CRIPTOATIVOS: CONCEITO, CLASSIFICAÇÃO, REGULAÇÃO JURÍDICA NO BRASIL E PONDERAÇÕES A PARTIR DO PRISMA DA ANÁLISE ECONÔMICA DO DIREITO

Manoel Gustavo Neubarth Trindade[1]

Márcio dos Santos Vieira[2]

Sumário: I – Introdução; II – Ponderações Introdutórias sobre Blockchain; III – Criptoativos e a sua Classificação; IV – Initial Coin Offering (ICO); V – A Regulação dos Criptoativos no Brasil; VI –Necessidade de Marco Regulador Universal; VII – A Eficiência Econômica dos Criptoativos; VIII – Conclusões; IX – Referências Bibliográficas

Palavras-Chave: Criptoativos. Regulação Jurídica. Análise Econômica do Direito.

I – INTRODUÇÃO

1 Advogado. Economista. Pós-Doutorando na Faculdade de Direito da Universidade de Lisboa (FDUL). Doutor em Direito (UFRGS). Mestre em Direito (UFRGS). Especialista em Processo Civil (UFRGS). Professor Permanente do Mestrado Profissional em Direito da Empresa e dos Negócios da UNISINOS. Editor da Revista de Direito da Empresa e dos Negócios do Programa de Mestrado Profissional em Direito da Empresa e dos Negócios da UNISINOS. Coordenador e Professor do LLM em Direito dos Negócios da UNISINOS. Coordenador e Professor da Especialização em Direito dos Contratos e da Responsabilidade Civil da UNISINOS. Professor da Graduação em Direito da UNISINOS Porto Alegre LES (*Law, Economics and Society*) e da Graduação em Direito da UNISINOS São Leopoldo.

2 Advogado. Mestre em Direito pela Faculdade de Direito da Universidade do Vale do Rio dos Sinos (UNISINOS). LLM em Direito dos Negócios pela UNISINOS. Especialista em Processo Civil pela UNISINOS. Membro da Associação Brasileira de Direito e Economia – ABDE e do Instituto de Direito e Economia do Rio Grande do Sul – IDERS.

A tecnologia, em especial da informação e da comunicação (TCI), observa um padrão que tem por característica a aceleração constante da sua evolução. Fala-se atualmente no crescimento exponencial, em oposição ao linear, que foi o paradigma dominante pelo menos ao longo de 10.000 (dez mil) anos de história da civilização humana.3

E, a cada nova geração, o ritmo de mudanças aumenta. Isso permite o surgimento de uma cultura da experimentação, da inovação e de um ambiente em que, cada vez mais, a mudança é a principal certeza. A evolução das tecnologias da informação e da comunicação atingiu um estágio em que não apenas afeta a maneira como as pessoas se relacionam, mas também já materializa a possibilidade de alterar a maneira como as sociedades produzem riqueza e, ainda mais, a forma como essa (riqueza) circula entre os diferentes agentes econômicos.

A profundidade de tais mudanças recém principia a ser percebida. No limite, tenderá a reequilibrar as forças que determinam os rumos da evolução humana. As ditas promessas não cumpridas da modernidade, pelo menos não até agora, como o acesso praticamente universal aos bens da vida e a promoção integral e permanente do ser humano, têm a chance de se tornarem viáveis, não por meio de luta armada ou da revolução dos ditos oprimidos, mas sim por intermédio de algoritmos matemáticos, da lógica de programação e de organizações autônomas distribuídas (ou, como mais conhecidas em inglês, *decentralized autonomous organization* – DAO).

Em síntese, o eixo do poder, de uma forma inédita no curso da humanidade, poderá ser deslocado, e com um grau

3 O que faz lembrar a Lei de Moore, que consiste na projeção de uma tendência relacionada à indústria de microchips e processamento de computadores, concebida por meio da observação de Gordon Earl Moore, que, em meados 1965, sustentava que o número de transistores dos chips teria um aumento de 100%, pelo mesmo custo, a cada período de 18 meses.

de eficiência também inédito. Caminha-se a passos largos para uma forma de arranjo social em que o paradigma da escassez poderá dar lugar ao paradigma da maximização, ainda que potencial, da eficiência econômica, haja vista o ensejo, cada vez maior, de todas as trocas possíveis.

E, nesse contexto, um dos fenômenos que é protagonista nesta viragem histórica é a arquitetura computacional chamada de *blockchain*. Justamente é esta tecnologia4 de registro distribuído que possibilita, dentre outras aplicações, o surgimento dos criptoativos, cuja emissão e circulação independem de uma autoridade estatal, central ou intermediadora.

Importante registrar que a temática é por demais recente, muito embora já venha impactando seriamente diversos mercados e agentes econômicos no mundo todo. Frise-se que o tema surge, timidamente, em finais de 2008, logo após a chamada Crise do *Subprime* nos Estados Unidos (que afetou os mercados financeiros no mundo inteiro), e, seguindo a lógica exponencial antes mencionada, vem ganhando relevância ano a ano.

No ano de 2017, o assunto extrapolou os circuitos próximos de sua origem e passou a chamar a atenção da sociedade de modo geral, muito em função da valorização muito célere e elevada do criptoativo chamado bitcoin, uma das primeiras aplicações concretas de uma estrutura de *blockchain*, ao lado de um número cada vez maior de criptoativos que vêm sendo lançados a cada dia.

O crescimento dos investimentos em criptoativos e o correlato movimento das chamadas *Initial Coin Offerings* (ou, como mais conhecidas, ICOs), operação de emissão de criptoativos e outros ativos virtuais, sobretudo para fins de transferência de recursos, captação de poupança pública e

4 Muito embora os profissionais da Tecnologia da Informação (TI) prefiram, para designar *blockchain*, ao invés de se referirem a uma tecnologia, a utilização do termo arquitetura computacional.

investimentos – fez com que as autoridades monetárias e do mercado de capitais ao longo do mundo despertassem o seu interesse e passassem a observar com muita atenção tais movimentos. De expectadores um tanto curiosos, passaram a considerar seriamente os meios de regular tais fenômenos nascentes.

Preocupações com a prática de ilícitos, como lavagem de dinheiro, tráfico de drogas e, também, fraudes financeiras, em larga medida animam as iniciativas estatais. Mas, para além destas preocupações coerentes, há também a preocupação com uma eventual troca de mãos no jogo do poder financeiro mundial. A desintermediação possibilitada pelo uso massivo de criptoativos e de outros ativos digitais, no limite, pode vir a tornar, pelo menos em teoria, desnecessárias ou, no mínimo, diminuir consideravelmente a importância das instituições financeiras tradicionais, também chamadas de incumbentes, pelo menos da forma como hoje as conhecemos.

Assim sendo, o presente trabalho busca contribuir para a necessária compreensão detalhada e sistematizada do fenômeno que está em curso. Para atingir tal mister, na primeira parte do presente trabalho, procura-se apresentar questões técnicas e conceituais elementares em torno da *blockchain*, que é a estrutura tecnológica que suporta todo o movimento ao qual aqui se debruça. Busca-se entender, por exemplo, o que é criptografia assimétrica, bem como a sua relevância no processo de transmissão e registro de informações. Analisam-se também algumas características fundamentais das plataformas construídas com base em *blockchain*.

Em seguida, pretende-se compreender o que são os criptoativos, em um cotejo analítico com as características e funções performadas por outros ativos e moedas tradicionais.

Na segunda parte do trabalho, passar-se-á então a abordar questões de ordem técnico-jurídicas, especificamente quanto à normatização e regulação dos criptoativos.

Observar-se-ão as iniciativas em curso no Brasil e também se ponderará com a de outras jurisdições. O tema, em sua essência, é transnacional e sua operação somente faz sentido quando sintonizada com os movimentos em curso nos demais mercados.

Por fim, ponderar-se-ão impressões a respeito da necessidade de um marco regulador universal. Contudo, dada a velocidade da evolução do tema e a dinâmica dos acontecimentos, é importante referir que o presente trabalho reflete o estado da arte ao tempo de sua produção, em que pese a velocidade dos avanços tornar necessária atualização constante. Há fundamentos aqui referidos que se mantém, porém, a crônica dos acontecimentos requer acompanhamento constante por todos quantos se interessam por estas realidades emergentes e com potencial de acelerar ainda mais os velozes processos de mudança testemunhados neste primeiro quarto do século XXI.

II – PONDERAÇÕES INTRODUTÓRIAS SOBRE BLOCKCHAIN

Uma advertência preliminar se faz necessária. As questões de ordem técnica relacionadas com a ciência da computação e a arquitetura de *blockchain* serão abordadas a partir de uma perspectiva introdutória, não constituindo pretensão deste artigo, portanto, prover informações com o matiz técnico que a ciência da computação confere ao assunto. A intenção é, isto sim, prover informações necessárias para sustentar o argumento central do trabalho, vinculado ao grau e conformação da regulação que se faz pertinente no tocante ao tema dos criptoativos.

Feita esta necessária advertência preliminar, é possível afirmar, em primeiro lugar, que *blockchain* não se trata apenas de mais uma novidade tecnológica. Não se está aqui a lidar

simplesmente com mais um passo no deveras célere avanço das tecnologias de informação e comunicação (TIC).[5]

As *blockchains* (e o plural fará sentido no curso do texto) se constituem em um fenômeno com o potencial de representar uma mudança paradigmática quase ou tão forte quanto foi a implantação da *World Wide Web* (ou "*www"*) 30 anos atrás. A arquitetura "*www"* foi o que possibilitou a popularização das comunicações remotas por meio da infraestrutura da *internet*. Os primórdios da rede mundial de computadores estão nos já longínquos anos 60 do século passado, como uma estratégia militar dos Estados Unidos da América, para garantir a descentralização e a redundância de informações em caso de ataques estrangeiros, por meio da *Arpanet*. O grande público, porém, somente tomou ciência das infindáveis possibilidades desta infraestrutura a partir de meados dos anos 90 do século passado, quando se iniciou a viabilização das aplicações comerciais da *World Wide Web*.

Os últimos 20 a 25 anos são testemunhas de uma verdadeira revolução na forma das pessoas se relacionarem, produzirem e fazerem circular riquezas. A democratização do conhecimento, a instantaneidade da informação, a drástica redução dos custos de transação nos mais variados mercados e o fenômeno das redes sociais são apenas alguns dos tantos efeitos do nascimento da sociedade do conhecimento, inclusive culminando na chamada Economia de Plataforma, novo paradigma de organização dos mercados que vem promovendo profundas alterações na forma de se transacionar, assim como desafiando profundamente o Direito a se adaptar a essas novas

5 "*Understanding blockchains is tricky. You need to understand their message before you can appreciate their potential. In addition to their technological capabilities, blockchains carry with them philosophical, cultural, and ideological underpinnings that must also be understood*". *In*: MOUGAYAR, Willian. *The Business blockchain. Promise, practice and application of the next internet technology*. New Jersey: John Willey & Sons. Inc, 2016, Capítulo 1, p. 2.

realidades.[6]

A arquitetura de *blockchain*, por sua vez, tem o potencial de representar uma virada paradigmática semelhante a "*www"*. Estamos no limiar de uma potencial profunda reorganização e de um consequente rearranjo nas formas de organização da civilização humana, e muito disso passa pela adoção das soluções possibilitadas por esta arquitetura e este ambiente computacional.

