

# Moedas Virtuais no Brasil: como enquadrar as criptomoedas

Julio Cesar Stella\*

*Introdução. 1 O que é criptomoeda? 1.1 Conceito. 1.2 Livro razão distribuído. 1.3 Emissão e circulação de criptomoedas. 1.4 Instrumentos semelhantes e associados. 2 Aspectos econômicos. 2.1 Funções de moeda. 2.2 Mercados de criptomoedas e serviços associados. 2.3 O caráter global das criptomoedas. 3 Aspectos jurídicos. 3.1 Enquadramentos precários. 3.2 Bem (coisa incorpórea). Conclusão.*

## Resumo

Este artigo explora a natureza jurídica das criptomoedas e das transações efetuadas por meio delas. As criptomoedas merecem atenção especial pelas inovações que introduzem nos meios de pagamento: a ausência da figura de um emissor centralizado e a possibilidade de transmissão da sua propriedade por meio da internet sem a necessidade de intermediários. Após a definição de um conceito para criptomoedas, observa-se o funcionamento de instrumentos que correspondem ao conceito proposto. O enquadramento desses instrumentos em institutos jurídicos tradicionais é bem pouco preciso, sendo necessário, em geral, recorrer aos negócios jurídicos efetivamente praticados com criptomoedas para fundamentar sua interpretação por analogia.

**Palavras chave:** Ativos digitais. Criptomoedas. Moeda criptografada. Moeda virtual. Regulação financeira.

---

\* Mestre em Economia pela Universidade de Brasília (UnB). Bacharel em Direito pela Universidade de São Paulo (USP) e em Administração Pública pela Escola de Administração de Empresas da Fundação Getúlio Vargas (EAESP/FGV). Analista do Banco Central do Brasil, lotado no Departamento de Regulação Prudencial e Cambial (Dereg).

## *Virtual Currencies in Brazil: how to construe cryptocurrencies*

### *Abstract*

*This article explores the legal nature of the cryptocurrencies and the transactions performed through them. Cryptocurrencies deserve special attention for the innovations they introduce in the means of payment: the absence of the figure of a centralized issuer and the possibility of transmitting their property through the internet without the need for intermediaries. After defining a concept for cryptocurrencies, we observe the use of instruments that correspond to the proposed concept. The framing of these instruments in traditional legal institutions is not very precise, being necessary, in general, to resort to the legal business effectively practiced with cryptocurrencies to substantiate their interpretation by analogy.*

**Keywords:** Digital Assets. Cryptocurrencies. Virtual Currency. Financial Regulation.

### **Introdução**

O objetivo deste trabalho é analisar, à luz do direito vigente, o fenômeno das criptomoedas e os negócios jurídicos praticados com esses instrumentos.

Empregamos criptomoeda ou moeda criptografada (como sinônimos) para se referir às moedas digitais que são emitidas de forma descentralizada e denominadas em unidade de conta própria e que têm a liquidação de suas transações efetivada em livro razão distribuído, sem a atuação necessária de contrapartes centrais.

Esses instrumentos também são referidos em textos acadêmicos, em documentos oficiais, na imprensa e na internet como moedas virtuais, moedas digitais, *bitcoins*, *altcoins*, ativos digitais, entre outros. Não há um consenso claro sobre qual termo melhor define o fenômeno em análise, mas, no decorrer desse artigo, elucidam-se diferenças entre os nomes listados e o conceito criptomoeda proposto.

Quando se fala de criptomoeda, a principal referência é o Bitcoin<sup>1</sup>, que foi o primeiro sistema de dinheiro eletrônico distribuído que confiou exclusivamente na sua tecnologia *blockchain*, um livro razão distribuído, com integridade protegida por consenso de algoritmos criptográficos, para efetuar suas emissões e demais transações.

Hoje é possível negociar centenas de moedas criptografadas, e tanto o volume transacionado quanto o valor de mercado de tais instrumentos têm crescido de forma significativa<sup>2</sup>.

Até o presente momento, não há lei ou norma infralegal que estabeleça uma definição específica para esses instrumentos no Brasil<sup>3</sup>. As manifestações de autoridades estatais, discussões de especialistas e legislações já vigentes no exterior a respeito de criptomoedas são referências para análise.

---

1 Conforme conclui Fernando Ulrich (2014, p. 108), trata-se de uma nova forma de moeda. É mister referir também ao próprio *white paper* do *bitcoin*, que descreve muito claramente o funcionamento desse instrumento. Disponível em <<https://bitcoin.org/bitcoin.pdf>>. Acesso em: 29 ago. 2017.

2 Nesse sentido, Cesar van der Laan (2014, 18) considera que o potencial do *bitcoin* ainda está longe de ser observável.

3 As criptomoedas, porém, já figuram em documentos produzidos por autoridades brasileiras, conforme discussão na seção de aspectos jurídicos, a seguir.

O presente estudo pretende, em suma, descrever a criptomoeda – conceitualmente e como um objeto já utilizado para realização de diversos negócios – e, considerando atributos específicos desse instrumento, avaliar o seu enquadramento em institutos<sup>4</sup> vigentes, apesar de ainda não haver regime jurídico específico para estes no direito pátrio.

## I O que é criptomoeda?

### I.1 Conceito

Criptomoeda, ou moeda criptografada, é um ativo digital denominado na própria unidade de conta que é emitido e transacionado de modo descentralizado, independente de registro ou validação por parte de intermediários centrais, com validade e integridade de dados assegurada por tecnologia criptográfica e de consenso em rede.

Trata-se de instrumentos desenhados para viabilizar transferências de valores em rede de maneira segura e independente de um sistema de intermediação financeira.

As características mais relevantes para a diferenciação conceitual entre criptomoedas e outros valores escriturais são: i) serem denominadas na própria unidade de conta; e ii) possuírem estrutura operacional descentralizada, com governança definida primordialmente no *software* por meio do qual funcionam.

Comparativamente a outras representações eletrônicas de valor, podemos classificar as criptomoedas da seguinte forma:

A categoria mais ampla, ativo digital, seria aquela que compreende qualquer representação digital de valor, ou seja, moedas virtuais, saldos em contas de pagamento (depósitos e dinheiro eletrônico) e outros valores cuja propriedade se adquira mediante registro no sistema eletrônico que os custodie, tais como títulos de crédito e valores mobiliários escriturais.

