Por processo de seleção memética, um arco narrativo conhecido como “a jornada do herói” foi fixado na nossa cultura. Esse arco também é chamado de monomito e representa uma história arquetípica de superação de adversidades e transformação de um protagonista. Isso permite que nos identifiquemos com o aprendizado que está sendo transmitido e torna mais fácil nos lembrarmos das lições transmitidas. Essa estrutura arquetípica é utilizada na maioria das histórias conhecidas pela humanidade e seus elementos são facilmente identificáveis por qualquer pessoa mais atenta.

Esse monomito também pode ser utilizado como lente para visualizar o processo que os bitcoinheiros atravessam, desde o início de seus estudos até o fundo da toca. Desde o mundo comum (o mundo normie), passando pelo chamado à aventura (o começo da queda na toca do coelho), a necessidade de mentores sábios (evitando os shitcoineiros grafistas) até o retorno com o elixir e a convicção que só a compreensão dos fundamentos do bitcoin permite.

E o que tudo isso significa? Bom, na verdade nada. O monomito é só uma estrutura arquetípica, não algo com poder preditivo. Mas entender onde você se encontra nesse arco da jornada do herói pode trazer tranquilidade para os mais nervosos com o dip atual. Estamos no momento de Provas e Inimigos, e agora é necessário a busca por Aliados e prova de trabalho para reforçar suas convicções nos fundamentos da tese. Essa é a diferença entre o herói que supera as provações e o mão de alface que vende na baixo.

No bitcoin, nada substitui a prova de trabalho individual dos estudos, ninguém pode construir convicção por você. Você que precisa ser o protagonista da sua jornada para se tornar um bitcoinheiro.



## PARTE 4 - CONSELHOS (OU MINHA VISÃO DE INVESTIMENTO)

*There is no dark side of the moon, really. As a matter of fact, it's all dark.  
The only thing that makes it look light is the sun.*

*Não há lado escuro da lua, realmente. Na verdade, está tudo escuro.  
A única coisa que a faz parecer clara é o sol.*

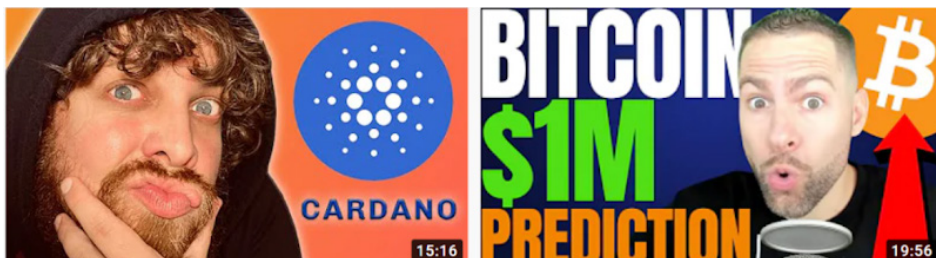
Eclipse – Pink Floyd

## CAPÍTULO 15

# SEPARANDO O JOIO DO TRIGO

Desde que comecei a investir em ações, um conceito que aprendi em minha formação científica me ajudou a ver algo com clareza: como existe uma grande mistura de ruído e sinal nas informações disponíveis para o investidor comum. Seja no Infomoney, no Valor Econômico ou no Wall Street Journal, sempre existe uma grande mistura entre informações relevantes e inúteis.

No mundo do bitcoin não é diferente. É possível encontrar de graça tanto informações de excelente qualidade, como também vídeos no youtube com traders fazendo boquinha, arregalando o olho e amplificando qualquer FUD ou FOMO disparado pelos meios de informação. As informações para investidores fundamentalistas de longo prazo e para daytraders são comumente apresentadas para os iniciantes de uma maneira desorganizada, de modo que a confusão é o estado comum de um iniciante. Basicamente, o iniciante não sabe separar o joio do trigo.



Dois youtubes gringos que são claramente ruído (temos os nossos também...)

Apesar deste ser o cenário comum, eu nunca vi muito conteúdo bom, com uma visão macro, que ensine alguém a interpretar e entender quais destas notícias são úteis e quais não são. Ou seja, o que é o joio e o que é o trigo para os seus investimentos?

### O que é sinal e o que é ruído?

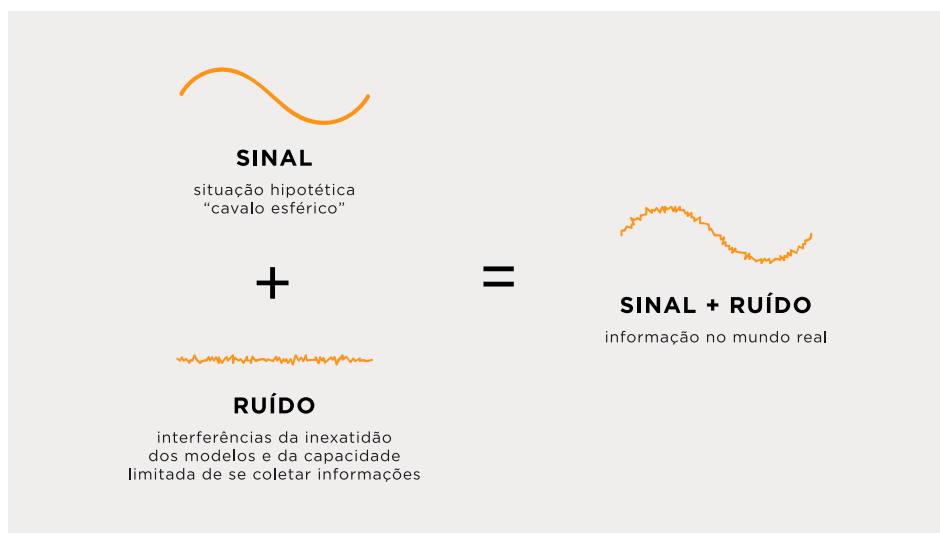
Esse pensamento de “ruído e sinal” vem das telecomunicações. De acordo com o Wikipedia<sup>146</sup>: “**Relação sinal-ruído** ou **razão sinal-ruído** é um conceito de telecomunicações, usado em diversos campos como ciência e engenharia que envolvem medidas de um sinal em meio ruidoso, definido como a razão da potência de um sinal e a potência do ruído sobreposto ao sinal”.

Ou seja, esse conceito de sinal e ruído foi apropriado das telecomunicações e transferido para diversos outros campos da ciência e da engenharia, tamanha é a sua utilidade como modelo mental para entender como o mundo funciona.

Explicando o conceito de maneira simples: “sinal” é um padrão macro, que pode ser observado e que carrega uma informação; já o “ruído” é aleatório e não afeta o padrão macro. Exemplificando: ruído é o “hummmm” contínuo que o amplificador faz quando um instrumento não está plugado nele, e sinal é o solo de guitarra que o amplificador toca quando o guitarrista sola.

Nas ciências essa linguagem de ruído e sinal é usada para observar o que faz sentido e o que é irrelevante para os processos maiores. Em diversos experimentos, os dados obtidos pelos cientistas precisam ser “limpos” e interpretados, retirando-se o ruído a fim de que seja permitida uma análise mais precisa do sinal. As duas próximas imagens ilustram esse pensamento.

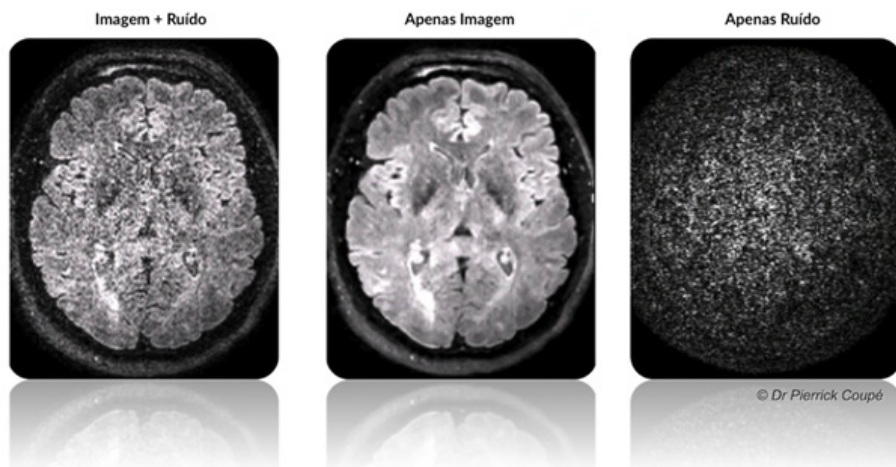




Na figura acima, é possível ver que o resultado, no mundo real, é a soma do ruído com o sinal e que, portanto, é viável separar um do outro na interpretação dos dados.

O sinal é o que os professores de física chamam de "cavalo esférico", isto é, são as condições ideais que não existem no mundo real. No exemplo do professor de física, é como calcular uma trajetória sem considerar a resistência do ar ou a força necessária para mover um objeto sem levar em conta o atrito, por exemplo. Já o ruído está relacionado aos limites humanos, seja nos modelos que não contemplam a totalidade de um fenômeno, seja na capacidade técnica de construção de equipamentos que conseguem captar informações mais precisamente.

