MISES: Revista Interdisciplinar de Filosofia, Direito e Economia
ISSN 2318-0811
Volume III, Número 2 (Edição 6) Julho-Dezembro 2015: 427-440

Sobre as Origens do Bitcoin: Estágios da Evolução Monetária – Parte I[*]

Konrad S. Graf[**]

Resumo: Nesta obra, o autor desenvolve um estudo econômico e histórico da origem do Bitcoin e de seu valor enquanto moeda. Em sua argumentação, o autor explora a relação entre a moeda digital Bitcoin e a Economia Austríaca, discutindo, em particular, o Teorema da Regressão de Ludwig von Mises e sua conexão com a evolução do mercado monetário, bem como a abordagem evolutiva seminal de Carl Menger.

Palavras-Chave: Criptomoedas, Teoria monetária, Teorema da Regressão, Evolução monetária.

On The Origins of Bitcoin: Stages of Monetary Evolution – Part I

Abstract: In this work, the author develops an economic and historical study of the origin of the Bitcoin and of its value as money. In his argument, the author explores the relation between the Bitcoin digital currency and Austrian Economics. Particularly, he discusses Ludwig von Mises' Regression Theorem and its connection to the evolution of the monetary market, as well as Carl Menger's seminal evolutionary approach.

Keywords: Cryptocurrencies, Monetary theory, Regression Theorem, Monetary Evolution.

Classificação JEL: G10, B53, E14, E42.

---

[*] Texto baseado na versão de 3 de novembro de 2014. A segunda parte do texto será publicada na próxima edição do periódico MISES: Revista Interdisciplinar de Filosofia, Direito e Economia. A segunda parte conterá duas novas seções empíricas que proporcionam interpretações de padrões de eventos por ano (Apêndice A) e um único gráfico de formação de preços em cinco anos (Apêndice B). Com base nisto, o primeiro padrão claro de utilização do Bitcoin como meio de troca é especificado, pelo autor, como não ocorrendo até 2011. A segunda parte deste texto será publicada na próxima edição de *MISES: Revista Interdisciplinar de Filosofia, Direito e Economia*.
Traduzido do inglês para o português por Claudio A. Téllez-Zepeda.

[**] **Konrad S. Graf** é autor de diversos artigos sobre a teoria monetária do Bitcoin e filosofia do Direito. Também é conferencista e trabalha como tradutor profissional.
Twitter: @konradsgraf

> *Com a expansão do tráfego no espaço e com a expansão das provisões para a satisfação de necessidades materiais ao longo de intervalos de tempo cada vez maiores, cada indivíduo aprenderia, a partir do seu próprio interesse econômico, a tomar o cuidado de ter trocado seus bens menos vendáveis por aquelas mercadorias especiais que apresentavam, além do atrativo de serem altamente comercializáveis na localidade particular, uma vasta gama de comerciabilidade no tempo e no espaço.*
> *Estes produtos seriam qualificados pelo seu alto preço, fácil transportabilidade e adequação para a preservação [...] para assegurar ao seu detentor um poder, não somente "aqui" e "agora", mais o mais ilimitado possível no espaço e no tempo em geral, com respeito a todos os demais bens no mercado.* (Carl Menger,1892)

> *Deve ser reiterado, aqui, que as escalas de valor não existem no vácuo para além das escolhas concretas da ação*. (Murray Rothbard, 1962)

I – A Batalha que Nunca Aconteceu: O Teorema da Regressão contra o Bitcoin

O teorema da regressão abrange vários passos distintos na explicação teórica da evolução de mercado monetário[1]. Tratou do processo pelo qual um meio de troca emerge a partir das permutas, o processo pelo qual uma moeda dominante emerge de uma constelação de meios de troca concorrentes, e da maneira como as percepções dos usuários dos preços do passado influenciam suas avaliações do poder de compra da moeda olhando na direção de um futuro mais ou menos distante. Essas diversas questões distintas não são sempre diferenciadas o suficiente no discurso.

A exposição desta sequência de desenvolvimento contrasta com as teorias da moeda da atribuição e do Estado, que sustentam que a moeda é um recibo, de outra forma sem valor, e que ela é criada e regulada pelos governantes para ser utilizada por suas populações governadas. Esta última perspectiva poderia ser apelidada, de forma ligeiramente não generosa, como a *teoria monetária do aceno do governante*, ou do criacionismo monetário. Outra visão sustenta que a moeda é uma "ilusão social" misteriosa, estabelecida mediante acordo somente pela convenção arbitrária, independente de se os atores estatais desempenharam um papel integral ou incidental na construção dessa ilusão. Entretanto, tais exposições parecem oferecer pouca explicação a respeito de como e por que uma tal ilusão acaba derrotando todas as outras ilusões candidatas em lugares e épocas específicos.

É em contraste a essas explicações insatisfatórias que as explicações baseadas na ação e da "Escola Austríaca" evolutiva têm se posicionado por muito tempo. Elas sustentam que: 1) a moeda também é um bem econômico em si mesma e não meramente um recibo substituto no estoque social de bens, e que 2) o desenvolvimento da moeda pode ser traçado de volta a processos econômicos graduais específicos. Cada um desses passos na evolução da moeda, de acordo com os austríacos, e segundo Ludwig von Mises (1881-1973) em particular, podem ser explicados claramente em termos de escolhas e ações humanas e em termos teóricos universais, sendo que também podem ser ilustrados com exemplos históricos/empíricos[2].

O Teorema da Regressão explica um conjunto de implicações lógicas derivadas de conceitos centrais da teoria econômica, tais como "bem" e "meio de troca". Entretanto, a explicação da evolução passo a passo do mer-

[1] Para um estudo rápido do teorema da regressão, ver: ROTHBARD, Murray N. **Man, Economy, and State, with Power and Market. The Scholar's Edition**. Auburn, Alabama: Ludwig von Mises Institute, 2004. p. 268-276.

[2] Esta é uma aplicação da divisão estrita entre os domínios próprios da teoria universal e a interpretação de caso específica. Ver, em particular: MISES, Ludwig von. **Theory and History: An Interpretation of Social and Economic Evolution**. Auburn, Alabama: Ludwig von Mises Institute, 2007. A obra está disponível em português como: MISES, Ludwig von. **Teoria e História: Uma Interpretação da Evolução Social e Econômica**. Tradução de Rafael de Sales Azevedo. São Paulo: Instituto Ludwig von Mises Brasil, 2014.

cado, associada ao Teorema da Regressão, tem sido geralmente aprendida e entendida por estudantes de economia no contexto de exemplos históricos, todos os quais correspondiam a bens tangíveis.