Nota-se que tanto os meios de pagamento eletrônicos quanto outros títulos negociáveis eletronicamente no Brasil são denominados em reais. Excluem-se dessa regra as moedas virtuais.

No conjunto das moedas virtuais, encontram-se os instrumentos de pagamento denominados nas próprias unidades de conta. Além das criptomoedas, essa categoria inclui moedas de jogos eletrônicos, pontos de programas de fidelidade e outros arranjos contendo valores eletrônicos que não estejam vinculados ao preço de nenhum bem ou direito externo ao arranjo.

As criptomoedas se diferenciam das demais moedas virtuais porque possuem estrutura descentralizada de registro e empregam tecnologia criptográfica para garantir a validade de cada transação e uma rede distribuída de registros para garantir a integridade de suas transações como um todo.

As transações nessas redes são originadas pela pessoa que deseja transferir saldo armazenado em um endereço público (conta) do livro razão distribuído da criptomoeda (sua escrituração contábil) para qualquer outro endereço público<sup>5</sup>. O emissor do pagamento assina a transação com a chave privada que corresponde ao endereço que possui e publica-a para registro na rede.

---

4 Conforme Oswaldo Aranha Bandeira de Mello (1979, p. 290), “Instituto jurídico é uma figura jurídica ou um grupo de categorias jurídicas constituindo um todo, portanto, perfazendo uma unidade estrutural, entre relações jurídicas coordenadas por fato central, e outras conexas”.

5 Endereço este que pode ser detido por qualquer pessoa, em qualquer parte do mundo, como uma conta de *e-mail*, conforme detalhado na seção do caráter global das criptomoedas, a seguir.

Quando a transação é confirmada no consenso dos participantes da rede dotados de capacidade para confirmá-la, ela se torna irreversível (final). A depender das regras e dos requisitos definidos nas políticas de cada instrumento para efetivação de registros de novas transações, essa confirmação pode ocorrer em segundos.

Embora seja possível armazenar e até transferir criptomoedas de forma completamente analógica<sup>6</sup>, esses instrumentos foram desenvolvidos para funcionar de maneira eletrônica e independente de qualquer documentação impressa. Sua natureza é digital, desde o início, pois foram criadas para efetivar pagamentos via internet.

As criptomoedas apresentam diferentes níveis de descentralização, sendo que suas transações ocorrem mediante validação por uma rede de usuários.

A emissão e o registro de novas transações podem ser efetivados por nós especializados da rede e também podem ser radicalmente descentralizados, ou seja, efetuados por qualquer usuário conectado à rede, num processo chamado “mineração”.

Quando se afirma que as criptomoedas são instrumentos que não possuem a garantia de um governo central, isso significa que tais moedas ainda não são aceitas por governos para liquidação de obrigações tributárias e não são legalmente definidas como moedas com poder liberatório de obrigações<sup>7</sup>, nem tampouco possuem respaldo de seguros de depósito (como ocorre com a moeda bancária).

O que assegura a integridade desses instrumentos, portanto, não é a confiança dos portadores do instrumento na pessoa do emissor ou em qualquer contraparte específica, mas, sim, a existência de algoritmos obrigatórios para todos os usuários da criptomoeda, que permitem a emissão e a transferência de propriedade desses ativos na rede de maneira segura e bastante robusta a fraude.

Nas seções 1.2 e 1.3, a seguir, descreve-se o funcionamento de dois aspectos tecnológicos que permitem a existência de uma estrutura descentralizada de transmissão de valor: a tecnologia de livro razão distribuído e o procedimento de emissão e de registro de transações nesses sistemas.

## 1.2 Livro razão distribuído

Normalmente, ao se referir à tecnologia de livro razão distribuído, utiliza-se o termo em inglês *distributed ledger technology* (DLT).

Recentemente o Comitê de Pagamentos e Infraestruturas de Mercado do Banco de Compensações Internacionais (CPMI/BIS) publicou relatório<sup>8</sup> contendo um quadro analítico no qual descreve de maneira generalizada a DLT. O conceito utilizado pelo CPMI no referido relatório é o seguinte: “*the processes and related technologies that enable nodes<sup>9</sup> in a network (or arrangement) to securely propose, validate and record state changes (or updates) to a synchronised ledger that is distributed across the network’s nodes*”<sup>9</sup>.

---

6 Um procedimento de armazenamento frio (*off-line*) é a chamada carteira de papel, que consiste na impressão do endereço público e da chave privada de uma carteira. A entrega de uma carteira de papel desse tipo a um terceiro transfere fisicamente os valores mas não fica registrada no blockchain. Disponível em: <[https://en.bitcoin.it/wiki/Paper\\_wallet](https://en.bitcoin.it/wiki/Paper_wallet)>. Acesso em: 29 ago. 2017.

7 O real, por exemplo, tem esse poder liberatório assegurado pelo art. 1º da lei nº 9.069, de 29 de junho de 1995: “A partir de 1º de julho de 1994, a unidade do Sistema Monetário Nacional passa a ser o REAL (Art. 2º da Lei nº 8.880, de 27 de maio de 1994), que terá curso legal em todo o território nacional.”

8 Disponível em: <<http://www.bis.org/cpmi/publ/d157.htm>>. Acesso em: 29 ago. 2017.

9 Tradução livre: “Os processos e as tecnologias relacionadas que permitem a nós<sup>3</sup> em uma rede (ou arranjo) propor, validar e registrar mudanças de estado (ou atualizações) de forma segura em um livro razão sincronizado que é distribuído através dos nós da rede”. A tradução livre da note de rodapé (3), mencionada na citação é: “<sup>3</sup> Na ciência da computação, um nó é a unidade básica de computação em uma rede. No contexto deste relatório, um nó refere-se a um computador que participa da operação de um arranjo DLT”.

O *blockchain*<sup>10</sup> do *bitcoin* é o exemplo primordial de DLT. Nesse sistema<sup>11</sup>, todos os usuários têm acesso a todos os dados do livro razão distribuído, que consiste num histórico encadeado de todas as transações já efetivadas.

Qualquer usuário que tenha capacidade computacional para tal pode se conectar para emitir moeda e validar transações. As novas transações são publicadas pelo emissor do pagamento mediante a aposição da chave privada que corresponde à sua carteira. Essa assinatura eletrônica garante a autenticidade de cada transação originada perante todos os usuários da rede.