Este extraordinário potencial levou o *Bank of England* a sugerir em um relatório de 2014 que a *blockchain* pode se transformar na "internet das finanças". Diz o relatório:

> With conventional bank deposits, banks hold the digital record and are trusted to ensure its validity. With digital currencies, by contrast, the ledger containing the record of all transactions by all users is publicly available to all. Rather than requiring users to have trust in special institutions, reliance is placed on the network and the rules established to reliably change the ledger.[7]

Como referido, a primeira aplicação efetiva de uma *blockchain* foi o bitcoin, criptoativo que muito se assemelha funcionalmente às moedas tradicionais (pelo menos quanto aos seus aspectos econômicos) e que se tornou amplamente

6 Para melhor compreensão do paradigma da Economia de Plataforma, ver: TRINDADE, Manoel Gustavo Neubarth Trindade. Economia de Plataforma (ou tendência à bursatilização dos mercados): Ponderações Conceituais Distintivas em relação à Economia Compartilhada e à Economia Colaborativa e uma Abordagem de Análise Econômica do Direito dos Ganhos de Eficiência Econômica por meio da Redução Severa dos Custos de Transação. *Revista Jurídica Luso-Brasileira*, Ano 6 (2020), n.º 4. Disponível em: <https://www.cidp.pt/publicacao/revista-juridica-lusobrasileira-ano-6-2020-n-4/209>. Acesso em: 07 de set. 2020.

7 Em tradução livre: "Com os depósitos bancários convencionais, os bancos detêm os registros digitais e detém a credibilidade necessária para assegurar a sua validade. Com as moedas digitais, ao contrário, o repositório dos registros de todas as transações efetuadas pelos usuários está disponível publicamente, para todos. Ao invés de demandar aos usuários que confiem em instituições especiais [os bancos], a confiança fica localizada na própria rede e nas regras estabelecidas para modificar os registros de forma absolutamente confiável", *in: Are you ready to blockchain?* Thomson Reuters. Disponível em: <https://www.thomsonreuters.com/en/reports/blockchain.html>. Acesso em: 07 de set. 2020.

conhecida em especial no segundo semestre do ano de 2017, em função de sua expressiva valorização. Por esta razão, o uso da *blockchain* está tão fortemente vinculado ao universo dos criptoativos, sobretudo das hipóteses em que se assemelham a moedas, embora a sua aplicação, absolutamente, não se limite.

Os fundamentos do funcionamento do bitcoin estão no seminal *white paper* de titularidade do pseudônimo Satoshi Nakamoto:[8]

> Este *paper* descreve o processo de criação de uma versão puramente *peer-to-peer* [ponto a ponto] de uma moeda eletrônica que pode ser enviada diretamente de uma parte à outra sem a intervenção de uma instituição financeira. A chave para manter a integridade do sistema é um livro-razão digital que certifica a hora e data das transações, registrando-as numa cadeia contínua de registros, assim fazendo a prova inequívoca de todas as transações operadas em determinada rede.[9]

Pertinente salientar que a arquitetura de *blockchain* é viabilizada pela integração de três elementos: (I) criptografia assimétrica; (II) rede distribuída; e (III) incentivos econômicos. Sobre a criptografia assimétrica (I) se falará mais adiante. Por ora, pertinente dizer que (criptografia assimétrica) é uma estrutura matemática que permite atribuir confiança e, portanto, certificar as transações que em seu âmbito são realizadas, pois permite provar a autoria e a autenticidade das operações. Tanto é assim que seu uso é disciplinado nas legislações nacionais e comunitárias mundo afora, o Brasil

8 NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Disponível em: <https://bitcoin.org/bitcoin.pdf. Acesso em: 07 de set. 2020.

9 Livre tradução de: "The paper outlines the process of creating a purely peer-to-peer version of electronic cash that can be sent directly from one party to another without going through a financial institution. The key to maintaining the integrity of that system is a digital ledger that time-stamps transactions by logging them into an ongoing chain of record, providing proof of all transactions on the network." *In: Are you ready to blockchain?* Thomson Reuters. Disponível em: <https://www.thomsonreuters.com/en/reports/blockchain.html>. Acesso em: 07 de set. 2020.

incluído.[10]

A rede distribuída (II) é representada graficamente pelo Diagrama de Baran:

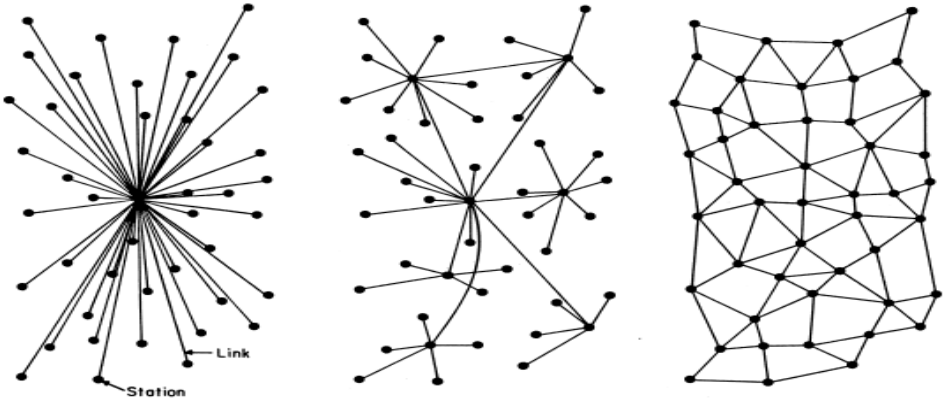


FIG. 1 — Centralized, Decentralized and Distributed Networks

Quanto à fundamental e disruptiva característica das redes distribuídas, consigna-se definição constante da própria Wikipédia (a qual, por sua vez, consubstancia-se justamente em uma rede distribuída no que tange ao desenvolvimento dos conteúdos, mas centralizada no que toca à armazenagem):

> Uma rede distribuída assemelha-se a uma malha ou a uma rede de pesca, na qual cada nó é independente do outro, mas está diretamente ligado ao outro completando assim a trama. Seu nome está ligado ao modo como gerencia processos: distribuidamente. Uma rede distribuída é indicada para redes de computadores que devam trabalhar em conjunto, somando seu processamento, mas ao mesmo tempo mantendo sua independência no caso de alguma das máquinas tornar-se indisponível. Como o próprio nome diz, este modelo de rede visa a distribuição de tarefas. Assim, a rede distribuída consiste em adicionar o poder computacional de diversos

10 Vide a Medida Provisória 2.200-2/2001, que "*Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências"*. Disponível em: http://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm. Acesso em: 07 de set. 2020.

> computadores interligados, para processar colaborativamente determinada tarefa de forma coerente e transparente, ou seja, como se apenas um único e centralizado computador estivesse executando a tarefa. A união desses diversos computadores com o objetivo de compartilhar a execução de tarefas e o *software* que faz esse gerenciamento leva o nome de sistema distribuído.[11]

O modelo de rede da *internet* tal qual a conhecemos, baseado na "www", é um modelo cliente-servidor. Mesmo um modelo cooperativo, como por exemplo a já mencionada Wikipédia, é distribuído, porém centralizado. Isso significa que, a princípio, qualquer pessoa pode colaborar com o conteúdo da Wikipédia e alimentar o seu banco de dados, mas este banco de dados está armazenado nos servidores da Wikipédia. Portanto, o conteúdo está centralizado. A Wikipédia detém o controle sobre este banco de dados e é responsável por sua manutenção e controle. Isto funciona de forma similar com bancos de dados de bancos ou entidades governamentais.

Com a arquitetura de *blockchain*, o banco de dados não está centralizado. O banco de dados está distribuído entre os integrantes da rede. Todos detêm uma cópia atualizada deste banco de dados, ou seja, de toda a informação daquela determinada rede.

Então, se o protocolo computacional viabiliza que todos os integrantes da rede tenham acesso à versão mais atualizada das informações, ou do banco de dados daquela rede, não há a necessidade de um terceiro de confiança das partes (*trusted third party*) para assegurar qual é a informação correta e mais atualizada.

A rede distribuída possibilita, portanto, que todas as tarefas necessárias ao funcionamento, por exemplo, de um meio de pagamento, sejam efetuadas pelos integrantes da rede, sem a necessidade de um comando central. A tarefa de

11 Modelos de Rede. Disponível em: <http://wiki.nosdigitais.teia.org.br/Modelos_de_Rede>. Acesso em: 07 de set. 2020.

confirmação das transações, como a de transferência de fundos, é efetuada pelos integrantes da própria rede.

Para evitar a ocorrência de fraudes, em especial o *double spending*,[12] quando o mesmo registro eletrônico de fundos é utilizado mais de uma vez, entram em cena os incentivos econômicos (III). Estes resolvem o problema que a literatura busca explanar com a analogia do dilema dos generais bizantinos.[13] E estes incentivos se dão por meio do processo que ficou conhecido como mineração.

Nesse ponto, os integrantes da rede são incentivados a confirmar as transações, por meio de testes matemáticos, sendo que, para efetuar estas confirmações, os mineradores disponibilizam a capacidade de processamento dos seus computadores, pelo que são remunerados por esta atividade. No caso dos criptoativos, a remuneração alcançada é uma fração do próprio criptoativo transacionado, seguindo-se o protocolo

12 A grande contribuição do "[...] criador do bitcoin, Satoshi Nakamoto (um pseudônimo, não se sabe se é uma ou mais pessoas), foi impedir que um participante do mercado gastasse o mesmo dinheiro duas vezes, já que, na internet, quando envia foto ou arquivo a um destinatário, o remetente sempre guarda uma cópia do anexo transmitido. Para evitar esse gasto duplo, em vez de usar intermediário único como um banco ou empresa de cartão, Satoshi teve a ideia de validar as transações por meio de tecnologia de supervisão pública e descentralizada, conhecida por blockchain ou, mais precisamente, por tecnologia de registro descentralizado, do inglês "distributed ledger technology", ou DLT". *In*: *A nova arte de fazer dinheiro*. Jornal Valor, edição de 19/01/2018. Disponível em: <http://www.valor.com.br/cultura/5266749/nova-arte-de-fazer-dinheiro?utm_source=Facebook&utm_medium=Social&utm_campaign=Compartilhar>. Acesso em 07 de set. 2020.

13 "Um mecanismo de consenso pode ser visto como uma solução ao clássico Problema dos Generais Bizantinos que consiste em resolver o dilema de atingir um consenso entre os participantes (que neste caso são os generais) com um objetivo comum (vencer uma batalha). Embora possam haver generais traidores, os quais têm objetivos opostos ao consenso e tentarão atrapalhar o processo, a ideia é que, se houver um número mínimo de generais leais (normalmente a maioria), o mecanismo de consenso garanta a conquista do objetivo comum, sem que os traidores consigam impedir. *In:* MAEHARA ALIAGA, Yoshitomi Eduardo. *Estudo sobre mecanismos de consenso de baixo custo para Blockchain*. Dissertação de mestrado. Universidade Estadual de Campinas. Faculdade de Engenharia Elétrica e de Computação. Campinas, 2019. Disponível em: <http://repositorio.unicamp.br/bitstream/REPOSIP/335887/1/Aliaga_YoshitomiEduardoMaehara_M.pdf.Acesso em: 07 de set. 2020.

computacional previamente definido. Esse processo de confirmação possibilita a emissão ou criação de moedas (ou mesmo frações destas), justamente para remunerar quem presta este serviço (emprestando energia e emprestando capacidade de processamento).

O engendrar destas três dimensões, quais sejam, (I) criptografia assimétrica, (II) rede distribuída e (III) incentivos econômicos possibilita que às transações efetuadas em uma rede de *blockchain* seja agregado o atributo da confiança ou, dizendo de outro modo, deixando esse atributo (qual seja, a confiança) de ser necessário, pelo menos no que toca a um terceiro verificador, uma vez que a rede, conformada por todos os seus componentes, é quem certifica e registra as operações (por isso, atribuindo-lhe confiança).

