ANÁLISE MONETÁRIA DO *BITCOIN*

Thiago Augusto Bueno[1],
Julio Cesar Aguiar[2]

RESUMO

O propósito do presente artigo é analisar se o chamado *bitcoin* pode ser definido como moeda. Para tanto, inicialmente é analisada a tecnologia do *bitcoin*, especialmente sua estruturação a partir do desenvolvimento de criptografia por *blockchain*. São tratadas as características principais dessa estrutura tecnológica que permitiu sua rápida difusão, com suficiente confiança e segurança nas transações, a baixo custo, e sem a necessidade da intervenção de terceiros, seja o Estado ou o sistema bancário. Posteriormente, o estudo se volta ao conceito de moeda, a partir do ponto de vista econômico, sob o enfoque das principais teorias desenvolvidas. Nesse ponto, é feita uma análise especial a partir dos estudos da escola austríaca de economia, especialmente por Luwig Von Mises e seu teorema da regressão, desenvolvido para explicar a origem da moeda. Estabelecidos esses parâmetros, é feita a análise dos atributos do *bitcoin,* tendo se concluído que sua volatilidade e falta de liquidez impedem, por ora, sua caracterização como moeda. De se registrar que o presente artigo serve como ponto de partida para um futuro trabalho acerca dos efeitos jurídicos do *bitcoin*, em especial na seara criminal. Para tanto, é preciso definir a natureza do *bitcoin*.

PALAVRAS-CHAVE: *Blockchain.* Moeda. Dinheiro. Teorema de Mises. *Bitcoin*.

MONETARY ANALYSIS OF THE BITCOIN

ABSTRACT

The purpouse of this paper is analyse if the called bitcoin can be defined as currency.Therefore, first is analysed the bitcoin tecnology, specially its structuring from the encryption development by blockchain. The main characteristics of this technological structure are studied, wich allowed its fast diffusion, with the sufficient confidence and security in the transactions, at low cost, without the intervention of third parties, be it the State or the banking system.Later, the study turns to the concept of money, from the economic point of view, under the focus of the main theories developed. At this point, a special analysis is made from the studies of the Austrian school of economics, especially by Luwig von Mises and his regression theorem, developed to explain the origin of the currency. Once these parameters have been established, bitcoin attributes are analyzed, having this paper concluded that its volatility and lack of liquidity prevent, for the moment, its characterization as currency. It should be noted that this paper serves as a starting point for future work on the legal effects of bitcoin, in particular in criminal law. However, it is necessary to define the nature of bitcoin.

[1] Procurador da República, Especialização em Curso em direito aplicado ao Ministério Público Federal pela Escola Superior do Ministério Público da União (2015).
[2] Bacharel em Direito e mestre em Filosofia pela Universidade Federal de Goiás. Doutor em Direito pela Universidade Federal de Santa Catarina. PhD in Law pela University of Aberdeen, UK. Professor da Escola de Políticas Públicas e Governo da Fundação Getúlio Vargas em Brasília.

KEYWORDS: Blockchain. Currency. Money. Mises theorem. Bitcoin.

INTRODUÇÃO

A tecnologia da *internet*, utilizada para diminuir distâncias, compartilhar conhecimentos, integrar pessoas e comunidades é a mesma empregada para a prática de ilícitos penais. Esse cenário do planeta conectado, onde informações são transmitidas em questão de segundos entre todas as partes do globo, aí se incluindo transações comerciais das mais diversas origens e com os mais diferentes objetos, foi determinante para o desenvolvimento de tecnologias que permitissem a realização de transações comerciais *on line* com garantia de segurança e privacidade aos usuários envolvidos, as chamadas *cybermoedas*.

O bitcoin é a tecnologia pioneira e mais difundida de *cybermoeda*. Muito da fama mundial do *bitcoin* é associada à prática de crimes na internet, especialmente na Deep Web, e se deve a casos como o do site *Silk Road*, que intermediava a negociação de armas e drogas, utilizando o *bitcoin* como sistema de pagamento.[3] No entanto, deve ser feita a necessária dissociação entre *bitcoin* e crimes cibernéticos, uma vez que a *cybermoeda* não é ilícita por si só, tendo sido, em verdade, utilizada como meio para troca indireta de valores entre os envolvidos nas ilicitudes praticadas via web. Manter esse raciocínio de ilicitude do uso de *bitcoins* como meio de transferência de valores seria o mesmo que tratar como integrantes de organização criminosa os dirigentes de um banco de onde tivesse sido sacado dinheiro utilizado para comprar uma porção de drogas. Fica claro que não faz sentido atrelar o uso de *bitcoins* ao cometimento de atividades ilícitas. Ocorre que, de fato, a segurança e a privacidade com que as operações de transferência de valores pela rede *bitcoin* são realizadas, através da aplicação de técnicas avançadas de criptografia (*blockchain*), são os maiores atrativos para a utilização das *cryptomoedas*.

Para melhor estudo desse cenário, no tópico 2 é feita análise da tecnologia do bitcoin, desenvolvida a partir de técnicas de criptografia por meio de blockchain. São analisadas as características conjugadas que permitiram a disseminação da utilização do bitcoin pela web.

No tópico 3 é feito o estudo dos predicados da moeda, seus atributos que fizeram com que no decorrer da história da humanidade fosse desenvolvido esse instrumento de troca de bens que uniu diferentes povos e foi determinante para a expansão humana no planeta. Após, toma-se por objeto a moeda em seu sentido econômico, especialmente à luz dos ensinamentos da escola austríaca da economia e o teorema da regressão de Ludwig Von Mises.