Os nós dessa rede que atuam como mineradores validam se há saldo no endereço pagador e organizam diversas transações em blocos de dados para registrá-los na rede. Cada bloco de dados é iniciado pela chave criptográfica do bloco anterior, produzindo um registro sequencial de transações (*timestamp*) que não permite alterações nem cancelamentos de transações já registradas.

Esse mecanismo se chama *blockchain*, “corrente de blocos” no vernáculo, em razão de cada bloco de operações iniciar pela chave criptográfica que fechou o bloco anterior, o qual iniciou com a chave do bloco imediatamente anterior e assim recursivamente até o primeiro bloco do *bitcoin*, o bloco Genesis<sup>12</sup>, formando uma corrente de registros em que a chave de cada bloco é um elo.

Esse registro é imutável porque apenas são adicionados novos elos a essa corrente mediante o consenso dos mineradores que dispõem seu poder computacional para “quebrar” a chave criptográfica desse novo bloco, que contém a chave imediatamente anterior da corrente, que valida seus dados e, conseqüentemente, a cadeia inteira de registros. Seria necessário o consenso desses mineradores para “voltar atrás” e publicar versões alternativas do registro, a partir de um elo já ultrapassado da corrente<sup>13</sup>.

Muitas criptomoedas são chamadas de *altcoins* por serem construídas e operadas em derivações desse mecanismo utilizado no *bitcoin*. As alterações mais relevantes são aquelas associadas à forma como um usuário se credencia para enviar transações e para validá-las.

A ideia de um bloco de transações imutável e distribuído é de grande utilidade não apenas para a transferência de valor pela internet, mas também para diversos outros fins econômicos e sociais. De fato, muitas aplicações fundadas em registro distribuído de dados já estão em operação, conforme se detalha na seção 1.4.

### 1.3 Emissão e circulação de criptomoedas

A forma de emissão e circulação das criptomoedas depende de configurações definidas nos algoritmos que operam o livro razão distribuído de cada instrumento. Até agora, a configuração mais descentralizada é aquela em que todos os nós da rede são capazes de ler todo o histórico de transações, originar novas transações, emitir criptomoeda e registrar novas transações.

São chamados mineradores os nós da rede que validam as transações efetivadas com criptomoedas. Esse termo faz mais sentido para DLTs que utilizam a prova de trabalho (*proof-of-work* ou PoW) como requisito para emissão e registro de transações. A prova de trabalho mais comum, em geral, é uma cópia do código do *bitcoin* com alguma alteração marginal.

---

10 Não confundir com Blockchain, empresa que detém o site blockchain.info, no qual se encontram informações sobre o *blockchain* e serviços como carteira eletrônica.

11 Disponível em: <[https://en.bitcoin.it/wiki/How\\_bitcoin\\_works](https://en.bitcoin.it/wiki/How_bitcoin_works)>. Acesso em: 29 ago. 2017.

12 Vale a pena ler na própria *wiki* do *bitcoin*, disponível em: <[https://en.bitcoin.it/wiki/Genesis\\_block](https://en.bitcoin.it/wiki/Genesis_block)>. Acesso em: 29 ago. 2017.

13 O processo em que parte dos mineradores decide minerar diferentes correntes se chama *hard fork* e não é um fenômeno raro, já ocorreu com as duas principais criptomoedas, o *bitcoin* e o *ether*. Para um entendimento melhor do conflito de poder que causou a divisão do livro razão do *bitcoin*, ver artigo “A power struggle erased billions of dollars off Bitcoin, and it’s about to get worse”. Disponível em: <<http://mashable.com/2017/08/23/bitcoin-power-struggle>>. Acesso em: 29 ago. 2017.

Ela consiste em encontrar uma chave criptográfica que atende a certos critérios, mediante aplicação de criptografia assimétrica em um bloco de dados composto: pela chave criptográfica que fechou o bloco anterior, por um conjunto de transações e por um texto aleatório chamado *nonce*.

O trabalho dos mineradores é recompensado pelo pagamento de tarifas e pela atribuição de direitos de emitir novas criptomoedas. Esse processo foi chamado de mineração justamente porque a chance de encontrar ouro em uma mina é um evento raro, que tem uma chance quase aleatória de ocorrer, e acaba por distribuir seus “prêmios” de forma proporcional à quantidade de trabalho empenhada.

Nas redes em que não se exige uma prova de trabalho para registro de transações e emissão, tais privilégios são atribuídos a tipos qualificados de nó da rede. Os nós com privilégio de emissão devem-no fazer de acordo com alguma regra especificada na DLT.

Os nós que registram novas transações se responsabilizam por garantir a prova de propriedade (*proof-of-stake* ou PoS) das criptomoedas transacionadas, que é averiguada mediante votação (consenso) entre esses nós ou entre um grupo de nós a respeito da existência ou não de saldo suficiente para uma transação ordenada a partir de certo endereço.

Em teoria, o *bitcoin* se encaixa na forma mais descentralizada de criptomoeda, que possui uma rede sem nós especializados. O que se observa, entretanto, é uma capacidade computacional exigida para emitir moeda e registrar novas transações tão monstruosa que, salvo raríssimas exceções, não é esperado que um usuário comum tenha a sorte de minerar lado a lado com *pools* de mineradores profissionais com quantidades vultosas de computadores desenhados desde o *hardware* para minerar *bitcoins* (os chamados ASICs).

No outro extremo, encontramos DLTs baseadas em provas de propriedade em que os privilégios de validação são distribuídos de forma muito concentradas e até, eventualmente, com emissão centralizada produzindo ativos virtuais que não se encaixam muito bem no conceito de criptomoeda aqui proposto.

## 1.4 Instrumentos semelhantes e associados

Ocorre que, muito além de permitir transferência de dinheiro sem intermediação de qualquer pessoa, via internet, as DLTs podem ser utilizadas para transferências de qualquer tipo de valor digital e viabilizam o compartilhamento e a atualização de um registro eletrônico seguro de informações de interesse público ou privado. A partir desse registro ubíquo, independentemente da existência de um fiador central da sua integridade, diversas aplicações inovadoras já foram desenvolvidas, e muitas outras que não foram ainda sequer imaginadas devem surgir em breve<sup>14</sup>.

