FÓRUM Liberdade Econômica
6 A 8 DE NOVEMBRO DE 2017
LOCAL: MACKENZIE – SP

# BITCOIN, CRIPTOMOEDAS, BLOCKCHAIN: DESAFIOS ANALÍTICOS, REAÇÃO DOS BANCOS, IMPLICAÇÕES REGULATÓRIAS[1]

Carlos Eduardo Carvalho[2], Desiree Almeida Pires[3], Marcel Artioli[4], Giuliano Contento de Oliveira[5]

**RESUMO**

O blockchain é uma inovação tecnológica de alcance bem mais amplo que as chamadas criptomoedas que nele se baseiam e tem potencial para transformar extensivamente os sistemas de pagamentos e o conjunto das práticas do sistema monetário e financeiro. O desdobramento mais conhecido são as criptomoedas, adjetivo que destaca a utilização de técnicas que permitem proteger dados transmitidos e armazenados de forma descentralizada. A mais utilizada das criptomoedas, o bitcoin, mostra que não se trata de uma moeda em sentido rigoroso, pela ausência das funções de padrão de preços e de reserva de valor e pelo uso muito limitado como meio de pagamento. O artigo destaca a reação dos grandes bancos ao surgimento destas inovações, com aplicação crescente a suas práticas e transações, o que parece apontar para a permanência da centralidade da moeda bancária e da moeda estatal fiduciária, com as criptomoedas ocupando papel de inovação financeira e de meios de pagamento auxiliares. O artigo aborda também os desafios regulatórios colocados pelo blockchains e pelas criptomoedas.

**PALAVRAS-CHAVE**

blockchain; bitcoin; criptomoedas; bancos; regulação financeira

**ABSTRACT**

The blockchain is a technological innovation of much wider scope than the so-called cryptocurrencies that are based on it and with the potential to transform payment systems and the whole range of practices of the monetary and financial system extensively. Its most well-known development is the cryptocurrencies, an adjective that indicates its basic characteristic, that is, the use of techniques that allow to protect data transmitted and stored in a decentralized way. Bitcoin, the most used of the cryptocurrencies, shows that it is not a currency in the strict sense, by the absence of the functions of standard of price and reserve of value and by the very limited use as means of payment. The article highlights the reaction of the big banks to the emergence of these innovations, with increasing application to their practices and transactions, which seems to point to the permanence of the centrality of the banking currency and the fiduciary state currency, with the cryptocurrencies occupying the role of financial innovation and means of payment. The article also addresses the regulatory challenges posed by blockchain and cryptocurrencies.

---

[1] Trabalho desenvolvido no âmbito do Grupo de Pesquisa em Moeda, Finanças e Desenvolvimento.

[2] Doutor em Ciências Econômicas pela Unicamp. Professor da PUCSP, Departamento de Economia e Programa de Pós-Graduação em Relações Internacionais San Tiago Dantas (Unesp/Unicamp/PUC/SP).

[3] Mestre em Relações Internacionais pela Universidade Federal de Santa Catarina. Doutoranda pelo Programa de Pós-Graduação em Relações Internacionais San Tiago Dantas (Unesp/Unicamp/PUC/SP). Bolsista do Instituto Nacional de Ciência e Tecnologia para estudos sobre os Estados Unidos (INCT/INEU).

[4] Graduado em Relações Internacionais pela Unesp/Franca. Mestrando pelo Programa de Pós-Graduação em Relações Internacionais San Tiago Dantas (Unesp/Unicamp/PUC/SP).

[5] Doutor em Ciências Econômicas pela Unicamp. Professor do Instituto de Economia da Unicamp e do Programa de Pós-Graduação em Relações Internacionais San Tiago Dantas (Unesp/Unicamp/PUCSP).

**KEY WORDS**
blockchain; bitcoin; cryptocurrencies; banks; financial regulation

## 1 Introdução

O amplo debate suscitado pelas criptomoedas, especialmente o bitcoin, envolve desde a caracterização de sua natureza e das transformações que provocam na estrutura do sistema monetário e financeiro e a reação dos bancos e instituições financeiras e dos bancos centrais, até os desafios para a regulação financeira e para o combate ao crime organizado. As criptomoedas são assim denominadas porque sua viabilização ocorre a partir de métodos criptográficos, ou seja, de um conjunto de técnicas que permitem proteger dados transmitidos e armazenados, a partir da transformação de informações legíveis em códigos ininteligíveis. Os avanços da tecnologia e dos sistemas de informática e comunicação, com a rede mundial de computadores, a internet, permitiram a criação de formas de moeda desregulamentadas e descentralizadas.

O bitcoin utiliza a tecnologia de um sistema de registro de transações em rede de dados *peer-to-peer* (P2P), conhecida como *blockchain*, ou cadeia de blocos, para ser transferido, comprado e vendido, sem necessidade de autenticação e verificação de uma terceira parte. Trata-se, pois, de uma criptomoeda, como outras menos conhecidas - litecoin, worldcoin, solidcoin, ixcoins, coinbuck, betacoin, tenebrix. zcash, para citar algumas dentre as mais de mil que existem agora, segundo alguns levantamentos. Uma das suas características básicas é não contarem com uma autoridade central responsável pela liquidação e compensação das transferências realizadas, a partir de mecanismos institucionalizados. A tecnologia utiliza enigmas computacionais da criptografia para regular e limitar a criação de bitcoins, assegurar o anonimato dos participantes e registrar as transações realizadas em um livro-caixa contábil (*ledger*), como forma de impedir o gasto duplo ou mesmo ilimitado da moeda, ou seja, que um usuário possa *gastar* o mesmo bitcoin mais de uma vez. É, portanto, um sistema de pagamento e um sistema de registro de transações inovador, descentralizado e privado, com grau de segurança bastante elevado, mas sem salvaguardas ou garantias do Estado.

Para seus defensores e entusiastas, as criptomoedas são moedas de fato, de natureza privada e descentralizada, livres do governo e incorruptíveis. No caso do bitcoin, há ainda o limite rígido de emissão. Alega-se, inclusive, que as criptomoedas têm elevada praticidade e custos mais baixos que outras formas de pagamento e de transferência de valores já existentes.

O bitcoin pode ser considerado também como ativo financeiro especulativo, com preço em dólares muito volátil e forte valorização - de centavos, em 2008, para mais de USD 6.000, atualmente, com fortes oscilações e desvalorizações, como a observada entre 2014 e 2015. Em muitos países, a posse e as transações com bitcoins são equiparadas a ativos financeiros para fins de regulação e tributação. O caráter de moeda é questionado pelos obstáculos que a volatilidade de sua cotação coloca para que assuma funções de padrão de preços e de reserva de valor, de um lado, e de avanço de sua função como meio de pagamento, de outro, atributos tidos como essenciais para que um ativo constitua, de fato, moeda. A volatilidade do preço do bitcoin em dólar decorre também de não existir um regulador de seu preço, um Banco Central que opere continuamente em um mercado amplo, como ocorre com moedas nacionais, ausência constitutiva da natureza do bitcoin. Além disso, parece difícil imaginar que possa surgir uma cadeia de crédito corrente e de longo prazo em bitcoins, algo inerente a uma economia de mercado, processo que levou à substituição das moedas metálicas pelas moedas fiduciárias estatais a partir de meados do século XIX.

O entusiasmo com a possibilidade de o bitcoin substituir a moeda estatal pode ser atribuído a uma visão mítica e deflacionária do padrão ouro. Vale lembrar que propostas de criação de moedas não estatais surgiram em diversos momentos, com

objetivos socialistas e comunitários, ou com propósitos antideflacionários em momentos de graves crises financeiras, como nos anos 1930, ou com objetivos de desenvolvimento em comunidades ou regiões de grande pobreza e ausência de crédito, caso das moedas locais criadas em alguns países em anos recentes. Em todos esses casos, as moedas privadas foram criadas com uso e objetivos restritos, em termos de tempo e de espaço econômico envolvido.

Pelo alcance, segurança e agilidade, os seus entusiastas e defensores sustentam que o bitcoin é uma forte ameaça aos sistemas de liquidação de pagamentos existentes, capaz de viabilizar a criação de uma nova ordem monetária em substituição à ordem atual, baseada na moeda estatal e na moeda de crédito criada pelos bancos, em razão da oferta de serviços de pagamento e de transferência de recursos com segurança, do custo relativo muito menor e do potencial de se tornar tão rápido quanto os meios de pagamentos eletrônicos atuais. É como se fosse uma generalização de redes privadas, como a *hawalla*, sistema asiático de transferências monetárias baseado em redes de confiança, mas com potencial de liquidar transações sem depender de proximidade ou vínculos desse tipo.

Por trás das chamadas criptomoedas, como apontam Lakomski-Laguerre e Desmedt (2015), há uma ideologia muito bem definida, a saber, anti-estatista e neo-metalista da moeda, que procura viabilizar a criação de uma ordem monetária livre dos bancos e das autoridades monetárias, ou seja, independente de qualquer poder central e baseada na ideia de autorregulação da oferta de moeda (Hayek, 1976). O fato de o bitcoin ter surgido no período imediatamente posterior à deflagração da crise global de 2008, com epicentro nos Estados Unidos (EUA), é bastante revelador nesse sentido: diante da fragilização do sistema bancário e da incapacidade de a autoridade central garantir uma ordem monetária estável, a partir da combinação *Banks-Government*, o bitcoin poderia viabilizar uma ordem monetária alternativa e estável. Segundo Lakomski-Laguerre e Desmedt (2015):

> O projeto Bitcoin surge imediatamente após o surgimento da crise financeira de 2008, cuja escala causou grande descrédito no setor bancário. Como qualquer inovação radical, a natureza disruptiva da tecnologia que transporta a cryptocurrency, apoiada pelas novas lógicas econômicas que a expansão da Internet gera, aparece como uma ameaça potencial em relação à ordem monetária existente. Além do único aspecto técnico, o sistema Bitcoin aparece claramente como uma alternativa ao capitalismo contemporâneo, cuja dinâmica é impulsionada por uma colusão Banks-Government. É também parte de um movimento de protesto dos poderes políticos e bancários, que foram considerados incapazes de oferecer uma moeda de qualidade. As criptomoedas constituiriam então um meio de "democratizar as finanças" em espaços alternativos (transnacionais) e de restaurar aos indivíduos o "bem comum" que é o dinheiro. (tradução livre).