1. A TECNOLOGIA DO BITCOIN

O *bitcoin* é uma tecnologia de livro-caixa digital cujo desenvolvedor até hoje é uma incógnita. O certo é que em 2008 foi lançada em uma lista de discussões de programadores uma pesquisa assinada por Satoshi Nakamoto, cuja real existência não se

3 ——— WIKIPÉDIA. *Silk Road.* Disponível em: <https://pt.wikipedia.org/wiki/Silk_Road>. Acesso em: 3 abr. 2018.

tem confirmada até hoje (há muitas especulações acerca de sua identidade, inclusive, de que, na verdade, tenha se tratado de um trabalho coletivo). A pesquisa denominada *Bitcoin: A Peer-to-Peer Electronic Cash System*[4] trazia ao mundo mais uma tentativa de desenvolvimento de tecnologia para transmissão de valores dissociada dos governos e sistemas bancários (TAPSCOTT; TAPSCOTT, 2016).

As transações envolvendo *bitcoins* se utilizam de técnica de criptografia por *blockchain.* Criptografia, em apertada síntese, é o estudo de meios para transmissão de informações a fim de que apenas o emissor e o destinatário tenham acesso, de modo a ser preservado seu conteúdo da indevida intromissão de terceiros. O que se busca com o emprego de criptografia é a transmissão de uma mensagem de forma segura, garantindo-se que somente seu destinatário terá acesso a seu conteúdo. Pelo que, ainda que seja extraviado o instrumento de transmissão da informação (escrito, desenho, fotografia etc), seu conteúdo não poderá ser acessado por outrem que não o destinatário. Existem técnicas de criptografia que remontam à Antiguidade, tendo seu desenvolvimento chegado à era digital e culminado com o desenvolvimento da tecnologia *blockchain*.

Em uma análise mais simples, os sistemas que operam como *blockchain* se utilizam de programas de computador desenvolvidos para a descentralização de dados, compartilhando os registros de forma difusa entre os integrantes do programa (cada um dos usuários), de modo que cada operação promovida por um desses "nós" (cada um dos usuários) acresça um novo bloco ao registro geral, que pode ser consultado por cada um dos usuários, garantindo segurança e confiança a cada uma das operações e ao sistema todo (HAYNES; O'BROLCHÁIN; REIJERS, 2016). É essa mesma tecnologia de criptografia por *blockchain* a utilizada pelo *bitcoin*, com a especificidade que se trata de um sistema voltado para o registro de operações de entrada e saída de valores, um verdadeiro livro-caixa.

Utilizando-se desse sistema difuso, espalhado em tantos computadores quantos seus usuários aquiesçam para sua manutenção (essa atividade de manutenção do sistema em cada máquina é conhecida como mineração e será estudada adiante), o *bitcoin* se utiliza de cada um desses computadores como um nó de sua rede, que tem a função de realizar, registrar e conferir a autenticidade das operações, conferindo legitimidade e segurança ao programa, sem a necessidade da intervenção de um terceiro, seja ele o Estado ou uma instituição bancária (BLUNDELL-WIGNALL, 2014).

As operações realizadas através do *bitcoin* exigem a utilização de duas chaves, uma privada e outra pública. A chave privada funciona como a assinatura de cada usuário. Os *bitcoins* são armazenados em "carteiras digitais" (aplicações que permitem o registro das operações de débito e crédito de cada usuário), cujo acesso é restrito a seu detentor (CASEY; VIGNA, 2015). É através da chave privada que se autoriza a transferência dos valores em *bitcoin* de uma carteira para outra, sendo disposta somente a seu titular.

Já a chave pública serve para conferir legitimidade às transações, permitindo que sejam auditadas por qualquer usuário do sistema. Em todas as operações são registrados os números das carteiras envolvidas e é gerada uma chave pública que pode ser

4 NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2009. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: maio 2018. Versão em português Disponível em: <http://www.usandobitcoin.com.br/files/BitcoinPaper_Portugues.pdf>.

consultada (toda operação de *bitcoin* gera uma chave pública diferente). A consulta a essa chave pública informa os números das carteiras que participaram da operação e o valor transferido.

Assim, a técnica criptográfica de *blockchain* aplicada ao *bitcoin* define quais as operações são válidas (ABRAMOWICZ, 2016), de modo a afastar fraudes, como a duplicidade de transações, em que haveria uma simulação do envio de valores, de modo que o mesmo montante do ativo deixaria por mais de uma vez a mesma carteira virtual. Essa possibilidade de fraude, também conhecida como problema do gasto duplo (*double spending*) por muito tempo atormentou os desenvolvedores de tecnologia de registro de operações, tendo sido solucionado somente com a adoção de criptografia pela técnica de *blockchain* (DE FILLIPI; WRIGHT, 2018). O emprego de *blockchain* com chaves públicas permite a qualquer usuário do sistema certificar que a unidade de *bitcoin* deixou efetivamente a carteira de um usuário e ingressou na de outro, impedindo operações simuladas.

De se destacar que as carteiras na rede *bitcoin* são identificadas apenas por números e não pelo nome do usuário, o que assegura o sigilo da identidade dos sujeitos envolvidos nas operações. Esse foi um dos pontos determinantes para a utilização do *bitcoin* como meio de remessa de valores envolvendo aquisição de produtos e serviços ilícitos, como no caso do já mencionado site Silk Road. O anonimato é um dos pontos chave dessa tecnologia. Essa característica tem íntima relação com o movimento *cyberpunk*, que pregava o desenvolvimento de tecnologias na internet que permitissem o anonimato e a livre manifestação dos usuários, avessos a qualquer intervenção estatal em sentido contrário (*BANKING ON BITCOIN*, 2016).