O ponto-chave da revolução do *blockchain* está na desintermediação da informação que até então dependia de uma autoridade central para validação, que pode ser criada a partir de algoritmos que não requerem a colaboração de nenhuma pessoa quando são atendidos os requisitos prescritos no seu código.

No que tange à transferência de valores, merece especial atenção uma classe de *tokens*, emitidos em *blockchain* ou outro tipo de DLT, que representa propriedade de algum outro bem ou direito externo à própria DLT, os *non-native tokens*<sup>15</sup>.

---

14 Para referência de aplicações inovadoras em DLT, é recomendada a leitura de relatório do governo Inglês “*Distributed ledger technology: beyond block chain*”. Disponível em: <<https://www.gov.uk/government/publications/distributed-ledger-technology-blackett-review>>. Acesso em: 29 ago. 2017.

15 Conforme descrito na publicação do CPMI “*Distributed ledger technology in payment, clearing and settlement: An analytical framework*”, p. 9. Disponível em: <<http://www.bis.org/cpmi/publ/dl157.pdf>>. Acesso em: 29 ago. 2017.

Esses criptoativos representantes de algum direito externo, tais como depósitos de moedas estatais<sup>16</sup>, não cabem no conceito de criptomoeda porque não possuem unidade de conta própria, ou seja, possuem uma taxa de câmbio fixa para o preço de algum outro bem, direito ou valor. Esses ativos gozam das mesmas propriedades de liquidez imediata e transferibilidade global, sem se submeter à crítica ou censura de qualquer parte, no entanto, por representar coisa externa ao próprio livro razão, assemelham-se mais a títulos de crédito eletrônicos. De fato, a utilização de *tokens* representativos de algum direito externo dá ensejo a uma extensa possibilidade de enquadramentos, podendo servir de instrumento para descentralizar provavelmente qualquer produto ou serviço financeiro hoje existente.

Uma espécie de *crowdfunding* chamada ICO (do inglês *Initial Coin Offering*) tem sido capaz de mobilizar investimentos de volume relevante<sup>17</sup>. Essa modalidade de financiamento tem sido atraída para novos empreendimentos envolvendo criptomoedas, outros ativos digitais ou mesmo a prestação de outros serviços por meio do *blockchain*. Em um ICO, uma companhia, para obter financiamento, promove a emissão de criptomoedas (ou outros ativos digitais) que serão vendidas aos financiadores do projeto contra pagamento em moeda soberana ou mesmo outras moedas virtuais.

Esse esquema constitui verdadeiro desafio de interpretação jurídica, pois não se trata necessariamente de uma ação da companhia, nem mesmo um pagamento antecipado por um bem a ser entregue no futuro, trata-se de um financiamento dado a um empreendimento com base na esperança que o saldo em criptomoeda (ou *token*), então adquirido, terá um valor de mercado significativamente maior no futuro.

Muitos desses empreendimentos vão além de meios de pagamento e oferecem serviços com base em contratos inteligentes (geralmente referidos no inglês *smart contracts*) que são registrados em livro razão distribuído e são capazes de disparar sua execução de forma automatizada com base em algum critério autoverificável e independente de qualquer atuação humana<sup>18</sup>.

## 2 Aspectos econômicos

### 2.1 Funções de moeda

O nome moeda criptografada, ou criptomoeda, sugere que tais instrumentos sejam semelhantes às moedas. Veremos adiante que não se trata de moeda no seu sentido jurídico. Em relação às propriedades econômicas, observa-se o seguinte:

As principais funções econômicas da moeda, segundo Lopes e Rosseti (2001, p.18), são: i) meio de troca, ii) medida de valor (unidade de conta), iii) reserva de valor, iv) instrumento liberatório de obrigações; v) padrão de pagamentos diferidos; e vi) instrumento de poder.

A função fundamental da moeda é ser meio de troca aceito por uma comunidade econômica. Em geral, a função liberatória, que é a atribuição legal de poder a certos instrumentos para saldar obrigações pecuniárias, não podendo este ser recusado legalmente pelo credor, garante a aceitação de um meio de troca.

---

16 Esquemas estes que se enquadrariam melhor como dinheiro eletrônico, no caso de moedas estatais. Notadamente o Tether (<https://tether.to/faqs/>) figura entre as criptomoedas de maior volume transacionado (tendo atingido mais de USD 300 milhões diário em alguns dias de agosto de 2017) e opera *tokens* criptográficos representativos de USD, EUR e JPY. A empresa Tether Limited é incorporada em Hong Kong, o Site “.to” é hospedado no Togo, uma ilha no Pacífico, e os termos de serviço são governados pela lei das Ilhas Virgens Britânicas (Caribe).

17 USD 103 mi em 2016, tendo acumulado mais de 1,7 USD bi desde o primeiro ICO até o início de agosto de 2017: Disponível em: <<https://www.coindesk.com/2016-ico-blockchain-replace-traditional-vc/>> e <<https://www.coindesk.com/ico-tracker/>>. Acesso em: 29 ago. 2017.

18 Destaca-se que esse mecanismo cria uma lei natural digital entre as partes, na qual “se A é, B é”, desafiando a ideia da proposição jurídica fundamental de Hans Kelsen (1999, p. 55), “se A é, então B deve ser”.

Segundo nota para discussão apresentada pelo corpo técnico do Fundo Monetário Internacional (FMI), até a data de sua publicação não havia evidência de que qualquer criptomoeda tivesse função de meio de troca, unidade de conta ou reserva de valor (FMI, 2016, p.17).

Na visão desses autores, a criptomoeda não funcionava como unidade de conta porque poucos fornecedores de bens e serviços definiam os preços de venda em termos de criptomoeda. Além disso, poucos agentes econômicos aceitavam liquidar pagamentos por meio de tais instrumentos. Por fim, dada a alta volatilidade dos preços das criptomoedas em relação a qualquer moeda soberana, parecia muito arriscada a utilização de tais instrumentos como reserva de valor.

Embora pouco tempo tenha decorrido da publicação da nota referida supra, mudanças recentes no ambiente regulatório e na indústria varejista têm trazido evidências de que a utilização de criptomoedas como meio de troca pode se tornar costumeira.

Ainda que a aceitação de tais instrumentos seja pouca se comparada à dos cartões de pagamento, grandes empresas de mídia, internet, tecnologia e até grandes escritórios de advocacia, além de pequenos entusiastas, já começam a aceitar ou estão se preparando para aceitar pagamentos em criptomoedas<sup>19</sup>.