Para os propósitos desse artigo, pois, importa enfatizar que, para além da inovação das criptomoedas em si, com destaque ao bitcoin, a tecnologia *blockchain* representa uma inovação de grande relevância, porque capaz de remodelar o sistema financeiro moderno, com desdobramentos diversos, alguns dos quais ainda desconhecidos. Nessa perspectiva, o artigo sustenta que as criptomoedas, embora representem uma inovação financeira importante, não tendem a alterar a prevalência da ordem monetária vigente em um período de tempo minimamente previsível, ordem esta baseada na moeda estatal e na moeda bancária. Isso porque, conforme argumentado ao longo do artigo, o sistema bancário, sob o acicate da ameaça potencial suscitada pelas criptomoedas e, sobretudo, pela tecnologia P2P, de um lado, e sob a liderança dos

grandes bancos internacionais, de outro, tem incorporado e desenvolvido rapidamente a tecnologia *blockchain* em suas operações. Não obstante, seria ocioso afirmar que essas transformações impõem desafios consideráveis à estabilidade financeira, à supervisão e à regulação do sistema, assim como à capacidade de tributação dos Estados, além dos problemas potenciais de utilização para atividades ilícitas e para o crime organizado.

Além desta introdução e de uma seção final com as conclusões preliminares, o artigo traz outras quatro seções: argumentos teóricos para a análise dos significados das criptomoedas e dos impactos da tecnologia do *blockchain* estão na seção 2, a partir da revisão do papel da moeda e dos ativos financeiros na economia capitalista; a seção 3 resume as questões técnicas envolvidas necessárias para a análise das criptomoedas e das inovações tecnológicas em que se apoiam; a seção 4 discute a reação dos grandes bancos em busca de incorporar as novas tecnologias a suas práticas; e a seção 5 resume os desafios colocados para a regulação financeira internacional.

## 2 Moeda, criptomoedas e blockchain

Esta seção tem o objetivo de discutir as diferenças fundamentais entre a moeda baseada em uma autoridade central, capaz de desempenhar as três funções fundamentais (meio de pagamento, unidade de conta e reserva de valor), e as denominadas criptomoedas, entendidas como moedas digitais do tipo criptográfica, desregulamentadas e descentralizadas.

A moeda e a confiança do público nela depositada constituem fenômenos coletivos, conformando, assim uma instituição social, no sentido de que organiza e atribui viabilidade ao sistema de trocas indiretas que caracteriza o capitalismo (Schumpeter, 2005; Belluzzo e Almeida, 2002). Nesse modo de organização da vida social, a moeda cumpre uma dupla função, a saber, instrumento de validação social do produto do trabalho individual (caráter público da moeda) e forma mais geral de riqueza que orienta as decisões de investimento e alocação da riqueza entre classes alternativas de ativos (caráter privado da moeda).

Para tanto, a moeda deve cumprir três funções: meio de pagamento, reserva de valor e padrão de preços ou unidade de conta. A primeira função permite a liquidação imediata das transações econômicas, assumindo o papel de equivalente geral do sistema. A segunda, por seu turno, decorre do fato de a moeda encarnar a própria noção da liquidez, condição que transforma, ela mesma, em um ativo que, embora não propicie o recebimento de juros pelo seu detentor, possui o prêmio de liquidez (Keynes, 1936). Por fim, a função unidade de conta ocupa papel central em uma economia monetária da produção, pois diz respeito à capacidade de a moeda definir quantidades nominais em termos de preços monetários, atribuindo comparabilidade e proporcionalidade entre diversos bens e serviços disponíveis em uma economia a partir de parâmetro objetivo, bem como de registrar transações, condições indispensáveis para o cálculo econômico. Como apontam Lakomski-Laguerre e Desmedt (2015), "Como uma unidade de conta, o dinheiro não resulta de forças endógenas dentro do sistema econômico, mas de um ato fora do mercado." (tradução livre)[6].

De acordo com Keynes (1936), a moeda possui duas propriedades essenciais, que a diferencia dos demais ativos em uma economia capitalista, a saber: i) nula ou negligenciável elasticidade de produção; e ii) nula ou negligenciável elasticidade de substituição. A primeira propriedade significa, essencialmente, que a produção de moeda não pode ser realizada mediante a contratação de trabalhadores, de modo que o

[6] No original: "En tant qu'unité de compte, la monnaie ne relève pas de forces endogènes au sein du système économique, mais d'un acte hors marché." (Lakomski-Laguerre e Desmedt, 2015).

aumento do grau de preferência pela liquidez do público provoca rupturas no circuito econômico, vale dizer, crises provocadas por insuficiência de demanda efetiva. Já a segunda propriedade essencial da moeda significa que o princípio da substituição não se aplica a esse ativo, no sentido de que a demanda do público por ela aumenta e não há outro ativo capaz de substituí-la. A partir dessas duas propriedades, Keynes (1936) formulou uma teoria de escolha de ativos, mostrando que os portfólios dos atores econômicos serão compostos por ativos mais ou menos líquidos, a depender do estado geral de expectativas prevalecente e do subsequente grau de preferência pela liquidez assumido. Uma formulação que alça a moeda à condição de um ativo capaz de ser quisto por ele mesmo e que, combinada com as noções de incerteza e expectativas, revela o caráter essencialmente monetário e instável das economias capitalistas.

Nesse sentido, uma economia capitalista deve ser entendida a partir de uma abordagem de fluxo de caixa, com posições ativas assumidas por uns atores correspondendo a posições passivas de outros – no caso de bancos com carteiras comerciais, essas posições se inserem em seus próprios balanços. Isto é, uma economia capitalista corresponde a um sistema de balanços inter-relacionados, com a moeda estatal (fiduciária) e, sobretudo, a moeda bancária (escritural) constituindo o núcleo do sistema de pagamentos moderno.

Posto isso, vale salientar que nos sistemas monetários contemporâneos as moedas nacionais são moedas estatais fiduciárias, sem lastro, no sentido de ter seu valor garantido apenas pela autoridade do Estado emissor e dotadas do princípio de curso forçado no espaço nacional, ou seja, devem ser aceitas obrigatoriamente pelos cidadãos e empresas no território nacional. Além disso, elas são a única forma aceita pelo Estado para pagamento de impostos e são as únicas aceitas pelo Banco Central para o fechamento das posições dos bancos diariamente. Ou seja, as moedas nacionais possuem autoridades centrais e circulam dentro de um território específico (Blanc, 1998). Quando uma moeda nacional é aceita internacionalmente, ela assume certo grau de moeda internacional, *a-territorial*. No capitalismo moderno, a moeda global por excelência é o dólar americano, uma vez que o sistema monetário-financeiro internacional contemporâneo é baseado em moedas nacionais, sendo, portanto, hierárquico e assimétrico[7].

Emitida pelos governos estatais, com o desenvolvimento do sistema bancário e do subsequente sistema de reservas fracionárias, as moedas nacionais foram se tornando essencialmente fiduciárias, passando a ser utilizadas, fundamentalmente, em razão da confiança do público em sua aceitação generalizada, sem lastro. O valor atribuído à moeda fiduciária, portanto, deve-se ao fato de que os governos nacionais aceitam apenas essas moedas como pagamento de taxas, garantindo sua demanda (Bissessar, 2016). Consequentemente,

> [...] o conceito de dinheiro é uma reflexão da confiança popular na capacidade de uma moeda sustentar um sistema de transações de valor. Essa confiança é tipicamente mantida pelos Estados-nação e sua associação aos Bancos Centrais. Entretanto, surge uma questão: se uma parte da população confia em um sistema de moeda alternativo, pode essa moeda alternativa ser considerada como dinheiro? (Bissessar, 2016, p. 11, tradução livre)[8].

[7] Sobre o caráter hierárquico e assimétrico do sistema monetário-financeiro internacional contemporâneo, ver Prates (2005), De Conti, Prates e Plihon (2013).

[8] No original: "[…] the concept of money is a reflection of popular confidence in the ability of a currency to support a system of value transactions. This confidence is typically upheld by nation states and their

Dessa forma, além das moedas estatais, os depósitos à vista nos bancos comerciais também são moeda, pela capacidade de liquidar pagamentos, mas com a condição de serem conversíveis na moeda estatal de forma imediata.

Blanc (1998) aponta que se desenvolveram, na economia, as chamadas moedas paralelas, meios de pagamento diferentes das moedas nacionais, mas que têm garantia de conversibilidade nesta moeda e cuja utilização vem se generalizando. Tais moedas são criadas com objetivo de reorganizar monetariamente uma economia. Para esse autor, as moedas, além de constituírem um sistema monetário ou de pagamento, são fruto da articulação entre os instrumentos que possibilitam a compra e o pagamento de dívidas e o sistema de pagamento que engloba esses instrumentos, portanto, os instrumentos monetários podem ser de diversos tipos, para além das moedas nacionais, variando de acordo com certos limites temporais, geográficos, sociais e econômicos.

Quatro grupos de moedas paralelas podem ser identificados a partir de suas criações e aceitação social: a) instrumentos monetários derivados de uma coletividade territorial, referentes a moedas estrangeiras ou municipais e regionais que circulam dentro de um Estado; b) instrumentos monetários derivados de organizações de tipo comercial ou administrativas, moedas criadas de forma privada, comumente em caráter emergencial ou *ad hoc*, estando limitadas no tempo e no espaço; c) instrumentos monetários derivados de grupos de pessoas com vocação não-comercial, que seguem uma lógica comunitária e são organizados e mantidos a partir de uma base social; e d) instrumentos de origem não especificamente monetária, associados a uma função monetária em determinadas circunstancias, mas que não tem essa função como principal (Blanc, 1998).