Além do anonimato, outro ponto fundamental para compreensão do funcionamento do sistema *bitcoin* é a natureza difusa do registro de seus dados. No *bitcoin* não há a concentração das informações referentes às operações em um único ou em poucos servidores centrais. Em verdade, cada um dos "nós" do sistema, ou seja, todos os computadores nos quais está instalado o programa funciona como ponto de registro de todas as operações. Há uma rede de computadores ligados ao mesmo sistema, espalhados pelo globo, dedicados ao registro das operações.

Uma das vantagens desse sistema difuso é a de impedir, como já ocorreu em outras oportunidades com instituições bancárias, a ocorrência de *cyberataques* a servidores que centralizam dados[5]. Não há o risco de se perderam os registros das operações realizadas em decorrência de um ataque virtual coordenado porque as informações não estão registradas em um único ou em alguns poucos servidores, sendo impossível atingir-se, de forma simultânea, todos os computadores, em escala global, que hospedam o programa.

Outra situação evitada pelo caráter difuso do sistema é a da falência do sistema em decorrência de cessação do acesso à *internet* determinada por governos locais. Utilizando-se de múltiplas plataformas espalhadas pelo planeta, eventual cerceamento de acesso dos computadores que mantêm o programa não obstaria a continuidade do

5 FINANCIAL TIMES. "Seven UK banks targeted by co-ordinated cyber attack". *Financial Times*. Londres, 25.04.2018. Disponível em: <https://www.ft.com/content/2e582594-48ab-11e8-8ee8-cae73aab7ccb>. Acesso em 9 jun. 2018.

processamento das operações, já que outras máquinas dedicadas aos registros continuariam operando.

Os registros das transações feitas pelos "nós" da rede, que geram as chaves públicas, são complexos cálculos matemáticos que exigem grande consumo de energia. Sem essas máquinas dedicadas a tanto, o sistema utilizado pelo *bitcoin* seria impraticável, justamente porque está fundado em uma rede difusa de computadores trabalhando para sua manutenção. Como estimular a continuidade dos computadores nessa rede? Essa pergunta foi respondida por Satoshi Nakamoto através do reforço da "mineração".

A "mineração" nada mais é do que uma recompensa atribuída pelo próprio sistema do *bitcoin* aos usuários que dedicam seus computadores para a manutenção da rede, permitindo que suas máquinas resolvam os complexos cálculos matemáticos que registram as operações de crédito e débito entre as carteiras virtuais. Ao conceder a utilização de seu computador para tanto, a cada operação que a máquina realiza é creditada uma fração de *bitcoin* à correspondente carteira. Observe-se que, tal como organizado, o sistema do *bitcoin* é autosustentável, já que foi disposto de modo que há estímulo para a manutenção de sua difusão, ponto fundamental para a consecução de seu fim.

No início das atividades do *bitcoin* era possível "minerar" utilizando um computador residencial. No entanto, atualmente, dadas as complexidades cada vez maiores dos cálculos exigidos para a confirmação das operações, decorrente do elevado número de transações diárias, para que haja sucesso na "mineração" é necessária a dedicação de máquinas incrivelmente potentes e especialmente preparadas para esse fim, de modo que ostentem grande *hashpower*. Além disso, outro desafio é o custo de manutenção desses equipamentos em razão do demasiado consumo de eletricidade envolvido no processo que funciona ininterruptamente, 24 horas por dia. Por esses motivos, hoje, há verdadeiras "fazendas de computadores" montadas para este exclusivo propósito, especialmente em localidades de temperatura mais amena e custo de energia elétrica mais barata, em países como China, Suécia e Islândia e áreas do Estado de Washington, nos Estados Unidos (CASEY; VIGNA, 2015).

Essa característica do *bitcoin* de remunerar os computadores que resolvem os cálculos decorrentes da técnica *blockchain* é fruto da adoção do protocolo de criptografia conhecido como Prova de Trabalho (*Proof-of-Work – PoW)*. Esse protocolo foi desenvolvido de modo que a participação de um usuário exige que ele comprove que tenha realizado alguma tarefa, como a solução dos problemas matemáticos, de modo que, somente após, possa criar um novo bloco e ser remunerado por isso (POPOV, 2016). Assim, há uma proteção do próprio sistema contra ataques de terceiros estranhos, além da indeterminação do próximo usuário responsável pela solução dos problemas matemáticos do *blockchain*.

Além da *mineração*, outro modo de se adquirir *bitcoin* é através da compra por meio das corretoras de investimento digital, utilizando-se, para tanto, de cartão de crédito ou diretamente através de outros investidores. Dessa maneira o usuário escolhe quanto quer investir em sua carteira digital, habilitando-se, a partir de então, a realizar transações na rede *bitcoin*.

De se registrar, ainda, que o *bitcoin* foi desenvolvido de modo que há um limite na sua emissão. A atividade de mineração, que gera o ingresso de unidades de *bitcoin* no sistema, tem um limite máximo de alcance, de modo que, tal como os minerais físicos, seu estoque é limitado. Tal como desenvolvido, o número máximo de *bitcoins* a serem minerados, ou seja, gerados pelo sistema mediante a remuneração dos computadores que dão sustentação à rede, é de 21 milhões. Disso decorre que tal como o ouro, o *bitcoin* também é um recurso não renovável.