A figura abaixo exemplifica a diferença entre o ruído e o sinal na prática, com um exame de ressonância magnética de um cérebro.



*J. V. Manjon, P Coupé et al. Adaptive Non-Local Means Denoising of MR Images with Spatially Varying Noise Levels. JMIR, 2010.*

Hoje as imagens de ressonância magnética estão mais límpidas do que nunca por "culpa" das técnicas cada vez mais eficazes de filtragem de ruído.

### Como isso se aplica aos investimentos?

Ok, mas como essa história de sinal e ruído se aplica aos investimentos? O primeiro passo de todo investidor é entender qual é o seu perfil e qual a sua estratégia. Sem uma estratégia definida, é impossível saber o que é ruído e o que é sinal. Ou, em outras palavras, para quem não sabe para onde ir, qualquer caminho serve.

Usando o meu próprio caso como exemplo, eu sou um investidor de longo prazo que investia na bolsa pensando em montar uma carteira previdenciária (dinheiro para a aposentadoria sem depender do Estado) e continuei com essa visão de longo prazo quando mudei meu foco para o bitcoin. No meu caso em específico, notícias de adoção em países, empresas começando a utilizar a moeda e outras coisas relacionadas à curva de adoção do bitcoin são o sinal, enquanto a volatilidade de curto prazo ou as análises gráficas com o padrão triângulo ascendente, o martelo de thor ou duplo twist carpado são apenas ruído.

Mas, para alguém que estuda análise gráfica e on-chain<sup>147</sup> e que extrai informações relevantes de notícias, ou seja, para os traders, isto é o seu sinal. Por outro lado, a adoção do bitcoin por El Salvador ou o anúncio de que a Blockstream<sup>148</sup> vai começar a fabricar computadores de mineração (conhecidos como ASICs) é ruído que não fez preço no curto prazo.

Em resumo, não existe certo e errado, uma vez que cada pessoa deve interpretar, de acordo com a sua estratégia, o que é ruído e o que é sinal. Mas eu tenho sim um motivo para optar em investir no longo prazo e não no curto, que é acreditar que é mais simples conseguir filtrar o ruído do sinal. O porquê disso tem relação com teoria dos jogos.

### Jogos de soma zero e jogos de soma não-zero

Na teoria dos jogos, um jogo de soma zero se refere a um jogo em que existe necessariamente um ganhador e um perdedor, isto é, para que alguém ganhe algo, outra pessoa está necessariamente perdendo. Já o jogo de soma não-zero é um jogo colaborativo em que o sucesso de um dos jogadores não representa a perda de outro jogador.

Na natureza, o jogo de soma zero é o jogo jogado entre o predador e a presa, enquanto o jogo de soma não-zero é o jogo jogado por espécies que possuem uma relação mutualística, como os humanos e os cães.



Jogos de soma zero e de soma não-zero sendo jogados na natureza.

Traduzindo a visão de teoria dos jogos para o mundo dos investimentos, os investimentos de curto prazo (day trade e trades de curto prazo) são jogos de soma zero em que não há mudança significativa na tese e nos fundamentos. O que existe são pessoas apostando entre si e tentando arbitrar o preço de curto prazo dos ativos de maneira a extrair dinheiro de outras pessoas que também estão tentando arbitrar o preço de curto prazo e extrair dinheiro de outras pessoas. Uma implicação direta disso é o surgimento e expansão de toda uma indústria de notícias que ganha mais cliques quando as manchetes são mais sensacionalistas. Desse modo, quem

foca no curto prazo e tenta operar notícias se torna o alvo ideal para quem quer manipular o mercado a partir de FUDs (como é explicado na segunda parte do texto “Sobre Tulipas e Manipulação”<sup>149</sup>).

Enquanto isso, o investimento de longo prazo surfa os fundamentos da tese. No caso do bitcoin, a curva de adoção de longo prazo e a escassez gerada pelos ciclos de halving garantem uma apreciação constante e previsível no longo prazo. Ocorre que, justamente por não saberem diferenciar entre ruído e sinal, muitos que focam no curto prazo ficarão pelo caminho.

Conforme foi dito anteriormente, o que é ruído e o que é sinal é diferente para cada pessoa e estratégia. A minha estratégia pessoal é simples: estudar os fundamentos do bitcoin e focar no longo prazo. Fazer aportes semanais independentemente do preço, uma vez que a volatilidade é mero ruído de curto prazo, e a curva de adoção o sinal de longo prazo. Nessa estratégia de aportes constantes, figuras de análise técnica, com olhos arregalados, boquinhinhas e manchetes sensacionalistas são ruído e podem ser ignorados. A vida é mais simples e tranquila jogando esse jogo de soma não-zero chamado longo prazo.

## CAPÍTULO 16

# O OURO DE TOLO DIGITAL

*There's a lady who's sure all that glitters is gold*

*And she's buying a stairway to heaven*

*Há uma senhora que tem certeza que tudo que reluz é ouro*

*E ela está comprando uma escada para o céu*

**Led Zeppelin - Stairway To Heaven**

"Ouro do tolo" é um apelido comum para pirita. Ela recebeu esse apelido porque não vale praticamente nada, mas possui uma aparência capaz de enganar as pessoas, fazendo-as acreditar que é ouro de verdade. Com um pouco de prática, existem muitos testes fáceis, os quais qualquer um pode fazer uso, para dizer, rapidamente, a diferença entre pirita e ouro. O apelido de "ouro de tolo" é usado há muito tempo por compradores e garimpeiros de ouro, que se divertiam com o entusiasmo de pessoas que pensavam ter encontrado ouro. Essas pessoas não sabiam diferenciar a pirita e o ouro, e esta ignorância as tornava tolas. Pior que isso, essa ignorância fez com que muitos perdessem suas economias e caíssem na pobreza.

Pareceu familiar? Pois bem, se o bitcoin é o ouro digital, nada mais natural que exista também a versão digital do ouro de tolo, ou seja, as shitcoins.

## O ouro e a pirita

Basicamente, o ouro pode ser caracterizado como um metal amarelo, brilhante, denso, maleável e dúctil, que não reage com outros produtos químicos ou sofre oxidação (não enferruja). Não à toa, seu nome vem do latim, *aurum*, que significa “brilhante”. É encontrado na natureza, principalmente, na forma de pepitas, sedimentadas nos leitos de alguns rios ou, em menor escala, embutidas em pedras.

Devido às características mencionadas, o ouro sempre foi considerado como precioso pelos humanos, tendo sido utilizado para cunhar moedas pelas principais culturas. Como se trata de um metal maleável, o ouro precisa ser endurecido para que possa ser utilizado e, geralmente, acaba sendo misturado com a prata e o cobre para formar ligas metálicas mais resistentes. O fato de ser maleável permite que o ouro seja utilizado para joalheria, visto que é possível moldá-lo sem que seja quebrado. Vale ressaltar que, para além da joalheria, o ouro é também utilizado na indústria eletrônica e no campo das finanças, como reserva de valor. Isso porque, em comparação a outros metais, o ouro é escasso, de maneira que seu valor acaba por ser elevado.



Pepita gigante de ouro encontrada em depósito de rio.

Já o ouro de tolo, como a pirita é conhecida de maneira informal, não apresenta nenhuma das principais características, a não ser a cor amarela com brilho. A pirita não é composta por nenhum metal precioso, mas sim pela mistura de ferro e enxofre, formando um sulfeto de ferro ( $\text{FeS}_2$ ). A cor e o

brilho da pirita se assemelham aos do ouro e podem enganar os iniciantes e os mais ingênuos.

Mas essas semelhanças param por aí. Diferentemente do ouro, a pirita apresenta feições quadradas ou hexagonais e reage com outros elementos químicos ou até mesmo ao ser aquecida, geralmente, exala um cheiro característico de dióxido de enxofre (cheiro de ovo podre). Apesar da coloração similar ao ouro, a pirita não pode ser usada para jóias, pois não é maleável como o ouro, e sim quebradiça. A pirita também é um mineral abundante e foi chamada de ouro de tolo pela primeira vez na corrida do ouro da Califórnia, quando garimpeiros menos experientes acreditavam que este material amarelado e brilhante era ouro de verdade.



Agregado de piritas cúbicas.

Na indústria da mineração, existem duas categorias de minerais: os minérios, que são o material de interesse econômico, e o mineral de ganga, que é o material sem valor comercial, o qual precisa ser separado do minério. Por definição, o ouro é um minério, enquanto a pirita é um mineral de ganga, sem valor comercial significativo. Desta maneira, é perigoso acreditar que “tudo que reluz é ouro”, como a senhora da música Stairway to Heaven.