Colabora para isso observar que os pagamentos em criptomoeda se efetivam, em geral, mais rapidamente e com custos inferiores do que aqueles processados por outras formas de transferência eletrônica de dinheiro, especialmente quando se trata de operações que dependem de estruturas de mercado com muitas camadas de intermediação, por exemplo, as remessas de fundos ao exterior.

Outro aspecto econômico que merece destaque é o lado político-econômico da atribuição de valor a uma moeda. As moedas estatais de curso forçado contam não apenas com reservas legais, mas também com uma infraestrutura estatal ou privada (fortemente regulada) e com as políticas monetária e cambial oficiais.

Cada criptomoeda, por sua vez, deve especificar uma política monetária em seus algoritmos. O *bitcoin*, por exemplo, possui um planejamento definido em seu código para emitir toda sua “base monetária virtual” até 2140<sup>20</sup>; a rede Stellar, por sua vez, emitiu no momento de sua fundação toda a base monetária de sua criptomoeda – o *lumen* –, que possui uma taxa de inflação nominal pré-definida de 1% ao ano<sup>21</sup>.

Muitas criptomoedas, mesmo que funcionem como instrumentos descentralizados, têm grande parte de sua base monetária em poder da organização que a desenvolveu, o que garante a tal entidade um grande poder de manipulação de taxa de câmbio entre esse e outros ativos digitais.

## 2.2 Mercados de criptomoedas e serviços associados

A criptomoeda encontra mais acesso ao consumidor final com a utilização de serviços que vão desde simples comodidades técnicas a sofisticados sistemas de intermediação de operações.

Entre as facilidades que esses intermediários proporcionam, destacam-se: i) custodiar saldo em criptomoeda e moedas soberanas; ii) converter criptomoeda em moeda soberana e vice-versa; iii) transferir saldos, de qualquer tipo, entre clientes; e iv) emitir cartões de pagamento em moeda local com saldo vinculado a conta de criptomoeda.

---

19 Conforme publicado em diversos meios. Disponível em: <<http://www.zerohedge.com/news/2017-05-28/who-accepts-bitcoins-payment-list-companies-stores-shops>>, <<http://www.businessinsider.com/5-big-companies-that-currently-accept-bitcoin-2017-7/#heres-why-more-businesses-arent-accepting-bitcoin-6>> e <<https://www.bna.com/law-firms-accepting-n73014464226/>>. Acesso em: 29 ago. 2017.

20 Disponível em: <<https://www.coindesk.com/top-10-bitcoin-myths-debunked/>>. Acesso em: 29 ago. 2017, estimativa essa que é coerente com o disposto na *wiki* do próprio *bitcoin*. Disponível em: <[https://en.bitcoin.it/wiki/Controlled\\_supply](https://en.bitcoin.it/wiki/Controlled_supply)>. Acesso em: 29 ago. 2017.

21 Disponível em: <<https://www.stellar.org/developers/guides/concepts/inflation.html>>. Acesso em: 29 ago. 2017.

As operações entre clientes intermediadas por prestador de serviços podem ser liquidadas por meio de contas escriturais custodiadas de forma centralizada e denominadas em termos de ativos digitais, sem que a transferência da propriedade desses ativos seja alterada efetivamente no livro razão distribuído da criptomoeda.

Isso ocorre, por exemplo, quando há transferência de saldo denominado em criptomoedas entre clientes de uma mesma corretora. Por custodiar as contas de ambas as partes, o prestador de serviço não precisa efetuar nenhum lançamento no livro razão distribuído para completar a transação, bastando atualizar os saldos escriturais de seus clientes após a transação.

O maior ponto de contato entre as criptomoedas e a economia financeira formal se encontra, portanto, nas empresas que fazem a compra e a venda de tais instrumentos contra a moeda estatal local para o público em geral, as quais chamaremos de casas de câmbio de criptomoedas<sup>22</sup>.

Comerciantes que desejam aceitar pagamentos denominados em criptomoeda, mas não querem arcar com o risco da volatilidade dos preços dessas em relação à moeda soberana local, por exemplo, beneficiam-se da existência de serviços de terceiros que se dedicam a mitigar esse risco.

Existem também plataformas de negociação *peer to peer*<sup>23</sup> que permitem a seus usuários efetuar compra e venda de diversos ativos digitais com qualquer outro usuário da plataforma. Trata-se de uma espécie curiosa de mercado organizado de negociações diretas (*over the counter*) *on-line* e sem fronteiras.

Destaca-se que certas bolsas de negociação de criptomoedas oferecem inclusive funcionalidades mais sofisticadas para investidores, como aluguel e empréstimo de saldos (sim, crédito em criptomoeda remunerado com juros pactuados livremente no mercado) e derivativos de criptomoeda.

As maiores bolsas de negociação de criptomoedas do mundo administram grandes volumes diários de operações de compra e venda de criptomoedas, sendo que as três maiores têm registrado, recentemente, para os principais pares de moedas, montantes superiores a centenas de milhões de dólares negociados em um período de 24 horas<sup>24</sup>.

Para se ter uma referência, o volume médio de movimentações diárias no Sistema de Liquidação Diferida das Transferências Interbancárias de Ordens de Crédito (Siloc) da Câmara Interbancária de Pagamentos (CIP), a principal câmara de compensação de ordens bancárias de varejo do Brasil, foi cerca de 5 bilhões de dólares para o mês de julho de 2017<sup>25</sup>.

As duas maiores corretoras de ativos digitais no país<sup>26</sup>, atualmente, divulgam um volume negociado diário de aproximadamente 8 milhões de reais, o que, apesar do crescimento recente, ainda é bastante pouco em comparação com o tamanho do mercado de pagamentos brasileiro.

No momento em que foi redigido esse artigo (setembro de 2017), já existiam mais de 850 criptomoedas, sendo que quinze destas possuíam valor de mercado, calculado pela cotação de cada unidade em dólares vezes a quantidade em circulação, superior a 250 milhões de dólares dos Estados Unidos (referido a partir daqui como dólares), sendo que doze destas possuíam volume de negociação superior a 50 milhões de dólares nas últimas 24 horas.