Segundo a programação do *bitcoin*, suas 21 milhões de unidades serão geradas até o ano de 2140. No entanto, ocorre que em janeiro de 2018 já se registrou a emissão de 80% dos *bitcoins*. Disso decorre que a atividade de mineração ficará cada vez mais difícil e cara.

Nesse ponto é importante assinalar que ao contrário das moedas nacionais, fracionadas em unidades de cem, o *bitcoin* é dividido em frações de 100 milhões. Assim, a menor unidade de *bitcoin* é a de 0,00000001, conhecida como satoshi, em homenagem ao criador da cryptomoeda. Isso se deve por conta do alto valor da unidade de *bitcoin*[6].

A constatação da finitude da emissão de *bitcoins* tem levado a questionamentos acerca da própria manutenção do sistema. A preocupação repousa no fato de que é a remuneração dos usuários que dedicam seus equipamentos para solução das equações que sustentam o sistema, através da emissão de fração de *bitcoins* (mineração), o estímulo para funcionamento dessa grande engrenagem. Sem essa contraprestação, ou seja, com o fim da emissão de bitcoins pela mineração, essa rede se sustentaria? A resposta a essa indagação está nas taxas de transação (*transaction fees*), constantes da programação de Satoshi, que servem para continuar remunerando os "nós" do sistema (CASEY; VIGNA, 2015). Comparativamente aos valores das tarifas praticadas pelas instituições bancárias, essa taxa para autenticação das operações é pequena, normalmente fixada em 0,0005 *bitcoin*, ou, em muitas vezes, nem é cobrada (TAYLOR, 2013). Assim, ainda que não existam mais *bitcoins* para serem incorporados ao sistema, cada uma das operações de registro entre os usuários é taxada para que permaneça o estímulo individual à manutenção do interesse coletivo.

Por fim, outra característica importantíssima do *bitcoin* é sua independência em relação à atuação de um terceiro, seja esse terceiro um governo ou uma instituição bancária.

No sistema bancário os correntistas precisam da atuação do banco para enviarem valores de uma conta para outra, pagarem contas ou quaisquer outras operações. Tudo isso é feito mediante o pagamento de taxas e outros valores. O mesmo ocorre nas operações realizadas por meio de cartões de crédito, onde há a cobrança de valores pelas operadoras em razão da utilização dos serviços de crédito e débito dispostos, bem como nas remessas de dinheiro de um país para outro envolvendo instituições financeiras com representação internacional. Assim, um trabalhador que queira enviar dinheiro para sua família em outro país precisará contratar os serviços remunerados de uma instituição financeira.

6 Em 09.06.2018 1 bitcoin era cotado no valor de R$ 29.935,00.

Esse cenário muda completamente com a adoção do sistema *bitcoin*. Nesse caso, as transações são realizadas com a tecnologia *peer to peer* (ponto a ponto), ou seja, diretamente entre as partes envolvidas, sem a necessidade da atuação de um terceiro intermediando a operação. É feito o registro de débito de determinado valor da carteira virtual da qual se origina o montante e, de outra parte, a anotação de crédito na carteira virtual destinatária, de forma direta, sem a intervenção de qualquer entidade privada ou governamental.

Essa engenhosidade decorre, mais uma vez, de ideais do movimento *cyberpunk*, que pregava a liberdade de manifestação e anonimato na internet, afastada a intervenção do Estado. No caso do *bitcoin* se logrou desenvolver um sistema de transmissão de valores com funcionamento totalmente alheio à atuação estatal.

Além disso, não se olvide que o *bitcoin* foi lançado em 2008, época na qual o mercado financeiro global enfrentava a crise econômica decorrente da falência do banco americano Lehman Brothers e de várias outras instituições financeiras que tiveram que se socorrer de capital estatal a partir da intervenção de diversos governos de países afetados pela crise (TAPSCOTT; TAPSCOTT, 2016).

O *bitcoin* se mostrava como uma alternativa ao sistema bancário que claramente não era confiável. Além disso, a ausência de um terceiro nas operações permitia a redução de custos, preservando os valores envolvidos nas transações.

Dessa forma, em apertada síntese, o *bitcoin* é um sistema de livro-caixa digital que permite a transferência de valores entre seus usuários através da técnica criptográfica de *blockchain*, de forma difusa, e sem a necessidade de participação de terceiros. Cabe analisar, à luz da teoria econômica, a definição de *bitcoin* ao conceito de moeda, sendo este o propósito do próximo tópico.

2. TEORIAS DA MOEDA

A moeda é, definitivamente, um dos fatores responsáveis pela evolução das sociedades humanas. Harari a define como sendo "um meio universal de troca que permite que as pessoas convertam quase tudo em praticamente qualquer coisa" (HARARI, 2011).

Sem a invenção da moeda não haveria cenário possível para o desenvolvimento de agrupamentos humanos minimamente complexos. Em uma visão elementar, não seria possível que nas sociedades agrícolas o produtor de raízes trocasse sua produção por um bocado de leite nos dias em que o dono da vaca não quisesse comer tubérculos. A necessidade da dupla coincidência de interesses nas relações de troca é impedimento intransponível para a circulação de riquezas e fomento da economia. Uma economia fundada em simples escambo não tem aptidão para crescimento (MANKIW, 2018).