Mais, a confiança que aqui se refere não significa confiar na lisura da outra parte com quem se está transacionando, que na maioria das vezes é um estranho. Confiança aqui se refere à veracidade e autenticidade das transações, sejam elas da natureza que forem, sendo que, quando utilizada a tecnologia de *blockchain*, as transações são validadas, assim como registradas, pela própria comunidade, pelos próprios integrantes da rede.

Assim, a *blockchain* pode ser compreendida, de uma maneira simples, como uma cadeia inquebrável de registros, imune de ser violada, e mantida pela comunidade que dela se utiliza. E, na medida em que as transações vão ocorrendo, vão sendo registradas em blocos de informações. E estes blocos vão se conectando em uma corrente contínua. Daí o termo *blockchain* – cadeia de blocos.

É possível se fazer uma analogia com a cadeia registral, própria do registro imobiliário e, consequemente, do Direito Registral e, também, Notarial. Não há como simplesmente "apagar" ou "modificar" um determinado registro. E mesmo que, em tese, isso fosse possível, no caso da

blockchain, deveria contar com o consentimento de toda a comunidade, toda a rede integrante de uma determinada *blockchain*.

Este atributo da confiança é possibilitado, em larga medida, pelo uso da criptografia. Dada a importância deste tema, dedicar-se-á a ele as linhas que seguem.

Criptografia significa, etimologicamente, escrita oculta. Consiste em um método para embaralhar uma mensagem de modo que somente quem conheça o código de embaralhamento possa acessar o significado e o conteúdo da mensagem. Pertinente é a seguinte definição:

> A criptografia (escrita oculta, do grego), desenvolvida dos antigos métodos de transposição e substituição de símbolos, consiste na técnica de embaralhamento, com códigos simétricos e assimétricos, de dados confidenciais, que poderão ser identificados apenas por fonte segura. Este é, na atualidade, um dos meios mais garantidos de manter o sigilo das informações na rede. O uso crescente da criptografia tem sido útil a assegurar, nos limites da previsibilidade, a integridade e o sigilo dos dados e das comunicações via Internet.[14]

Trata-se de um conceito matemático, aplicado à segurança da informação. Usa-se para garantir a confidencialidade e veracidade de informações, codificando-as, de modo a ocultar o seu conteúdo, impedindo alterações indevidas e mesmo o uso não autorizado.

Conta a história que a criptografia estava já presente nas conquistas militares empreendidas por Júlio César.[15] Uma técnica criptográfica incipiente era usada pelos romanos para enviar mensagens aos centuriões nos campos de batalha. Tal técnica era adotada para evitar traições por parte dos

14 CRUZ E TUCCI, José Rogério. *Eficácia probatória dos contratos celebrados pela Internet. In:* DE LUCCA, Newton (Coordenador). *Direito & Internet.* Bauru: Ed. Edipro, 2000. p. 277.

15 QUEIRÓZ, Régis Magalhães Soares de. *Assinatura Digital e o Tabelião Virtual. In:* DE LUCCA, Newton (Coordenador). Direito & Internet. Bauru: Ed. Edipro, 2000. p. 389.

mensageiros ou interceptação das mensagens pelos inimigos. Há quem diga inclusive que o desenvolvimento da criptografia estaria profetizado na Bíblia, no versículo 17 do capítulo 2 do Apocalipse.[16]

Na informática, a criptografia é utilizada por meio de chaves, que nada mais são do que funções matemáticas que embaralham ou encriptam as mensagens. Em redes fechadas, é possível utilizar uma única chave para encriptar e decriptar a mensagem, pois não há o risco de que esta chave seja interceptada. Era a técnica de que se utilizava o sistema bancário até anos atrás, quando da remessa de ordens de pagamento.

Já numa rede aberta, como a *internet*, um tal sistema com uma única chave não seria seguro, uma vez que no momento em que a chave fosse transmitida para que o receptor pudesse decriptar o documento, haveria a possibilidade desta chave ser interceptada, comprometendo a segurança dos dados.

Por conta disso, desenvolveu-se a criptografia por chaves assimétricas, que se utiliza de algoritmos para operacionalizá-la. A Marinha Americana foi quem primeiro divulgou um algoritmo capaz de produzir chaves assimétricas, o RSA, em 1978. Este algoritmo gera duas chaves, uma pública e uma outra privada, que são matematicamente relacionadas. No atual estágio do conhecimento matemático, é computacionalmente inviável calcular a chave privada a partir da chave pública.[17]

16 "Quem tem ouvidos, ouça o que o Espírito diz às igrejas: Ao que vencer darei Eu a comer do maná escondido, e dar-lhe-ei uma pedra branca, e na pedra um novo nome escrito, o qual ninguém conhece senão aquele que o recebe."

17 "A geração simultânea do par de chaves é feita por um algoritmo que divide números inteiros, descoberto por Euclides há 2500 anos. A assinatura e sua verificação são feitas por um algoritmo que executa exponenciação modular. Dos algoritmos que fazem isso, o mais eficiente conhecido, chamado FME (*Fast Modular Exponentiation*), é de complexidade linear. Para se quebrar o RSA, isto é, para se derivar a chave privada a partir da chave pública, precisa-se fatorar números inteiros, e o algoritmo mais eficiente hoje conhecido para isso é o NFS (*Number Field Sieve*), de

FUNCIONAMENTO DA CRIPTOGRAFIA

O que se passa agora a descrever é o processo pelo qual se assina digitalmente um documento. A maioria dos passos aqui descritos ocorrem dentro do computador, e não são vistos pelo usuário. Sua compreensão, no entanto, é crucial para que se possa compreender e se posicionar criticamente acerca dos aspectos juridicamente relevantes do tema.

Assim, importante ressaltar que a assinatura digital de um documento implica duas etapas. Na primeira, utiliza-se um processo matemático, denominado algoritmo *hash*, para produzir um resumo da mensagem (*message digest*). Este resumo consiste numa série de números, letras e símbolos aparentemente sem sentido, porém matematicamente relacionado com o documento que se está assinando. É altamente

complexidade exponencial. Esses algoritmos juntos atingem o propósito da criptografia assimétrica, devido a uma propriedade de números inteiros descrita por um teorema, demonstrado há 250 anos por um juiz de Direito de Toulouse na França, que era matemático nas horas vagas: Pierre de Fermat, um dos mais geniais matemáticos de todos os tempos. Enquanto a relação entre o custo para se gerar e usar as chaves, e o custo para derivar uma da outra, for uma relação linear/exponencial, o controle de custo da fraude pela manipulação da chave de verificação estará com o indivíduo que gera as chaves. [...] Poderá ser descoberta amanhã uma forma mais eficiente de se fatorar números. Esta descoberta só inviabilizaria o RSA se este novo método de se fatorar números tiver complexidade sub-exponencial. Mas será que existe algoritmo para isso? Em tese poderia existir, pois nenhum matemático até hoje provou que um tal algoritmo não possa existir. Mas se existir, qual a probabilidade de que tal algoritmo venha a ser descoberto? Aqui faz-se necessário registrar que os matemáticos mais brilhantes que a humanidade já produziu têm buscado este algoritmo há pelo menos 2500 anos sem sucesso, e que dentre os contemporâneos, muito poucos admitiriam acreditar na possibilidade de sua existência. A outra possibilidade para a fatoração sub-exponencial é a computação quântica, que poderia linearizar a complexidade da fatoração, através da paralelização exponencial de um dos algoritmos de fatoração já conhecidos. Mas a computação quântica é por enquanto apenas uma promessa." REZENDE, Pedro Antonio Dourado de. *Carta aberta ao Dr. Renato Opice Blum. Proposta de Debate na 1ª Conferência Internacional de Direito na Internet e na Informática*. São Paulo, 6 e 7 de novembro de 2000. Disponível em: < https://www.cic.unb.br/~rezende/trabs/gesso.htm>. Acesso em: 07 de set. 2020.

improvável que dois documentos diferentes resultem no mesmo resumo.

A segunda etapa consiste em criptografar o resumo do documento. O usuário autoriza o computador a utilizar a sua chave privada para realizar uma operação matemática que criptografa, embaralha, o resumo. O resumo do documento, criptografado, pode ser considerado a assinatura propriamente dita.

Uma vez assinado o documento, este será enviado ao destinatário. O que se envia ao destinatário é o documento, seu resumo criptografado e a chave pública, esta que deverá ser utilizada para verificar a autenticidade da assinatura e a integridade do documento. Ao receber a mensagem, o computador do destinatário também executa duas etapas para promover a verificação da assinatura. Em primeiro lugar, identifica-se o processo matemático utilizado para criar o resumo do documento e, utilizando este mesmo processo, cria-se um resumo do documento.

A seguir, utilizando-se a chave pública do remetente, o computador decripta, desembaralha o resumo criptografado do documento. Se estes dois resumos gerados pelo computador do destinatário forem idênticos, está provado que o documento recebido foi gerado pelo titular daquela chave pública, e que este documento não foi alterado durante a transmissão. Se uma única vírgula for modificada, os dois resumos não serão coincidentes, o que acusará a adulteração do documento.

O processo acima referido, em que se utiliza a chave privada para assinar o documento e a chave pública para verificar a autenticidade da assinatura, atesta a autoria do mesmo, permite identificar a origem do documento, assim como que este não foi adulterado. Porém, se alguém interceptá-lo no trajeto entre remetente e destinatário, terá acesso a todo o seu conteúdo, embora não possa modificá-lo, pois se assim o fizesse, a conferência detectaria a modificação.

Para isto, basta que a pessoa interessada em conhecer o teor da mensagem que está sendo enviada use a chave pública do remetente para decriptografar o documento, uma vez que esta, como o próprio nome diz, está à disposição de qualquer pessoa que a queira utilizar.

Se o signatário de um documento quer também evitar que um terceiro tenha acesso a seu conteúdo, ou seja, quer que a confidencialidade seja preservada, deve fazer, simultaneamente ao processo acima descrito, o processo inverso. Este se dá utilizando a chave pública do remetente para criptografar o *message digest*. Vale dizer, o documento é assinado duas vezes. Uma vez com a chave privada do remetente e outra vez com a chave pública do destinatário. Desta forma, somente o detentor da chave privada relacionada a esta chave pública poderá decriptografar o documento, estando, deste modo, garantida a confidencialidade do mesmo.

Para que o destinatário da mensagem tenha acesso a seu conteúdo, deve primeiramente utilizar sua chave privada para decriptografar o documento. Com isto estar-se-á conferindo a confidencialidade do mesmo. Concluída esta etapa, deverá então utilizar a chave pública do remetente, a fim de conferir a autenticidade e integridade do documento. Se esta segunda verificação for positiva, estar-se-á tendo acesso a um documento absolutamente autêntico e confidencial.

Na *blockchain*, a criptografia de chaves assimétricas é integrada a mais dois elementos: uma rede distribuída com um "livro de registros" compartilhado na rede, e um sistema de incentivos para que os integrantes da rede validem as transações.[18]

Toda a arquitetura de *blockchain* pode ainda ser descrita segundo três aspectos: o técnico, o empresarial (*business-wise*) e o legal. Tecnicamente, a *blockchain* é um banco

18 Disponível em: <https://www.coindesk.com/information/how-does-blockchain-technology-work/>. Acesso em: 07 de set. 2020.

de dados que mantém um sistema de registro distribuído na rede e descentralizado, o qual pode ser inspecionado a qualquer tempo.

Do ponto de vista de negócio (empresarial), a *blockchain* é uma rede de transações e trocas, que movimenta valores e ativos entre pares, sem a necessidade da intervenção de intermediários confirmando a veracidade destas transações.