As valorações iniciais das unidades de moeda fiduciária de papel menos tangível, e digital totalmente intangível, também são rastreáveis a bens mais tangíveis em seus longos *pedigrees* históricos. Combinações de *redemption defaults* ("suspensões de pagamentos" legalizadas), aquiescência pública gradual por falta de alternativas melhores, e transições a taxas fixas forçadas e permitidas legalmente possibilitaram que unidades cada vez mais abstratas assumissem as funções sociais dos seus ancestrais que eram mercadorias mais tangíveis. Atores políticos poderiam, então, manipular muito mais livremente a quantidade de moeda, particularmente depois que o último vestígio de uma barreira fisicamente ligada à inflação fiduciária caiu em 1971[3].

É importante distinguir o desenvolvimento de preços orgânico e de livre flutuação, tal como o Bitcoin, das conversões legalmente forçadas a taxas fixas entre uma moeda oficial aposentada e seu novo substituto oficial[4]. Um exemplo recente disto foi a substituição legalmente orquestrada de diversas moedas políticas nacionais correntes na Europa pelo euro. O euro (notas de papel e dígitos de computador) herdou sua valoração inicial como moeda a partir das valorações monetárias de suas moedas correntes predecessoras, mediante a conversão forçada a taxas fixas. Essas moedas predecessoras, por sua vez, tiveram, da mesma forma, seus valores iniciais obtidos a partir de taxas de câmbio fixadas legalmente contra lingotes e moedas de metal precioso, taxas de câmbio que se degradaram, por sinal, progressivamente e que, eventualmente, foram varridas por completo.

Tais conversões de valor forçadas legalmente de uma moeda para uma sucessora oficial contrastam bruscamente com as evoluções monetárias originais no mercado. Discussões a respeito destas últimas têm utilizado tipicamente a palavra "mercadoria" para categorizar nitidamente todos os exemplos históricos disponíveis. Esta palavra parece especificar algum material tangível, divisível.

Quando Carl Menger (1840-1921) expôs os problemas que iria abordar em *On the Origins of Money*, em 1892[5], enquadrou a questão das origens em termos de dois paradigmas explicativos concorrentes e usou a terminologia "mercadoria" por toda parte.

> É a moeda um membro orgânico no mundo das mercadorias, ou é uma anomalia econômica? Iremos referir seu giro comercial e seu valor de troca às mesmas causas que condicionam aqueles outros bens, ou são eles o produto distinto da convenção e autoridade[6]?

Uma razão para utilizar a palavra mercadoria (*commodity*) foi que os bens literalmente comercializados nos mercados de mercadorias, tais como cereais e algodão, foram referenciados em discussões sobre precificação, liquidez e distinções entre as posições respectivas de compradores e vendedores. O uso de exemplos mais líquidos de mercadorias comercializadas no mercado foi contrastado com itens de uso único ou especial, tais como tintas ou instrumentos técnicos, para os quais é muito mais fácil e rápido para um

---

[3] Para uma história concisa dos principais desenvolvimentos monetários, ver: HÜLSMANN, Jörg Guido. **The Ethics of Money Production**. Auburn, Alabama: Ludwig von Mises Institute, 2008. Recomendo altamente este trabalho em sua totalidade.

[4] Para uma discussão destes pontos, veja meu texto do dia 22 de Julho de 2013. "Bitcoin, price denomination and fixed-rate fiat conversions". Em: *konradsgraf.com*. Hülsmann também aponta que: "*Historicamente, o estabelecimento do monopólio dos metais preciosos foi um passo importante na consolidação e centralização dos sistemas monetários nacionais sob controle governamental. A proscrição da prata abriu o caminho para uma inflação dos certificados de reserva fracionada lastreados em ouro*" (HÜLSMANN. **The Ethics of Money Production**, p. 117).

[5] MENGER, Carl. **On the Origins of Money**. Auburn, Alabama: Ludwig von Mises Institute, 2009.

[6] Idem. *Ibidem*, p. 13.

comprador localizar um vendedor pronto, do que para um vendedor encontrar um comprador pronto.

Não obstante, para os leitores modernos na era da informação, com sua abundância de "bens digitais" incorpóreos, a palavra "bem" deveria servir no lugar de mercadoria, com menos distração materialista. Muitos dos grandes escritores austríacos, principalmente Mises, insistiram repetidamente em que não deveríamos ser enganados pelas aparências externas das coisas. Todavia, as conotações materialistas parecem ter conspirado para confundir os observadores quando se trata de interpretar a moeda corrente digital e o sistema de pagamentos do Bitcoin.

Isto é compreensível diante da natureza intangível e tecnicamente evasiva das unidades transacionadas dentro da rede – tais como os "*inputs* assinados" e os "*outputs* não dispendidos" criptograficamente. De um ponto de vista técnico, em oposição ao ponto de vista dos usuários, um item específico que pode ser fixado como "um Bitcoin" nem sequer existe. Contudo, é suficiente, do ponto de vista de um usuário final, utilizar a metáfora da existência putativa de um tal item para entender como fazer uso vantajoso da rede de Bitcoin.

Os diversos elementos técnicos enigmáticos dos Bitcoin cruzam os domínios de vários campos de estudo altamente especializados. Enquanto importantes em seus próprios termos, tais detalhes podem ser uma distração para o lado especificamente econômico da análise, o qual está preocupado com a estrutura real das ações dos usuários finais. Assim como a utilização de moedas de prata no comércio não foi seriamente contestada com base no fato de que a prata é, "na realidade", somente uma configuração peculiar de partículas subatômicas entre muitas outras configurações possíveis, também não devemos ficar confusos com o fato de que o Bitcoin é "na realidade" somente um arranjo peculiar de relações criptográficas especificadas, que são mantidas e verificadas dentro de uma rede de computadores global, *peer-to-peer* e de código aberto. Químicos e metalúrgicos participam do negócio de entender os detalhes no primeiro caso; criptografistas, cientistas da computação e programadores estão no negócio de entender as complicações do outro caso.