No âmbito da economia foram desenvolvidas teorias que tem a moeda como objeto de estudo, se destacando as teorias cartalista e metalista. A teoria cartalista defende ser a moeda uma criatura originada do Estado, que a utiliza, eminentemente, como unidade de conta e meio de pagamento (LERNER, 1947). Diferindo de Lerner, Knapp entende que moeda, não obstante tenha sua gênese no Estado, não tem como característica inata ser um meio de troca (KNAPP, 1905). Na verdade, moeda seria mais

do que um meio de troca, se constituindo como uma forma de pagamento que, no momento da efetivação das trocas de mercadorias, preserve sua condição de valor. No entanto, essa característica exige a atuação do Estado, pelo que, ambos concordam quanto à necessidade da origem estatal da moeda, de modo a se utilizar desse instrumento de sistema monetário de pagamentos.

Keynes (1930), a partir do pensamento de Knapp, entende a moeda como ponto central do sistema monetário das economias capitalistas, em razão da necessidade de regulação estatal desse meio de pagamento, que tem alcance nos institutos contratuais atuais e futuros.

Em oposição ao pensamento de Knapp, Mises (1934) defende a existência de duas classificações para análise da moeda. Uma primeira, catalática, que se preocupa com sua função de meio de troca, possui grande enfoque na lei demanda, e outra acatalática, cuja preocupação é a definição estatal do que seja moeda.

É interessante notar a articulação de Goodhart (1998), ao retomar o raciocínio das teorias cartalistas, no sentido de que não seria possível a existência de uma moeda não reconhecida pelo Estado, ainda que as teorias que sustentassem o contrário se assentassem em premissas de diminuição de gastos dos custos de transação. No entanto, seu estudo analisava a moeda nos países na zona do euro, sob a perspectiva supranacional/comunitária. Não se imaginava, ainda, o que viria 10 anos depois com a divulgação do trabalho de Satoshi.

Pela teoria metalista, a moeda é vista como um fenômeno social, responsável pela realização de trocas indiretas de bens e serviços (tendo papel secundário as funções de unidade de contagem e reserva de valor), cujo processo de formação independe da participação do Estado. O nome da teoria remete à predileção pela determinação de metais como moeda (*v.g.* ouro e prata), ante suas características de durabilidade e divisibilidade. Além disso, para os metalistas, o valor intrínseco do objeto escolhido como moeda é determinante para sua definição como tal (SCHUMPETER, 1994: 63, apud BELL, 2001).

Para fins do nosso estudo, serão desconsideradas as teorias acataláticas e cartalistas, uma vez que se fundam no reconhecimento estatal da moeda, sendo que, no caso do *bitcoin*, esse fato não existe. Não há intervenção do Estado na sua aplicação, criação ou desenvolvimento, de modo que, de plano, já se verifica que jamais poderia ser identificado como moeda sob a ótica das teorias acataláticas e cartalistas.

Fixado que a teoria metalista é a que permite a continuidade do desenvolvimento do nosso estudo, é importante frisar o ponto determinante do elemento confiança na definição de moeda. Com efeito, sejam sementes de cevada, conchas, ouro, prata, moedas metálicas ou papel-moeda, a confiança das pessoas naquele instrumento de trocas indiretas de bens e serviços é essencial.

A confiança do *bitcoin* é inerente à tecnologia de criptografia a partir da qual foi desenvolvido. A utilização de *blockchain* em rede difusa de computadores, conforme explicado alhures, confere segurança e auditabilidade a todas as transações, permitindo sua verificação por qualquer usuário da rede.

Não se olvidando de casos como o do administrador de carteiras virtuais Mt. Gox[7], que, em fevereiro de 2014, após um ataque de hackers, sofreu prejuízos astronômicos que levaram à sua falência por conta do acesso indevido aos dados de seus clientes, tem-se que a técnica de criptografia por *blockchain*, analisada em si mesma, é muito segura, exigindo-se, assim, o desenvolvimento de ferramentas seguras às chamdas casas de câmbio virtuais. Atualmente são múltiplos os procedimentos adotados pelos administradores desses negócios virtuais, com a execução de rigorosos protocolos de segurança. De qualquer forma, todos casos registrados de subtração de *bitcoins* envolveram falhas nos sistemas responsáveis pela administração das carteiras virtuais, não tendo nenhum deles versando acerca de defeitos na segurança da tecnologia do *bitcoin* propriamente dita.

É senso comum dos manuais de economia que a moeda se presta, basicamente, a três propósitos, servindo como (i) meio de troca, (ii) unidade de contagem, e (iii) reserva de valor (MANKIW, 2011).

Funcionando como meio de troca, a moeda evita o já mencionado problema da dupla coincidência de interesses nas relações de escambo. Com o emprego da moeda supera-se o problema da necessidade de convergirem os interesses de troca dos agentes envolvidos na relação. A partir da adoção da moeda como padrão de troca é possível que o sapateiro compre pão do padeiro sem que este precise de um novo par de sapatos. A moeda passa a ser, portanto, o instrumento utilizado para aquisição de bens e serviços em razão da confiança de que aquele pedaço de papel colorido ou de metal cunhado será aceito em razão das inscrições nele existentes, por pessoas que nunca se viram na vida.

A análise do atributo "meio de troca" exige o estudo de outra característica da moeda, qual seja, sua liquidez. Por liquidez entende-se a facilidade com a qual um ativo pode ser negociado para aquisição de outros bens e serviços (MANKIW, 2011). Assim, a moeda é, por excelência, o ativo com maior liquidez, já que tem como uma de suas funções servir como meio de troca.