### O bitcoin e as shitcoins

O bitcoin ficou popularmente conhecido como ouro digital por conta de uma das suas principais características: a escassez. O bitcoin é mais escasso que o próprio ouro, uma vez que a sua oferta é inelástica. Além da escassez absoluta, o bitcoin possui também diversas características

irreplacáveis por outras criptomoedas, tais como ser a única blockchain realmente descentralizada (e, portanto, a única blockchain resistente à censura), ser a rede com maior poder computacional e possuir concepção imaculada (sem tokens pré-minerados e sem vantagens para os “amigos do rei”), além de possuir um efeito de rede gigantesco.

Já as criptomoedas alternativas, também conhecidas como altcoins ou shitcoins, não possuem nenhuma dessas características. Assim como a pirata, as shitcoins não são escassas, e existe uma oferta ilimitada de projetos parecidos e genéricos. Do mesmo modo, as shitcoins também não são descentralizadas. Exemplos claros disso são a atuação do Vitalik Buterin na rede ethereum e do Charles Hoskinson na rede cardano. Ou, de maneira mais geral: qualquer moeda que possua uma equipe fundadora conhecida não é descentralizada o bastante, pois estas moedas não são imunes à atuação coercitiva, ou seja: elas podem ser desligadas se alguém ameaçar a família de membros chave dessas equipes.

É importante salientar que descentralização significa a capacidade de usuários comuns de validar a rede. No bitcoin, isso é possível, uma vez que o custo para rodar um node é baixo (> \$500). Já na rede ethereum, os nodes podem ser rodados na AWS (da Amazon, uma empresa centralizada). Hoje, o custo de utilizar a AWS para rodar o node do ethereum<sup>150</sup> é \$999 por ano (\$0.243/hora). Na ethereum 2.0 (atualização do ethereum que talvez saia do papel algum dia), os usuários precisarão ter, pelo menos, 32 ETHs<sup>151</sup> para poder rodar um node validador, o que, nos preços atuais, significa quase \$110.000,00 para poder validar a rede ethereum.

O poder computacional das blockchains também é um fator relevante para garantir a segurança das criptomoedas e, como visto na comparação das hashrates, na prática, só existe uma blockchain com poder computacional relevante: o bitcoin.

### **A corrida pelo ouro digital**

Assim como ocorreu na corrida do ouro da Califórnia, hoje existem milhares de moedas tentando atrair os mais ingênuos. São pessoas que ainda não entenderam as características irreplacáveis do bitcoin e buscam, ingenuamente, encontrar “o novo bitcoin”, afinal, “é mais fácil essa shitcoin passar de 1 para 2 reais do que o bitcoin passar de 250mil para 500mil reais”.



Da mesma forma que aconteceu com o ouro de tolo físico, porém, essa incompreensão das qualidades que tornam o ouro digital realmente valioso faz e continuará fazendo com que pessoas percam suas economias.

Mas, então, como saber se determinada criptomoeda é um ouro de tolo digital?

Se pergunte:

- Existe algum fundador conhecido?
- Existe equipe de marketing que tenta vender essa moeda?
- É possível rodar o seu próprio node por um valor baixo ou só os muito ricos podem validar essa blockchain?
- Existem moedas que foram pré-mineradas e distribuídas para os “amigos do rei”?
- Existem pessoas com privilégios na rede, que podem validar transações pelo simples motivo de terem mais de uma determinada criptomoeda (ou, em outras palavras, quem tem mais pode mais)?

Se a resposta para qualquer uma dessas características for sim, cuidado, essa moeda não é ouro digital.

Assim como ocorre no ouro, as características do bitcoin também são irreplicáveis. Nunca existirá outra criptomoeda com o mesmo efeito de rede, capacidade de processamento computacional, resistência à censura derivada da descentralização e concepção imaculada do bitcoin.

Mas alguns tolos ainda não perceberam isso, o que os torna alvo fácil para os golpistas das shitcoins.

## APÊNDICE

*O propósito do conhecimento é ação, não conhecimento.*

Aristóteles

### **O pleb por trás dessas palavras: minha história com o bitcoin**

Nota do autor: Este texto foi escrito para comemorar meu primeiro aniversário na toca do coelho e foi publicado originalmente em outubro de 2021. Para esse livro, ele foi expandido e atualizado com tudo que aconteceu após a publicação da versão original.

*“O Bitcoin é um enxame de vespas cibernéticas servindo à deusa da Sabedoria, se alimentando do fogo da Verdade, crescendo exponencialmente mais inteligente, mais rápido e mais forte protegidos por um muro de energia criptografada.”*

Michael Saylor<sup>152</sup>

Para comemorar o meu primeiro ano dentro da toca do coelho, eu resolvi contar a minha história com o bitcoin. Talvez os passos que eu fui dando e também os pensamentos que eu tinha nesse caminho ajudem os iniciantes. Eu só sei que eu gostaria muito de ter lido um texto como esse no meu primeiro mês na toca.

COMPRA OU VENDA	PREÇO BTC EM TO	QUANTIDADE	DATA	CUSTO (R\$)	VALOR ATUAL	VALORIZAÇÃO	EM VEZES
COMPRA	R\$67.399,99	0.00184326	20/10	R\$124,24	R\$579,61	366,54%	<b>4,67</b>
COMPRA	R\$72.344,95	0.00137259	22/10	R\$99,30	R\$431,61	334,65%	<b>4,35</b>
COMPRA	R\$72.404,62	0.00377151	22/10	R\$273,07	R\$1.185,94	334,29%	<b>4,34</b>

Um ano de bitcoin - minhas primeiras compras foram há um ano, no dia 20 de outubro de 2020.

Bom, primeiramente deixa eu me apresentar: meu nome é Caio, também conhecido como Leta. Eu tenho formação em geologia, que é a ciência natural que estuda pedras (a natureza e seus processos físicos que formam as rochas da superfície terrestre). Ou seja, eu estudei pedras por 5 anos ao longo da minha graduação e estudei pedras, isótopos e formação de depósitos minerais por mais 6 anos ao longo do meu mestrado e doutorado.

Eu já tinha escutado falar de bitcoin algumas vezes antes na vida, mas nunca prestei muita atenção (infelizmente). Amigos meus até chegaram a usar o Silkroad, mas eu tive preguiça de aprender o processo todo. Eu não sou muito bom em "coisas de computador" e a preguiça falou mais alto.

Há cinco anos eu comecei a investir meu dinheiro. Peguei o começo do movimento de aumento de CPFs na bolsa brasileira, na época (2017) éramos menos de 1 milhão de investidores na bolsa. Nessa época eu estava no meio do meu doutorado, o que significa que eu possuía bastante autonomia sobre como utilizar meu tempo e que eu acabei sendo tragado para o mundo da educação financeira.

Como um bom acadêmico, eu nunca tinha me importado muito com dinheiro, como ganhar dinheiro, como investir e qualquer outra coisa relacionada ao tema. Eu não chegava a ser aquele tipo de pessoa que acha que o dinheiro é ruim, mas eu simplesmente não tinha começado a me interessar pelo tema. Nesse meio as pessoas tendem a não serem ambiciosas e, com exceção da faculdade de engenharia, economia, direito e medicina (e talvez mais uma ou outra como odonto e farmácia), são bem desconectadas do mundo real. A USP é uma bolha que olha muito pouco para fora do campus e para a vida pós-universidade, ao melhor estilo Terra do Nunca.

Nos últimos anos do doutorado, conciliei o estudo formal com o estudo sobre o mercado acionário. Estratégias diferentes, estudo das referências como Warren Buffett, Charlie Munger, Peter Lynch, Joel Greenblatt, Ray Dalio,

além dos brasileiros como Luiz Barsi Filho, Luiz Paes de Barros, Stuhlberger etc. Horas e mais horas de podcasts específicas como a Stock Pickers, assinatura de casa de research (valeu mestres Vicente Guimarães e Dica de Hoje!) e por aí vai.

Nesses estudos, alguns tweets do Henrique Bredda se destacaram como uma fonte de conhecimento e um tema que particularmente me chamou a atenção foi o da inflação de ativos. O Bredda já fez alguns fios muito bons sobre o tema, que sempre me fizeram entender o porquê a minha geração (millenials) estar tão fudida em comparação aos meus pais (baby boomers), mas sem propor qualquer saída para a questão. Também escutava sempre a respeito dos QEs (kiwis para os mais íntimos) e que isso significava impressão de dinheiro, mas nunca parei para realmente me aprofundar no tema, só tinha a impressão difusa de que “tem caroco nesse angu”.

Minha estratégia estava bem definida: 80% em ações e FIs focados em dividendos e 20% para oportunidades com pensamento em curto-médio prazo (obrigado Louise Barsi) e o desempenho estava satisfatório. Estava conseguindo obter boa rentabilidade e uma curva de evolução constante nos meus dividendos. O foco era seguir a estratégia do Barsi e focar em empresas perenes (especialmente elétricas) e com isso receber dividendos constantemente. A lógica é simples: uma vez que os dividendos anuais passarem o custo de vida anual você chegará à independência financeira. Uma ótima receita de bolo.