Entretanto, o Bitcoin na realidade funciona "por debaixo dos panos" e, não obstante as especulações e opiniões a respeito de suas perspectivas no longo prazo, ele já está sendo transacionado *agora*, ano após ano, como um bem, e está sendo utilizado *agora* como um meio de troca com aceitação cada vez mais ampla em uma escala global. Portanto, agora ele entra nas categorias da teoria econômica baseadas na ação e em cada uma de suas implicações lógicas. Não é possível haver contradição entre o Bitcoin e as percepções da teoria econômica associadas ao Teorema da Regressão. Entretanto, o entendimento de como é possível que não existam tais contradições parece ter se mostrado como um desafio.

Tenho escrito e falado muitas vezes sobre o Bitcoin e a origem da moeda, assim como também Peter Šurda e Daniel Krawisz[7]. Como confusões absolutamente fundamentais parecem, contudo, persistir, ofereço a seguir algumas perspectivas e abordagens adicionais a respeito deste tópico. Não somente o Bitcoin deve ser entendido com mais atenção, mas também o próprio Teorema da Regressão, inclusive sua formulação abstrata e baseada na ação, bem como seus vários componentes distintos. Mais ainda, acrescentar algumas perspectivas adicionais sobre a natureza do dinheiro contribui para clarificar ainda mais as questões.

---

[7] KRAWISZ, Daniel. The Original Value of Bitcoins (2 de julho de 2013). Em: *themisescircle.org*; ŠURDA, Peter. **Economics of Bitcoin: Is Bitcoin an Alternative to Fiat Currencies and Gold?** Tese para a Universidade de Economia e Negócios de Viena, 2012; e, mais recentemente "Professor Walter Block is clueless about Bitcoin" (22 de setembro de 2013), em: *economicsofbitcoin.com*.

II – A Falácia da "Moeda ou Nada"

Um reconhecimento informal das opiniões de alguns economistas a respeito de se o Bitcoin é ou não "moeda" apareceu recentemente no website do *Economic Policy Journal*[8]. O consenso razoável foi que o Bitcoin está agora funcionando como um meio de troca e poderia algum dia ser considerado como moeda, se e quando for aceito muito mais amplamente e se torne o meio de troca "comumente utilizado" ou "mais comumente utilizado".

Opiniões sobre a aplicação de palavras tais como moeda são muito menos importantes do que entender o que está acontecendo no mundo real. Em um comentário perspicaz sobre o relatório acima referido, Peter Šurda, um pesquisador sobre o Bitcoin instruído sobre as abordagens da Escola Austríaca, rotulou a obsessão contínua de julgar o Bitcoin com base na questão da moeda como a "falácia da moeda ou nada" (se o Bitcoin não for moeda, então não é nada).

Ademais, argumentei recentemente que, em vez do vago "utilizado comumente", um critério mais preciso para qualificar algo como "moeda" seria qual unidade a maior parte das pessoas em uma comunidade estão utilizando para a formação dos preços e para a contabilidade (cálculo econômico). Dito isto, a identificação de um item como moeda de forma alguma elimina a possibilidade de *na realidade pagar* os preços designados com qualquer outro meio que o vendedor esteja disposto a aceitar a uma taxa de conversão acordada para o preço pedido, expresso na unidade de preços local comum[9]. Para aqueles que o desejarem, por exemplo, já há serviços de pagamento que permitem a conversão instantânea dos pagamentos recebidos em Bitcoin em moeda fiduciária. Os desenvolvedores também estão trabalhando para possibilitar serviços semelhantes para os compradores. Isto daria a opção, para alguns usuários hesitantes diante da corrente volatilidade de preços do Bitcoin no estágio inicial, para que mantenham os Bitcoin somente por frações de segundos. Tais serviços permitem que qualquer um possa tirar vantagem dos aspectos de sistema de pagamentos da rede e, ao mesmo tempo, evitar riscos de volatilidade, caso se deseje isso.

No entanto, a visão de que há uma alegada oposição entre a realidade do Bitcoin e as supostas implicações do teorema da regressão persiste mais do que qualquer outra coisa. Outro comentador sobre o levantamento do *Economic Policy Journal* perguntou se, com os sucessos contínuos do Bitcoin tornando-se cada vez mais difíceis de serem negados, o Teorema da Regressão não teria de ser revisado para além do escopo da Economia Austríaca. Este sentimento, o qual reaparece em discussões online de tempos em tempos, parece ser razoável à primeira vista, mas somente quando baseado na concepção errônea e muito difundida de que o teorema, na realidade, requer que qualquer moeda (sólida) seja material ou tangível, pelo menos na sua origem ou "lastro".

Argumentei anteriormente por que não há razão teórica para que um meio de troca tenha que começar sendo material[10]. É suficiente que seja um bem escasso. A era digital, e o próprio Bitcoin, têm deixado claro que os bens não precisam ser tangíveis. Apesar da escolha de palavras tais como mercadoria nos escritos clássicos sobre este assunto, não há uma razão *econômica* fundamental para que um meio físico tenha que ser o que assegura as características monetárias essenciais – aci-

---

[8] WENZEL, Robert. Is Bitcoin Money: What Economists Have to Say (7 de outubro de 2013). Em: *economicpolicyjournal.com*.

[9] Abordo isto com algum detalhamento no meu artigo de 14 de setembro de 2013: Bitcoin as medium of exchange now and unit of account later: The inverse of Koning's medieval coins. Em: *konradsgraf.com*.

[10] Bitcoins, the Regression Theorem, and that Curious but Unthreatening Empirical World (27 de fevereiro de 2013). Em: *konradsgraf.com*; The Sound of One Bitcoin: Tangibility, Scarcity, and a 'Hard-Money' Checklist (19 de março de 2013). Em: *konradsgraf.com*.

ma de tudo, a escassez. A suposta necessidade de tangibilidade é uma associação restante da extensão dos exemplos que estavam disponíveis antes da era da internet.

III – A Escassez em Números

Em nossos dias, estamos totalmente familiarizados com os bens digitais. Parte da aparente mágica do Bitcoin é que se trata de um dos primeiros bens digitais que também é escasso e competitivo em sua natureza. Isto contrasta com quase todos os demais bens digitais, os quais são fundamentalmente copiáveis e não-competitivos[11]. Isto significa que podem ser copiados sem causar efeitos nos "originais" dos quais as cópias são feitas, e as múltiplas cópias resultantes podem ser todas utilizadas simultaneamente, sem interferência mútua direta entre os usuários[12].