Blanc (1998) destaca também a existência de paramoedas, as quais funcionam à margem da moeda nacional, mas não contra esta, ou seja, de forma complementar à moeda nacional. De acordo com o autor, as paramoedas são utilizadas por agentes específicos e em trocas específicas de bens e serviços, podendo, inclusive, corresponderem a sistemas de pontuação para fidelização de clientes.

## 3 Bitcoin e blockchain

Para além da inovação financeira representada pelas criptomoedas, que carecem das funções essenciais da moeda baseada na combinação Estado-bancos, uma importante inovação tecnológica que está por detrás das criptomoedas, o *blockchain*, tem a capacidade de remodelar o sistema financeiro.

Desde o surgimento da internet, a evolução dos meios de comunicação e dos meios de pagamento online abriu espaço para inovações tecnológicas relevantes nos sistemas financeiros, tanto nacionais como internacional. Dentre elas, por exemplo, pode-se apontar o avanço na arquitetura intermediária das transações via cartão de crédito, desenvolvida por empresas como Visa e MasterCard, as quais estabeleceram padrões de criptografia que possibilitaram o aumento da segurança e, logo, da confiança no uso da rede. O consórcio que envolvia a www (*World Wide Web*) buscava constituir protocolos comuns para o sistema de transações financeiras, tal como a extensão do HTTP, que é base de comunicação de dados da internet (Narayanan et. al, 2016).

A convergência entre padrões de criptografia e as comumente denominadas *moedas digitais* está circunscrita a essa dinâmica inovadora da internet associada aos progressos muito acelerados no âmbito da tecnologia da informação. De acordo com

---

associated Central Banks. However the question now arises: if a portion of the population places confidence in an alternate system of currency, can such an alternate currency be considered as money?" (Bissessar, 2016, p. 11).

Lakomski-Laguerre e Desmedt (2015), a moeda moderna também é digital, eletrônica, virtual, em uma acepção mais geral, uma vez que mediada por transferências de dados viabilizadas por sistemas computacionais cada vez mais sofisticados. Nessa perspectiva, segundo os autores, não é o caráter digital do bitcoin, em particular, e das criptomoedas, em geral, o fator distintivo com relação ao sistema monetário hodierno. Para os autores, a grande inovação e, portanto, diferença da ordem monetária proposta pelo bitcoin relativamente à ordem monetária atual, ancorada na moeda estatal e na moeda bancária, diz respeito à ausência de autoridade central e ao processo de auto-regulação do chamado dinheiro criptográfico. Nos termos de Lakomski-Laguerre e Desmedt (2015):

> A novidade de Bitcoin não reside em seu caráter "digital", "virtual", "eletrônico" ou "digital", como muitos comentadores parecem pensar. A existência de uma série de mal-entendidos nos leva de volta à questão central da natureza do dinheiro. É importante distinguir, por um lado, os invariantes teóricos, e, por outro, as diferentes formas que a moeda assumiu ao longo da história, assim como seus diferentes modos de regulação. Se o Bitcoin surgir como um sistema de pagamentos, a alternativa que ele propõe reside na ausência de autoridade central e na auto-regulação da moeda criptografada. (tradução livre)[9].

Na essência da inovação das criptomoedas se coloca a tecnologia *blockchain*, a qual permite esse sistema de pagamentos sem autoridade central e baseada na auto-regulação. Essa tecnologia, portanto, constitui o traço distintivo do sistema de pagamentos baseado nas criptomoedas *vis-à-vis* ao sistema atual, ancorado na combinação entre moeda estatal e moeda bancária, conforme já reportado.

De modo simplificado, a ideia é a de que toda criptomoeda reivindicada por um usuário está atrelada a sua identidade, a qual é criptografada por meio de uma sequência alfanumérica aleatória, de modo que somente o usuário pode decodificá-la. Assim, toda vez que o usuário desejar realizar uma transação, a base de dados que mantém o registro das transações requererá uma chave privada deste para a validação da operação (Lee, 2015; Narayanan et. al., 2016). Nos anos 1990, esta concepção passou a ser comercializada e implementada por alguns bancos nos Estados Unidos na forma do que se chamou de *ecash*, constituído pela empresa *DigiCash*.

A trajetória da *DigiCash* teve curta duração no sistema financeiro americano, já que havia se tornado razoavelmente complicado persuadir os bancos e operadores a adotá-la de forma massiva. Além disso, a dinâmica do protocolo de criptografia estava atrelada à relação entre o usuário e a terceira parte responsável pela compensação da transação. Nesse caso, o anonimato era garantido somente ao usuário e não aos terceiros, fiadores da transação. Embora se argumente sobre outras razões a respeito do malogro da *DigiCash* e que o fundador da empresa, David Chaum estivesse atrelado à lista de e-mails denominada de *Cypherpunks*, os protocolos de criptografia criados por sua empresa influenciaram o movimento de forma geral (Narayanan et. al., 2016).

A notoriedade do bitcoin, primeira criptomoeda lançada no mundo, se deu no contexto de turbulência das finanças internacionais. Apesar do documento de fundação ter sido divulgado pelo pseudônimo Satoshi Nakamoto no ano de 2008, o

[9] No original: "La nouveauté du Bitcoin ne réside pas dans son caractère « digital », « virtuel », « électronique » ou « numérique », comme beaucoup de commentateurs semblent le penser. Faire table rase d'un certain nombre de malentendus nous ramène à la question centrale de la nature de la monnaie. Il est important de distinguer d'une part les invariants théoriques, d'autre part les différentes formes qu'a pu prendre la monnaie au cours de l'histoire et ses différents modes de régulation. Si le Bitcoin apparaît bien comme un système de paiement, l'alternative qu'il propose repose dans l'absence d'autorité centrale et dans l'autorégulation de la monnaie cryptographique." (Lakomski-Laguerre e Desmedt, 2015).

desenvolvimento do conjunto de ideias que deu forma à estrutura tecnológica por trás do bitcoin teve sua origem nas concepções do movimento dos *cypherpunks*, termo que combina as ideias de criptografia (*cypher*) e de rebeldia (*punk*) (Assange et. al., 2012), ainda nos anos 1990. Nesse período, as interações entre economia e internet estimularam o surgimento de concepções relacionadas às liberdades de comunicação, bem como de realização de transações de forma privada. Os seus entusiastas argumentavam que, a partir da noção do uso da criptografia como instrumento de não-violência e combate às forças coercitivas do Estado, seria necessário estabelecer uma arquitetura sistêmica na qual as transações estivessem distribuídas de forma descentralizada entre os usuários, o que retiraria o poder de uma unidade central decisória em reter e interferir no registro de pagamentos e transações compensadas (Assange et.al, 2012).

No longo caminho para a construção das criptomoedas, o suporte às transações P2P é, sem dúvida, um elemento central para compreender o bitcoin. No entanto, no mundo digital, para a criação de uma moeda com atributos de livre circulação e com valor real baseada na escassez, como o ouro, a forma encontrada foi o desenvolvimento de um sistema no qual a emissão de moeda demandasse a resolução de um problema computacional (enigma) que tomasse certo tempo para ser solucionado. Esta ideia de atribuir algum tipo de valor a objetos digitais por meio da resolução de algoritmos computacionais foi elaborada na proposta do *hashcash* de Adam Back, cujo objetivo inicial envolvia o bloqueio de *spams* em e-mails (Narayanan et al., 2016).

As propriedades específicas das ideias do *hashcash* englobam quatro aspectos relevantes para compreender as criptomoedas. O primeiro diz respeito ao fato de que cada transação deve ter seu próprio enigma computacional a ser resolvido. Segundo, o usuário receptor na transação deve ser capaz de resolver facilmente o enigma sem ter que repetir o processo de solução. Em terceiro lugar, cada enigma deve ser totalmente independente dos outros, no sentido de que a resolução de um deles não diminua a quantia de tempo necessária à resolução de outro. Finalmente, quanto mais as partes (computadores) resolvem os enigmas, adquirindo aperfeiçoamento nas suas soluções, em termos de custo e velocidade (tempo), mais os enigmas das novas transações devem ser complexas, cujas funções de criptografia são intrínsecas (Narayanan et. al., 2016).

Diante disso, podem-se exemplificar as transações criptografadas da seguinte forma: Alice deseja enviar ao Bob uma mensagem de forma anônima. Para tanto, ela usa a criptografia que transforma informação a ser enviada em uma sequência alfanumérica, ou valor *hash*, cuja função é esconder a identidade dela, como ilustra a Figura 1. Para receber a mensagem, Bob precisa decodificar esta sequência criptografada, transformando-a na informação original (Lee, 2015).

**Figura 1:** Criptografia e valor *hash*

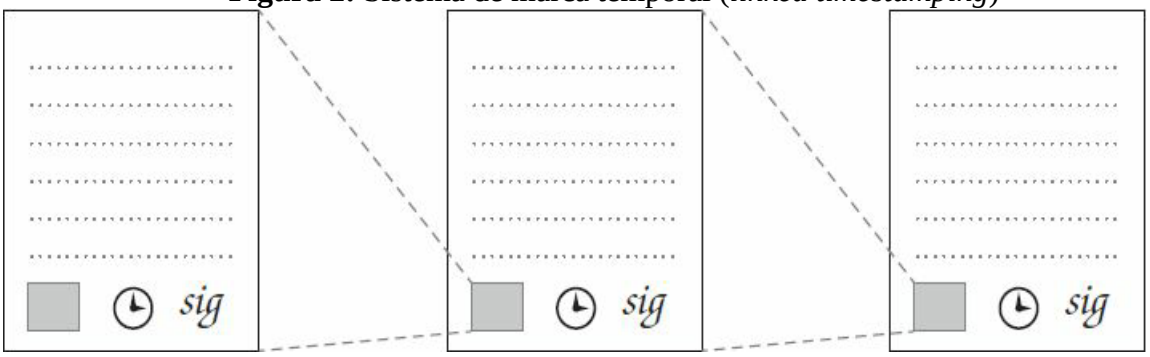
- ✓ **Informação Alice:** *Transferência de 100 bitcoins para Bob*
- ✓ **Valor *Hash*:** *46550fef 26f87ddd 5e15407f 45a0b8d2 9513291c 4e0f0acc*

**Fonte:** Elaboração própria com base em Lee (2015)

O conjunto dessas e de outras ideias se apresentaram reunidas no artigo de Nakamoto (2008), documento inaugural do bitcoin. Para Nakamoto (2008), uma criptomoeda pode ser definida como uma série de assinaturas digitais. Além disso, o fator estrutural-chave para o bitcoin, vale insistir, corresponde à tecnologia *blockchain*. Esta inovação pode ser entendida como um sistema de contabilidade no qual as

transações em bitcoins, ou criptomoedas, são registradas num livro-caixa (*ledger*). De modo geral, umas das propriedades importantes dessa rede de dados em que há o registro das transações é que, uma vez gravada, não há possibilidade de alteração *a posteriori.* O sistema é de caráter público (*open source) e é um arquivo computacional que aumenta de tamanho à medida que as transações são incorporadas no decorrer do tempo.* O conceito que dá alicerce à tecnologia *blockchain* corresponde ao sistema de marca temporal (*linked timestamping*), no qual os documentos estão encadeados e relacionados, já que o documento na sequência detém informações e a assinatura digital do documento prévio, formando uma série, certificando assim sua validade, conforme mostra a Figura 2 (Narayanan et. al., 2016).