E então um meteoro atingiu a terra.

## **Março de 2020**

Não foi literalmente um meteoro, mas o impacto na psique coletiva foi grande. O mundo estava em pânico e isso foi refletido em praticamente todos os ativos, e ocorreu uma busca por liquidez. Naquele contexto, papel higiênico valia mais que ações da Vale ou Magalu. E os Bancos Centrais tentaram ajudar a situação dando dinheiro para as pessoas não circularem e aumentarem a taxa de transmissão do vírus. Money printer go brrr na linguagem dos bitcoinheiros.

Nesse contexto, as bolsas mundiais se recuperaram rapidamente, o Ibovespa saiu dos 65 mil pontos para os 90 mil pontos rapidamente, como se a pandemia e a economia estivessem resolvidas. E isso estava ótimo para a

minha carteira, eu havia aportado toda minha reserva de oportunidade por volta dos 75-70 mil pontos e em ações que recuperaram bem (JHSF3 <3), mas a sensação de que “tem caroço nesse angu” não desapareceu. “Como a bolsa está tão bem se a economia real está tão prejudicada? Os fundamentos não fazem sentido”. Este era o pensamento que ficava me martelando.

Neste momento eu já havia acabado o doutorado e havia iniciado uma startup focada em educação no Ensino Médio. Por volta de setembro de 2021, nós estávamos pesquisando sobre as diferenças geracionais e eu esbarrei no conceito de “Fourth Turning”<sup>153</sup> e nas mudanças profundas que sempre ocorrem no mundo de acordo com as mudanças geracionais. E um dos vídeos que vi para estudar o assunto citava o bitcoin como um dos exemplos de mudanças geracionais e o colocava como o dinheiro da Fourth Turning.

Eu já tinha um amigo que ficou tranquilo na vida pois investia em bitcoin pelo menos desde 2014 - 2015, mas na época eu não havia me interessado por ter entendido (que nem um idiota) que seria necessário ficar fazendo trade pra valer a pena colocar dinheiro em bitcoin. Ele me explicou como ele fazia trade em 2015 e eu não fiz nada a respeito. Não conversamos sobre o HODL.

Como dói escrever isso.

Ao mesmo tempo eu também já estava na bolsa a bastante tempo vendo a Magazine Luiza ter rentabilidade recorde atrás de rentabilidade recorde e sempre evitava entrar nela com medo de “bolha” e que ela iria corrigir eventualmente. Isso me fez entender que nós humanos temos um viés platô, ou seja, “já subiu o que tinha que subir e agora tende a ficar estável num platô” e que esse viés não faz sentido. Uma coisa que subiu 10x pode subir outras 10x tranquilamente, caso a tese continue fazendo sentido.

Nesta época, eu tinha visto um vídeo<sup>154</sup> do Real Vision e já estava bastante intrigado com o conceito do bitcoin ser o bote salva-vidas para o contexto macro, mas confesso que eu ainda não entendia direito o conceito. Até que um belo dia, o CEO da Microstrategy (Michael Saylor) comprou 450 mil dólares de bitcoin e fez um tour em diversos podcasts de investimento para explicar o racional. E um desses podcasts era uma conversa no Real Vision<sup>155</sup>.

Estes dois vídeos literalmente mudaram a minha vida. Eles explicaram

qual era o caroço que tinha no angu.

A expansão da base monetária gera a inflação dos ativos e faz todo o dinheiro se desvalorizar.

Ou, nas palavras do Michael Saylor: “Meu dinheiro é um cubo de gelo derretendo, se eu perder 1-2% dele por ano (juros reais negativos) o que vai sobrar dele daqui a 30 anos?”. E isso ainda considerando a inflação oficial (no Brasil, o IPCA ou o IGP-M; nos EUA, o CPI), o que eu também entendi que são medidas bastante enviesadas e tendenciosas de inflação. A inflação real, diferente da oficial, também precisa levar em conta a inflação dos ativos para fazer sentido, pois famílias também querem comprar suas casas e investir em ativos para suas aposentadorias. A inflação é um vetor, não um único dado.

## **A evolução da alocação e os modelos mentais para cada uma delas**

### **Molhando os pés (1-5%)**

20 de outubro de 2020

Inicialmente eu comprei 1% da minha carteira em bitcoin, pois já tinha 5% reservado para investimentos mais arriscados e entendia que o bitcoin também era arriscado. Eu comprei 1% com o modelo mental de que o bitcoin basicamente é uma opção sem data de validade, ou seja, pode ir a 0, mas possui uma grande assimetria e pode explodir para cima. Na linguagem faria limer, o bitcoin é uma PUT fora do dinheiro sem vencimento, algo assimétrico por definição que se encaixa em qualquer portfólio<sup>156</sup>. Este é um modelo mental confortável para quem não estudou nada e só quer se expor de maneira macro ao bitcoin.

Conforme eu me aprofundava nos estudos, eu fui entendendo mais sobre os fundamentos por trás do bitcoin e entendi que 1% não fazia sentido, pois eu possuía significativamente mais convicção nesta tese “arriscada” do que eu tinha convicção nas outras teses mais arriscadas e com isso minhas ações de Oi, Braskem, Helbor e JHSF foram substituídas por mais satoshis.

### **Ganhando confiança (5-30%)**

20 de novembro de 2020

Mas, como todo bitcoinheiro sabe, o bitcoin tem a gravidade de um

buraco negro<sup>157</sup> para quem é curioso intelectualmente. Em poucas semanas eu já havia estudado todo o material que eu conseguia encontrar sobre o tema e, ao entender melhor os fundamentos, construído uma convicção de que o bitcoin poderia ocupar a mesma proporção das minhas maiores posições na carteira (na época 10% em Itaúsa, 10% em Engie e 10% em Taesa). Então os 5% se tornaram 10%.

Eu também sempre me perguntei sobre o que era melhor: diversificação ou focar nas teses de maior confiança? Entendo os argumentos a favor da diversificação, mas as grandes fortunas são construídas com portfólios concentrados: O Mark Zuckerberg possui somente uma ação, o Facebook, assim como o Jeff Bezos que construiu sua fortuna com as ações da Amazon, por exemplo. A diversificação protege melhor o patrimônio, mas é a concentração que constrói (e destrói) patrimônios.

E eu já tinha visto minhas JHSF3 multiplicarem por 3x e ficado putíssimo de ter colocado somente 1% nessas ações, quando eu tinha convicção que elas se recuperariam rapidamente.

Foi uma sensação agri-doce de ter previsto o futuro corretamente e ter ganhado pouco por falta de convicção (fui pau mole, em outras palavras). Com isso em mente, e com mais estudos, e, portanto, mais convicção, eu subi a alocação em bitcoin para o meu limite de alocação em um determinado setor (30%), e fiquei tranquilo por mais uma ou duas semanas.

## **Repensando tudo (30-50%)**

01 de dezembro de 2020

Mas a força gravitacional da toca é realmente forte e eu não consegui parar de me aprofundar no tema. Todo dia eram, no mínimo, uma ou duas horas dedicadas a estes estudos. E eu achava pouco para o tamanho da minha curiosidade, mas era o máximo que eu conseguia me dedicar sem deixar a peteca cair na startup. Assim, a minha compreensão do que é o bitcoin e o que ele realmente representa foi ficando cada vez mais clara.

O que é o bitcoin? Ele é um novo sistema monetário que roda atualmente em paralelo com o sistema tradicional. Os dois sistemas estão em uma briga darwiniana e só um deles sairá vencedor. Um sistema inexoravelmente desmonetizará o outro em uma janela de tempo longa o bastante (talvez 20-30 anos?)

Quando eu entendi isso, deixou de fazer sentido ter menos de 50% em bitcoin, visto que se temos 2 sistemas e queremos fazer uma aposta agnóstica é só dividir o portfólio entre os dois. Na visão de alguém que ainda está preso na mentalidade fiat isso soa extremamente agressivo e ousado, na cabeça de um bitcoinheiro soa muito pouco e significa que 50% do patrimônio continua sendo um bloco de gelo derretendo. Como eu ainda não tinha certeza de quem seria o vencedor, entendi que uma alocação de 50-50 fazia sentido.

### Será que eu sou maluco? (50-80%)

20 de dezembro de 2020



*“Se você tem tanta certeza assim, por que você não coloca logo tudo nessa merda?”*

**Reclamação de amigo, na época ainda nocoiner.**

É difícil se manter agnóstico quando a comparação entre duas coisas mostra tão claramente a superioridade de uma delas. Os meus grupos de whatsapp sobre investimentos que o digam, eu realmente não conseguia calar a boca (e ainda não consigo) sobre o assunto. Eu sei que o pensamento de concentrar seus investimentos em bitcoin soa agressivo para a maioria dos investidores, especialmente para aqueles que nunca estudaram mais de 1000 horas sobre o bitcoin como eu estudei e não entendem os seus



fundamentos e o que ele representa.