O bem digital não-competitivo (não escasso no sentido da teoria da propriedade) prototípico é um arquivo digital. Alguns têm tentado tornar arquivos digitais escassos acrescentando restrições legais ou técnicas (copyright e gestão de direitos digitais) no topo de sua natureza básica subjacente de copiabilidade. Tais tentativas de criar escassez após o fato são significativamente distintas de uma escassez incorporada como característica inseparável da natureza do próprio bem. A escassez do Bitcoin é um componente *do que significa ser um Bitcoin*, em oposição a alguma coisa que não é Bitcoin.

Mesmo a maior parte dos outros tipos de moedas digitais anteriores ao Bitcoin eram capazes de ser copiadas (aumentadas em quantidade) de acordo com as decisões ou políticas de um emissor central. Exemplos de moedas digitais existentes e geridas centralmente incluem o ouro de *World of Warcraft* (WoW) e os lançamentos contábeis de bancos centrais denominados em moedas correntes fiduciárias. Inflações no WoW podem ocorrer com base em diversas mudanças no balanço dos parâmetros do jogo. Já para as unidades dos bancos centrais, a oferta tanto de notas quanto dos agora dominantes lançamentos contábeis digitais arbitrários está na discricionariedade sempre mutável dos comitês de políticos nomeados e cuidadosamente selecionados. Essas fundações vacilantes são obviamente incapazes de sustentar uma moeda digital confiável para aplicações mais abrangentes na sociedade.

O Bitcoin superou, de maneira completamente nova, a eterna ameaça de que uma autoridade emissora central possa diluir o valor de uma unidade digital arbitrariamente. Não está dentro do escopo deste estudo descrever os diversos detalhes técnicos entrelaçados, as nuanças e as diferenciações por meio das quais este resultado foi atingido. O ponto chave, aqui, é que o Bitcoin estabelece sua trajetória de crescimento quantitativo *dentro da definição do que a unidade é e de como é criada*. Uma moeda corrente digital com mais que um potencial teórico de 21 milhões de unidades de Bitcoin (2.1 quatrilhões de Satoshis) não *seria* Bitcoin, por definição de protocolo. Qualquer um é livre para criar outras moedas correntes digitais como os Bitcoin e muitos têm feito isso. Mas nenhuma dessas outras unidades é, em qualquer sentido, Bitcoin. Elas são *litecoins*, *freicoins*, e assim por diante.

---

[11] Para mais fundamentação teórica sobre estes conceitos, ver: KINSELLA, Stephan. Against Intellectual Property. **Journal of Libertarian Studies**, Vol. 15, No. 2 (2001): 1-53; e TUCKER, Jeffrey A. & KINSELLA, Stephan. Goods, Scarce and Nonscarce. Mises Daily, 25 de agosto de 2010.

[12] Desenvolvi esta definição de bens não rivais e examinei diversos sentidos distintos da palavra escassez no meu artigo de 19 de março. Šurda nota que os endereços IP e os nomes de DNS também deveriam ser considerados como exemplos iniciais de bens digitais escassos. Mesmo que sejam somente cadeias de caracteres, em contexto, tentativas de utilização simultânea são incompatíveis, tornando-os rivais.

IV – Sobre as Preocupações Técnicas e o Realismo Comparativo

Mais ainda, alguns estão naturalmente preocupados com a ideia de que uma falha total da rede poderia deixar os Bitcoin repentinamente sem valor. É importante identificar isto desde o início como uma preocupação que deve ser levada em consideração com base amplamente técnica em vez de econômica. Isto é melhor abordado por meio de referências ao conhecimento e pelo debate dentro dos campos mais relevantes. Entre esses campos, está a criptografia, especialmente algoritmos de dispersão, e o uso e verificação de assinaturas criptográficas; desenho e segurança de redes *peer-to-peer*, os princípios da construção de registros contábeis criptográficos não falsificáveis descentralizados, e as dificuldades para superar o consenso distribuído, ou o Problema dos Generais Bizantinos (tendo tolerância bizantina a falhas), com ajuda do conceito de um servidor de *timestamp* distribuído.

Na consideração de cenários imaginados de falhas catastróficas do sistema, ou mesmo de dificuldades técnicas mais modestas, o conhecimento relevante de tais campos também pode ser proveitosamente suplementado nos lugares com métodos especificamente econômicos, tais como a análise econômica da rentabilidade da mineração e incentivos aos mineradores. Não deve ser necessário tornar-se um especialista nos detalhes técnicos internos de cada campo para fazer referência útil a eles. Deve bastar entender suficientemente bem a relevância desses campos para compreender *como* os vários detalhes técnicos participam do funcionamento do sistema e o desenvolvimento de avaliações bem informadas a respeito de sua confiabilidade.

Para o economista interessado na utilização econômica do Bitcoin, um ponto de partida suficiente deve ser observar que todas as pessoas que atualmente utilizam Bitcoin de fato o julgam, seja racionalmente ou de outro modo, como suficiente para servir aos propósitos para os quais o estão utilizando. Isto inclui as várias escalas temporais que têm em mente para esses propósitos, cada qual de acordo com sua própria série discreta de julgamentos na margem.

Assim como não esperamos que ninguém possa tornar-se um engenheiro aeronáutico antes de comprar uma passagem de avião, não é necessário obter nenhum status de cripto-mago da matemática para utilizar ou mesmo para analisar produtivamente o Bitcoin. É somente necessário que cada um, pelos seus próprios padrões, decida que o sistema é bom o suficiente para seu próprio conjunto particular de usos imaginados.

Sem aprofundar em quaisquer dessas matérias altamente técnicas[13], diversas considerações gerais podem ajudar a colocar tais preocupações a respeito de catástrofes sistêmicas em melhor perspectiva. No que é absolutamente o pior dos casos, mesmo se o Bitcoin falhasse devido a alguma fraqueza não antecipada, o conceito e a utilidade das criptomoedas em geral já foram demonstrados na prática. Uma atualização do Bitcoin ou mesmo uma substituição muitas vezes mais segura pode ser aplicada, sendo que os desenvolvedores já aprenderam bem a partir de quaisquer erros atualmente não imaginados e que poderiam ter, o que é improvável, levado a uma falha técnica grande e não antecipada.