Do ponto de vista legal, a *blockchain* valida as transações, agrega o atributo da certeza e segurança jurídica, substituindo as entidades tradicionais de certificação, sejam elas bancos, tabeliães, registradores ou entidades governamentais de modo geral.

Como visto, em síntese, trata-se de tecnologia de registro distribuído que visa a descentralização como medida de segurança, servindo como um livro-razão (*ledger*) digital, certificando e registrando as transações em uma cadeia (*chain*) contínua de blocos (*blocks*), fazendo prova de todas as transações operadas em uma determinada rede. Com a arquitetura de *blockchain*, os bancos de dados não estão centralizados (descentralização), encontrando-se distribuídos entre os integrantes da rede. Todos detêm uma cópia atualizada deste banco de dados, ou seja, de toda a informação daquela rede. A tarefa de confirmação das transações, por exemplo a transferência de fundos, é efetuada pelos próprios integrantes da rede.

III – CRIPTOATIVOS E A SUA CLASSIFICAÇÃO

Desde já, podemos conceituar criptoativos como ativos virtuais, que são expressos por meio de um código de computador. Este código é a representação da titularidade, ou da propriedade, destes ativos. Vale salientar que as suas validações se dão baseadas em criptografia, conforme o

mecanismo de conferência demonstrado no item anterior.

Nesse sentido, importante dizer que o bitcoin foi o primeiro dos criptoativos com tais características, tendo os seus fundamentos lançados no já referido *paper* seminal do pseudônimo Satoshi Nakamoto, que pode ser uma única pessoa ou um grupo de pessoas, intitulado *Bitcoin: A Peer-to-Peer Electronic Cash System*.[19]

Neste *paper* estão estabelecidas as bases do funcionamento dos criptoativos, como o bitcoin, que exercem as funções econômicas de moedas, mediante a utilização da *blockchain*,[20] quais sejam:

- Transações e interações ponto a ponto;

- Ausência de intermediação de instituições financeiras;

- Comprovação criptográfica ao invés de uma entidade central que atribua confiança;

- Deslocamento da confiança de uma instituição central para a própria rede.[21]

Segundo Yermack,[22] Nakamoto teria minerado e colocado em circulação as primeiras unidades de bitcoin em 2009, basicamente para demonstrar o método a um grupo de observadores *online*. Já a circulação de bitcoin ocorreu

19 NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Disponível em: <https://bitcoin.org/bitcoin.pdf. Acesso em: 07 de set. 2020.

20 NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Disponível em: <https://bitcoin.org/bitcoin.pdf. Acesso em: 07 de set. 2020.

21 *Peer-to-peer electronic transactions and interactions*; *Without financial institutions*; *Cryptographic proof instead of central trust*; *Put trust in the network instead of in a central institution*; *in:* NAKAMOTO, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. Disponível em: <https://bitcoin.org/bitcoin.pdf. Acesso em: 07 de set. 2020 e, de forma semelhante, MOUGAYAR, Willian. *The Business blockchain. Promise, practice and application of the next internet technology*. New Jersey: John Willey & Sons. Inc, 2016, Cap. 1, p. 7.

22 YERMACK, David. *Is bitcoin a real currency? An economic appraisal*. Working Paper 19747, NATIONAL BUREAU OF ECONOMIC RESEARCH 1050, Cambridge (MA), dezembro 2013, p. 8. Disponível em: <http://www.nber.org/papers/w19747>. Acesso em: 07 de set. 2020.

primeiramente entre voluntários e entusiastas do mundo digital. Então, o interesse cresceu ao ponto de o criptoativo começar a ser transacionado em 2010, por uma plataforma japonesa, a Mt. Gox, que havia sido originalmente criada para transacionar cartões de um jogo chamado *Magic*. No primeiro dia de *trading* na Mt. Gox, 20 bitcoins trocaram de mãos, ao preço de 4,951 (quatro vírgula novecentos e cinquenta e um centavos de dólar) cada, com volume total de um pouco menos de um dólar.

A primeira aquisição na qual foram utilizados bitcoins teria sido de 2 (duas) pizzas, ao custo de 10.000 (dez mil) bitcoins, ainda em 2009. Conta-se que a pizzaria não aceitava bitcoins diretamente, então um intermediário aceitou pagar as pizzas com seu cartão de crédito, recebendo bitcoins em troca. Considerando o pico de mais de 19 mil dólares em dezembro de 2017, esta transação chegou a equivaler a 190 milhões de dólares.[23]

Saliente-se que todo criptoativo é suportado por um sistema, que possibilita que transações sejam efetuadas sem a necessidade da intermediação de uma autoridade central, seja um banco ou um sistema de pagamentos.

A estrutura de criptografia e o sistema de validação matemática propiciados por estes sistemas que sustentam os criptoativos possibilitam que estas operações financeiras sejam efetuadas de forma segura, verificável e imutável.

CLASSIFICAÇÃO DOS CRIPTOATIVOS

Uma classificação possível[24] é a que considera pelo

23 YERMACK, David. *Is bitcoin a real currency? An economic appraisal*. Working Paper 19747, NATIONAL BUREAU OF ECONOMIC RESEARCH 1050, Cambridge (MA), dezembro 2013, p. 8. Disponível em: <http://www.nber.org/papers/w19747>. Acesso em: 07 de set. 2020.

24 "Em tese, os 'tokens' podem ser atrelados ao direito de uso dos recursos computacionais de uma rede, aos direitos de uso de um aplicativo, às fichas de aposta em um

menos 3 espécies[25] de criptoativos, a depender da finalidade para a qual são utilizados, sendo que, aliás, a partir daí, é possível identificar a categoria jurídica a qual se inserem, bem como, consequentemente, o tratamento jurídico que deve ser destinado.

COINS OU "CRIPTOMOEDAS"

É a espécie que mais se assemelha a uma moeda no sentido tradicional. As *coins*, por sua vez, utilizam-se da criptografia para serem geradas e transacionadas, e todos os seus registros são efetuados dentro de uma arquitetura de *blockchain*, sem a intervenção de um ente estatal, como ocorre com as moedas soberanas.

Mas justamente nesse ponto é que se estabelece uma das discussões mais acirradas acerca da natureza dos criptoativos, sobretudo desta espécie. Afinal, consubstanciariam os criptoativos do tipo *coin* moedas? No que toca à sua natureza econômica, a discussão se dá em torno dos 3 atributos que tradicionalmente se associam às moedas tradicionais, quais sejam: meio de troca, unidade de conta e reserva de valor.[26]

Embora para os presentes Autores os criptoativos do tipo *coin* desempenhariam, pelo menos do ponto de vista econômico e potencialmente, todos os três atributos das moedas

---

cassino digital, a dólares, à fração de um título público, à fração de propriedade de um imóvel, enfim, qualquer coisa." O que são Tokens e para que servem? O que é uma ICO? Como as Altcoins são lançadas no mercado? O que são criptomoedas e para que servem? *In*: https://steemit.com/bitcoin/@cryptofinancas/o-que-sao-tokens-e-para-que-servem-o-que-e-uma-ico-como-as-altcoins-sao-lancadas-no-mercado-o-que-sao-criptomoedas-e-para-que. Acesso em: 12 de outubro de 2020.

25 Veja: Entenda a diferença entre Coins, Utility Tokens/App Coins e Security Tokens. Disponível em: <https://criptoeconomia.com.br/entenda-diferenca-entre-coins-utility-tokens-app-coins-e-security-tokens/>. Acesso em: 12 de outubro de 2020.

26 YERMACK, David. *Is bitcoin a real currency? An economic appraisal*. Working Paper 19747, NATIONAL BUREAU OF ECONOMIC RESEARCH 1050, Cambridge (MA), dezembro 2013, p. 18. Disponível em: <http://www.nber.org/papers/w19747>. Acesso em: 07 de set. 2020.

tradicionais, para outros estudiosos do tema, os criptoativos apenas atenderiam, e com alguma precariedade, o primeiro dos atributos antes listados, ou seja, de ser um meio de troca, mas não se prestariam como unidade de conta ou como reserva de valor.[27]

Para o economista Gustavo Loyola, o bitcoin, por exemplo, é imprestável como reserva de valor ou como unidade de conta, em razão da excessiva volatilidade do seu preço. E, como meio de pagamento, não traria vantagens em relação a outras possibilidades que o mundo digital já oferece. O Economista cita também o atributo do anonimato como algo a desaconselhar a utilização das chamadas "criptomoedas". Por conta da inevitável regulação que o Economista antevê que tais criptoativos hão de sofrer, este imagina que o aumento dos custos de transação para a sua operação haverá de lhes retirar "parte relevante do charme que poderiam ter como meio de pagamento". [28]

Seguindo a mesma linha de pensamento, YERMACK[29] afirma, também falando especificamente do bitcoin, que para este se estabelecer como uma moeda fiduciária, o seu valor diário necessita se tornar mais estável (ou seja, atingir menor volatilidade), o que levaria a uma maior credibilidade como reserva de valor e como unidade de conta junto aos mercados e aos agentes econômicos.

BAROSSI-FILHO e SZTAJN, igualmente falando

27 No mesmo sentido, LOYOLA, Gustavo. *Bitcoin: criptomoeda ou pseudomoeda*. *Disponível em:* <http://www.valor.com.br/opiniao/5305917/bitcoin-criptomoeda-ou-pseudomoeda?utm_source=Facebook&utm_medium=Social&utm_campaign=Compartilhar>. Acesso em 07 de set. 2020.

28 Mais uma vez, LOYOLA, Gustavo. *Bitcoin: criptomoeda ou pseudomoeda*. *Disponível em:* <http://www.valor.com.br/opiniao/5305917/bitcoin-criptomoeda-ou-pseudomoeda?utm_source=Facebook&utm_medium=Social&utm_campaign=Compartilhar>. Acesso em 07 de set. 2020.

29 YERMACK, David. *Is bitcoin a real currency? An economic appraisal*. Working Paper 19747, NATIONAL BUREAU OF ECONOMIC RESEARCH 1050, Cambridge (MA), dezembro 2013, p. 18. Disponível em: <http://www.nber.org/papers/w19747>. Acesso em: 07 de set. 2020.

sobre o bitcoin, mas em assertiva que se aplicaria aos demais criptoativos do tipo *coin*, não lhe reconhecem como moeda no sentido convencional, justamente pela ausência dos atributos aqui referidos, e porque "se variações frequentes e elevadas nos respectivos preços ocorrem, há sujeição desse ativo a riscos elevados de seus retornos, uma descaracterização do papel econômico de um ativo enquanto moeda".[30]

Referidos Autores, no entanto, reconhecem no bitcoin um meio de troca que facilita operações e que reduz os custos de transação, em especial os de intermediação.[31]

Um dos pontos de discussão quanto à natureza dos criptoativos (notadamente da espécie *coin*), e quanto à sua viabilidade para fazer as vezes de uma moeda no sentido tradicional, é a sua vinculação a algum outro determinado ativo, ou seja, a existência de lastro. Não há, no caso dos criptoativos, do tipo *coin* (ou quiçá, também, possam ser mesmo denominados, inclusive em razão da disseminação do uso do termo, de "criptomoedas", embora tecnicamente não sejam, sobretudo do ponto de vista jurídico, moedas, como veremos ainda mais detalhadamente adiante), sequer a vinculação à crença no resgate por parte de um poder estatal.

Conforme aponta YERMACK, a lógica que governa a emissão dos criptoativos, ao se vincular ao rigor de um algoritmo matemático, retiraria a prerrogativa dos governos, por

30 BAROSSI-FILHO, Milton; SZTAJN, Rachel. Natureza Jurídica da Moeda e Desafios da Moeda Virtual. Revista Jurídica Luso-Brasileira, Ano 1 (2015), nº 1, p. 1669-1690. Disponível em: <https://www.cidp.pt/revistas/rjlb/2015/1/2015_01_1669_1690.pdf>. Acesso em: 12 de outubro de 2020.