Para cuidar-se do *bitcoin* como meio de troca, antes é ilustrativo trazer o caso de um ativo com liquidez limitada. Nas prisões o cigarro é comumente utilizado como meio para trocas indiretas, sendo empregado para transações envolvendo a aquisição de outros gêneros dentro do cárcere, como itens de higiene pessoal e alimentos. No entanto, essa característica é adstrita aos limites dos estabelecimentos penitenciários, não se prestando como meio de aquisição de bens e serviços em outras situações fora daquele contexto. Pelo que, em razão dessa limitação de sua liquidez, não pode ser considerado como moeda.

No caso do *bitcoin*, em que pese haver registro da sua utilização para a compra de imóveis[8] e, inclusive, do funcionamento de caixa eletrônico em São Paulo para o saque,

7 WIKIPEDIA. *Mt. Gox.* Disponível em: <https://en.wikipedia.org/wiki/Mt._Gox>. Acesso em: 8 maio. 2018.

8 ÉPOCA NEGÓCIOS. Bitcoins ganham espaço na compra de imóveis de alto padrão no país. *Agência Reuters*, 22 de dezembro de 2017. Disponível em: <https://epocanegocios.globo.com/Mercado/noticia/2017/12/epoca-negocios-bitcoins-ganham-espaco-na-compra-de-imoveis-de-alto-padrao-no-pais.html>. Acesso em: 3 abr. 2018.

em reais, do ativo virtual[9], seu emprego, atualmente, ainda acaba adstrito ao mercado *on line*. Além disso, conforme apontado por Yermack (2013), o grande volume das transações envolvendo *bitcoin* é de cunho especulativo, isto é, são operações de compra e venda praticadas entre portadores de carteiras virtuais objetivando lucro com a oscilação da cotação diária e não propriamente para a aquisição de bens.

No entanto, essa atividade de especulação pode ser encarada sob outro viés, já que, de qualquer maneira, acaba atraindo mais investidores e, via de consequência, incrementando a circulação do *bitcoin* (ULTICH, 2014).

Outra crítica de Yermack no tocante à característica de meio de troca, é que a aquisição de *bitcoin* exige o exercício da atividade de mineração ou a aquisição, através de moedas nacionais, o que dificulta sua circulação. Todavia, a mesma situação ocorre quando se busca adquirir moeda estrangeira para uma viagem, por exemplo. É necessária a atuação de uma casa de câmbio ou de uma instituição bancária autorizada para a realização da compra do ativo. Da mesma forma, através dos serviços de uma administradora de carteiras virtuais, mediante transferência bancária, são adquiridos *bitcoins* que, por outro lado, podem ser vendidos e liquidados em moeda oficial local, da mesma forma.

Como unidade de contagem, uma moeda se presta a fixar valor aos bens e serviços, servindo de padrão para a medida de seus valores. Nesse ponto repousa a maior dificuldade do *bitcoin* dentro da análise das funções da moeda, ou seja, a sua volatilidade. Como parâmetro da grande volatilidade do ativo virtual, registre-se que em 2018, até o dia 03 de maio, por 43 vezes a volatilidade diária foi maior do que $ 1,000 (mil dólares americanos)[10].Essa grande alternância em seus valores em tão curto espaço de tempo decorre, especialmente, do caráter especulativo da maioria dos investidores nesse ativo digital, conforme apontado por pesquisas indicadas por LOI (2018).[11]

Por fim, como reserva de valor, uma moeda permite sua troca por bens e serviços em tempo futuro, à escolha de seu titular. Outra vez é ínsita a característica da confiança, ficando claro que a falta dela como reserva de valor é determinante para entender as situações nas quais muitas economias naufragaram, como a Alemanha pós primeira guerra munida, o Brasil nos anos 80, a Argentina nos anos 90 e, atualmente, a Venezuela (CASEY; VIGNA, 2015).

Sem confiança na moeda como reserva de valor, as pessoas tendem a se desfazer dela, buscando outras formas de indexação de seus bens e valores, como moeda estrangeira, ouro. Sem a confiança de se saber que a quantificação fixada hoje para determinado bem, *v.g.*, um pão, será a mesma amanhã, não há ambiente para o desenvolvimento econômico sadio. É justamente esta situação a tratada pela Lei de Gresham, sob

9 TOZETTO, Claudia. Caixa eletrônico de bitcoins movimenta R$ 180 mil em dois meses. *Veja*, 31 de julho de 2014. Disponível em: <https://veja.abril.com.br/tecnologia/caixa-eletronico-de-bitcoins-movimenta-r-180-mil-em-dois-meses/>. Acesso em: 10 jun. 2018.

10 GODBOLE, Omkar. *Daily Volatility Decline? Bitcoin Has Seen $1K Range 43 Times In 2018*. 3 de maio de 2018. Disponível em: <https://www.coindesk.com/daily-volatility-decline-bitcoin-seen-1k-range-43-times-2018/>. Acesso em: 10 jun. 2018.

11 GOLDMAN SACHS, 2014; HENCIC; GOURIEROUX, 2015; CHEUNG et al., 2015; CHEAH; FRY, 2015.

a famosa expressão *bad money drives out good* (a moeda ruim expulsa a moeda boa – em livre tradução) (SULLIVAN, 2005).

Mais uma vez a volatilidade do valor do *bitcoin* atrapalha seu emprego como reserva de valor, justamente porque não se tem certeza de seu poder de compra em uma projeção de futuro.

Nesse sentido, a Comissão de Valores Mobiliários (CVM), através do Ofício Circular nº 1/2018/CVM/SIN, de 12.01.2018[12], proibiu fundos de investirem em *bitcoins* e outras moedas virtuais, ante o risco no tocante à sua utilização como reserva de valor.