**Figura 2:** Sistema de marca temporal (*linked timestamping*)




**Fonte:** Narayanan et al, 2016, p. 45

Embora próximo dessa dinâmica, o bitcoin apresentou uma novidade em relação ao *sistema de marca temporal*. Ao invés de estabelecer a ligação entre documentos digitais individuais, o aprimoramento consistiu em reunir os registros em uma lista que forma um bloco, ligando-o a outros, o que, subsequentemente, origina uma rede de blocos (*blockchain*). Essa estrutura promove a diminuição do número de vezes necessárias para a verificação de um documento em um ponto aleatório da história do sistema (Narayanan et. al. 2016). O *timestamping* garantiria, portanto, que os dados das transações existam no tempo, incluindo as datas e horas da transação anterior no código da moeda de modo a formar uma cadeia (Nakamoto, 2008). Isto é, todas as transações em bitcoin são registradas e sua validade está condicionada ao registro e aprovação do sistema, criando uma sequência de ações, conforme descrito por Nakamoto (2008, p.3):

> 1) Novas transações são transmitidas para todos os nós. 2) Cada nó coleta novas transações em um bloco. 3) Cada nó trabalha para encontrar uma *proof-of-work*[10] para seu bloco. 4) Quando um nó encontra um *proof-of-work*, ele transmite o bloco para todos os nós. 5) Os nós aceitam o bloco apenas se todas as transações nele são válidas e ainda não foram gastas. 6) Os nós expressam seu aceite do bloco trabalhando na criação do próximo bloco na cadeia, usando a *hash* do bloco aceito como *hash* anterior. (tradução livre)[11].

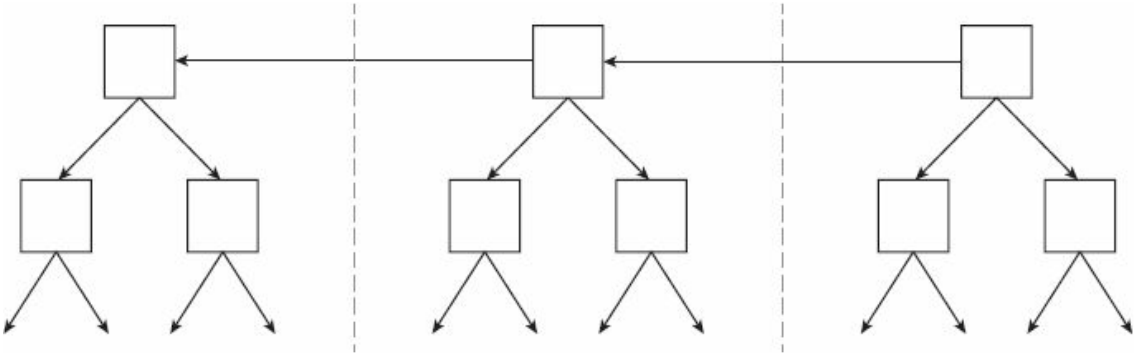
[10] *Proof-of-work* é um sistema que faz uma varredura para os valores das moedas, conferindo autenticidade às transações (Nakamoto, 2008). Em outras palavras, é um algoritmo que requer uma quantidade de trabalho para ser calculado, tal como o *hashcash*, cuja resolução atribui validade às informações incorporadas na rede de dados.

[11] No original: "1) New transactions are broadcast to all nodes. 2) Each node collects new transactions into a block. 3) Each node works on finding a difficult proof-of-work for its block. 4) When a node finds a proof-of-work, it broadcasts the block to all nodes. 5) Nodes accept the block only if all transactions in it are valid and not already spent. 6) Nodes express their acceptance of the block by working on creating

A disposição dos registros assume então o formato de um encadeamento de blocos, conforme pode ser verificado na Figura 3.

Diante desses esquemas, pode-se argumentar que Nakamoto (2008) uniu as ideias do protocolo dos enigmas computacionais do *hashcash* ao aperfeiçoamento do *timestamping* como forma de promover a segurança do sistema. Cada transação no livro-caixa (*ledger*) de caráter público não necessita ser garantido por uma terceira parte, tal como no *DigiCash*.

**Figura 3:** Sistema de marca temporal eficiente (e*fficient linked timestamping)*



**Fonte**: Narayanan et. al., 2016, p. 49

A descentralização do sistema de pagamentos é outra característica importante desta inovação tecnológica. Não é necessário que haja um intermediário que detenha todo o repositório de registro dos dados, já que as transações nesta cadeia de blocos utilizam uma rede de dados para aprovar uma determinada operação. Em outras palavras, removem-se, consequentemente, os custos de transação. Desse modo, o *blockchain* é uma base na qual as informações gravadas são públicas e mantidas, em escala global, por computadores que registram sequencialmente todos os lançamentos efetuados, inclusive transferências, pagamentos, conversões em outras moedas (Blundell-Wignall, 2014). Nesse sentido,

> [...] nós propomos uma solução para o problema da despesa dupla usando um servidor com carimbo de data e hora nas distribuições pessoa a pessoa para gerar prova computacional da ordem cronológica das transações. O sistema é seguro enquanto os nós honestos controlarem mais poder de CPU do que qualquer outro grupo cooperativo de nós atacantes. (Nakamoto, 2008, p. 1, tradução livre)[12].

Atualmente, os pagamentos realizados via internet a partir das transações realizadas são basicamente viabilizados por meio de instituições financeiras, plataformas de comércio e sistemas de pagamentos que funcionam como terceiras-partes intermediárias do processo. Ressalta-se que, com a crise financeira de 2008, muito da confiança nessas instituições foi perdido (Blundell-Wignall, 2014). Por este

---

the next block in the chain, using the hash of the accepted block as the previous hash." (Nakamoto, 2008, p. 3).

[12] No original: "[...] we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes." (Nakamoto, 2008, p. 1).

motivo, Nakamoto (2008) aponta que o sistema de pagamentos introduzido pelo bitcoin baseia-se, sobretudo, em um modelo de confiança. Trata-se de transações não-reversíveis com custos de transações que minimizam a possibilidade de efetivação de pequenas transações casuais.

A partir dessas considerações, Nakamoto (2008) ressalta a necessidade de uma moeda eletrônica que permita aos negociantes efetuarem suas transações sem intermediação de uma terceira-parte, sendo que a irreversibilidade do processo de pagamento impede fraudes e protege os usuários. O bitcoin atrai, principalmente, dois grupos de atores: entusiastas da tecnologia que o utilizam para comércio *online* e grupos com convicções políticas libertárias que aprovam a moeda por não ter conexão com governos (Yermack, 2014).

Yermack (2014) aponta, contudo, que o volume diário de 70 mil transações em bitcoins, então verificado, envolvia na maior parte as transferências entre investidores especulativos e não as compras de bens e serviços, o que indica sua pouca utilização como meio de pagamento. Ademais, porém não menos importante, há grande dificuldade em utilizar o bitcoin como unidade de conta, visto que a alta volatilidade de seu preço a cada dia exige que os preços em bitcoin das mercadorias sejam remarcados constantemente. Por fim, além da elevada volatilidade, as carteiras digitais, nas quais são mantidos os bitcoins, podem ser alvo de ataques cibernéticos, diminuindo a segurança de sua posse e, consequentemente, minando seu potencial de uso como reserva de valor. Esses fatos indicam que as criptomoedas, apesar da nomenclatura, não são moedas no sentido de cumprir as suas três funções fundamentais, a saber, meio de pagamento, padrão de preços e reserva de valor.

O uso das *moedas digitais*, entretanto, traz algumas questões, como a possibilidade de gerar volatilidade de mercado e fraudes, a emergência de novas moedas que podem ser consideradas melhores que outras, eliminando as primeiras da concorrência, além da necessidade de regulação. Levantamento da regulação nacional até 2014, apresentado por Blundell-Wignall (2014), indicava que alguns países haviam banido o uso do bitcoin, como a China, e outros, como Alemanha, França, Tailândia e Coreia do Sul, repudiaram o uso bitcoin como moeda. Ademais, o anonimato garantido pelas criptomoedas evita regulações financeiras, garantindo vantagens às atividades ilegais, como financiamento de terrorismo, lavagem de dinheiro e evasão fiscal.

Não obstante, as criptomoedas apresentam potencial para ter seu uso difundido, especialmente como meio de pagamento, pois não apresentam custos de estocagem e têm como vantagens a possibilidade de serem divididas digitalmente, bem como não necessitam de intermediários para suas trocas (Blundell-Wignall, 2014). Contudo, a utilização das criptomoedas envolve alguns problemas, como a questão dos preços negociados que devem ser indicados com quatro ou cinco casas decimais; as volatilidades dos preços e da taxa de câmbio diária dessas moedas, a qual, apesar de ser calculada em relação ao dólar, não tem nenhuma correlação com a taxa de câmbio desta ou de qualquer outra moeda, impedindo aos agentes calcularem possíveis riscos em relação ao preço, a potencial ocorrência de ataques cibernéticos e roubos virtuais (Yermack, 2014).