- O bitcoin é claramente superior ao sistema financeiro atual. Em praticamente qualquer critério de avaliação.

- A rede é mais segura;

- O sistema inteiro é descentralizado (o que significa que não existe um rei e seus amigos, como é atualmente com o FED e os Bancos Centrais); Ser descentralizado também significa que o sistema é incensurável e não pode ser utilizado como coerção geopolítica;

- A base monetária não pode ser expandida (considerando o limite máximo de 21 milhões de bitcoins), o que significa que as suas economias não serão desvalorizadas intencionalmente pelos amigos do rei;

- Existe um ethos na comunidade, existem princípios sólidos e coerentes com os quais eu me identifico (don't trust, verify; todo mundo é um scammer até que se prove o contrário; pseudônimo é melhor que nome real, inválida argumentos e perseguições ad hominem, etc).

Neste momento, um novo conceito também começou a se manifestar na minha cabeça: o custo de oportunidade não é o CDI e nem mesmo o S&P500, o custo-oportunidade é o desempenho do bitcoin. Este conceito caiu como uma bigorna na minha cabeça. Se o custo de oportunidade é o bitcoin, nenhum investimento faz sentido enquanto a adoção dele ainda estiver no início e com taxa acentuada.



“Espere, o custo oportunidade de tudo é o bitcoin?” “Sempre foi.”

O bitcoin não é um ativo arriscado como pensam as pessoas que ainda estão presas na mentalidade fiat. Muito pelo contrário, ele é o único ativo livre de risco, a única forma real de propriedade privada. Existe volatilidade dele em relação ao dólar? Sim. Mas 1 bitcoin = 1 bitcoin e ninguém consegue tomar ele de você. Ninguém consegue bloquear a sua conta ou te cancelar. Ninguém consegue passar um cheque sem fundo. Não existe o come-cotas no bitcoin e nem taxas, de maneira que o seu bitcoin se mantém estável para sempre enquanto você estiver fazendo o hodl dele. Além disso, o bitcoin de fato é um culto e uma religião, e uma religião não vai para zero, como eu expliquei no capítulo 7 (Precificando o bitcoin).

O limite de 80% foi mantido para eu ter alguma forma de reserva de emergência em fiat, mas a vontade já era estar 100% comprado.

**Não, maluco são os outros (100% - maximalista)**

18 de fevereiro de 2021



A questão é que o custo de oportunidade do bitcoin vai ficando cada vez mais clara e a percepção de que o fiat ou mesmo ações que eu havia mantido (Engie, EDP, Taesa e Copasa) não faziam sentido também. O que adianta ter uma ação com expectativa de 10% de dividendos anuais, se a expansão monetária é superior a isso? É praticamente a certeza de perder dinheiro, ou sendo mais específico e correto, certeza de perder o poder de compra do seu dinheiro, mesmo que o valor nominal siga aumentando...

A mudança de 80% para 100% foi natural e tranquila, nessa fase eu já entendia que esses meus 20% no mercado tradicional corriam muito mais risco do que os 80% em bitcoin. Vale ressaltar que o meu 100% na realidade é 80% em bitcoin e 20% em ações da Microstrategy, a empresa do Michael Saylor. Meu racional é diversificar minha custódia, assim mesmo se eu for incompetente e fizer merda com a custódia, eu ainda não me fodo 100%, só 80%.



Obrigado, mas não obrigado.

## Pleb no Twitter

No início de 2020 eu jamais pensei que eu escreveria isso, mas o Twitter foi a minha principal ferramenta de estudos. Eu tive a sorte de já seguir uma galera do fintwit (o povo que fala do mercado tradicional) e ter tido um estalo de buscar a #bitcoin por lá. Eu encontrei alguns poucos e bravos plebs brasileiros tentando espalhar a palavra e muitos plebs gringos, além de podcasters, escritores, investidores e outros membros do ecossistema do bitcoin.

O Bitcoin Twitter é um espaço sem frescuras, onde argumentos ad hominem não fazem sentido (afinal, nós nos autodenominamos plebs e usamos avatares ridículos), e a verdade é buscada a ferro e sangue. Lá você pode encontrar os piores golpistas e as pessoas mais brilhantes e honestas. O seu único trabalho é filtrar bem o ruído do sinal.

## Os memes

*"Meme é criptografia antiboomer"*

algum pleb no Twitter

Os memes também foram peças centrais do meu aprendizado. É impressionante a quantidade e densidade de informações que uma imagem bem selecionada pode transmitir. Imagens realmente mexem com a gente, e essa cena do meme “Pump it up” mandando eu investir mais (“Bet more”) sempre me provocava. Com certeza essa cena em específico contribuiu significativamente para eu converter mais reais em satoshis no início.



Cena de uma das várias versões do Pump it up<sup>158</sup> – meme clássico para os dias de altismo.

Abaixo, eu fiz uma seleção de três memes com significado que me ajudaram a entender alguma parte da tese:



Saindo da Matrix: “Você está tentando me dizer que eu vou poder trocar meu bitcoin por milhões algum dia?” “Não Neo, eu estou te dizendo que quando você estiver pronto, você não vai precisar.”



Trecho do meme “Pump it up”. No começo da minha jornada, eu não tinha entendido a parte revolucionária do bitcoin e estava comprando só pela tecnologia NGU. Essa cena foi no meme que me abriu os olhos.



A melhor definição dos campos do conhecimento que uma pessoa deve dominar para compreender o bitcoin

## O Explica Bitcoin

Para me forçar a levar a sério meus estudos sobre o bitcoin, eu criei o Explica Bitcoin, onde compartilho textos autorais e traduções do inglês, pensando nos plebs brasileiros que não falam a língua. Quando eu comecei o Explica em maio de 2021, existiam relativamente poucas fontes de conteúdo em português. Eu nunca fui fã de conteúdo de trader, acho que até funciona eventualmente, mas sempre considerei como uma espécie de zodíaco para

meninos. Então vários dos conteúdos sobre o bitcoin em português não me interessavam. Pra mim, os Bitcoinheiros<sup>159</sup> sempre foram (e ainda são) a principal referência, o que esses caras fizeram e fazem pelos brasileiros é incrível. O Korea<sup>160</sup> também já existia e também era uma grande referência para mim. Mas fora eles eu só seguia e estudava com conteúdos gringos. Eu sentia que faltava material para estudar em português e eu senti o impulso de retribuir ao bitcoin e ajudar os brasileiros a encontrarem o que eu havia encontrado.

### **Textos autorais**

A minha formação acadêmica me ensinou que o melhor jeito para estudar e organizar o pensamento é escrever sobre o tema que você está estudando. Ou como o Jordan Peterson diz, pensar e escrever são a mesma coisa.

E eu precisava estudar muito ainda. O que me levou a escrever sobre os temas que eu mais queria entender a cada momento. Quando eu conversava com alguém e percebia furos em determinados aspectos da minha compreensão da tese ou quando eu cansava de repetir a mesma coisa várias vezes para pessoas diferentes eu anotava o tema e pesquisava mais a respeito dele. Assim surgiram vários textos autorais.

Você pode ver todos eles no [www.explicabitcoin.com.br](http://www.explicabitcoin.com.br) na seção de "textos autorais".

### **Textos traduzidos**

Fora os textos autorais, a minha principal ferramenta de estudos sempre foi a tradução de textos clássicos e atuais sobre o bitcoin do inglês para o português. Esse exercício é muito bom pois me força a ler muitos textos e ainda consigo ajudar outros brasileiros (e lusófonos em geral) que não falam inglês mas querem se aprofundar nos estudos. Todas as mais de 90 traduções podem ser encontradas no site [www.explicabitcoin.com.br](http://www.explicabitcoin.com.br) na seção de "traduções".

## Coisas que não são sobre o bitcoin, mas que me ajudaram a entender o bitcoin

Depois que você entende um conceito novo, é normal começar a ver este conceito em todos os lugares. E isso também é verdade para o bitcoin. De fato, várias das pecinhas que me ajudaram a solucionar o quebra-cabeças chamado bitcoin foram livros e filmes que não estão diretamente relacionados ao tema que me ensinaram. São eles:

**O Gene Egoísta - Richard Dawkins.** Livro sobre biologia evolutiva que se aprofunda e explica bem os conceitos de teoria dos jogos. A biologia evolutiva utiliza muitos raciais embasados em teoria dos jogos, então esse livro realmente ajuda a entender melhor essas dinâmicas em ações no ecossistema do bitcoin.

**Antifrágil - Nassim Taleb.** É até engraçado citar o Taleb quando o assunto é bitcoin, mas ainda sim foi nesse livro que eu entendi realmente as vantagens de um sistema descentralizado que processa as informações in situ versus um sistema centralizado. O bitcoin é a definição de antifragilidade, apesar do próprio Taleb não enxergar assim, o que diz mais a respeito dele do que da criptomoeda.