---

[13] Um bom exemplo de tal conteúdo é como acessar as características relativas de segurança teórica dos diversos algoritmos de assinatura digital de curvas elípticas (ECDSA). Tais assuntos altamente técnicos não podem ser abordados a partir de reflexões vagas de sofá, mas devem ser abordados com base em conhecimento adequado dos campos apropriados de conhecimento especializado e avaliação de risco. Pode ser importante, por exemplo, que o Bitcoin utilize a curva menos comum sepc256*k*1 para seus pares de chaves, em oposição à curva sepc256*r*1, muito mais utilizada. Em geral, ver: SULLIVAN, Nick. A (Relatively Easy to Understand) Primer on Elliptic Curve Criptography. **Arstechnica** (24 de outubro de 2013). Em particular, ver: BUTERIN, Vitalik. Satoshi's Genius: Unexpected Ways in which Bitcoin Dodged some Cryptographic Bullets. **Bitcoin Magazine** (28 de outubro de 2013).

No caso muito mais provável, contudo, é necessário reconhecer que, enquanto protocolo de código aberto, descentralizado e totalmente voluntário, o Bitcoin é claramente capaz de ser adaptado e atualizado em uma base contínua. Seus colaboradores de programação, usuários, e mesmo os principais críticos trabalham todos, implacavelmente (em altos níveis de sofisticação técnica relevante), para imaginar, discutir, ponderar, antecipar e abordar constelações de ameaças ao sistema, maiores e menores, reais e teorizadas.

Parte da cultura de segurança de código aberto, que aqueles que se encontram fora dela raramente apreciam, é que programadores muito habilidosos, sejam eles de chapéu branco[14] ou preto, fazem das tentativas de quebrar sistemas "seguros" suas missões pessoais. Do ponto de vista definitivo da verdadeira força da rede funcional e da segurança de dados, esta ameaça constante e os testes de interação são considerados como características essenciais ao invés de falhas no desenvolvimento da segurança. O próprio fato de que um sistema seguro – em particular como o Bitcoin, com uma recompensa monetária direta na forma de moedas extraídas – na realidade permaneça seguro ao longo do tempo, ano após ano, já sugere, ao menos circunstancialmente, que está passando por uma bateria contínua de testes de segurança conduzidos por adversários motivados e habilidosos e também por apoiadores igualmente motivados e habilidosos.

Mais ainda, seguindo-se mesmo a um colapso catastrófico altamente hipotético, uma rede de Bitcoin revisada poderia ser potencialmente relançada a partir da cadeia de blocos existente, começando a partir da última constelação de propriedade verificada. Como Jay Smith costuma argumentar, o verdadeiro coração do Bitcoin é o próprio registro corrente do status de propriedade. A cadeia de blocos serve como um registro de títulos massivo global. Michael Goldstein colocou de forma comovente a importância social (fácil de ser subestimada) de tais registros de propriedade em um contexto mais amplo, citando o romance de Milan Kundera, *The Book of Laughter and Forgetting* (1978): "A luta do homem contra o poder é a luta da memória contra o esquecimento".

Os mecanismos técnicos e as operações de rede que circundam a cadeia de blocos são, cada qual, tecnologias específicas e aprimoráveis, ou métodos *para mudar os registros de uma forma aceitável e verificada*. Cada um desses elementos circundantes pode ser modificado, aperfeiçoado ou substituído indefinidamente no futuro (naturalmente, alguns elementos são mais fáceis de alterar; outros, os elementos mais centrais, são mais desafiadores). O Bitcoin é, neste sentido, não tanto um alvo fixo, mas sim um alvo que se move de forma altamente adaptativa.

Deve também ser lembrado que não existe perfeição neste mundo real. Existem apenas opções reais relativamente melhores e piores. Por exemplo, moedas políticas, longe de serem inseguras de forma meramente hipotética, na verdade diminuem constante e precipitadamente o poder de compra do usuário final. Fazem isso agora e têm feito isso em todos os casos conhecidos através da história[15]. O ouro e a prata, no que lhes diz respeito, também acabaram fracassando, na prática, como sistemas monetários. Alguma configuração da antiga e persistente inflação e da aliança de dívida dos bancos estatais tem sempre recorrido, eventualmente, ao confisco de tais substâncias valiosas de qualquer cofre significativo e do público em geral, em parte ou no todo, finalmente recorrendo-se à substituição total dos metais preciosos em circulação monetária por papéis fiduciários e lançamentos contábeis livremente multiplicáveis.

---

[14] N. do T.: Um hacker de chapéu branco é aquele que trabalha para o aperfeiçoamento dos sistemas de segurança.

[15] Dizer que uma moeda fiduciária corrente particular é "forte" é um eufemismo. Todas as moedas fiduciárias correntes perdem valor constantemente. Uma moeda fiduciária corrente "forte" refere-se a uma que está perdendo seu valor de forma relativamente mais lenta em comparação com outras.

Os próprios metais preciosos, embora apresentem certas vantagens relativas em relação às moedas políticas (assim como algumas fraquezas relativas), são, em princípio, ainda *mais* suscetíveis à fraqueza da variação da oferta agregada do que o Bitcoin, especialmente no longo prazo. No caso extremo, por exemplo, seriam suscetíveis à mineração de asteroides ricos em minérios e ao retorno à Terra desses metais extraídos e refinados[16]. Em contraste, dado que a trajetória de oferta do Bitcoin é pré-determinada como parte da definição do que ele *é*, então ele é impérvio a tais mudanças físicas na constelação de recursos minerais disponíveis e tecnologias de processamento.

Uma mistura de prós e contras do mundo real deve ser considerada na comparação das perspectivas de longo prazo para a utilização e estabilidade das diversas opções. As pessoas reais, enfrentando decisões marginais, deveriam idealmente equilibrar os prós e os contras de suas opções verdadeiramente disponíveis, em vez de assumirem uma perfeição eterna ou imaginária para algumas delas.