Atualmente, o uso dessas moedas é voltado, em grande medida, para pagamentos em mercados *online*, sendo seu uso comercial pouco relevante em escala mundial. O Fundo Monetário Internacional (FMI) destaca, também, o fato de que essas *moedas* não desempenham as três funções da moeda. Além da alta volatilidade de preços que limita seu uso como reserva de valor, o Fundo aponta para a restrição como meio de pagamento devido à sua aceitação limitada e para a pouca evidencia de que são

utilizadas como unidade de conta (International Monetary Fund, 2016). Essas *moedas* tampouco podem ser depositadas em bancos, como ocorre com moedas nacionais, sendo que sua posse ocorre por meio de carteiras virtuais, as quais não apresentam nenhuma garantia de segurança aos depósitos (Yermack, 2014).

No caso do bitcoin, em particular, a trajetória tendencial de aumento expressivo de seu preço em dólar pode ser explicada pela existência de uma regra rígida de criação de Bitcoin, associada ao aumento significativo de seu uso, ainda que relativamente restrito mundialmente, a ao processo especulativo que essa criptomoeda tem sofrido. Isso porque a oferta de Bitcoin provém da atividade de *mineração*, ou seja, da contribuição com a rede Bitcoin a partir de tecnologia empregada (processamento computacional) para permitir uma solução para o problema criptográfico envolvido em um bloco de transações com o uso da criptomoeda[13]. O processo de criação de BTC[14] funciona do seguinte modo: os dados de uma transação envolvendo BTC são transmitidos para todos aqueles que participam da rede (nós P2P), sendo que para a transação ser viabilizada ela precisa ser processada (atividade dos mineradores), ou seja, o problema criptográfico deve ser resolvido. Atualmente, o minerador recebe 25 BTCs para cada bloco de transações descoberto, um pagamento por ter concedido seu poder computacional viabilizar as transações realizadas em BTC. Isso, vale observar, desde que os demais participantes da rede aceitem o bloco de transações descoberto, de tal modo a torná-lo parte da cadeia de consenso. Além desse subsídio, os mineradores também podem ser recompensados por taxas das transações oferecidas opcionalmente pelos usuários de BTC e incluídas nos blocos candidatos dos mineradores. As taxas são oferecidas pelos usuários de BTC para que suas transações sejam priorizadas pelos mineradores na formação de seus blocos candidatos, aumentando, assim, a chance de a transação ser viabilizada mais rapidamente.

A regra rígida de criação de bitcoin diz respeito ao fato de que a criação de novos BTC depende, exclusivamente, da atividade de mineração, a partir da seguinte sistemática: 50 BTC para a inserção de um novo bloco de transações na cadeia de blocos (blockchain) a cada 10 minutos, nos primeiros quatro anos de sua existência; de 25 BTC a partir do quinto ano, sempre a cada 10 minutos (inserção de um novo bloco na cadeia de blocos), até atingir 210 mil blocos. E sendo reduzido esse subsídio à metade a cada 210 mil blocos. Com essa redução à metade da recompensa da atividade de mineração a cada quatro anos, em média, chega-se ao limite máximo arbitrário de 21 milhões de BTC em 2140, estima-se. Essa rigidez de oferta de novos BTC implica o fenômeno de *orfanização de bitcoins* no sistema, introduzindo um viés deflacionário ao bitcoin. Esse elemento também condiciona, evidentemente, a especulação com essa criptomoeda, diante de seu uso crescente, embora mundialmente ainda restrito, vis-à-vis uma oferta pouco sensível ao ritmo de crescimento da demanda por BTC.

Portanto, a elevada rigidez de criação de bitcoins dificulta a sua transformação em moeda de fato, uma vez que a alta variabilidade de seu preço dificulta que essa criptomoeda assuma as funções indispensáveis da moeda, introduzindo, inclusive, uma

[13] O processo de mineração tem sido viabilizado, cada vez mais, a partir de circuitos integrados de aplicação específica, em substituição às CPUs, as quais se tornaram obsoletas para realizar a solução dos problemas criptográficos de forma rentável para o minerador, já que o custo de energia decorrente da mineração supera a recompensa em bitcoin gerada pela atividade. Atualmente, a atividade de mineração é realizada a partir de software de mineração bitcoin e hardware especializado, envolvendo elevada competição. A sofisticação crescente da atividade de mineração tornou a *mineração doméstica* ou *individual* inviável economicamente. Hoje em dia, a atividade é realizada *data centers* de mineração altamente profissionalizados.

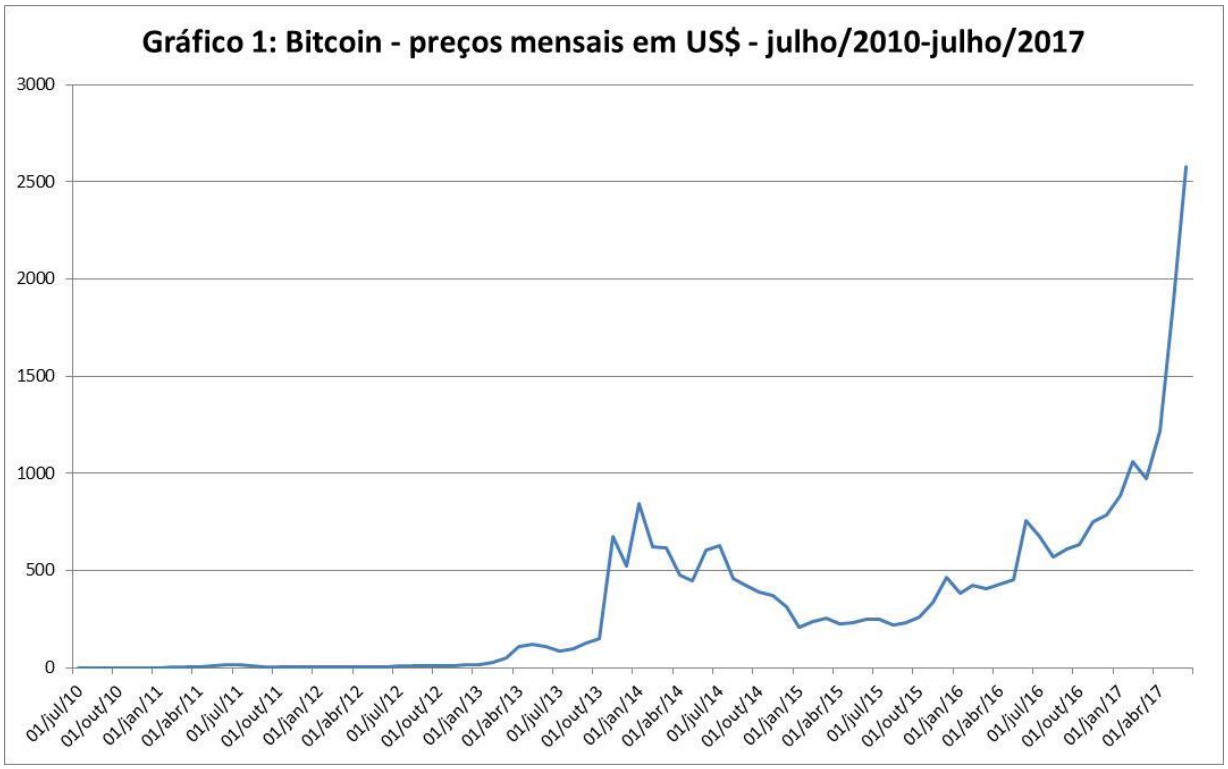
[14] Símbolo utilizado para representar o bitcoin.

tendência deflacionária ao sistema. Ironicamente, pois, os defensores do bitcoin sustentavam que essa nova *moeda* evitaria processos inflacionários, sobretudo, decorrentes de regras de emissão monetária frouxas, quando existentes, praticadas pelos bancos centrais. Deixaram de considerar, contudo, que a sistemática rígida de criação de bitcoins frente à demanda crescente introduz elevada variabilidade e tendência deflacionária ao bitcoin. Afinal, não há bancos capazes de criar BTC nesse sistema, sendo que uma economia capitalista constitui um sistema fundamentalmente de endividamento. Não por acaso, o principal meio de acesso aos bitcoins se dá no âmbito das plataformas de câmbio dedicadas. Por isso, de acordo com Lakomski-Laguerre e Desmedt (2015):

> Como você consegue bitcoins? Se formularmos a hipótese de um circuito fechado e um raciocínio fechado, seria lógico assumir que o acesso aos bitcoins decorre de uma venda (de bens, serviços, força de trabalho) significando uma contribuição para a produção (do espaço comercial correspondente). Embora seja possível obter bitcoins em troca da venda de bens ou serviços dentro de uma rede de comerciantes que os aceitam, esta consideração é, por outro lado, ainda extremamente limitada. De fato, o acesso a bitcoins é principalmente através da venda de moedas oficiais em plataformas de negociação dedicadas a um preço de mercado que flutua com a oferta e demanda. Portanto, o bitcoin torna-se uma divisa entre outras em um espaço monetário globalizado e competitivo e, portanto, pode ser usado como um ativo específico por qualquer investidor motivado por uma lógica financeira de otimização de portfólio. Com a valorização fenomenal que tem sido sujeita desde a sua criação e a volatilidade do seu preço em relação às moedas oficiais, é claro que hoje, o bitcoin parece muito mais como um ativo especulativo do que como um meio de pagamento. (tradução livre)[15].

A teoria do *greater fool* também pode explicar o rápido crescimento da procura por bitcoin, uma vez que pode haver uma alta demanda especulativa em que os agentes acreditam que vale adquirir a moeda por um valor 10 ou 20 vezes superior, pois haverá outro agente disposto a comprar essa moeda por outro valor ainda maior do que o primeiro. Nesse sentido, a volatilidade do valor do bitcoin não se relaciona, necessariamente, ao valor justo da moeda (Blundell-Wignall, 2014). No Gráfico 1 é possível notar a tendência crescente do preço do bitcoin em dólar, bem como os movimentos de forte oscilação de seu preço, com destaque à sua significativa desvalorização entre o início de 2014 e o começo de 2015.