**Sapiens - Yuval Harari.** Livro que conta a história da nossa espécie e explica a diferença entre realidades objetivas e subjetivas. Com isso ele nos mostra como histórias podem fazer sentido e organizar uma sociedade, mesmo não existindo no mundo real físico. Um exemplo citado no livro é justamente o dinheiro.

**Matrix.** Esse filme é basicamente um documentário sobre o bitcoin. O filme bebe diretamente na fonte dos cypherpunks, movimento ideológico que originou o bitcoin. Diversos elementos da linguagem memética comuns aos bitcoinheiros envolve elementos do filme, como o “follow the white rabbit” e a escolha entre a pílula vermelha e a pílula azul, como essa versão do meme “pump it up”<sup>161</sup> mostra bem.

**V de Vingança.** Um documentário fantasioso sobre o mundo da pandemia, em especial a Austrália, mas também Canadá, Europa e partes dos EUA.

**A Grande Aposta.** Parte importante do processo de compreensão da tese do bitcoin é entender como o sistema fiduciário atual é problemático, como esse sistema é composto por incompetentes e criminosos, que não

sofrem na pele as consequências dos seus atos. Na linguagem do mercado, eles não têm a pele em risco (skin in the game na linguagem da Faria Lima), ou em bom português, eles não têm o cu na reta. Nos termos bitcoinheiros, eles são os cantillionários. Vale ressaltar que o Michael Burry é um dos principais personagens do filme, o gênio que descobriu sozinho toda a fraude do sistema de crédito imobiliário nos EUA. Hoje em dia ele é um dos críticos do bitcoin.

**Killing in The Name - Rage Against The Machine<sup>162</sup>.**

*"They use force to make you do what the deciders have decided you must do!"*

*"Eles usam a força para te obrigar a fazer o que os tomadores de decisão decidiram que você deve fazer!"*

A letra e o sentimento de raiva anti-sistema dessa música diz tudo. Se você ainda não encontrou essa raiva primitiva dentro de você e não sente ela pelo sistema atual, você ainda está na superfície da toca do coelho. Mas com o tempo ela virá.

**Cannabis**, a boa e velha maconha. Qualquer maconheiro que se preze já estudou um pouco a história da proibição e sabe quão patético é o estado tentar proibir uma planta medicinal usada há milênios pela humanidade. Essa foi a minha toca do coelho inicial, ainda na adolescência. Ela me ensinou como as regras do estado não precisam fazer sentido e me fez desprezar essas regras. Se o que um pedaço de papel do estado diz não fizer sentido para mim, ele não significa nada. Uma coisa não é moralmente correta só por estar escrita em um pedaço de papel. Quem quiser começar a se aprofundar nessa toca do coelho, eu indico o documentário Grass<sup>163</sup> sobre a história da proibição da cannabis nos EUA.

## O caminho a frente

Quanta coisa. Pareceu bem mais de um ano para falar a verdade. Impressionante o quanto eu aprendi, o quanto minha visão de mundo amadureceu, como finalmente várias questões que eu tinha em relação ao mundo fizeram sentido.

Ainda preciso estudar MUITO, quanto mais eu sou puxado pela gravidade da toca do coelho mais eu vejo o tamanho da minha ignorância. É tanta coisa que a única certeza que eu tenho é que essa toca do coelho ainda



tem muita coisa para me ensinar. Só sei que esse ano foi incrível, inesperado, surpreendente e fascinante intelectualmente. Que venham os próximos!

## 4 meses depois...

Essa foi a história do meu primeiro ano na toca, entre outubro de 2020 e outubro de 2021 e o final da versão original do texto “Minha história com o bitcoin”. Agora, enquanto escrevo essa atualização pro livro, estamos em fevereiro de 2022, ou seja, 5 meses após a publicação original e é impressionante quanta coisa mudou.

O Explica Bitcoin surgiu como um hobby despretenso e se transformou no projeto da minha vida. Hoje, grande parte da minha atenção é dedicada a ele. Nesses últimos 5 meses, deixei de ser só um entusiasta e passei a trabalhar no ecossistema do bitcoin como colunista no Livecoins<sup>164</sup>, além de continuar tocando o Explica. Inclusive, a maioria dos textos deste livro foram publicados originalmente lá.

Além dos textos, também criei duas linhas de podcasts para explorar diferentes regiões da toca do coelho. O Sessão de Hopium é um podcast de mesa de bar, no qual plebs maximalistas conversam sobre o bitcoin e o que torna esses extremamente altistas com o seu futuro. Já o Sessão Temática é o podcast onde eu me aprofundo em temas específicos do ecossistema, seja empreendedorismo, mineração, teses específicas e qualquer outro tema que eu tenha curiosidade e queira explorar. Ambos podcasts podem ser encontrados em qualquer agregador de podcast ou no YouTube, é só buscar por “Explica Bitcoin” ou “Sessão de Hopium”.

O que os próximos meses e anos trarão? Impossível de prever, o ecossistema se move muito rápido. Então é focar em seguir espalhando a palavra de Satoshi e ver até onde isso leva...

## REFERÊNCIAS

*Se eu vi mais longe, foi por estar sobre ombros de gigantes.*

Sir Isaac Newton

Referências utilizadas em cada texto do livro.

### Introdução

- 1 - <https://holdbtc100.com.br/>
- 2 - [https://pt.wikipedia.org/wiki/Hip%C3%B3tese\\_do\\_mercado\\_eficiente](https://pt.wikipedia.org/wiki/Hip%C3%B3tese_do_mercado_eficiente)
- 3 - <https://twitter.com/IIICapital/status/1314197544239497216>
- 4 - <https://www.rollingstone.com/politics/politics-news/melania-trump-nft-auction-1301222/>
- 5 - [https://bitcoin.org/files/bitcoin-paper/bitcoin\\_pt\\_br.pdf](https://bitcoin.org/files/bitcoin-paper/bitcoin_pt_br.pdf)

### Capítulo 1 - O que o bitcoin conserta?

- 6 - <https://twitter.com/BitcoinExplica/status/1516052397277208581>
- 7 - [https://pt.wikipedia.org/wiki/Fast\\_fashion](https://pt.wikipedia.org/wiki/Fast_fashion)
- 8 - <https://www.metropoles.com/mundo/homem-e-flagrado-com-ouro-debaixo-da-peruca-e-no-reto-em-aeroporto>
- 9 - <https://bitcoinmagazine.com/culture/bitcoin-a-currency-of-decolonization>

- 10 - <https://g1.globo.com/mundo/noticia/metade-da-populacao-da-republica-centro-africana-precisa-de-ajuda-humanitaria.ghtml>
- 11 - <https://www.cambridge.org/core/journals/journal-of-modern-african-studies/article/abs/devaluation-of-the-cfa-franc-in-senegal-the-reaction-of-small-businesses/FA4259BC53AEF7F8F658C9F39A34CB08>
- 12 - <https://amlmiguel.medium.com/mestres-e-escravos-do-dinheiro-dfa218b5e17e>
- 13 - <https://forbes.com.br/listas/2018/06/10-paises-com-mais-pessoas-sem-conta-bancaria/>
- 14 - <https://valorinveste.globo.com/produtos/servicos-financeiros/noticia/2021/04/27/34-milhoes-de-brasileiros-ainda-nao-tem-acesso-a-bancos-no-pais.ghtml>
- 15 - <https://livecoins.com.br/el-salvador-quer-bitcoin-como-moeda-de-uso-comum-e-reserva-de-valor/>

## **Capítulo 2 - Efeito Cantillon**

- 16 - [https://www.youtube.com/watch?v=ZG\\_Im-DiUN8](https://www.youtube.com/watch?v=ZG_Im-DiUN8)
- 17 - <https://pt.wikipedia.org/wiki/Comunismo>
- 18 - [https://pt.wikipedia.org/wiki/Liberalismo\\_cl%C3%A1ssico](https://pt.wikipedia.org/wiki/Liberalismo_cl%C3%A1ssico)
- 19 - <https://wtfhappenedin1971.com/>
- 20 - <https://pt.wikipedia.org/wiki/Petrod%C3%B3lar>
- 21 - <https://forbes.com.br/negocios/2020/04/airbnb-assegura-novo-emprestimo-de-us-1-bi-apos-emissao-de-us-1-bi-em-titulos/>

## **Capítulo 3 - O que é o bitcoin?**

- 22 - <https://satoshi.nakamotoinstitute.org/posts/p2pfoundation/2/#selection-37.1-37.308>
- 23 - <https://twitter.com/halfin/status/1110302988>
- 24 - [https://golden.com/wiki/Nakamoto\\_consensus-AMB5VWM](https://golden.com/wiki/Nakamoto_consensus-AMB5VWM)
- 25 - <https://pt.wikipedia.org/wiki/SHA-2#Pseudoc%C3%B3digo>
- 26 - <https://md5calc.com/hash/sha256>
- 27 - <https://xorbin.com/tools/sha256-hash-calculator>
- 28 - <https://tools.superdatascience.com/blockchain/blockchain>