31 "Na verdade, pode-se afirmar que é uma criação própria da engenhosidade dos agentes econômicos para se desviarem dos custos incorridos em transações intermediadas pelo sistema financeiro. Nesse sentido, a bitcoin meio de troca, cuja função primordial é evitar custos que os agentes privados incorreriam se utilizassem bancos e ou instituições financeiras outras como intermediários.", *in*: BAROSSI-FILHO, Milton; SZTAJN, Rachel. *Natureza Jurídica da Moeda e Desafios da Moeda Virtual*. Revista Jurídica Luso-Brasileira, Ano 1 (2015), nº 1, p. 1669-1690. Disponível em: <https://www.cidp.pt/revistas/rjlb/2015/1/2015_01_1669_1690.pdf>. Acesso em: 12 de outubro de 2020, p. 1686.

meio de seus bancos centrais, de manipular a oferta de tais ativos.[32 e 33]

A ausência de vinculação ou a alguma forma de garantia ou de confiança no ente estatal, e a correlata subtração a este ente estatal da possibilidade de controlar a oferta da moeda, por certo tangencia uma questão nevrálgica, ao limitar sobremaneira o poder de condução da economia por parte dos governos centrais. Em verdade, pode limitar o poder estatal em um dos pontos que justamente mais lhe outorga poder, qual seja, a política monetária.

Conforme sustentado por BAROSSI-FILHO e SZTAJN, nem sempre a autoridade monetária age no melhor interesse dos agentes econômicos, mas sim no melhor

32 "[…] bitcoin attempts to overcome the weaknesses of both fiat and gold-based money, functioning as an algorithmic currency with a deterministic supply and growth rate tied to the rigor of mathematics. No government or other central authority can manipulate the supply of bitcoins. Instead the currency is governed by cryptographic rules that are enforced by transparent computer code in a decentralized manner. While some enthusiasts have suggested a connection between bitcoin's algorithmic growth rate and the monetary orthodoxy espoused by Milton Friedman, the bitcoin protocol appears to give little or no attention to any optimal rate of monetary growth", *in*: YERMACK, David. *Is bitcoin a real currency? An economic appraisal*. Working Paper 19747, NATIONAL BUREAU OF ECONOMIC RESEARCH 1050, Cambridge (MA), dezembro 2013, p. 4. Disponível em: <http://www.nber.org/papers/w19747>. Acesso em: 07 de set. 2020.

33 Ainda, segundo o mesmo Autor: "For much of the 19th and 20th centuries, the world's most successful currencies were convertible into fixed amounts of gold or other precious metals, and for thousands of years prior to that, many currencies were minted directly from gold or silver specie. This direct connection between money and gold, secured by sovereign inventories such as the Fort Knox depository in the U.S., created public confidence in a currency's value. The gold standard collapsed in most economies between the 1920s and 1970s, partly due to the pressures of financing two World Wars, but probably even more because worldwide production of gold did not keep pace with economic growth. Since then, nearly every major economy has issued paper fiat currency, the value of which relies on public belief that a nation's government or central bank will not increase the supply of new banknotes too rapidly.", *in*: YERMACK, David. *Is bitcoin a real currency? An economic appraisal*. Working Paper 19747, NATIONAL BUREAU OF ECONOMIC RESEARCH 1050, Cambridge (MA), dezembro 2013, p. 4. Disponível em: <http://www.nber.org/papers/w19747>. Acesso em: 07 de set. 2020.

interesse do governo ou do tesouro, por conta de um comportamento oportunista, denominado de custo de agência.[34] Ou seja, é comum que as decisões acerca da emissão de moeda não levem em conta o bem-estar dos agentes econômicos envolvidos, ainda que vinculadas à ideia abstrata de atuação em nome da coletividade.

Os supracitados Autores fazem um importante resgate histórico a esse respeito, ao mencionarem os papéis que o Banco da Inglaterra exerceu a partir de fins do século XVIII:

> O fiscal, inicialmente, não era fiscalizado e enquanto guardião das preocupações do governo inglês, o Banco da Inglaterra assumiu funções clássicas de banco central. Se, enquanto controlador ou fiscalizador do sistema bancário, além de emprestador de última instância, o Banco da Inglaterra atuava como moderador das assimetrias de informação, o mesmo não pode ser afirmado quanto à função que assumia com exclusividade, principalmente a partir de fins do século XVIII, a de emissor da única fonte de papel moeda em Londres.[35]

Assim é que a aparente desvinculação dos criptoativos (ou "criptomoedas") a um ente estatal emissor, ao invés de contribuir para uma eventual fragilidade, em verdade milita em favor da sua força, e justamente justifica o seu diferencial.

Mais, também não serve para sustentar que os criptoativos, especialmente os do tipo *coin*, não se consubstanciariam em moedas o simples fato de não possuírem lastro ou valor

---

34 "[...] o modelo fiduciário de curso forçado dá espaço, além de assimetrias de informação, a comportamentos oportunistas por parte da autoridade monetária, no sentido de que a gestão monetária não é feita no melhor interesse dos agentes econômicos e sim no melhor interesse do governo ou do Tesouro. Esse tipo de comportamento oportunista é denominado custo de agência.", *in*: BAROSSI-FILHO, Milton; SZTAJN, Rachel. *Natureza Jurídica da Moeda e Desafios da Moeda Virtual.* Revista Jurídica Luso-Brasileira, Ano 1 (2015), nº 1, p. 1680. Disponível em: <https://www.cidp.pt/revistas/rjlb/2015/1/2015_01_1669_1690.pdf>. Acesso em: 12 de outubro de 2020.

35 BAROSSI-FILHO, Milton; SZTAJN, Rachel. *Natureza Jurídica da Moeda e Desafios da Moeda Virtual.* Revista Jurídica Luso-Brasileira, Ano 1 (2015), nº 1, p. 1679. Disponível em: <https://www.cidp.pt/revistas/rjlb/2015/1/2015_01_1669_1690.pdf>. Acesso em: 12 de outubro de 2020.

intrínseco. Embora tal questão seja frequentemente levantada, não passa de um ledo engano. Ressalte-se que o padrão-ouro clássico, com integral conversibilidade entre moeda e ouro, foi abandonado em 1914, sendo que os Estados Unidos da América do Norte, por sua vez, aboliram unilateralmente a conversibilidade do dólar em ouro em 15 de agosto de 1971, dando fim ao sistema de Bretton Woods, determinando o surgimento do sistema flutuante. No Brasil, saliente-se que Getúlio Vargas já havia decretado, em meados de 1933, o fim da paridade da moeda brasileira com o ouro, passando a mesma a ser uma moeda fiduciária (de fidúcia, confiança, também chamada de moeda fiat), a depender da confiança nos seus emissores, ou seja, no caso, do governo brasileiro.[36] [e] [37]

De qualquer forma, há algumas características distintivas fundamentais entre os criptoativos e as moedas tradicionais. Em essência, a principal distinção é a descentralização e a desvinculação a um ente estatal, senão vejamos.

No que tange à descentralização e desvinculação dos criptoativos a um ente estatal emissor, importa dizer que não há controle por parte de alguma instituição oficial. Elas são suportadas por redes de computadores – em geral abertas, mas também podendo ser fechadas – distribuídas ao redor do mundo. O controle sobre os criptoativos é exercido pelo protocolo objeto de consenso da comunidade, que se conecta à determinado sistema de *blockchain*.

Alguns referem, também como elemento distintivo, a limitação da oferta, sendo desde já pertinente pontuar que as moedas tradicionais são emitidas pelos bancos centrais na medida das necessidades de política econômica em curso. Em

36 O que, no ponto específico, não se distingue dos criptoativos, porquanto as suas cotações dependem do crédito que os agentes econômicos depositam nelas, diferenciando, contudo, na existência de um ente central e estatal responsável pela emissão.

37 Importante ponderar, então, que as moedas tradicionais são fiduciárias, da mesma forma que normalmente o são os criptoativos do tipo *coin* ou, como também chamados, criptomoedas, uma vez que não possuem lastro.

tese, portanto, as suas ofertas é são ilimitadas. O controle sobre esta oferta, exercido pelos bancos centrais, é um dos elementos que influenciam em sua cotação. Com os criptoativos, a demanda já está previamente definida no algoritmo que a criou. No caso do bitcoin, por exemplo, desde a sua criação, já há a definição de que será emitido o limite máximo de 21 milhões de bitcoins. Os bitcoins, ou qualquer outro criptoativo, vão sendo emitidos no processo de mineração, ou seja, no processo de verificação matemática da validade das transações que vão sendo geradas na rede.

Importante desde já ressaltar, contudo, o que será adiante melhor explanado, como antes referido, que os criptoativos, inclusive os do tipo *coin* (ou "criptomoedas"), não se consubstanciam propriamente moedas, e isso não porque deixem de atender alguma das funções econômicas atribuídas às moedas tradicionais, mas sim porque moeda, notadamente no Brasil, revela-se um instituto jurídico, estando previsto inclusive na Constituição Federal, o que iremos explanar detalhadamente na seção V deste artigo.

SECURITY TOKEN

Os chamados *security tokens* (*ou security tokens crypto*), por sua vez, são os que representam um investimento, uma parcela de um empreendimento (à semelhança de uma ação), uma participação em um projeto, portanto, em tese, sujeitos à regulação da autoridade responsável pelo mercado de capitais. São a espécie de *tokens* que mais se aproxima ou mesmo pode consubstanciar um valor mobiliário e, justamente por isso, sobre esta espécie recaem as maiores discussões quanto à necessidade de regulação ou mesmo incidência do arcabouço regulatório já existente, próprio do mercado de capitais.

No entanto, também os *utility tokens* (abaixo referidos)

podem ser objeto de transação em um eventual mercado secundário. Vale dizer, o potencial comprador deste *token* pode fazê-lo com o intuito de transacionar os direitos dele emergentes, obviamente contando com a possibilidade de auferir resultados financeiros positivos como produto desta operação. Portanto, ambas as modalidades (*utility ou security tokens*), em tese, podem vir a se enquadrar na definição de valor mobiliário, o que configuraria a hipótese de incidência das normas regulatórias. No caso do Brasil, como referido, das normas da Comissão de Valores Mobiliários – CVM.

UTILITY TOKEN

Já os *utility tokens* são serviços ou unidades de serviços ou utilidades. Também conhecidos como *app coins*, por definição não foram desenhados para funcionarem como um investimento, mas sim como via de acesso a um serviço ou utilidade, ou também para funcionarem como uma espécie de licença de uso. [38]

Projetos com alta demanda de infraestrutura podem utilizar esse tipo de *token* para capitalizar os custos compartilhados de seus servidores ou apenas para organizar o acesso à *blockchain*.

Ademais, pertinente salientar que os *utility tokens* podem ser vistos, grosso modo, como uma espécie residual, para

38 "[…] blockchain-based tokens generally fall within two separate categories: 'investment' tokens, on the one hand, and 'utility' tokens, on the other hand. According to a recent study of over 250 token sales by researchers at the Università Bocconi and the Polytechnic University of Milan, utility tokens represent the majority of tokens issued to date. Approximately 68% of token sales involve rights to access an online platform, and nearly 25% provide some sort of governance rights, like voting on decision polls. Only 26.1% of token sales offer an overt profit right". *In*: Cardozo Blockchain Project. Research Report #1. *Not So fast—Risks Related to The Use of a "Saft" for Token Sales*, November, 21, 2017, p. 2. Disponível em: https://cardozo.yu.edu/programs- centers/blockchain-project. Acesso em: 12 de outubro de 2020.

as hipóteses em que não se subsumem às espécies antes mencionadas.