[15] No original: "Comment obtient-on des bitcoins? Si nous émettons l'hypothèse d'un raisonnement en circuit fermé et bouclé sur lui-même, il serait alors logique de penser que l'accès aux bitcoins s'effectue en contrepartie d'une vente (de marchandises, de services, de la force de travail) signifiant une contribution à la production (de l'espace marchand correspondant). S'il est possible d'obtenir des bitcoins en échange de la vente de biens ou de services au sein d'un réseau de marchands qui les accepte, cette contrepartie est, en revanche, encore extrêmement limitée. De fait, l'accès aux bitcoins s'effectue principalement par la vente de devises officielles sur des plateformes d'échanges dédiées, à un cours de marché qui fluctue en fonction de l'offre et de la demande. Dès lors, le bitcoin devient une devise parmi d'autres dans un espace monétaire mondialisé et concurrentiel et il peut, de ce fait, être utilisé comme actif spécifique par tout investisseur motivé par une logique financière d'optimisation de portefeuille. Avec la valorisation phénoménale dont il a fait l'objet depuis sa création, et la volatilité de son cours relativement aux devises officielles, force est de constater qu'aujourd'hui, le bitcoin apparaît bien plus comme un actif spéculatif que comme un instrument au service d'une économie d'échanges et de paiements." (Lakomski-Laguerre e Desmedt, 2015).




**Fonte:** elaboração própria, a partir de Coindesk, 2017.

## 4 A reação dos grandes bancos internacionais

Nesta seção, discute-se como o sistema bancário, sob a liderança dos grandes bancos internacionais, tem reagido aos impactos relevantes provocados pelo uso, pelo desenvolvimento e pela aplicação da tecnologia *blockchain*, chamando a atenção para o fato de que essas instituições têm atuado de forma altamente ativa nesse âmbito.

Certamente, maior do que a inovação das criptomoedas foi a tecnologia que as tornaram possíveis, a saber, a tecnologia *blockchain*. Trata-se de uma tecnologia de alto impacto, capaz de gerar grandes mudanças nos sistemas financeiros nacionais e internacional. Isso porque essa tecnologia facilita a transferência de dados, atribuindo maior eficiência e segurança às transações financeiras, tanto em termos de tempo como de custos de transação. Segundo JPMorgan (2017, p. 3), isso em razão, sobretudo, "de dados compartilhados e protegidos a partir de um padrão comum, baixa necessidade de reconciliação e transferência contínua de ativos digitais" (tradução livre)[16], altamente funcional para o sistema financeiro moderno, não-descentralizado. Isso porque a tecnologia *blockchain*, ao permitir uma infraestrutura simplificada, ágil e eficiente, além dos efeitos positivos mais imediatos sobre o *backoffice* e o processo internos dessas instituições, tem o potencial de permitir a transferência de dados em alta velocidade, viabilizando flexibilidade de liquidação de contratos capaz de viabilizar modelos de precificação e de oferta de serviços altamente inovadores (JPMorgan, 2017, p. 4). Por isso, de acordo com o JP Morgan (2017, p. 3):

> O conceito da tecnologia do livro contábil – ou *blockchain* como é comumente chamado – causou tempestade no setor de serviços financeiros,

[16] No original: "shared data with common standards; reduced need for reconciliation; and seamless transfer of digital assets" (JPMorgan, 2017, p 3).

> com capital de risco e investimentos fluindo para as startups de tecnologia. O debate sobre as promessas do *blockchain*, bem como suas limitações, está em andamento. Para cada entusiasta que diz que o *blockchain* é a plataforma tecnológica mais revolucionária a emergir desde a internet, há céticos que defendem que é apenas a mais recente tulipa.
> Entretanto, emerge um amplo consenso que isso representa uma inovação real sobre muitos dos outros sistemas e processos usados nos serviços financeiros e bancários hoje. (tradução livre)[17].

Não por outra razão, os investimentos em startups que fazem uso do *blockchain* têm crescido expressivamente em todo o mundo, especialmente no segmento das chamadas *Fintechs*, sobretudo nos EUA. Os grandes bancos internacionais estão muito atentos a essa combinação entre P2P Networking, criptografia assimétrica e *hashing* criptográfico (*Cryptographic hashing*)[18], subjacente ao bitcoin. Contudo, no caso dessas instituições, diferentemente das criptomoedas, essa tecnologia tem sido apropriada, desenvolvida e aplicada dentro de um marco regulatório e institucional autorizado pelo Estado. Isso porque ela permite a descentralização da confiança dos agentes (por requerer a anuência dos demais participantes da rede) e um sistema de processamento de dados potencialmente capaz de viabilizar milhares de transações por segundo, muito mais que os bancos de dados hoje utilizados pelos bancos (JPMorgan, 2017).

O *blockchain* tem o potencial de permitir a diminuição do risco das garantias, atribuir viabilidade ao cálculo em tempo real do risco do ativo subjacente e, assim, uma precificação mais acurada dos ativos, possibilitar maior segmentação e posicionamento de produtos e serviços financeiros, propiciar economias de escala e escopo das instituições financeiras bancárias e não-bancárias, viabilizar um sistema mais eficiente de gerenciamento de ativos, entre outros. Enfim, o uso do *blockchain* tende a permitir uma utilização mais eficiente dos recursos, proporcionando maior celeridade nas operações e menores cursos de produtos e serviços financeiros oferecidos nos diferentes segmentos de atuação dos bancos, em particular, e do sistema financeiro, em geral (JPMorgan, 2017). Por isso, afirma JPMorgan (2017, p.4): "*Nossa visão é que o impacto do blockchain pode eventualmente remodelar estrutura do mercado, capacidades do produto e experiência do cliente, tendo finalmente uma influência duradoura sobre o sistema econômico global"* (tradução livre)[19].

Isso mostra, portanto, que a tecnologia *blockchain* está muito além do surgimento e da viabilização das denominadas criptomoedas, pois tem sido cada vez mais utilizada por corporações inseridas na ordem monetária vigente. Recentemente, grandes bancos internacionais se uniram ao banco de investimento suíço UBS de modo

---

[17] No original: "The concept of distributed ledger technology — or blockchain as it is commonly called — has taken the financial services sector by storm, with venture capital and investment pouring into technology startups. Debate over blockchain's promise, as well as its limitations, is ongoing. For every believer who says blockchain is the most revolutionary technology platform to emerge since the internet, there are skeptics who claim it is merely the latest tulip mania.
Nonetheless, a broad consensus is emerging that it represents a real innovation over many of the systems and processes used in financial services and banking today." (JP Morgan, 2017, p. 3).

[18] De acordo com JPMorgan (2017, p.3), enquanto a criptografia assimétrica diz respeito à possibilidade de transferência de informações passível de verificação de autenticidade do remetente, mas com a permissão de apenas os destinatários terem capacidade de ter acesso ao conteúdo dessas informações, o *hashing* criptográfico corresponde à capacidade de comparação e certificação de grande conjunto de dados (informações).

[19] No original: "Our view is that blockchain's impact may eventually reshape market structure, product capabilities and the client experience, ultimately having a lasting influence on the global economic system." (JP Morgan, 2017, p. 4).

a criar uma moeda virtual que possa compensar e liquidar transações financeiras e que comece a ser operada ao final de 2018. A iniciativa busca superar as dúvidas e riscos de fraudes que envolvem a tecnologia *blockchain* e, por esse motivo, bancos centrais e agências reguladoras também têm participado dos diálogos sobre o tema (Valor Econômico, 2017).

O projeto visa tornar os mercados financeiros mais eficientes, por meio da criação de uma moeda que permita compensações e liquidações. Redução de riscos, aceleração dos sistemas de liquidação de *back-office*, liberação de capital para operações financeiras internacionais são apenas algumas das metas do UBS em parceria com grandes bancos internacionais (Valor Econômico, 2017).

> A moeda de liquidação, baseada em um produto desenvolvido pela Clearmatics Technologies, tem como objetivo permitir que grupos financeiros realizem pagamentos entre si ou comprem instrumentos financeiros, como títulos e ações, sem esperar que as tradicionais transferências de dinheiro sejam concluídas. Em vez disso, eles usariam moedas digitais diretamente conversíveis em dinheiro nos bancos centrais, reduzindo o tempo, custo e capital necessários para a compensação e liquidação pós-negócios. As moedas digitais, cada uma delas conversíveis em diferentes divisas, seriam armazenadas usando o blockchain – um esquema de contabilidade distribuída -, permitindo que sejam trocadas rapidamente pelos instrumentos financeiros negociados. (Valor Econômico, 2017).

De acordo com o UBS (2017), em completa sintonia com J.P,Morgan (2017) a esse respeito, a tecnologia *blockchain* pode permitir uma reformulação do sistema financeiro, tornando suas transações menos caras e mais simples, além de garantir, por um lado, maior controle e privacidade sobre as transações financeiras aos indivíduos e, por outro, mecanismos melhores de monitoramento e proteção aos agentes reguladores.

O Banco ressalta ainda dificuldades técnicas, sistêmicas, de legalidade e regulatórias que podem surgir da tecnologia *blockchain*, como a necessidade de operar as transações com velocidade, escala e segurança; como transferir dinheiro real na cadeia; questões de privacidade e identidade digitais; como serão feitos os contratos relativos às transações realizadas pela nova tecnologia; e como será a jurisdição internacional que regulará o *blockchain*, protegendo tanto indivíduos quanto o sistema financeiro (UBS, 2016).