---

22 Tais companhias têm sido escolhidas em diversas jurisdições que já regulam criptomoedas como as pessoas a quem se atribui, entre outras, a responsabilidade de identificação de clientes para efeitos de prevenção à lavagem de dinheiro.

23 Em vernáculo: "pessoa a pessoa". A expressão em inglês é utilizada para referir a quaisquer operações sem intermediários.

24 Para uma referência desse número atualizado, verificar o site Comarketcap. Disponível em: <<https://coinmarketcap.com/currencies/volume/24-hour/>>. Acesso em: 29 ago. 2017.

25 R\$ 15,8 bilhões, conforme <<http://www.bcb.gov.br/pom/spb/Estatistica/Port/Siloc.csv>>, a uma taxa de câmbio aproximada de 3,14 BRL/USD.

26 Entre aquelas que atuam ostensivamente na internet, consideramos as listadas no site: <<https://bisoint.io/br/bitcoin/price-comparison/exchange-fees>>, e duas maiores: Foxbit e MercadoBitcoin anunciam em seus portais, respectivamente 585,5 e 241,17 *bitcoins* negociado a uma taxa de aproximadamente 14 mil reais (em 24 ago. 2017: <https://foxbit.com.br/> e <https://www.mercadobitcoin.com.br/>).

Para se ter noção da velocidade do crescimento desses números, em março de 2017 eram 650 criptomoedas negociadas, sendo 25 com valor de mercado superior a 10 milhões de dólares, e agora 184 delas superam essa cifra. Apenas dez destas possuíam volume diário superior a 1 milhão de dólares, e atualmente são 69. Destaca-se que esse *site* até o momento não inclui dados de negociação efetuados em casas de câmbio de moedas virtuais no Brasil.

## 2.3 O caráter global das criptomoedas

As criptomoedas são desenhadas para funcionar em rede e, tal como a própria internet, os critérios para adesão a essas redes são técnicos e insensíveis à jurisdição. Qualquer pessoa que possua um computador (ou *smartphone*) com *software* aderente ao protocolo que regula a DLT desse ativo digital, em qualquer parte do mundo, pode acessar o sistema e efetuar transações.

Disso decorre que um endereço no *blockchain* pode ser detido por um usuário em qualquer país e, portanto, quase não se vê diferença entre fazer uma transferência de criptomoeda “pessoalmente” no ponto de venda ou para um endereço de uma loja *on-line* além-mar.

O fato de o custo das transações liquidadas com criptomoedas não ser dependente da localização do pagador e do recebedor gera uma grande atratividade para o desenvolvimento de negócios transfronteiriços nesses arranjos.

Seu caráter global, e a mudança de paradigmas que esses instrumentos representam para os meios de pagamento, é comparável ao que o *e-mail* representou para as correspondências internacionais.

A relevância dessa característica sobressai quando se considera que o capitalismo financeiro se desenvolveu junto com o estado de direito moderno, e as jurisdições consideradas mais desenvolvidas são aquelas em que a tutela jurisdicional mais se aproxima da lei natural, nas quais, se ocorre um evento, ocorre naturalmente uma consequência.

Os mecanismos de execução contratual automatizada de obrigações presentes no ecossistema das criptomoedas (previsto, muitas vezes, na mesma DLT que registra pagamentos) criam operações em que não há dependência de tutela jurisdicional para se forçar o cumprimento de um pacto, observada determinada condição.

Trata-se de instrumentos que se autoexecutam, conforme avençado entre as partes, no momento em que ocorre seu evento de ativação, sem que qualquer ação ou inação de qualquer parte possa impedir a consequência prevista no código.

Ao contar com uma camada de valor independente de jurisdição, a atividade econômica na internet encontrou o elemento que faltava para se desenvolver como um fenômeno global e autocontido, prescindindo das jurisdições locais para assegurar seu funcionamento.

## 3 Aspectos jurídicos

### 3.1 Enquadramentos precários

Examina-se a aderência dos fatos anteriormente descritos a regimes jurídicos já estabelecidos no direito positivo brasileiro. É notável que, para cada figura jurídica que tenta se ajustar à criptomoeda e aos negócios com ela praticados, algum aspecto específico fica mal encaixado<sup>27</sup>.

---

<sup>27</sup> Roma e Silva (2016) consideram que essa ausência de segurança jurídica pode ser prejudicial à própria aceitação das criptomoedas. Verçosa

Descrevemos as incompatibilidades para enquadramento das criptomoedas no ordenamento jurídico brasileiro como moeda, moeda eletrônica, título de crédito e valor mobiliário.

As teorias jurídicas da moeda mais conhecidas são a teoria estatal e a social<sup>28</sup>. A primeira argumenta que moeda é o meio de pagamento que tem poder liberatório assegurado pelo estado. A segunda aponta a característica de ser uma unidade abstrata de conta aceita socialmente como fundamental para a moeda, e sua aceitação pode ser por determinação estatal ou por usos e costumes do mercado.

Pelo lado da teoria estatal, hoje em dia é esperado que as autoridades monetárias venham a utilizar a mesma tecnologia empregada nas criptomoedas para emitir dinheiro estatal, as chamadas *central bank cryptocurrencies* (CBCCs)<sup>29</sup>.

Diversos países, como Canadá, Singapura e Brasil<sup>30</sup>, já efetuaram testes para emissão desse tipo de instrumento, mas ainda não há jurisdição que tenha concedido poder liberatório a qualquer moeda criptografada e há poucos casos de governos locais que tenham aceitado recolher tributos por meio de tais instrumentos<sup>31</sup>.

Mesmo que as CBCCs venham a circular, não seriam criptomoedas, no conceito definido nesse artigo, se fossem denominadas na unidade de conta da moeda estatal.

Pelo lado da teoria social, a aceitação de criptomoedas como meio de pagamento, embora presente, conforme visto nos aspectos econômicos acima, ainda não é tão relevante a ponto de se justificar considerar esses instrumentos moeda de fato.

Outro enquadramento que não se aplica às criptomoedas é o de moeda eletrônica. Numa leitura estreita da definição legal vigente de moeda eletrônica – “recursos armazenados em dispositivo ou sistema eletrônico que permitem ao usuário final efetuar transação de pagamento”<sup>32</sup> –, que é muito ampla, parece até razoável enquadrar as moedas virtuais como tal.