## **Capítulo 4 - A descoberta do bitcoin**

29 - <https://www.scielo.br/j/rbh/a/G6z3gmqHCJPXzxrTNj8mQP/?lang=pt>

30 - [https://en.wikipedia.org/wiki/Leibniz%E2%80%93Newton\\_calculus\\_controversy](https://en.wikipedia.org/wiki/Leibniz%E2%80%93Newton_calculus_controversy)

31 - [https://pt.wikipedia.org/wiki/Sopa\\_primordial](https://pt.wikipedia.org/wiki/Sopa_primordial)

32 - [https://pt.wikipedia.org/wiki/Fundo\\_gen%C3%A9tico#:~:text=Fundo%20gen%C3%A9tico%2C%20fundo%20g%C3%A9nico%2C%20pool,fundo%20gen%C3%A9tico%20da%20gera%C3%A7%C3%A3o%20seguinte](https://pt.wikipedia.org/wiki/Fundo_gen%C3%A9tico#:~:text=Fundo%20gen%C3%A9tico%2C%20fundo%20g%C3%A9nico%2C%20pool,fundo%20gen%C3%A9tico%20da%20gera%C3%A7%C3%A3o%20seguinte)

33 - [https://en.wikipedia.org/wiki/Meme\\_pool](https://en.wikipedia.org/wiki/Meme_pool)

34 - <https://escolacripto.com.br/linha-do-tempo-da-pre-historia-do-btc/>

## **Capítulo 5 – Os Fundamentos do bitcoin**

35 - <https://twitter.com/BitcoinExplica/status/1471629159529164805>

36 - <https://bitinfocharts.com/comparison/hashrate-btc-eth-doge-bch.html#alltime>

37 - <https://www.blockchain.com/pt/charts/hash-rate>

38 - <https://mempool.space/pt/>

39 - <https://explicabitcoin.wordpress.com/2021/11/12/o-que-e-o-problema-dos-generais-bizantinos/>

40 - <https://twitter.com/BitcoinExplica/status/1485693868066680838>

41 - <https://www.youtube.com/watch?v=QjHiQK4vKas>

42 - <https://explicabitcoin.wordpress.com/2021/07/22/como-o-exercito-de-dca-vai-levar-o-preco-do-bitcoin-a-1-milhao/>

43 - [https://en.wikipedia.org/wiki/Persistence\\_hunting](https://en.wikipedia.org/wiki/Persistence_hunting)

44 - [https://www.youtube.com/watch?v=826HMLoiE\\_o](https://www.youtube.com/watch?v=826HMLoiE_o)

## **Capítulo 6 – Precificando o bitcoin**

45 - <https://www.theguardian.com/technology/2011/jun/30/myspace-sold-35-million-news>

46 - <https://ge.globo.com/esports/noticia/magic-the-gathering-black-lotus-e-vendida-por-r-28-milhoes-em-leilao.ghtml>

47 - <https://ge.globo.com/esports/noticia/pokemon-tcg-lista-cartas-mais-caras-do-jogo-precos.ghtml>

48 - <https://bitcointalk.org/index.php?topic=831547.0>

49 - <https://www.bbc.com/portuguese/internacional-54229154>

- 50 - <https://www.reuters.com/article/us-crypto-currencies-jpm-idUSKBN29A1IF>
- 51 - <https://www.imf.org/Publications/fandd/issues/2019/09/tackling-global-tax-havens-shaxon>
- 52 - <https://medium.com/capriole/bitcoin-value-energy-equivalence-6d00d1baa34a>
- 53 - <https://twitter.com/100trillionUSD>
- 54 - <https://stats.buybitcoinworldwide.com/s2fx/>
- 55 - <https://medium.com/@100trillionUSD/modeling-bitcoins-value-with-scarcity-91fa0fc03e25>
- 56 - <https://medium.com/@100trillionUSD/bitcoin-stock-to-flow-cross-asset-model-50d260feed12>
- 57 - <https://www.forbes.com/sites/stevenehrlich/2021/04/29/demystifying-bitcoins-remarkably-accurate-price-prediction-model-stock-to-flow/?sh=267c5857476a>
- 58 - <https://www.youtube.com/watch?v=28OYldJ15IA>
- 59 - <https://www.coindesk.com/veteran-investor-bill-miller-calls-bitcoin-a-rat-poison-but-for-cash>
- 60 - <https://www.bloomberg.com/news/articles/2020-05-07/paul-tudor-jones-buys-bitcoin-says-he-s-reminded-of-gold-in-70s>
- 61 - [https://www.youtube.com/watch?v=-\\_QWFH-GobA](https://www.youtube.com/watch?v=-_QWFH-GobA)
- 62 - <https://ciclovivo.com.br/planeta/meio-ambiente/planta-do-cerrado-floresce-queimada/>
- 63 - <https://www.snopes.com/fact-check/paul-krugman-internets-effect-economy/>

## **Capítulo 7 – A tecnologia NGU**

- 64 - <https://explicabitcoin.medium.com/como-o-ex%C3%A9rcito-de-dca-vai-levar-o-pre%C3%A7o-do-bitcoin-a-1-milh%C3%A3o-5ee77bd7c512>
- 65 - <https://www.youtube.com/watch?v=DURlNHTxuJM>

## **Capítulo 8 – A melhor empresa do mundo**

- 66 - <https://www.suno.com.br/artigos/fluxo-de-caixa-descontado/>
- 67 - <https://www.siteware.com.br/lideranca/como-avaliar-valor-empresa/>
- 68 - <https://yenom.com.br/valuation-empresas-fluxo-de-caixa-descontado-dcf/>

69 - [https://pt.wikipedia.org/wiki/Lato\\_sensu](https://pt.wikipedia.org/wiki/Lato_sensu)

70 - [https://pt.wikipedia.org/wiki/Stricto\\_sensu](https://pt.wikipedia.org/wiki/Stricto_sensu)

71 - <https://www.innoscience.com.br/o-que-eu-aprendi-sobre-cultura-de-inovacao-com-um-googler/>

72 - <https://ri.ambev.com.br/visao-geral/sonho-gente-cultura/>

73 - <https://www.youtube.com/watch?v=iJNvxWemhI4>

74 - <https://www.independent.co.uk/tech/paul-krugman-nobel-prize-bitcoin-b1850539.html>

75 - <https://www.criptofacil.com/bilionario-dispara-bitcoin-uma-religiao-nao-serve-protecao-contra-criises/>

76 - <https://www.youtube.com/watch?v=l7GdLQlChNA>

77 - <https://pt.wikipedia.org/wiki/Cypherpunk#:~:text=Cypherpunk%20%C3%A9%20um%20grupo%20informal%20de%20pessoas%20interessadas%20em%20Criptografia.>

78 - <https://computerworld.com.br/carreira/retencao-de-talentos-e-um-dos-maiores-desafios-da-ti-em-2019/>

79 - [https://pt.wikipedia.org/wiki/Net\\_Promoter\\_Score](https://pt.wikipedia.org/wiki/Net_Promoter_Score)

80 - <https://www.consumidormoderno.com.br/2019/09/11/inovacao-boca-boca-digital/>

81 - <https://www.forbes.com/sites/biancamillercole/2019/01/10/innovate-or-die-how-a-lack-of-innovation-can-cause-business-failure/?sh=4e3797c22fcb>

82 - <https://www.amazon.com.br/Move-Fast-Break-Things-Undermined/dp/0316275778>

83 - [https://twitter.com/Croesus\\_BTC](https://twitter.com/Croesus_BTC)

84 - [https://www.youtube.com/watch?v=mDFNClyCbHI&t=12s&ab\\_channel=Bitcoinheiros](https://www.youtube.com/watch?v=mDFNClyCbHI&t=12s&ab_channel=Bitcoinheiros)

85 - <https://www.bbc.com/portuguese/internacional-57377160>

86 - <https://www.youtube.com/watch?v=3ZhpoVhHU-k>

87 - <https://canaltech.com.br/saude/o-que-e-taxa-r-quando-e-hora-de-afrouxar-a-quarentena-166440/>

88 - <https://br.investing.com/news/cryptocurrency-news/bitcoin-brilha-em-corrida-da-indy-500-em-esforco-para-disseminar-a-adocao-874722>

89 - <https://investidoremvalor.com/fosso-economico/>

90 - [https://pt.wikipedia.org/wiki/Efeito\\_de\\_rede](https://pt.wikipedia.org/wiki/Efeito_de_rede)

- 91 - <https://www.bitcoinbeach.com/>
- 92 - <https://explicabitcoin.wordpress.com/2021/05/24/a-adocao-do-bitcoin/>
- 93 - <https://explicabitcoin.wordpress.com/2021/06/02/a-curva-dupla-de-adocao-do-bitcoin/>
- 94 - <https://www.conjur.com.br/2011-mai-16/processo-antitruste-microsoft-acaba-depois-10-anos>
- 95 - <https://www.amazon.com/Blocksize-War-controls-Bitcoins-protocol/dp/B08YQMC2WM>