Tendo em vista esses pontos, em 2016, a parceria inicial entre o UBS, o Deutsche Bank, Banco Santander, BNY Mellon e a empresa de tecnologia financeira (*fintech*) Clearmatics, e que hoje conta com outros bancos internacionais como NEX, Barclays, Credit Suisse, Canadian Imperial Bank of Commerce, HSBC, MUFG e State Street (Valor Econômico, 2017) lançou a USC (*utility settlement coin*), a moeda digital baseada na tecnologia *blockchain* de modo que:

> [...] as instituições financeiras possam usar para transacionar diretamente *securities* entre si, contornando o processo tradicional de liquidações. [...] o USC pretende ser diretamente convertido na moeda do banco central. Assim, os bancos podem reduzir significativamente o tempo e o custo de liquidação e compensação pós-negociação. (UBS, 2016, tradução livre)[20].

[20] No original: "[…] financial institutions could use to directly transact securities with each other, bypassing the traditional settlement process. […] the USC is intended to be directly convertible into central bank cash. With it, banks could significantly reduce the time and cost of post-trade settlement and clearing." (UBS, 2016).

Para Hyder Jaffrey, chefe de investimento estratégico e inovação de tecnologia financeira do UBS, o USC poderá tanto auxiliar a gerir melhor o risco bancário quanto aumentar a eficiência do capital. Ele ressalta que a iniciativa não será uma nova criptomoeda (*criptocurrency*), mas um novo *criptocash*, visto que será uma forma de representar as moedas nacionais em um registro contábil, ou seja, um valor em USC corresponderá ao mesmo valor em moeda nacional. Portanto, *"o dinheiro está no registro contábil e sempre será apoiado por dinheiro real mantido no banco central – da mesma forma que o dinheiro é tecnicamente uma nota promissória que costumava ser lastreado por ouro"*. (Financial Institutions Hub, 2017, tradução livre)[21].

De acordo com Jaffrey, é possível delinear um espectro para as criptomoedas: em um extremo, estariam aquelas sem regulação e fora do controle governamental, como o bitcoin; no outro extremo, as criptomoedas dos bancos centrais as quais são moedas digitais do tipo criptográfica das moedas existentes. No meio desse espectro, estaria o USC, marcado por características do bitcoin, como a capacidade de liquidar transações em tempo real, e por características das moedas reais dos bancos centrais, visto que por ser lastreado nessas moedas terá sempre o mesmo valor, ou seja, não sofrerá as variações de preço como o bitcoin (Financial Institutions Hub, 2017). Ele aponta ainda as possíveis vantagens envolvidas:

> O USC pode ser visto como um facilitador essencial para mudanças significativas dentro dos modelos institucionais bancários. O USC combinado com outros blocos como a identidade digital será transformador. Modelos novos e altamente eficientes para liquidações, para gestão colateral, para conhecer clientes, anti-lavagem de dinheiro, para informar, etc serão possíveis. Outra iteração permitirá securities totalmente digitais como títulos, ações e derivativos digitais presentes em um mercado de Transações Contábeis Distribuídas. (Financial Institutions Hub, 2017, tradução livre)[22].

O JPMorgan Chase, em parceria com o Royal Bank of Canada e o Australia and New Zealand Banking Group, por sua vez, anunciou o lançamento do Interbank Information Network (IIN) em meados de outubro de 2017, um sistema de transferências interbancárias baseado em tecnologia *blockchain* própria que irá viabilizar a redução significativa do tempo de transferência de recursos entre os bancos em escala global, em razão da redução do tempo necessário para verificação dos pagamentos. De acordo com o banco, esse prazo será reduzido de semanas para apenas algumas horas. É emblemático o fato de o CEO e Chairman do JPMorgan Chase, Jamie Dimon, depois de ter afirmado no mês anterior ao lançamento do IIN que o bitcoin é uma "fraude" que "não vai acabar bem", quando do anúncio do IIN declarar que "O blockchain é uma tecnologia que é uma boa tecnologia. Nós realmente usamos isso. Será útil em muitas coisas diferentes. Deus abençoe a cadeia de blocos"[23] (Cheng, 2017).

---

[21] No original: "[...] cash is on the ledger and will always be backed by real cash held at the central bank – in much the same way cash is technically a promissory note that used to be backed by physical gold." (Financial Institutions Hub, 2017).

[22] No original: "USC can be viewed as an essential facilitator to significant change within institutional banking models. USC combined with other building blocks like digital identity will be transformational. New and highly efficient models for settlement, collateral management, know your customer (KYC), anti-money laundering (AML), reporting, etc. will all be made possible. A further iteration will start to enable new fully digital securities such as digital bonds, equities and derivatives that all live on a Distributed Ledger marketplace." (Financial Institutions Hub, 2017).

[23] No original: "The blockchain is a technology which is a good technology. We actually use it. It will be useful in a lot of different things, God bless the blockchain." (Cheng, 2017).

Esses movimentos, em seu conjunto, mostram que os grandes bancos internacionais têm não apenas reagido ao surgimento da tecnologia *blockchain*, mas, mais do que isso, atuado de forma altamente ativa e estratégica nesse processo, seja mediante parcerias e aquisições de *Fintechs*, seja a partir de avanços relevantes no desenvolvimento e na aplicação dessa tecnologia em suas operações. Essas instituições sabem, muito bem, que para além das criptomoedas, a tecnologia *blockchain* representa um ativo capaz de remodelar o sistema financeiro baseado na moeda estatal e, sobretudo, na moeda bancária. Isso, certamente, os entusiastas das criptomoedas, desreguladas e descentralizadas, não esperavam.

## 5 Desafios para a regulação

Apresenta-se aqui uma breve discussão sobre os desafios que a regulação financeira enfrenta diante da aplicação da tecnologia *blockchain* em inovações financeiras não reguladas, como o bitcoin.

O uso da tecnologia *blockchain* para o surgimento e a utilização de criptomoedas levanta questões sobre sua regulação e novas formas de crimes internacionais. Um primeiro problema em relação à regulação das moedas virtuais é a dificuldade em definir o que são de fato tais moedas, visto que combinam características de moedas, sistemas de pagamentos e *commodities*. Nesse sentido, seria necessária uma padronização da classificação para que as autoridades regulatórias possam aplicar as mesmas políticas regulatórias. Por serem descentralizadas e transnacionais, as transações em moedas virtuais tornam-se não apenas difíceis de rastrear, mas também de serem submetidas a uma jurisdição, sendo preciso definir regulações para além das fronteiras nacionais e que sejam diferentes dos modelos tradicionais de regulação. É possível destacar ainda que os países têm lidado de forma diferente com essas moedas, alguns baniram seu uso, como a Bolívia e a Rússia, enquanto outros têm alertado para os riscos que as envolvem (International Monetary Fund, 2016).

No 13º Congresso da Organização das Nações Unidas sobre Prevenção de Crime e Justiça Criminal, em 2015, em documento de trabalho elaborado sobre meios de prevenção e respostas a novas formas de crimes transnacionais, os crescentes pagamentos por meio de moedas virtuais anônimas são apontados como mecanismo para financiamento de grupos terroristas, bem como forma de incitar violência *online*. O relatório aponta ainda que as novas tecnologias de anonimato na internet podem encorajar o envolvimento de mais indivíduos com atividades criminosas, dadas as dificuldades em identificar e aplicar leis sobre aqueles que cometem tais crimes, e que as moedas virtuais, especificamente, podem ser um novo *modi operandi* para o crime transnacional (United Nations, 2015a).

No mesmo sentido, o FMI (2016) aponta que riscos como lavagem de dinheiro, financiamento de terrorismo e evasão fiscal podem ser associados ao anonimato da tecnologia, a qual pode, inclusive, trazer riscos à proteção dos consumidores e à estabilidade financeira, caso o volume de transações aumente consideravelmente, além de questões relacionadas à regulação de movimentos de capitais. Ademais, a instituição aponta que a tecnologia *blockchain* seria menos preocupante do que as moedas virtuais, pois pode ser utilizada em sistemas fechados administrados e regulados pelas instituições financeiras.

No Congresso da ONU, foi ressaltada também a necessidade de fortalecimento de parcerias entre autoridades responsáveis pela aplicação de leis e pesquisadores para o desenvolvimento de técnicas que permitam investigar e caracterizar as transações em moedas virtuais. Recomendou-se aos países membros da Organização que técnicas de

investigação em relação ao uso das moedas virtuais para lavagem de dinheiro, dentre outros crimes via internet como fraudes financeiras e tráfico online de drogas, sejam compartilhadas, de modo a desenvolver as habilidades necessárias às autoridades no combate a tais crimes (United Nations, 2015b).

Para o United Nations Office on Drugs and Crime (UNODC), alguns desafios investigativos envolvem as moedas virtuais como a dificuldade de aplicar as leis sobre os usuários devido ao caráter anônimo que dificulta a identificação e detecção de possíveis criminosos; a existência de poucas ferramentas e técnicas que permitam investigar as ações envolvendo tais moedas; o fato de que todas as evidências de crimes executados por meio dessas moedas serão eletrônicas, o que exige novas formas de investigação e aplicação de leis. A agência da ONU aponta que a elaboração de relatórios sobre o tema, a conscientização pública e institucional, a harmonização das questões jurídicas e a cooperação entre agências devem ser medidas a serem adotadas (United Nations Office on Drugs and Crime, 2016).

Algumas opções que vêm sendo adotadas envolvem aplicar as regulações sobre os participantes desse mercado ou sobre instituições, como os bancos, restringindo sua interação com os participantes. Em nível internacional, múltiplas agências têm promovido discussões sobre as moedas internacionais, apontando riscos e benefícios associados a seu uso, buscando identificar áreas de cooperação entre Estados e instituições para regulação e supervisão, bem como desenvolvimento de tecnologias para lidar com a inovação e troca de experiências bem sucedidas que possa resultar em padrões de investigação e processamento jurídico (International Monetary Fund, 2016).

Ainda em 2013, Financial Crimes Enforcement Network (FinCEN), ligado ao Departamento do Tesouro dos Estados Unidos, lançou um comunicado sobre a aplicação de regulações sobre usuários (aqueles que possuem moedas virtuais para compra de bens e serviços), administradores (que conseguem colocar e tirar as moedas de circulação) e indivíduos que trocam moedas virtuais (aqueles que visam trocar as moedas virtuais por moedas reais), ou seja, pessoas que criam, obtêm, distribuem, trocam, aceitam ou transmitem tais moedas. Para o FinCEN, a moeda virtual não tem *status* legal em nenhuma jurisdição (Financial Crimes Enforcement Network, 2013).