Entretanto, o funcionamento dos arranjos de pagamento conforme estabelecido na mesma lei e na regulamentação pertinente não é compatível com a maior parte dos esquemas de criptomoedas que não possui as figuras do instituidor do arranjo de pagamentos e do emissor de moeda eletrônica.

Além disso, a regulamentação do Banco Central do Brasil (BCB) obsta cabalmente a hipótese de se tratar criptomoeda como moeda eletrônica ao restringir esta a recurso em reais armazenado em sistema ou dispositivo eletrônico<sup>33</sup>. A autoridade monetária reforçou esse óbice em dois comunicados sobre moedas virtuais que emitiu<sup>34</sup>.

Por fim, semelhante aresta jurídica impede o encaixe das criptomoedas como espécie de título de crédito ou valor mobiliário escritural.

A criptomoeda aqui mencionada pressupõe uma unidade de conta particular e abstrata. Essa definição implica não ser representação eletrônica específica de qualquer coisa, obrigação ou direito externo ao seu sistema.

---

(2016), por sua vez, considera que o desligamento das criptomoedas do mundo real, associado à sua precária interpretação jurídica e econômica, pode trazer riscos para o sistema financeiro e para a economia, como um todo.

28 Conforme F.A. Mann (1992, p. 14-28).

29 Conforme Bech e Garratt (2017, p. 55-56).

30 Disponível em: <[http://www.bcb.gov.br/htms/public/microcredito/Distributed\\_ledger\\_technical\\_research\\_in\\_Central\\_Bank\\_of\\_Brazil.pdf](http://www.bcb.gov.br/htms/public/microcredito/Distributed_ledger_technical_research_in_Central_Bank_of_Brazil.pdf)>. Acesso em: 29 ago. 2017.

31 A cidade Zug, na Suíça, já aceita, em fase de testes desde 2016, pagamentos de certas taxas municipais em criptomoeda. Ainda que seja para valores baixos, é interessante observar a atuação de tal cidade no interesse de se tornar um polo de *fintechs* associadas a implementação de aplicações para tecnologias em *blockchain*. Disponível em: <<https://www.coindesk.com/swiss-city-bitcoin-payments-government-services/>> e <<https://bitcoinmagazine.com/articles/swiss-crypto-valley-create-digital-identities-its-citizens-ethereum-blockchain/>>. Acesso em: 29 ago. 2017.

32 Lei nº 12.865, de 9 de outubro de 2013, art. 6º, VI.

33 Conforme §1º do art. 2º da Circular BCB nº 3.683, de 4 de novembro de 2013. Além desse normativo, o BCB emitiu dois comunicados.

34 Comunicado nº 31.379, de 16 de novembro de 2017, e Comunicado nº 25.306, de 19 de fevereiro de 2014.

No caso de títulos de crédito escriturais, apesar de toda a abstração, seus valores, além de serem denominados em reais, representam uma obrigação pecuniária devida pelo sacado ao beneficiário. Os valores mobiliários, por sua vez, representam direitos que o portador possui perante uma sociedade.

Esses instrumentos eletrônicos tradicionais, portanto, assemelham-se às criptomoedas por serem emitidos e transacionados eletronicamente, mas divergem destas por serem dependentes de uma estrutura centralizada de registro e por possuírem lastro em direitos externos.

As ofertas iniciais de moedas (ICOs) chamam atenção para o fato de que instrumentos emitidos com o intuito de levantar capital para algum empreendimento, dependendo dos direitos que o instrumento representa, podem ser enquadrados como valores mobiliários<sup>35</sup>.

A *Securities and Exchange Commission*, órgão responsável pela circulação de títulos e valores mobiliários dos Estados Unidos, concluiu em julho desse ano uma investigação<sup>36</sup> a respeito da aplicabilidade da lei de valores mobiliários federal americana ao caso da “The DAO”, empresa que teria captado 12 milhões de Ethers (ETH) pela venda de 1.15 bilhões de DAO Tokens (DAO).

O relatório da investigação é histórico porque define, em um único documento, que a quantia paga em ETH é dinheiro e que os *tokens* entregues aos investidores são valores mobiliários (*securities*), sujeitos, portanto, à lei federal que os rege.

A utilização de DLTs como infraestruturas descentralizadas de negociação também é interessante para a circulação de ativos digitais que representam direitos ou bens concretos externos. Nesses casos, não se trata de criptomoedas, mas sim de *tokens* criptográficos (ou criptoativos) que funcionam como representações eletrônicas da titularidade dos respectivos bens ou direitos subjacentes, nada interferindo na natureza jurídica destes<sup>37</sup>.

### 3.2 Bem (coisa incorpórea)

Considerando a falta de aderência às premissas dos instrumentos mencionados supra, o propósito de sua criação e a forma descentralizada como são emitidas e transacionadas as criptomoedas, uma abordagem possível para a natureza jurídica destas seria, simplesmente, um bem, uma *commodity* virtual ou coisa incorpórea.

Embora a aparente contradição interna num conceito do tipo “coisa imaterial” ou “coisa incorpórea”, conforme Thomas Marky (1995, p. 41), desde o direito romano Gaio já distinguia as coisas incorpóreas das corpóreas para diferenciar coisas concretas de direitos, respectivamente.

No direito vigente, conforme Diniz (2007, p. 119), “Admitimos os *bens incorpóreos* como objeto de propriedade, pois em face de nosso ordenamento jurídico a propriedade imaterial é regulada como uma relação de domínio do mesmo teor de um bem corpóreo”.

Além disso, o desenvolvimento recente da nossa legislação torna aceitável a existência de coisas cuja propriedade se transmite escrituralmente, como é o caso de certos títulos de crédito e valores

---

35 A Comissão de Valores Mobiliários alertou, em comunicado de 11 de outubro de 2017, que ativos digitais oferecidos em ICOs enquadráveis no conceito de valor mobiliário e que não obtiverem os devidos registros (ou dispensa se registros) serão considerados emissões irregulares e estarão sujeitos às sanções cabíveis.

36 A *Securities and Exchange Commission* (SEC) considerou em certos eventos que a oferta não atendia à legislação sobre *crowdfundings* e qualificou as moedas emitidas nesses casos como *securities*. Para referência, ver o alerta emitido recentemente pela SEC, disponível em: <[https://www.sec.gov/oiea/investor-alerts-and-bulletins/ib\\_coinofferings](https://www.sec.gov/oiea/investor-alerts-and-bulletins/ib_coinofferings)> e <<https://www.sec.gov/news/press-release/2017-131>>. Acesso em: 29 ago. 2017.