Doutro giro, não procedem as críticas feitas por Yermack no tocante à característica imaterial do *bitcoin*, na medida em que hodiernamente a grande maioria das transações bancárias são feitas de forma virtual, através de internet banking, caixas eletrônicos, cartões de crédito e de débito, sem a utilização de papel-moeda, o que não inviabiliza o seu reconhecimento como moeda.

3 TEOREMA DA REGRESSÃO DE MISES

O teorema da regressão de Luwig Von Mise foi desenvolvido para explicar a origem do dinheiro, tendo sido apresentada pela primeira vez na obra "Theorie des Geldes und der Umlaufsmittel" (Teoria do Dinheiro e da Moeda Fiduciária) (1924).

Antes do desenvolvimento do teorema da regressão, a ciência econômica se deparava com o "problema da circularidade", pelo qual, aparentemente, não se conseguia determinar o preço da moeda, uma vez que sua utilidade dependia de seu valor préexistente, sendo que a utilidade da moeda não é intrínseca, ou seja, não se revela em seu consumo próprio, mas sim como forma de aquisição de bens e serviços (IORIO, 2010).

A solução proposta por Mises exige o raciocínio regressivo do valor da moeda, dia a dia, até o ponto em que se possa determinar qual era o valor da moeda como utilidade própria, inerente a si mesma, momento este em que ela deixou de ser um bem de consumo e passou a servir como meio de pagamento indistintamente aceito (DAVIDSON; BLOCK, 2015).

Mises demonstra que a moeda, propriamente, não é criação do governo, mas sim decorrência da aceitação geral da utilidade dela pela sociedade. Pelo que, antes dessa aceitação como elemento indistinto de troca, a moeda passou pelo processo de valorização de sua utilidade própria (MISES, 1949).

Usando como referência o ouro, temos que, antes de ser aceito como elemento indistinto de troca, o metal possuía seu valor próprio para confecção de adornos. A partir do momento em que sua aceitação, pelo valor da sua utilidade, atingiu o grau de permitir a realização de trocas indiretas indistintas, tem-se a origem da moeda, calculando-se, a partir daí, seu valor, sua utilidade, sua demanda.

12 COMISSÃO DE VALORES MOBILIÁRIOS. *Ofício Circular n. 1/2018/CVM/SIN*. Disponível em: <http://www.cvm.gov.br/export/sites/cvm/legislacao/oficios-circulares/sin/anexos/oc-sin-0118.pdf>. Acesso em: 8 maio. 2018.

Analisando o *bitcoin* a partir do teorema da regressão, temos, como vantagem, a precisão da determinação do momento de seu lançamento. Em 03 de janeiro de 2009 surgiu o primeiro bloco de *bitcoins*, tendo sido realizado em 05 de outubro de 2009 a primeira conversão em dólar, equivalendo 1 dólar a 1.309,03 BTC, sendo que em 22 de maio de 2010 foi realizada a primeira transação com *bitcoin*, o pagamento de uma pizza com 10 mil moedas, equivalentes a 25 dólares na época.

Assim, desde o início, o *bitcoin* teve utilidade própria (ULTICH, 2017). O projeto, desde seu nascedouro, tinha valor estipulado das unidades, ainda que para os poucos usuários iniciais. Ao longo do tempo, com a percepção das funcionalidades dispostas pela iniciativa, tais como a privacidade, o baixo custo das operações, a não intervenção de terceiros, o alcance mundial, seu valor de utilidade própria aumento vertiginosamente.

Outro ponto a ser sopesado é que o fato de não ter existência material não impede o reconhecimento da utilidade do *bitcoin*. Nesse sentido, é só lembrarmos de que atualmente a grande maioria das transações envolvendo moedas reconhecidas pelos governos são feitas eletronicamente, através de computadores, cartões de créditos, aplicativos e outras formas de tecnologia, de forma que o papel-moeda vem sendo substituído gradativamente.

Conclusão

A cada dia se verifica que o *bitcoin* tem se consolidado como um meio de troca indiretas de bens e serviços com alto grau de difusão, havendo, assim, incremento na sua liquidez. No entanto, seu atual estágio de aceitação ainda não permite sua classificação como moeda, haja vista que, por ora, ainda não cumpre com propriedade as funções que se espera de uma moeda, quais sejam, servir como meio de troca, unidade de contagem e reserva de valor. Muito dessa dificuldade é atribuída à volatilidade com a qual o ativo virtual é comercializado nas casas de câmbio virtuais. A multiplicidade de transações envolvendo as carteiras virtuais de *bitcoins* faz com que em um intervalo de horas seu valor atinja grandes variações. No entanto, essa volatilidade pode ser entendida como uma etapa de na fixação da liquidez do ativo. Só o futuro dirá o que será do *bitcoin*. De qualquer forma, a enormidade de transações na internet é um reflexo da confiança que vem sendo depositada pelo mercado, aí se incluindo o pagamento até de imóveis através do ativo virtual. Sopese-se, todavia, que sob o aspecto da aplicação do teorema da regressão de Mises, que explica a origem do dinheiro, o *bitcoin* observa o paradigma da escola austríaca. Pelo que, em um mundo cada vez mais digital, o *bitcoin* tem aptidão para atingir a liquidez apta a mudar seu patamar.

REFERÊNCIAS BIBLIOGRÁFICAS

ABRAMOWICZ, Michael. *Autonocoin: A Proof-of-Belief Cryptocurrency*. ISSN 2379-5980. DOI 10.595/Ledger.2016.37.