Ainda, registra-se que a regulação jurídica incidente a cada uma das espécies aqui elencadas será vista adiante, em tópico próprio.

IV – INITIAL COIN OFFERING (ICO)

Feitas as considerações acerca dos atributos da arquitetura de *blockchain*, assim como do conceito, classificação e principais características dos criptoativos, importante agora, como fechamento da primeira parte do trabalho, discorrer a respeito dos seus mecanismos de criação e emissão.

O mecanismo que vem sendo utilizado, por excelência, para tal fim é o chamado *Initial Coin Offering* ou ICO, em analogia ao procedimento tradicional de *Initial Public Offering* ou IPO, por meio do qual as empresas dão início à oferta de suas ações no mercado bursátil, isto é, quando abrem o seu capital social.

A Comissão de Valores Mobiliários descreve as ICOs como "captações públicas de recursos, tendo como contrapartida a emissão de ativos virtuais, também conhecidos como *tokens* ou *coins*, em favor do público investidor".[39]

As ICOs, geralmente, contam com um documento base, denominado de *white paper*, com informações sobre o projeto, à semelhança do que ocorre com a necessidade de prospecto no IPO, porém não são necessariamente técnicos. Normalmente, os *white papers* visam apenas a esclarecer o objetivo do financiamento e o projeto a ser financiado, enquanto o prospecto de um IPO tem a obrigação de esclarecer os fatores de risco e as perspectivas de rentabilidade do

39 OFÍCIO-CIRCULAR CVM/SRE Nº 01/18. Disponível em: <http://www.cvm.gov.br/legislacao/oficios-circulares/sre/OC_SRE_0118.html>. Acesso em: 12 de outubro de 2020.

investimento, em atenção aos estritos regramentos da Comissão de Valores Mobiliários.40

Muitas vezes, os investidores neste tipo de operação o fazem motivados pelas possibilidades de sucesso do projeto a que determinado criptoativo está vinculado, o que pode levar a uma acentuada valorização do seu investimento. A título de exemplo, o Ethereum, a plataforma muito utilizada para a elaboração dos chamados *smart contracts*, foi lançada em 2014. O Ether, criptoativo vinculado ao projeto, estava cotado a US$ 0,40 centavos quando do lançamento. Arrecadou-se, na ocasião, o equivalente a US$ 18 milhões. Em 2016, o Ether valia (cotação) US$ 14,00, e o valor de mercado do empreendimento já havia passado de US$ 1 bilhão. Em março de 2018, o Ether estava cotado a US$ 530,00, e o valor de mercado já ultrapassava os US$ 52 bilhões. O pico de valorização do Ether, até o presente momento, foi em janeiro de 2018, quando a moeda esteve cotada a aproximadamente US$ 1.380,00.

Ao longo do ano de 2017, as ICOs arrecadaram globalmente a soma de 5 bilhões de dólares em investimentos. Para que se tenha uma ideia do dinamismo desta modalidade de captação, estatísticas demonstram que menos de 1% das *startups* que buscam investimentos tradicionais o obtém por meio de investidores anjo, e apenas 0,05% recebem investimento de empresas de *Venture Capital*. Já no que toca às ICOs, 25% dos projetos lançados atingem as metas de arrecadação. Há, portanto, um potencial de efetividade ainda muito maior.[41]

Como parte do processo das ICOs, são emitidos criptoativos ou *tokens* em troca do investimento realizado. Basicamente, o *token* pode ser de três espécies, conforme já visto

40 Importante desde já salientar que, caso o ICO se subsuma à hipótese de emissão de valor mobiliário, deverá atender às exigências para tanto, conforme regulamentado pela Comissão de Valores Mobiliários.

41 *Can Your Startup Run An Initial Coin Offering? Yes, And Here's How*. Disponível em: <https://www.forbes.com/sites/jonathanchester/2018/02/28/can-my-startup-run-an-initial-coin-offering/#597441925a30>. Acesso em: 16 de out. 2020.

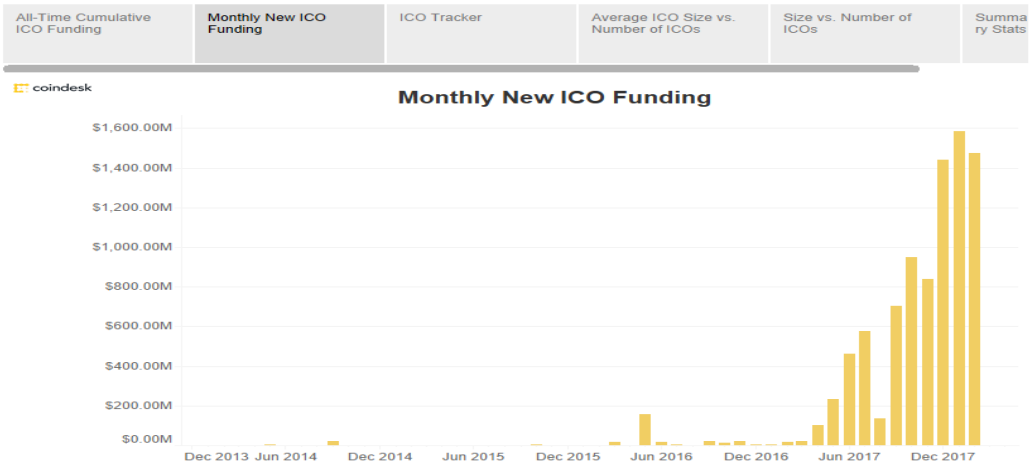
acima. Vale nesse ponto referir que, ao lado dos criptoativos do tipo *coin*, o *security token* é aquele que mais se assemelha a um valor mobiliário, na medida em que pode assegurar participação nos dividendos do empreendimento e, sendo passível de circulação, podem assegurar a seu titular retorno financeiro com a expectativa de valorização do empreendimento. Já o *utility token*, em regra, dá direito ao seu detentor de desfrutar das utilidades, ou os serviços, ou algum tipo de benefício ou preferência, providos pela organização que os emitiu.

V – A REGULAÇÃO DOS CRIPTOATIVOS NO BRASIL

O tema da regulação dos criptoativos está presente na pauta das agências regulatórias e dos demais integrantes do sistema financeiro e do mercado de capitais no mundo todo. No Brasil isto não é diferente. Trata-se de realidade deveras recente, e que vem experimentando crescimento vertiginoso – a primeira ICO ocorreu em 2013, por meio da qual a empresa Mastercoin arrecadou US$ 5 milhões. Em 2016, foram 64 ICOs. No ano de 2017, ocorreram 382 operações de ICO, com valor arrecadado próximo a US$ 6 bilhões.[42] Desde então, observa-se uma lógica exponencial. A tabela 1 demonstra o volume mensal de investimento arrecadado desde a primeira ICO, ocorrida em 2013.

Tabela 1 (Fonte: https://www.coindesk.com/ico-tracker/)

42 Criptomoedas e Mercado de ICOs – Visão Geral de 2017. Disponível em: <https://portaldobitcoin.com/criptomoedas-icos-visao-geral-2017/>. Acesso em: 16 de out. 2020.



Trata-se, portanto, de um mercado que está em franca ebulição e expansão ao redor do mundo, com as diferentes jurisdições procurando entender o fenômeno e discutindo quais os meios e em que medida aplicar medidas regulatórias.

Oportuno salientar que a primeira iniciativa brasileira no sentido de regulamentar o tema por meio de legislação ordinária foi o Projeto de Lei n.º 2.313/15, apresentado em 29 de setembro de 2015, do qual a ementa dispunha sobre a inclusão das moedas virtuais e programas de milhagem aéreas na definição de arranjos de pagamento sob a supervisão do Banco Central, contando com manifestação do Relator do projeto no sentido de criminalizar parte das atividades envolvendo o assunto. Tal atitude pode ser creditada ao então ainda baixo nível de informação e conhecimento sobre a temática, e à associação do bitcoin, em seus primórdios, à lavagem de dinheiro e ao tráfico de entorpecentes.

Nesse sentido, é de se reconhecer mesmo a necessidade da criação de um referencial legal mínimo que possa conferir segurança jurídica e previsibilidade. Deve-se ter presente, a propósito, a lúcida advertência de Milton Barossi-Filho e Rachel Sztajn, segundo os quais:

> "Por circular sem supervisão de qualquer autoridade monetária, por não haver garantia de conversibilidade em outra moeda, de inexistir lastro, como se dá com as moedas de curso forçado ou metais preciosos, por exemplo, esse mercado de moeda virtual pode levar a desastres financeiros. Não há como garantir limites de criação para tal espécie de moeda e, portanto, de determinar de forma clara sua paridade com qualquer outro bem. Falta-lhe a liquidez típica das moedas de curso forçado. E, nada obstante esses problemas, a criação dessa moeda virtual, expressão do exercício da autonomia privada, não viola norma cogente, não é ilegal."[43]

Mais recentemente, observou-se o Projeto de Lei n.° 2060/2019, apresentado em 04 de abril de 2019, visando dispor sobre um regime jurídico dos criptoativos. Ainda, o Projeto de Lei n.° 3825/2019, que propõe a regulamentação do mercado de criptoativos no País, mediante a definição de conceitos, diretrizes, sistema de licenciamento de *exchanges*, supervisão e fiscalização pelo Banco Central e pela Comissão de Valores Mobiliários, medidas de combate à lavagem de dinheiro e de outras práticas ilícitas, além de penalidades aplicadas à gestão fraudulenta ou temerária de *exchanges* de criptoativos. Ainda, o Projeto de Lei n.° 3949/2019, também de 2019, o qual dispõe sobre transações com moedas virtuais e estabelece condições para o funcionamento das *exchanges* de criptoativos, assim como visa a alterar a Lei n.º 9.613, de 1998, que, por sua vez, dispõe sobre lavagem de dinheiro; assim como igualmente busca a alterar a Lei n.º 6.385, de 1976, a qual dispõe sobre o mercado de capitais; além de pretender alterar, ainda, a Lei n.º 7.492, de 1986, que define crimes contra o sistema financeiro nacional; tudo pretendendo regulamentar a utilização de moedas virtuais e o funcionamento das empresas intermediadoras (*exchanges*) dessas operações.

---

43 BAROSSI-FILHO, Milton; SZTAJN, Rachel. Natureza Jurídica da Moeda e Desafios da Moeda Virtual. Revista Jurídica Luso-Brasileira, Ano 1 (2015), nº 1, p. 1669-1690. Disponível em: <https://www.cidp.pt/revistas/rjlb/2015/1/2015_01_1669_1690.pdf>. Acesso em: 12 de outubro de 2020.

Portanto, muito embora não haja no ordenamento jurídico norma expressa vedando a emissão e circulação de criptoativos e, por via de consequência, vedando os procedimentos atualmente mais usuais para as suas emissões, quais sejam, as ICOs, o certo é que também ainda não há um quadro normativo e regulatório apropriado a esta nova realidade; uma vez que muito embora seja, em essência, desnecessário, haja vista que, de acordo com o princípio da legalidade, sobretudo no que tange ao campo de atuação da iniciativa privada, o que não é proibido está permitido; a existência de um quadro normativo mínimo e sistematizado certamente contribuiria para elevar a confiança dos agentes econômicos, assim como ensejar maior segurança jurídica, inclusive de modo a estimular o desenvolvimento deste importante e novel segmento.