Para os entusiastas da "moeda dura" em particular, a história tradicional da superioridade passada e futura das moedas lastreadas em metais preciosos sobre as moedas fiduciárias deve ser revisada à luz da emergência recente de formas monetárias totalmente novas, que nunca antes foram antecipadas na antiga visão binária. Devemos aprender com o passado. Contudo, também tem sido observado, sabiamente, que "não há futuro no passado".

V – Mostre o Seu Desenvolvimento: Passos Lógicos Minuciosos

Um elemento de confusão constante por trás da dialética do "Bitcoin contra o teorema da regressão" é que este último cobre não somente uma, mas ao menos diversas questões teóricas distintas, cada uma das quais é bastante específica.

Uma delas é explicar o poder de compra do dinheiro em termos do nível de preços, sem recorrer a um argumento circular no qual os preços de hoje explicam o poder de compra hoje e vice-versa. A solução para isto foi introduzir um elemento temporal. O poder de compra do dinheiro "hoje" (indo para o futuro) baseia-se, em parte, nas avaliações dos usuários de seu poder de compra de "ontem" (percepções dos usuários da constelação passada de preços mais recente).

Contudo, esta resposta já levanta a próxima questão: o que acontece quando a "regressão" nos leva por todo o caminho de volta até uma época anterior àquela quando o que viria a se tornar um meio de troca tivesse ganhado o componente de valor de meio de troca? Este é o aspecto que se relaciona mais diretamente à confusão teórica sobre o Bitcoin. Ele explica a primeira emergência de qualquer tipo de meio de troca a partir de um estado prévio no qual ainda não havia nenhum.

Mises enfatizou, em *Ação Humana*[17], que o Teorema da Regressão não é uma generalização feita a partir de casos históricos, mas sim a identificação de uma necessidade teórica universal:

> Não faz afirmativas do tipo: isto aconteceu naquele momento e naquele lugar. O que afirma é: isto sempre acontece quando ocorrem determinadas condições [...] *nenhum bem pode ser empregado* como meio de troca se já não tiver um valor de troca em razão de seus outros empregos [...] As coisas *têm* de acontecer assim. Ninguém poderá conceber um caso hipotético no qual as coisas pudessem ocorrer de forma diferente[18].

Mises não disse "devem ser" ou "têm sido"; disse que "nenhum bem *pode* ser em-

[16] Já se sabe que a maior parte do ouro acessível no planeta veio de quedas de meteoritos na superfície. O ouro original da Terra muito provavelmente afundou nas profundezas do núcleo fundido com base em sua densidade relativa, bem no início do desenvolvimento geológico do planeta.

[17] MISES, Ludwig von. **Ação Humana: Um Tratado de Economia**. São Paulo: Instituto Ludwig von Mises, 2010.

[18] Idem. *Ibidem*, p. 478. A ênfase é minha.

pregado", uma afirmação de impossibilidade lógica. Este aspecto "de origens" do Teorema da Regressão (em oposição aos aspectos do poder de compra e da moeda dominante) estabelece que nenhum bem pode ser valorizado para utilização *como* meio de troca *antes de* assumir tal uso pela primeira vez. Esta é uma afirmação de necessidade, de definição.

Mais ainda, para assumir um componente de valor enquanto meio de troca, um bem precisa primeiramente ser valorizado com base em algum *outro* componente de valor aos olhos de alguns dos atores relevantes. Este outro componente de valor deve, obviamente, ter sido distinguível de qualquer valor de meio de troca subsequente. Isto ocorre porque tais componentes posteriores *não podem já existir antes de seu primeiro aparecimento*. Novamente, isto segue-se por definição do desafio de evitar a circularidade lógica[19].

Quando pessoas jovens fazem um curso de matemática, o professor requer que os estudantes "mostrem seus desenvolvimentos", isto é, que demonstrem cada um dos estágios no processo de chegar a uma conclusão. Isto pode ser tedioso e requer muitos pequenos passos. O Teorema da Regressão, em seu contexto, proporcionou alguns desses passos lógicos do tipo "mostre seu desenvolvimento".

Recorde que elementos do Teorema da Regressão foram depurados no contexto dos debates entre explicações concorrentes sobre as origens da moeda. Um lado afirmava que a moeda foi uma invenção do Estado e que tem sido decretada pelos governantes em benefício da sociedade. O seu valor foi determinado e regulado por várias ações estatais. Outro lado defendia que a moeda funcionava como um bem em si mesmo, emergiu dos processos do mercado, e somente então foi adotada e manipulada de várias formas pelos governantes ao longo do tempo.

O lado da teoria estatal do dinheiro[20], em grande parte alemã, encontrou algumas fraquezas técnicas nos argumentos do lado da evolução do mercado, os quais, sendo associados com a Universidade de Viena e a partir daí para o sul, foram rotulados como (aqueles caipiras) "austríacos". Os críticos têm exigido, essencialmente, que o lado da evolução do mercado "mostre o seu desenvolvimento" com relação a cada passo de sua teoria da emergência do dinheiro no mercado (assumindo, ao mesmo tempo, que não teriam realmente sucesso em fazê-lo).

O aspecto de origens do Teorema da Regressão cobre um período estreito de transição que vai desde quando um bem que não era utilizado como meio de troca passa a ser utilizado dessa maneira pela primeira vez, e então este papel ganha tração social gradualmente. Somente se exige que este aspecto de origens explique a primeira emergência de um *meio de troca* (um meio de pagamento). Também não se requer que explique a próxima fase da emergência de uma moeda (uma unidade dominante de precificação e contabilidade) dentre um campo de meios de troca concorrentes.

Este último é um processo de efeito de rede competitivo e orientado, no qual uma das opções no mercado sobe para o topo em um dado contexto. Uma das características cruciais de tais bens é o que Menger chamou de grau de vendabilidade, um indicador de quanto é a estreiteza da diferença entre o preço ao qual pode-se imediatamente comprá-lo e o preço ao qual pode-se imediatamente vendê-lo[21].

Ao explicar a emergência da moeda *a partir de* um campo de meios de troca concorrentes, a sequência caminha para a frente no tempo, o que é o oposto de "regressar" para trás. Analiticamente, a regressão para

---

[19] A próxima seção desenvolve um exemplo de ação-situação para clarificar o que é exigido para evitar essa circularidade lógica, e por que.