Em relatório da Comissão Econômica para a América Latina e o Caribe (CEPAL), foram levantados os riscos e oportunidades envolvendo as moedas virtuais. Para a Comissão, a visão negativa associada aos propósitos criminosos do uso de tais moedas minimiza a possibilidade de governos e populações confiarem na indústria dessas moedas de modo a aproveitar os benefícios potenciais da tecnologia. No relatório, ressalta-se a necessidade de diálogo entre os criadores da tecnologia e os membros do Estado para que leis e mecanismos regulatórios possam ser desenvolvidos, visando à utilização dos sistemas baseados em moedas virtuais em prol da sociedade (CEPAL, 2015).

Se, por um lado, as moedas virtuais facilitam atividades ilícitas e crimes cibernéticos, por outro, resolvem o problema do duplo gasto associado às primeiras formas de moedas eletrônicas. Para evitar a utilização em atividades criminosas, é preciso que as transações sejam investigadas a fundo e que sistemas para reconhecimento dos clientes sejam desenvolvidos, de modo que as transações anônimas possam ser rastreadas (CEPAL, 2015).

## 6 Conclusões

Embora as criptomoedas constituam uma inovação importante, a grande inovação financeira envolvida nesse âmbito diz respeito à tecnologia *blockchain*. E os grandes bancos internacionais têm se posicionado muito ativamente nesse processo.

Isso significa duas coisas relevantes, a saber: i) as criptomoedas em geral, e o bitcoin, em particular, embora representem uma inovação financeira importante, estão muito longe de modificar a ordem monetária vigente, baseada na moeda estatal e na moeda bancária, em um futuro minimamente previsível; e ii) a maior inovação por detrás das criptomoedas, que as viabilizou e leva alguns a prever uma possível nova ordem monetária desregulada e descentralizada, a tecnologia *blockchain*, tem sido não apenas incorporada, mas desenvolvida e operada pelos grandes bancos internacionais. Isso restringe a construção de uma nova ordem monetária baseada nas criptomoedas, sem bancos e banco central.

Considerando o conceito atual de criptomoedas, é muito difícil imaginar ou antever uma ordem monetária desregulada. Além das questões estritamente monetárias e financeiras, o controle sobre o dinheiro pelos Estados-nação constitui um dos pilares fundamentais da soberania dos Estados e da hegemonia dos países centrais no sistema monetário e financeiro internacional.

Uma economia capitalista é, essencialmente, uma economia de endividamento. O *blockchain*, talvez, a partir da tecnologia P2P e, assim, do melhoramento dos modelos de precificação, pode atenuar os riscos do sistema, mas sem eliminar sua tendência a gerar sempre perturbações e instabilidades em meio a seu grande dinamismo.

A ideia de uma ordem monetária baseada no uso da tecnologia *blockchain* não é apenas possível, mas parece ser a macrotendência dos sistemas financeiros modernos, haja vista o processo de internalização, desenvolvimento e aplicação dessa tecnologia que os grandes bancos têm realizado. Esse processo pode tornar o sistema bancário ainda mais eficiente nas suas operações, inclusive no financiamento no sistema interbancário.

## Referências


ASSANGE, Julian; APPELBAUM, Jacob; MULLER-MAGUHN, Andy; ZIMMERMANN, Jerémie. **Cypherpunks:** Freedom and the Future of the Internet. OR books, 2016.

BELLUZZO, Luiz Gonzaga de Mello; ALMEIDA, Julio Gomes de. **Depois da queda**: a economia brasileira da crise da dívida aos impasses do Real. Rio de Janeiro: Civilização Brasileira, 2002. Cap.1.

BISSESSAR, Shiva. 2016. **Opportunities and risks associated with the advent of digital currency in the Caribbean.** CEPAL: Subregional Headquarters for the Caribbean. Disponível em: <https://www.cepal.org/en/publications/39860-opportunities-and-risks-associated-advent-digital-currency-caribbean>. Acesso em: 7 set. 2017.

BLANC, Jérôme. 1998. **Las monedas paralelas:** evaluación y teorias del fenómeno. Disponível em: <https://halshs.archives-ouvertes.fr/halshs-00111649>. Acesso em: 26 ago. 2017.

BLUNDELL-WIGNALL, Adrian. **The Bitcoin Question:** Currency versus Trust-less Transfer Technology, OECD Working Papers on Finance, Insurance and Private Pensions, No. 37, OECD Publishing. 2014. Disponível em: <http://dx.doi.org/10.1787/5jz2pwjd9t20-en>. Acesso em: 22 maio 2017.

COINDESK. **Bitcoin price.** Disponível em: <http://www.coindesk.com/price/>. Acesso em: 4 jul. 2017.

CEPAL – Comissão Econômica para a América Latina e o Caribe. 2015. **Report of the second expert group meeting on opportunities and risks associated with the advent of digital currency in the Caribbean.** Disponível em: <http://repositorio.cepal.org/bitstream/handle/11362/38260/LCCARL461_en.pdf?sequence=1>. Acesso em: 26 ago. 2017.

CHENG, Evelyn. **Jamie Dimon is betting big on the technology behind 'fraud' bitcoin**. Disponível em: < https://www.cnbc.com/2017/10/16/jpmorgans-dimon-betting-on-blockchain-even-as-he-calls-bitcoin-stupid.html>. Acesso em: 20 out. 2017.

DE CONTI, Bruno Martarello; PRATES, Daniela Magalhães; PLIHON, Dominique. O sistema monetário internacional e seu caráter hierarquizado. In: CINTRA, M. A. M.; MARTINS, A. R. A. (orgs.). **As transformações no sistema monetário internacional**. Brasília: IPEA, 2013.

FINANCIAL INSTITUTIONS HUB. 2017. **Interview:** Banking on the Blockchain. Disponível em: <http://financialinstitutions.bakermckenzie.com/2017/06/07/banking-on-the-blockchain/>. Acesso em: 05 set. 2017.

FINANCIAL CRIMES ENFORCEMENT NETWORK. 2013. **Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies.** Disponível em: <https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering>. Acesso em: 19 set. 2017.

HAYEK, Friedrich. [1976] **Denationalisation of Money**: The Argument Refined. An Analysis of the Theory and Practice of Concurrent Currencies, London, The Institute of Economic Affairs, 3rd edition, 1990.

INTERNATIONAL MONETARY FUND, 2016. **Virtual Currencies and Beyond:** Initial Considerations. Disponível em: <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf >. Acesso em: 26 ago. 2017.

JPMorgan. Unlocking Economic Advantage with Blockchain: a guide for asset managers. New York: JPMorgan, 2017.

KEYNES, John Maynard. (1936) **A teoria geral do emprego, do juro e da moeda**. 3. ed. São Paulo: Nova Cultural, 1985. (Os economistas).

LAKOMSKI-LAGUERRE, Odile; DESMEDT, Ludovic. L'alternative monétaire Bitcoin: une perspective institutionnaliste. Revue de la régulation. 18 | 2e semestre/Autumn 2015: Contestations monétaires. Une économie politique de la monnaie.

LEE, Larissa. **New Kids on the Blockchain**: How Bitcoin's Technology Could Reinvent the Stock Market. Hastings Bus. LJ, v. 12, p. 81, 2015.

NAKAMOTO, Satoshi. 2008. **Bitcoin:** A Peer-to-Peer Electronic Cash System. 9p. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 22 maio 2017.

NARAYANAN, Arvind; BONNEAU, Joseph; FELTEN, Edward; MILLER, Andrew; GOLDFEDER, Steven. **Bitcoin and Cryptocurrency Technologies: A comprehensive Introduction**. Princeton University Press, 2016.

PRATES, Daniela Magalhães. As assimetrias do sistema monetário e financeiro internacional. **Revista de Economia Contemporânea**, Rio de Janeiro - RJ mai/ago, v. 9, n.2, p. 263-288, 2005.

SCHUMPETER, Joseph. (2005). **Théorie de la Monnaie et de la Banque**, 2 vol. , Paris, L'Harmattan.

UBS. 2016. **Building the trust engine.** Disponível em: <https://www.ubs.com/magazines/news-for-banks/en/products-and-services/2016/building-the-trust-engine.html>. Acesso em: 05 set. 2017.

UNITED NATIONS. 2015a. **Thirteenth United Nations Congress on Crime Prevention and Criminal Justice:** Working Paper - Comprehensive and balanced approaches to prevent and adequately respond to new and emerging forms of transnational crime. Disponível em: <https://www.unodc.org/documents/congress/Documentation/A-CONF.222-8/ACONF222_8_e_V1500538.pdf>. Acesso em: 26 ago. 2017.

_____. 2015b. **Thirteenth United Nations Congress on Crime Prevention and Criminal Justice:** Background Paper - Workshop 3: Strengthening crime prevention and criminal justice responses to evolving forms of crime, such as cybercrime and trafficking in cultural property, including lessons learned and international cooperation. Disponível em: <https://www.unodc.org/documents/congress/Documentation/A-CONF.222-12_Workshop3/ACONF222_12_e_V1500663.pdf>. Acesso em: 26 ago. 2017.

UNITED NATIONS OFFICE ON DRUGS AND CRIME. 2016. **Anti corruption alert: laundering of crime proceeds using virtual currencies.** Disponível em: <http://www.unodc.org/documents/indonesia//publication/alert/POIDN_Alert_No._1_-_2016.pdf>. Acesso em: 26 ago. 2017.

VALOR ECONÔMICO. 2017. **Seis grandes bancos internacionais aderem a projeto de moeda digital.** Disponível em: <http://www.valor.com.br/financas/5103260/seis-grandes-bancos-internacionais-aderem-projeto-de-moeda-digital>. Acesso em: 05 set. 2017.

YERMACK, David. **Is bitcoin a real currency?** An economic appraisal. 2014 (revisado). Massachusetts: National Bureau of Economic Research. 24p. Disponível em: <http://www.nber.org/papers/w19747>. Acesso em: 22 maio 2017.