Assim é que se identifica a necessidade de ao menos a existência de um enquadramento elementar de diretrizes a serem aplicadas, para que se possa prosseguir no desenvolvimento destes modelos de negócio com um *standard* mínimo de segurança jurídica. Aliás, esta é a ponderação, por exemplo, de Rosine Kadamani, ao dizer que:

> Neste contexto, ao meu ver, precisamos ter em conta que o simples enquadramento e cumprimento das regras existentes já não cabe mais nesse momento. O mercado local precisa de sinalizações mais efetivas do que poderia efetivamente ser construído ou evoluído a partir desse novo paradigma que se instala - e dentro do tempo da realidade empresarial -, sob o risco de perdermos o bonde de vez. Timing é fundamental.[44]

De qualquer forma (e tendo em conta as normas já existentes e potencialmente aplicáveis às hipóteses aqui estudadas), frise-se que o ponto de partida - para se pretender regular (*de lege ferenda*) ou mesmo buscar identificar qual a

44 KADAMAI, Rosine. *Criptos, Brasil e as chances que se vão... rápido*. *In*: Linkedin. Disponível em: <https://www.linkedin.com/pulse/criptos-brasil-e-chances-que-se-v%25C3%25A3o-r%25C3%25A1pido-rosine-kadamani/>. Acesso em: 25 de outubro de 2020.

normatização já existente incide sobre os criptoativos e às suas espécies - passa primeiro por entender a finalidade para a qual os criptoativos são utilizados em cada caso e, assim, identificar em qual categoria jurídica se inserem, pelo que se faz então possível compreender qual mercado integram e, dessa forma, qual a autoridade reguladora se faz competente e mesmo quais as diretrizes regulatórias lhe são pertinentes. Daí também é possível identificar, como dito, quais tratamentos jurídicos já existentes porventura se subsumem aos correspondentes quadros fáticos.

Nesse sentido, como já mencionado, a possível classificação[45] é a que considera basicamente 3 espécies[46] de criptoativos, a depender da finalidade para a qual se utilizam, notadamente no âmbito do sistema financeiro *lato sensu*, sendo que, aliás, dessa forma, é possível identificar a categoria jurídica a qual se inserem e, consequentemente, o tratamento jurídico que deve ser aplicado. Ou seja, é a partir da definição jurídica e da classificação quanto à finalidade de uso que irá se identificar o tratamento jurídico apropriado, ou seja, a sua normatização, tanto por meio de regulação setorial quanto pela legislação aplicável.

Portanto, reitera-se que, de modo geral, os criptoativos podem ser considerados como *coins*, que são os que mais se aproximam das moedas tradicionais ou soberanas; os *security tokens*, os quais podem ou mesmo configuram valores

45 "Em tese, os 'tokens' podem ser atrelados ao direito de uso dos recursos computacionais de uma rede, aos direitos de uso de um aplicativo, às fichas de aposta em um cassino digital, a dólares, à fração de um título público, à fração de propriedade de um imóvel, enfim, qualquer coisa." *In*: *O que são Tokens e para que servem? O que é uma ICO? Como as Altcoins são lançadas no mercado? O que são criptomoedas e para que servem?* Disponível em: <https://steemit.com/bitcoin/@cryptofinancas/o-que-sao-tokens-e-para-que-servem-o-que-e-uma-ico-como-as-altcoins-sao-lancadas-no-mercado-o-que-sao-criptomoedas-e-para-que>. Acesso em: 12 de outubro de 2020.

46 Veja: *Entenda a diferença entre Coins, Utility Tokens/App Coins e Security Tokens.* Disponível em: <https://criptoeconomia.com.br/entenda-diferenca-entre-coins-utility-tokens-app-coins-e-security-tokens/>. Acesso em: 12 de outubro de 2020.

mobiliários; e, por fim, os *utility tokens*, que se assemelham a licenças de uso ou créditos para utilidades. Nesse sentido, iremos abordar tanto as normas que eventualmente se aplicam de forma indistinta aos criptoativos, como também às espécies em particular, respectivamente.

Desse modo, inicialmente quanto aos criptoativos classificados como *coins*, também frequentemente chamados de criptomoedas (depois ressaltaremos porque sustentamos incorreta, pelo menos do ponto de vista da estrita técnica jurídica, a utilização dessa nomenclatura), muito se assemelham a moedas soberanas, pelo menos porquanto parecem desempenhar ou emular as funções básicas por ela desempenhadas, quais sejam, meio de troca, reserva de valor e unidade de conta, em que pese as particularidades já antes ressaltadas a esse respeito.

Mas então por que não são moedas, pelo menos do ponto de vista jurídico?47 Isso porque, sobretudo diante do ordenamento jurídico brasileiro, moeda é mais do que um fenômeno econômico, alcançando conotações jurídicas e legais que delimitam a sua definição. Vejamos.

A Constituição Federal Brasileira, por sua vez, em seu artigo 21, inciso VII,[48] estabelece como competência da União a emissão de moeda. Mais adiante, o seu artigo 164 estabelece competência exclusiva do Banco Central para a emissão de moeda.[49] Só por isso, já se percebe a impossibilidade de se denominar os criptoativos como moedas, pelo menos do ponto de vista técnico e jurídico.

Além disso, o que evidentemente se consubstancia em mais uma clara distinção, não gozam os criptoativos de curso forçado. No Brasil, a Lei n.º 8.880/1994, que dispôs sobre o

47 Muito embora possam consubstanciar moedas do ponto de vista econômico.
48 "Art. 21. Compete à União:
VII - emitir moeda;".
49 "Art. 164. A competência da União para emitir moeda será exercida exclusivamente pelo banco central."

Programa de Estabilização Econômica e o Sistema Monetário Nacional, institundo a Unidade Real de Valor (URV), além de dar outras providências, define o Real como a moeda dotada de curso legal e forçado para servir exclusivamente como padrão de valor monetário no País, assim como meio de pagamento dotado de poder liberatório.

Há que se salientar que os criptoativos também não são moedas eletrônicas, como previstas na Lei n.º 12.865/13, as quais, por sua vez, são recursos em reais mantidos em meios eletrônicos pelas instituições financeiras.

O próprio Banco Central assim define:

> As chamadas "moedas virtuais" ou "moedas criptográficas" são representações digitais de valor, o qual decorre da confiança depositada nas suas regras de funcionamento e na cadeia de participantes.
>
> Não são emitidas por Banco Central, de forma que não se confundem com o padrão monetário do Real, de curso forçado, ou com o padrão de qualquer outra autoridade monetária.
>
> Além disso, não se confundem com a moeda eletrônica prevista na legislação, que se caracteriza como recursos em Reais mantidos em meio eletrônico, em bancos e outras instituições, que permitem ao usuário realizar pagamentos e transferências.50

Ademais, oportuno mencionar que há dispositivo expresso no Código Penal criminalizando a emissão de título ao portador, bem como o recebimento de dinheiro em troca destes títulos.[51]

---

50 Banco Central do Brasil. *Perguntas e Respostas. Moedas Virtuais*. Disponível em: https://www.bcb.gov.br/acessoinformacao/perguntasfrequentes-respostas/faq_moedasvirtuais. Acesso em: 25 de outubro de 2020.

51 "Art. 292 - Emitir, sem permissão legal, nota, bilhete, ficha, vale ou título que contenha promessa de pagamento em dinheiro ao portador ou a que falte indicação do nome da pessoa a quem deva ser pago:

Pena - detenção, de um a seis meses, ou multa.

Parágrafo único - Quem recebe ou utiliza como dinheiro qualquer dos documentos referidos neste artigo incorre na pena de detenção, de quinze dias a três meses, ou multa."

Aliás, não sendo os criptoativos moedas, importante considerar que, por exemplo, ao se adquirir um determinado ativo mediante contraprestação em criptoativo, não estaremos diante de um contrato de compra e venda, mas sim de uma permuta. Vejamos como o Código Civil disciplina o contrato em questão:

> Art. 533. Aplicam-se à troca as disposições referentes à compra e venda, com as seguintes modificações:
> I - salvo disposição em contrário, cada um dos contratantes pagará por metade as despesas com o instrumento da troca;
> II - é anulável a troca de valores desiguais entre ascendentes e descendentes, sem consentimento dos outros descendentes e do cônjuge do alienante.

Estaríamos sim frente a um contrato de Compra e Venda se se tratasse da aquisição de criptoativos mediante pagamento em dinheiro, conforme disposições do Código Civil a respeito, assim como diretrizes correlatas:

> Art. 481. Pelo contrato de compra e venda, um dos contratantes se obriga a transferir o domínio de certa coisa, e o outro, a pagar-lhe certo preço em dinheiro.
> Art. 315. As dívidas em dinheiro deverão ser pagas no vencimento, em moeda corrente e pelo valor nominal, salvo o disposto nos artigos subsequentes.
> Art. 318. São nulas as convenções de pagamento em ouro ou em moeda estrangeira, bem como para compensar a diferença entre o valor desta e o da moeda nacional, excetuados os casos previstos na legislação especial.

Portanto, os criptoativos, mesmo aqueles que se classificam como *coins*, em tradução livre do inglês, moedas, não assim o são, pelo menos não do ponto de vista eminentemente jurídico, sendo melhor definidos como ativos virtuais.

Contudo, ainda que os criptoativos não sejam moedas, podem se submeter ao crivo do Banco Central do Brasil. *Verbi gratia*, no que diz respeito à utilização dos criptoativos em instituições financeiras submetidas à regulação pelo BACEN, especialmente as chamadas *fintechs*, ou mesmo quando pertencente a arranjos de pagamentos, deverão observar as

diretrizes para tanto estipuladas.

O Banco Central do Brasil, por sua vez, por meio do Comunicado BACEN n.º 25.306, de 19 de fevereiro de 2014, buscou diferenciar os criptoativos das moedas eletrônicas. Já por meio do Comunicado BACEN 31.379, de 16 de novembro de 2017, alertou sobre riscos de operações de guarda, negociação e câmbio. Ainda, seguindo recomendação do Fundo Monetário Internacional, o Banco Central do Brasil reconheceu a inclusão, em 26 de agosto de 2019, dos criptoativos nas estatísticas envolvendo a balança comercial.

Já quanto aos *security tokens*, a Comissão de Valores Mobiliários, em comunicado sobre o tema, em 11 de outubro de 2017, por meio de chamada "Nota da CVM a respeito do tema", "Initial Coin Offering (ICO)", manifestou-se a respeito, posicionando-se inicialmente de forma cautelosa, do seguinte modo:

> Considerando o avanço das operações conhecidas como *Initial Coin Offerings* (ICOs), a CVM julga pertinente esclarecer que está atenta às recentes inovações tecnológicas nos mercados financeiros global e brasileiro. A Autarquia vem acompanhando tais operações e buscando compreender benefícios e riscos associados, seja por meio de fóruns internos, como o Comitê de Gestão de Riscos – CGR e o Fintech Hub, ou de discussões no âmbito internacional, como em trabalhos desenvolvidos pela IOSCO.
>
> Em linha com as competências definidas na Lei 6.385/76, a CVM busca estimular o empreendedorismo e a introdução de inovações tecnológicas no mercado de valores mobiliários, sempre que alinhados ao norte da segurança dos investidores e da integridade do mercado.
>
> [...]
>
> 1. Podem-se compreender os ICOs como captações públicas de recursos, tendo como contrapartida a emissão de ativos virtuais, também conhecidos como *tokens* ou *coins*, junto ao público investidor. Tais ativos virtuais, por sua vez, a depender do contexto econômico de sua emissão e dos direitos conferidos aos investidores, podem representar valores mobiliários, nos termos do art. 2º, da Lei 6.385/76.