[20] *The State Theory of Money*, de G. F. Knapp (1842-1926), apareceu em alemão em 1895 e os cartalistas [N. do T.: adeptos da Teoria Cartalista da Moeda] da época moderna avançam elementos desta tradição.

[21] MENGER. **On the Origins of Money**, p. 24-25, n. 2.

trás, conforme ilustrado por uma metáfora evolutiva, tenderá a perder todas as demais ramificações na árvore. Encontrará somente uma cadeia direta de ancestrais remontando a partir do ponto inicial da regressão. Ir para a frente no tempo, contudo, pode revelar outras ramificações (todos os meios de troca concorrentes), incluindo tanto os becos sem saída quanto os novos começos. Um padrão que se repete na evolução de longo prazo da vida é a extinção das antigas espécies que já foram dominantes e a emergência de novas espécies dominantes, em geral com tamanhos, velocidades, habitats e estratégias radicalmente diferentes em comparação com os reis da selva anteriores.

É por isto que rodar a lógica da regressão somente para trás no tempo e não também para a frente poderia levar a supersimplificações. As únicas opções vistas ao ir para trás a partir da moeda corrente serão logicamente os ancestrais diretos do que quer que tenha terminado por se tornar a moeda corrente naquele ponto no tempo. Perderá qualquer coisa que não pertença a essa linhagem em particular. Rodar o processo para a frente outra vez, a partir de cada meio de troca iniciado, pode revelar competidores em diferentes linhas, muitos dos quais podem ter sido tentados, alguns dos quais tiveram sucesso em algum grau, outros dos quais podem ter ganhado terreno, e somente um dos quais é a unidade dominante de precificação e contabilidade em uma área de mercado relevante – até o tempo presente.

VI – A Presença de Constelações de Preços Pré-Existentes

É simples para as pessoas, hoje, valorizarem o poder de compra relativo do Bitcoin referenciando seu valor de troca contra a moeda local por meio da utilização de uma taxa de câmbio de mercado em tempo real disponível para qualquer dispositivo conectado à internet. O Bitcoin, hoje, funciona como um meio de troca. Tenho definido isto como algo que pode ser ofertado para pagar preços. Preços são denominados em "moeda", o que concebo como a unidade dominante de precificação, contabilidade e cálculo econômico em um dado contexto. Não existe uma razão fundamental para a razão por que o Bitcoin não poderia também, algum dia, assumir tais papéis mais abrangentes, caso ele venha a se tornar relativamente mais estável, mais global, ou de outra maneira mais adequado para isto do que o seu competidor ativo mais próximo. Ele já preenche a função de denominação de preços dentro de certos contextos limitados no interior da economia do Bitcoin.

Em contraste com esta situação, algumas apresentações do Teorema da Regressão tratam a evolução de um meio de troca em um contexto no qual nenhuma unidade de precificação prévia já existia. Isto significa que nenhuma constelação de preços relativos estava em uso na sociedade, desde o início[22]. O caso da evolução original do Bitcoin introduz a necessidade de algumas qualificações relativas a tais explicações, dado que ele emergiu como um novo meio de troca em um contexto no qual já existia uma gama avançada de preços relativos de moedas para bens e serviços.

Os desafios evolutivos do Bitcoin foram, portanto, facilitados consideravelmente em relação a uma situação na qual não existia nenhum conhecimento dos preços relativos no mercado. Neste caso contrafactual, uma gama inteiramente nova de preços de mercado *diretamente relativos ao Bitcoin* teria que ter se desenvolvido através de processos de ten-

[22] Rothbard utiliza um hipotético para contrastar uma situação na qual preços relativos da moeda existem com uma na qual eles repentinamente deixam de estar disponíveis: "*Dado que a utilidade marginal da moeda mercadoria depende de preços da moeda previamente existentes, uma eliminação dos mercados existentes e do conhecimento dos preços da moeda tornaria impossível o restabelecimento direto de uma economia monetária. A economia seria destruída e jogada de volta para um estado altamente primitivo de escambos, após o que uma economia monetária poderia somente ser restabelecida vagarosamente, como tinha sido antes*" (ROTHBARD. **Man, Economy, and State, with Power and Market**, p. 271-272).

tativa e erro de trocas diretas de Bitcoin por bacon, Bitcoin por ovos e Bitcoin por cavalos, enquanto também tentasse referenciar taxas de câmbio não-mediadas entre ovos e bacon, entre bacon e cavalos e assim por diante – todas elas, até que uma constelação razoável de preços de mercado relativos começasse a tomar forma, novamente denominada na nova unidade.

No caso factual, entretanto, o Bitcoin somente teve que saltar um obstáculo muito mais simples (apesar de ainda ser bastante desafiador à sua própria maneira). Precisou somente desenvolver um valor de troca no mercado contra a moeda existente em cada local de troca. Poderia, então, "inicializar" seu valor relativo de meio de troca sobre toda a constelação de preços de mercado, dado que esses já estavam expressos em moedas em cada região geográfica[23].

Até o presente, a maior parte das coisas compradas e vendidas com Bitcoin são precificadas em moedas locais. Uma soma equivalente de Bitcoin baseada na taxa de câmbio corrente é, então, utilizada para pagar verdadeiramente esses preços[24]. Insistir na evolução independente de uma nova constelação de preços relativos diretamente em termos de Bitcoin, entretanto, terá sido absurdo e desnecessário. Não havia necessidade prática de reinventar esse conjunto particular de rodas nos lugares relevantes e no período 2009-2010.

Se algo como o Bitcoin *poderia* possivelmente emergir diretamente de um estado de puro escambo é algo tão hipotético quanto entrar no domínio não somente da ficção científica, mas da fantasia. Isto ocorre porque um estado de puro escambo somente poderia sustentar uma economia tão primitiva e próxima à produção direta através da caça, coleta e talvez de algum cultivo limitado, que o *output* elétrico necessário, a infraestrutura de internet, o desenvolvimento de tecnologias de chips de computador, as telas e assim por diante não poderiam também existir ou persistir no contexto postulado, tornando discutível esse cenário hipotético.

Enquanto os princípios do Teorema da Regressão são aplicáveis a quaisquer instâncias do universal, o contexto técnico requerido aqui também inclui um estágio de complexa evolução social e técnica construída em uma divisão de trabalho abrangente e em outros estágios prévios. Tais altas tecnologias obviamente não poderiam continuar existindo se suas fundamentações fossem perdidas[25]. Um estado de escambo puro poderia sustentar somente talvez uns poucos pontos percentuais da população humana corrente. No máximo. Isto significa que a perda da conveniência de uma moeda de internet estaria entre as menores dificuldades a serem encontradas em um cenário desse tipo.