## **Capítulo 9 – A mineração de bitcoin**

- 96 - <http://mineralis.cetem.gov.br/bitstream/cetem/1103/1/14%20BAUXITA%201.pdf>
- 97 - <https://en.wikipedia.org/wiki/Iceland>
- 98 - [https://en.wikipedia.org/wiki/Mantle\\_plume](https://en.wikipedia.org/wiki/Mantle_plume)
- 99 - <https://www.theglobeandmail.com/globe-drive/culture/technology/why-steaming-hot-iceland-has-very-cheap-power/article593551/>
- 100 - <https://blog.bizvibe.com/blog/industrial-supplies/top-10-largest-aluminium-producing-countries>
- 101 - <https://www.latimes.com/business/la-xpm-2011-mar-26-la-fi-iceland-economy-20110326-story.html>
- 102 - <https://aluminiuminsider.com/winter-coming-icelands-aluminium-smelters/>
- 103 - <https://blockstream.com/satellite/>

## **Capítulo 10 – as implicações da mineração do bitcoin para o setor de energia**

- 104 - <https://bitcoinminingcouncil.com/bitcoin-mining-electricity-mix-increased-to-59-5-sustainable-in-q2-2022/>
- 105 - <https://exame.com/future-of-money/o-mundo-de-amanha-energia-e-chave-para-transformacao-e-o-bitcoin-pode-ter-papel-importante-nisso/>
- 106 - <https://arthurmining.com/>

## **Capítulo 11 – O ethos de um bitcoinheiro**

- 107 - <https://pt.wikipedia.org/wiki/Ethos>
- 108 - [https://pt.wikipedia.org/wiki/Diagrama\\_de\\_Venn](https://pt.wikipedia.org/wiki/Diagrama_de_Venn)

109 - [https://pt.wikipedia.org/wiki/Te%C3%ADsmo#:~:text=Te%C3%ADsmo%20\(do%20grego%20%CE%B8%CE%B5%C3%B3%CF%82%20%5Bthe%C3%B3s,um%2C%20pode%20existir%20um%20supremo.](https://pt.wikipedia.org/wiki/Te%C3%ADsmo#:~:text=Te%C3%ADsmo%20(do%20grego%20%CE%B8%CE%B5%C3%B3%CF%82%20%5Bthe%C3%B3s,um%2C%20pode%20existir%20um%20supremo.)

110 - [https://www.youtube.com/watch?v=Td\\_ieom1g88](https://www.youtube.com/watch?v=Td_ieom1g88)

111 - <https://finance.yahoo.com/news/4-2-billion-lost-bitcoin-154948781.html#:~:text=Approximately%2020%25%20of%20all%20Bitcoins,After%20Hackers%20Steal%20%24600%20Million%3F>

112 - <https://www.nytimes.com/2021/01/12/technology/bitcoin-passwords-wallets-fortunes.html>

113 - [https://pt.wikipedia.org/wiki/N%C3%BAmero\\_de\\_Dunbar](https://pt.wikipedia.org/wiki/N%C3%BAmero_de_Dunbar)

114 - <https://twitter.com/prestonpysh/status/1347206346647740422>

115 - [https://pt.wikipedia.org/wiki/O\\_Caminho\\_da\\_Servid%C3%A3o](https://pt.wikipedia.org/wiki/O_Caminho_da_Servid%C3%A3o)

116 - [https://pt.wikipedia.org/wiki/Experimento\\_do\\_marshmallow](https://pt.wikipedia.org/wiki/Experimento_do_marshmallow)

117 - [https://www.youtube.com/watch?v=QX\\_oy9614HQ](https://www.youtube.com/watch?v=QX_oy9614HQ)

118 - <https://www.youtube.com/watch?v=bnpyWjkuB1U>

119 - [https://pt.wikipedia.org/wiki/Argumentum\\_ad\\_hominem](https://pt.wikipedia.org/wiki/Argumentum_ad_hominem)

120 - <https://www.youtube.com/watch?v=dhQ3AFpV52o>

## **Capítulo 12 – A personalidade de um bitcoinheiro**

121 - <https://www.youtube.com/watch?v=Smwrw4sNCxE>

122 - [https://pt.wikipedia.org/wiki/C%C3%B3digo\\_de\\_Holland](https://pt.wikipedia.org/wiki/C%C3%B3digo_de_Holland)

123 - <https://eadvoltage.com.br/testeVocacional/>

124 - <https://www.16personalities.com/br/teste-de-personalidade>

125 - <https://www.16personalities.com/articles/our-theory>

126 - <https://www.16personalities.com/br/personalidade-intj>

127 - <https://www.16personalities.com/br/personalidade-intj>

128 - <https://www.16personalities.com/br/personalidade-istj>

129 - <https://twitter.com/bquittem/status/1438170707754618883?s=24>

130 - <https://www.16personalities.com/br/personalidade-isfj>

131 - <https://www.16personalities.com/br/personalidade-esfj>

132 - <https://twitter.com/bitdov/status/1468966107058872328>

133 - <https://twitter.com/LaserHodl>

134 - <https://explicabitcoin.wordpress.com/2021/07/01/eu-estou-atrasado-pro-bitcoin/>



- 135 - <https://www.infomoney.com.br/colunistas/ifl-instituto-de-formacao-de-lideres/resenha-de-livro-de-zero-a-um-de-peter-thiel/>
- 136 - [https://www.google.com.br/books/edition/De\\_zero\\_a\\_um/EtmxBAAQBAJ?hl=pt-BR&gbpv=0](https://www.google.com.br/books/edition/De_zero_a_um/EtmxBAAQBAJ?hl=pt-BR&gbpv=0)
- 137 - <https://www.16personalities.com/insights/surveys/practical-mind/results>
- 138 - <https://www.youtube.com/watch?v=Nt6ILTNaqQ8>
- 139 - <https://twitter.com/GhostofSvetski>
- 140 - <https://explicabitcoin.wordpress.com/2021/09/23/bitcoiners-sao-os-remanescentes-as-massas-nao-importam/>
- 141 - <https://explicabitcoin.wordpress.com/2021/12/04/os-remanescentes-o-parasita-e-as-massas/>
- 142 - <https://explicabitcoin.medium.com/o-remanescente-a-guerra-dos-tronos-do-bitcoin-20c6e3607f60>
- 143 - <https://hrf.org/team/alex-gladstein/>
- 144 - <https://twitter.com/gladstein>

### **Capítulo 13 – A personalidade de um bitcoinheiro brasileiro**

- 145 - [https://docs.google.com/spreadsheets/d/1bmAAvxcxB\\_j052ULEsJkRmwJs\\_xK8OfelLyJlQ1Cq1U/edit#gid=0](https://docs.google.com/spreadsheets/d/1bmAAvxcxB_j052ULEsJkRmwJs_xK8OfelLyJlQ1Cq1U/edit#gid=0)

### **Capítulo 15 – Separando o joio do trigo**

- 146 - [https://pt.wikipedia.org/wiki/Rela%C3%A7%C3%A3o\\_sinal-ru%C3%ADdo](https://pt.wikipedia.org/wiki/Rela%C3%A7%C3%A3o_sinal-ru%C3%ADdo)
- 147 - <https://glassnode.com/>
- 148 - <https://livecoins.com.br/blockstream-importante-pro-bitcoin/>
- 149 - <https://explicabitcoin.medium.com/sobre-tulipas-e-manipula%C3%A7%C3%A3o-9c25ca53b70f>

### **Capítulo 16 – O ouro de tolo digital**

- 150- <https://aws.amazon.com/marketplace/pp/prodview-6hnlavs4r2yhc>
- 151 - <https://copper.co/insights/creating-cryptocurrency-yield-how-to-stake-eth-2-0>

## Apêndice

152 - <https://twitter.com/saylor/status/1307029562321231873>

153 - <https://www.youtube.com/watch?v=8Yfb2zQjKWE>

154 - <https://www.youtube.com/watch?v=qL2LfVRI3J0&t=8s>

155 - <https://www.youtube.com/watch?v=Cg10yYZjK94&t=309s>

156 - <https://explicabitcoin.medium.com/bitcoin-%C3%A9-a-op%C3%A7%C3%A3o-perfeita-e-os-bancos-centrais-ter%C3%A3o-que-comprar-3fbfae2354a0>

157 - <https://explicabitcoin.medium.com/a-gravidade-do-bitcoin-a50685170793>

158 - <https://www.youtube.com/watch?v=k001JX-D-dA&t=13s>

159 - <https://www.youtube.com/c/Bitcoinheiros>

160 - <https://www.youtube.com/KoreacomK>

161 - <https://www.youtube.com/watch?v=EFDMum1vs7Q>

162 - <https://www.youtube.com/watch?v=8de2W3rtZsA>

163 - <https://www.youtube.com/watch?v=NnpBLIH6kKk&t=2239s>

164 - <https://livecoins.com.br/author/pudim/>