37 Destaca-se que a legislação brasileira autoriza a assinatura eletrônica em documentos privados por meio de qualquer meio considerado válido entre as partes (Medida Provisória n° 2.200-2, de 24 de agosto de 2001, art. 10). Nesse sentido, uma ordem de pagamento representada por uma moeda virtual pode ser alcançada pelo nosso direito como uma convenção privada formal, com suporte em documento eletrônico legalmente existente.

mobiliários, mencionados na seção anterior. A propriedade da criptomoeda também é transmitida mediante um registro público (o seu livro razão distribuído).

Complementarmente, a Receita Federal do Brasil<sup>38</sup> instrui o contribuinte brasileiro a declarar suas criptomoeda como “outros bens” e equipara-os a ativos de financeiros para fins de apuração de ganhos de capital.

Anota-se, ainda, que as criptomoedas são coisas fungíveis, porque são determinadas por seu gênero, ou seja, em geral nenhuma unidade vale mais ou menos que outra por ter alguma característica específica. Também se observa que as criptomoedas são divisíveis, ou são emitidas de modo que uma unidade possua um valor pequeno o bastante para não precisar ser dividido. O *bitcoin*, por exemplo, é divisível até a centésima milionésima parte<sup>39</sup>.

Essas características – transmissão escritural, fungibilidade e divisibilidade – são, não por acaso, muito convenientes para uma coisa que se deseja utilizar como meio de pagamento eletrônico. A emissão descentralizada, entretanto, adiciona uma camada de abstração inexistente nos meios de pagamento até então: os valores de criptomoeda não representam nenhum direito nem bem externo ao seu sistema.

## Conclusão

A criptomoeda ainda não pode ser chamada de moeda no sentido legal (estatal) da palavra. Entretanto, sob o ponto de vista socioeconômico, sua procura crescente tem sinalizado a esperança dos agentes econômicos de que estes instrumentos, no futuro, terão valor de troca superior ao seu valor presente, ainda que represente unidade de conta privada de caráter puramente escritural.

A confiança nesses *tokens* se estabelece de forma nunca antes registrada: a percepção de fidedignidade e esperança de aceitação do instrumento como meio de pagamento no futuro é amparada por uma rede anônima de usuários, sem depender de entidade estatal ou privada, personificada na figura do emissor do instrumento.

Sua utilização ainda encontra interpretações legais pouco padronizadas por meio das jurisdições, apesar de sua utilização apresentar um caráter tão internacional quanto a própria internet, o que pode ser o fundamento daquele que é um de seus principais riscos sociais: ser utilizado para lavagem de dinheiro.

As jurisdições que optaram por regular sua utilização como meio de pagamento, em geral, criam regimes equivalentes aos de outras empresas que atuam nos mercados de meios de pagamento ou no mercado de câmbio, tais como remetentes de pagamentos e corretoras de câmbio, atribuindo direitos e deveres a essas entidades, em especial a observância de normas relativas à prevenção da lavagem de dinheiro e de requisitos prudenciais.

Quanto à leitura do fenômeno das criptomoedas sob as molduras do ordenamento jurídico brasileiro, considerando-se as normas gerais de direito, os usos dados a esses instrumentos, a regulamentação de institutos semelhantes e as manifestações de autoridades a respeito, é adequado o tratamento destas como uma coisa incorpórea, mais especificamente, um domínio eletrônico com valor abstrato ao qual se atribui direito de propriedade.

---

38 Perguntas 447 e 607 do documento “Perguntão”. Disponível em: <<http://idg.receita.fazenda.gov.br/interface/cidadao/irpf/2016/perguntao>>. Acesso em: 29 ago. 2017.

39 A fração equivalente a 0,00000001 *bitcoin* é apelidada de Satoshi.

## Referências

- BANDEIRA DE MELLO, Oswaldo Aranha. **Princípios gerais de direito administrativo**. 2. ed. São Paulo: Forense, 1979. v. I.
- BECH, Morten; GARRAT, Rodney. Central bank cryptocurrencies. **BIS Quarterly Review**, September 2017. Disponível em: <[https://www.bis.org/publ/qtrpdf/r\\_qtr1709f.pdf](https://www.bis.org/publ/qtrpdf/r_qtr1709f.pdf)>. Acesso em: 29 ago. 2017
- DINIZ, Maria Helena. **Curso de direito civil brasileiro: teoria das obrigações contratuais e extracontratuais**. 23. ed. São Paulo: Saraiva, 2007. v. 3.
- FUNDO MONETÁRIO INTERNACIONAL. **Virtual Currencies and Beyond: Initial Considerations**. Disponível em: <<https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf>>. Acesso em: 9 mar. 2017.
- KELSEN, Hans. **Teoria Pura do Direito** [tradução João Baptista Machado]. 6. ed. São Paulo: Martins Fontes, 1999.
- MARKY, Thomas. **Curso Elementar de Direito Romano**. 8. ed. São Paulo: Saraiva. 1995.
- MANN, Frederick Alexander. **The legal aspect of money**. 5. ed. Oxford: Clarendon press. 1992.
- ROMA, Bruno Marques Bensal; SILVA, Rodrigo Freitas da. O desafio legislativo do bitcoin. **Revista de Direito Empresarial**. vol. 20. ano 4. p. 109-128. São Paulo: Ed. RT, 2016.
- ULRICH, Fernando. **Bitcoin: a moeda na era digital**. São Paulo: Instituto Ludwig Von Mises Brasil, 2014.
- VAN DER LAAN, Cesar Rodrigues. É Crível uma Economia Monetária Baseada em **Bitcoins? Limites à disseminação de moedas virtuais privadas**. Disponível em: <<https://www12.senado.leg.br/publicacoes/estudos-legislativos/tipos-de-estudos/textos-para-discussao/td163/view>>. Acesso em: 9 mar. 2017.
- VERÇOSA, Haroldo Malheiros Duclerc. Breves considerações econômicas e jurídicas sobre a criptomoeda. Os bitcoins. **Revista de Direito Empresarial**. vol. 14. ano 4. p. 139-154. São Paulo: Ed. RT, mar.-abr. 2016.