---

[23] Diferenças de preços perceptíveis permanecem entre as maiores negociações de Bitcoin, com a MtGox como o principal caso fora da curva devido aos seus desafios específicos na transferência de dólares americanos para clientes localizados nos Estados Unidos. A movimentação do próprio Bitcoin é simples e eficiente em uma base global, mas a arbitragem de intercâmbio eficaz ainda é bastante limitada devido aos lados não-Bitcoin destas negociações. Esta é a maior dificuldade, custo e prazo necessários para transferir moedas correntes fiduciárias dentro do sistema bancário internacional convencional. Para ajudar a lidar com isto, o BitPay e o Coindesk desenvolvem preços de referência do Bitcoin que são construídos de maneiras ligeiramente diferentes. Elas combinam dados em tempo real de muitos dos principais câmbios. O BitPay reúne uma carteira de demandas consolidada a partir de vários câmbios, enquanto o Coindesk constrói sobre o índice. Ambos atualmente excluem o *outlier* de preço McGox.

[24] Ver, neste contexto, também meu artigo de 14 de setembro de 2013.

[25] Matt Ridley detalha os vários séculos de um longo declínio tecnológico e do know-how na ilha da Tasmânia, depois que a pequena população foi excluída de uma rede de comércio anteriormente mais ampla. Ver: RIDLEY, Matt. **The Rational Optimist: How Prosperity Evolves**. New York: Harper Perennial, 2011.

VII – De Volta ao Bife, Ovos e Farinha

Um cenário hipotético razoavelmente primitivo pode, contudo, ajudar a trazer o componente "de origens" do Teorema da Regressão de volta da *abstratosfera*, onde as confusões podem persistir mais facilmente, para um domínio muito mais próximo da experiência concreta. Não é suficiente apenas mostrar que o Bitcoin é explicável em termos de uma teoria econômica. Também deve ser esclarecido que o Teorema da Regressão não é ameaçado por este desenvolvimento empírico.

Começando com um cenário hipotético de puro escambo, desejo trocar bife por alguma farinha. Entretanto, o moleiro é um ovo-vegetariano. A dupla coincidência de desejos necessária para que ocorra uma troca está ausente.

Preciso encontrar outra *coisa* para trocar com o moleiro se desejo comprar a sua farinha. Qualquer coisa que eu obtenha para facilitar esta troca já funcionará tecnicamente como um "meio de troca" dentro do contexto limitado da minha transação desejada, independente do que todos os demais estiverem fazendo na minha comunidade hipotética. Um meio de troca, neste sentido o mais simples, é um bem que facilita uma troca que não está ocorrendo diretamente entre duas partes devido à ausência da correspondência de uma coincidência mútua de desejos.

Adotar um meio de troca a partir do zero começa com um único ato criativo de troca, em dois passos, entre três partes. Somente uma vez que ele tiver começado a ser colocado em prática, poderá possivelmente começar a ser copiado e difundido. A própria prática da troca indireta é uma invenção e uma descoberta. Processos subsequentes podem separar *quais* tipos de bens tenderão a ser mais ou menos úteis nesta função social em um dado contexto. Descobrir como levar a cabo trocas indiretas com mais frequência e efetivamente, e com o quê, é uma camada de experimentação distinguível da ideia geral de engajar-se em trocas indiretas[26].

Neste caso, observo que, sendo um *ovo*-*-vegetariano*, o moleiro come ovos. Vou até Friedrich, o criador de galinhas, e troco um bife por alguns ovos. Então, volto até o moleiro e troco os ovos por farinha. O que se requer, aqui, é que o moleiro aceite os ovos. Se ele não aceitar, a minha tentativa de troca indireta fracassa. Se ela tiver sucesso, os ovos já terão funcionado como um meio de troca dentro dessa transação.

O moleiro precisa valorizar os ovos *enquanto ovos* para que isto conte como *primeira emergência* de uma troca indireta de valor por ovos. Obtenho ovos pelo seu uso como meio de troca para minha transação. Ao fazer isso, *eu* os valorizo para este propósito. Se o moleiro não aceitar os ovos, contudo, minha valoração dos ovos como meio de troca é defeituosa, trata-se de uma perda empresarial da minha parte. Fico somente encalhado com alguns ovos adicionais. Este empenho depende do meu sucesso prático para entender o que meus parceiros comerciais em potencial irão ou não aceitar nas trocas.

A única forma para que este componente de valor dos ovos *como* meio de troca possa primeiramente vir a ser é se alguém mais os aceitar como ovos *porque* querem *ovos*, e *não* porque já querem trocar novamente os ovos com alguém mais. Um processo circular de autorreforço da demanda social pode funcionar somente depois de que a prática de troca indireta usando ovos tiver começado a ser colocada em movimento em um dado contexto social. Somente então as expectativas deste componente adicionado de ampliação da vendabilidade podem começar a ser construídas entre os atores relevantes.

---

[26] Isto também implica que, uma vez que a ideia geral da troca indireta se torna familiar pela primeira vez em uma sociedade, novas possibilidades para a questão "com o quê?" podem ser reconhecidas mais rapidamente do que no caso em que a ideia geral da troca indireta é inteiramente desconhecida, como ocorre em um verdadeiro contexto de escambo puro.

Depois que o novo componente de valor do meio de troca emerge e persiste em um dado contexto, os componentes de valor dos que não são meios de troca poderiam então, teoricamente, desvanecer por completo[27].

Contudo, ovos em particular não tenderão a ir muito longe neste papel. Eles estragam depois de um tempo. Podemos usar algumas datas de validade, mas isto cria uma heterogeneidade fatal entre as unidades, devido à depreciação. E ovos são razoavelmente pesados e difíceis de transportar para longe sem quebrar. Itens muito mais duráveis têm se tornado, repetidamente, mais bem-sucedidos neste papel. ∽

[27] Murray Rothbard observa este ponto, por exemplo, em sua discussão do teorema da regressão (ROTHBARD. **Man, Economy, and State, with Power and Market**, p. 275).