AGGIO, Gustavo de Oliveira; ROCHA, Marco Antonio da. Dois momentos para a teoria cartalista da moeda – De Knap a Goodhart. *Revista da ANPEC – Associação Nacional dos Centros de Pós-Graduação em Economia*. v. 10, n. 1, 2009.

BANKING ON BITCOIN. *Direção: Chistopher Cannucciari.* 2016.

BLUNDELL-WIGNALL, Adrian. The Bitcoin Question: Currency versus Trust-less Transfer Technology. *OECD Working Papers on Finance, Insurance and Private Pensions*, No. 37, 2014. OECD Publishing. Disponível em: <http://dx.doi.org/10.1787/5jz2pwjd9t20-en>.

CASEY, Michael, J. VIGNA, Paul. *The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order*. E-book edition. 2015.

COMISSÃO DE VALORES MOBILIÁRIOS. *Ofício Circular n. 1/2018/CVM/SIN.* Disponível em: <http://www.cvm.gov.br/export/sites/cvm/legislacao/oficios-circulares/sin/anexos/oc-sin-0118.pdf>. Acesso em: 8 maio. 2018.

DAVIDSON, Laura; BLOCK, Walter E. Bitcoin, the regression theorem, and the emergence of a new medium of exchange. *The quaterly journal of austrian economics.* v. 18, n. 3, p. 311-338. Fall 2015.

DE FILLIPI, Primavera; WRIGHT, Aaron. *Blockchain and the law: the rule of code*. Harward Universiy Press, 2018. edição digital.

ÉPOCA NEGÓCIOS. Bitcoins ganham espaço na compra de imóveis de alto padrão no país. *Agência Reuters,* 22 de dezembro de 2017. Disponível em: <https://epocanegocios.globo.com/Mercado/noticia/2017/12/epoca-negocios-bitcoins-ganham-espaco-na-compra-de-imoveis-de-alto-padrao-no-pais.html>. Acesso em: 3 abr. 2018.

GODBOLE, Omkar. *Daily Volatility Decline? Bitcoin Has Seen $1K Range 43 Times In 2018.* 3 de maio de 2018. Disponível em: <https://www.coindesk.com/daily-volatility-decline-bitcoin-seen-1k-range-43-times-2018/>. Acesso em: 10 jun. 2018.

GOODHART, C. A. E. Two concepts of money: Implications for the analysis of optimal currency areas. *European Journal of Political Economics,* v. 1, p. 407–432, 1998.

HARARI, Yuval Noah. *Sapiens: uma breve história da humanidade.* 2011. edição digital.

HAYNES, Paul; O'BROLCHÁIN, Fiachra; REIJERS, Wessel. *Governance in Blockchain Technologies & Social Contract Theories.* 2016.62.

IORIO, Ubiratan Jorge. *A teoria monetária austríaca*. Disponível em: <https://www.mises.org.br/Article.aspx?id=697>. Acesso em: 1 jun. 2010.

KEYNES, J. M. A treatise on money. *In The Collected Writings of John Maynard Keynes,* Macmillan, Londres. v. 5 e 6. 1930.

KNAPP, G. F. *The State Theory of Money*. San Diego: Simon Publications 2003, 1905.

LERNER, A. P. Money as a creature of the state. *American Economic Review,* v. 37, p. 312–317, 1947.

LOI, Hio. The liquidity of bitcoin. *International Journal of Economics and Finance;* v. 10, n. 1; 2018.

MANKIW, N. Gregory. *Macroeconomia.* Tradução Ana Beatriz Rodrigues. 8. ed. Edição eletrônica. 2018.

MENGER, K. On the origin of money. *Economic Journal,* v. 2, p. 238–55, 1892.

MISES, Ludwig von. *Ação humana: Um tratado de economia.* Tradução Donald Stewart Jr. Yale Press University, 1949.

NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System.* 2009. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: maio 2018.

POPOV, Serguei. A Probabilistic Analysis of the Nxt Forging Algorithm. 2016.46.

SULLIVAN, Noel. Gresham's Law, Fact or Falsehood? *Student Economic Review,* v. 19, 2005.

TAPSCOTT, Alex; TAPSCOTT, Don. *Blockchain Revolution.* Edição digital. 2016.

TAYLOR, M. , "Bitcoin and The Age of Bespoke Silicon". *International Conference on Compilers, Architecture and Synthesis for Embedded Systems (CASES),* n. 13898761, Montreal, QC, Canada, 29/09 – 04/10. 2013.

TOZETTO, Claudia. Caixa eletrônico de bitcoins movimenta R$ 180 mil em dois meses. *Veja,* 31 de julho de 2014. Disponível em: <https://veja.abril.com.br/tecnologia/caixa-eletronico-de-bitcoins-movimenta-r-180-mil-em-dois-meses/>. Acesso em: 10 jun. 2018.

ULTICH, Fernando. *Bitcoin: A moeda na era digital.* 2014. Misses brasil. Edição digital.

YERMACHK, David. Is Bitcoin a real currency? An economic Appraisal. *Working Paper,* n. 19747. December 2013. Revised April 2014.

VILLARREAL ROBLEDO, Omar Eliud. The Ontological Sociology of Cryptocurrency: A Theoretical Exploration of Bitcoin. *Electronic Theses and Dissertations.* 2016. 5119.

WIKIPEDIA. *Mt. Gox.* Disponível em: <https://en.wikipedia.org/wiki/Mt._Gox>. Acesso em: 8 maio. 2018.

WIKIPÉDIA. *Silk Road.* Disponível em: <https://pt.wikipedia.org/wiki/Silk_Road>. Acesso em: 3 abr. 2018.