> 2. Nesse contexto, a CVM esclarece que certas operações de ICO podem se caracterizar como operações com valores mobiliários já sujeitas à legislação e à regulamentação específicas, devendo se conformar às regras aplicáveis. Incorrem na mesma situação companhias (abertas ou não) ou outros emissores que captem recursos por meio de uma ICO, em operações cujo sentido econômico corresponda à emissão e à negociação de valores mobiliários.
> 3. As ofertas de ativos virtuais que se enquadrem na definição de valor mobiliário e estejam em desconformidade com a regulamentação serão tidas como irregulares e, como tais, estarão sujeitas às sanções e penalidades aplicáveis. A CVM alerta que, até a presente data, não foi registrada nem dispensada de registro nenhuma oferta de ICO no Brasil.
> 4. Por outro lado, há operações de ICO que não se encontram sob a competência da CVM, por não se configurarem como ofertas públicas de valores mobiliários.
> 5. A CVM esclarece que valores mobiliários ofertados por meio de ICO não podem ser legalmente negociados em plataformas específicas de negociação de moedas virtuais (chamadas de *virtual currency exchanges*), uma vez que estas não estão autorizadas pela CVM a disponibilizar ambientes de negociação de valores mobiliários no território brasileiro.
> [...]
> A CVM permanece atenta à evolução das ICOs e, sendo o caso, tomará, no momento apropriado, as medidas cabíveis no âmbito de sua competência legal, de forma a assegurar a estabilidade e o contínuo desenvolvimento do mercado de capitais brasileiro.

Corroborando a manifestação anterior, a Comissão de Valores Mobiliários, em 2018, reconheceu[52] que as ICOs e os ativos virtuais que as acompanham representam um desafio "para os reguladores do mercado financeiro e de capitais não apenas no Brasil mas também em outras jurisdições." E se posiciona de forma cautelosa, afirmando que a depender do contexto econômico de sua emissão e dos direitos conferidos aos

52 OFÍCIO-CIRCULAR CVM/SRE Nº 01/18. Disponível em: <http://www.cvm.gov.br/legislacao/oficios-circulares/sre/OC_SRE_0118.html>. Acesso em: 12 de outubro de 2020.

investidores, tais ativos virtuais podem vir a se enquadrar em sua competência regulatória:

> [...] as ofertas de ativos virtuais que se enquadrem na definição de valor mobiliário e estejam em desconformidade com a regulamentação serão tidas como irregulares e, como tais, estarão sujeitas às sanções e penalidades aplicáveis.

O que tem chamado a atenção e fomentado discussões na comunidade que acompanha a evolução da matéria é a incerteza quanto a tais operações poderem representar valores mobiliários, nos termos do art. 2º, IX, da Lei 6.385/76. O efeito prático deste posicionamento é que, conforme apontado por Kadamani no texto já referido, a maior parte dos projetos mais concretos ou promissores está buscando jurisdições externas para poder operar, como, por exemplo, Estônia e Suíça, consideradas mais acessíveis.

De outra banda, enquanto as questões regulatórias seguem um caminho ainda não tão bem definido no Brasil, é possível vislumbrar alternativas dentro das normas já em vigor em nosso arcabouço jurídico. Por exemplo, a modalidade de *equity crowdfunding*, disciplinada pela Instrução CVM n.º 588/2017. Os requisitos de enquadramento, em síntese, são que a empresa seja registrada no Brasil e que tenha receita bruta anual de até 10 milhões de reais; que o valor de captação não seja superior a 5 milhões de reais; que o prazo de captação não seja superior a 180 dias; que seja garantido ao investidor um período de desistência de, no mínimo, sete dias; que o montante total aplicado por investidor e por período seja limitado a 10 mil reais (com exceções); e que a plataforma eletrônica responsável pela intermediação do investimento obtenha registro junto à Comissão de Valores Mobiliários.

Ainda que não seja uma situação ideal, e que conte com limitadores importantes – além dos acima mencionados, há também a vedação à realização de um mercado secundário – trata-se de importante iniciativa, servindo, ao menos, para empreendimentos de pequeno ou médio portes.

Outra possibilidade seria o enquadramento na Instrução CVM n.º 476/09, que regulamenta a oferta de valor mobiliário destinada a um público restrito e qualificado. Como se disse, estas são alternativas ainda iniciais, até que haja um arcabouço regulatório que possibilite o florescimento deste mercado de forma mais consistente, a exemplo do que já vem acontecendo em outras jurisdições.

Muito embora a Comissão de Valores Mobiliários tenha afirmado, no OFÍCIO-CIRCULAR CVM/SRE Nº 01/18,[53] de 27 de fevereiro de 2018, que "há ICOs que não se encontram sob a competência da CVM, por não se configurarem como ofertas públicas de valores mobiliários", é importante ter presente que mesmo os assim chamados *utility tokens* podem vir a ser considerados ativos mobiliários, sobretudo se porventura daí houver a compreensão da existência de algum tipo de expectativa de rendimento.

Este também é o entendimento do advogado Guilherme Potenza, em matéria jornalística.[54] Para ele, a criação de um mercado secundário, em que os investidores (inclusive os de *utility tokens*) pretendessem revender tais ativos em busca de lucro, poderia ser passível de regulação pela CVM.

Ademais, em que pese no OFÍCIO-CIRCULAR CVM/SRE Nº 01/18, já antes referido, tenha sido consignado que "[...] a interpretação desta área técnica é a de que as criptomoedas não podem ser qualificadas como ativos financeiros, para os efeitos do disposto no artigo 2º, V, da Instrução CVM nº 555/14, e por essa razão, sua aquisição direta pelos fundos de investimento ali regulados não é permitida.", o

53 OFÍCIO-CIRCULAR CVM/SRE Nº 01/18. Disponível em: <http://www.cvm.gov.br/legislacao/oficios-circulares/sre/OC_SRE_0118.html>. Acesso em: 12 de outubro de 2020.

54 Folha de São Paulo. Oferta de criptomoeda entra na mira da CVM. Disponível em: <https://www1.folha.uol.com.br/mercado/2018/03/oferta-de-criptomoeda-entra-na-mira-da-cvm.shtml?utm_source=whatsapp&utm_medium=social&utm_campaign=compwa>. Acesso em: 12 de outubro de 2020.

OFÍCIO-CIRCULAR CVM/SRE Nº 11/18,55 de 19 de setembro de 2018, permitiu o investimento por meio de fundos, desde que realizadas em plataformas que estejam submetidas a jurisdições (portanto, no exterior) nas quais já se exerça supervisão normatizada sobre tais fenômenos, nos seguintes termos:

> A Instrução CVM nº 555, em seu arts. 98 e seguintes, ao tratar do investimento no exterior, autoriza o investimento indireto em criptoativos por meio, por exemplo, da aquisição de cotas de fundos e derivativos, entre outros ativos negociados em terceiras jurisdições, desde que admitidos e regulamentados naqueles mercados. No entanto, no cumprimento dos deveres que lhe são impostos pela regulamentação, cabe aos administradores, gestores e auditores independentes observar determinadas diligências na aquisição desses ativos.
>
> Um primeiro que se destaca é aquele já aventado pelos mais diversos órgãos reguladores e supervisores no mundo em relação à possibilidade de financiamento, direta ou indiretamente, de operações ilegais nesse mercado como a lavagem de dinheiro, práticas não equitativas, realização de operações fraudulentas ou de manipulação de preços, dentre outras práticas similares. Nesse contexto, e levando em conta também a exigência de combate e prevenção à lavagem de dinheiro imposta pela Instrução CVM nº 301, entendemos que uma forma adequada de atender a tais preocupações é a realização de tais investimentos por meio de plataformas de negociação ("exchanges"), que estejam submetidas, nessas jurisdições, à supervisão de órgãos reguladores que tenham, reconhecidamente, poderes para coibir tais práticas ilegais, por meio, inclusive, do estabelecimento de requisitos normativos.
>
> Embora se recomende que os investimentos sejam feitos por meio dessas exchanges, como não há vedação explícita a que os investimentos sejam feitos de outra forma, em razão de seus deveres fiduciários administradores e gestores

55 OFÍCIO-CIRCULAR CVM/SRE Nº 11/18. Disponível em: < http://www.cvm.gov.br/legislacao/oficios-circulares/sin/oc-sin-1118.html>. Acesso em: 30 de outubro de 2020.

> deverão se assegurar que a estrutura escolhida seja capaz de atender plenamente às exigências legais e regulamentares acima referidas.
>
> Ainda sobre o tema da normalidade de funcionamento dos mercados em que são negociados os criptoativos e seus derivativos, é importante que o gestor verifique se determinado criptoativo não representa uma fraude, como, aliás, tem sido visto com grande recorrência, por exemplo, nas operações recentes de ICO pelo mundo. Assim, é importante que o gestor adote diligências para minimizar o risco de fomentar a oferta de um criptoativo fraudulento, com a verificação das variáveis relevantes associadas à emissão, gestão, governança e demais características do criptoativo.

Assim, dada a possibilidade de os criptoativos funcionarem como um *security token* ou mesmo *utility token*, conforme acima já especificado, permitindo lhes agregar direitos e faculdades que os aproximam dos valores mobiliários, há uma tendência de que assim sejam considerados. Ou seja, os criptoativos, a depender dos atributos que a eles estejam associados, podem ser consideradas como valores mobiliários.

A este respeito, a Comissão de Valores Mobiliários, acompanhando o entendimento de órgãos reguladores de outras nações, tem adotado uma postura de considerar como valores mobiliários passíveis de se submeter a sua regulação aqueles criptoativos que ostentam "a presença, na relação contratual, de direitos conferidos ao adquirente, tais como, participação no capital ou em acordos de remuneração préfixada sobre o capital investido ou de voto em assembleias que determinam o direcionamento dos negócios do emissor."[56]

56 "Nesse contexto, a CVM esclarece que certas ICOs podem se caracterizar como ofertas públicas de valores mobiliários, portanto, sujeitas à legislação e à regulamentação específicas, devendo se conformar às regras aplicáveis. Incorrem na mesma situação companhias (abertas ou não) ou outros emissores que captem recursos por meio de uma ICO, em operações cujo sentido econômico corresponda à emissão e à negociação de valores mobiliários. As ofertas de ativos virtuais que se enquadrem na definição de valor mobiliário e estejam em desconformidade com a regulamentação serão tidas como irregulares e, como tais, estarão sujeitas às sanções e penalidades

A Comissão de Valores Mobiliários, no mesmo Ofício circular aqui referido (OFÍCIO-CIRCULAR CVM/SRE Nº 01/18), também faz questão de afirmar que há, ou pode haver, procedimentos de emissão de criptoativos que não configuram oferta pública de valores mobiliários, e portanto não estão sob a sua competência.[57]

Em essência, quiçá no Brasil a definição seja legamente um pouco mais alargada, se a emissão do criptoativo se enquadrar naquele que ficou conhecido como *Howey Test*, criado pelo *Security Exchange Act* de 1934, nos Estados Unidos da América, há a atração da competência da Comissão de Valores Mobiliários. O teste em questão leva em conta basicamente as respostas às perguntas abaixo listadas, as quais, sendo afirmativas, considera-se haver subsunção à valor mobiliário e, portanto, objeto de regulação da Comissão de Valores Mobiliários:

i) Existe investimento?

ii) O investimento é formalizado por um título ou contrato?

iii) O investimento é coletivo?

iv) Há promessa de remuneração, oportunidade de participação ou parceria? A remuneração tem origem nos esforços do empreendedor ou de terceiros?

v) Os títulos ou contratos são ofertados publicamente?

Portanto, como já salientado, sendo as respostas positivas, há a competência da autoridade reguladora em questão. Não sendo positivas, estar-se-á fora do âmbito da competência da Comissão de Valores Mobiliários.58

aplicáveis". *In*: OFÍCIO-CIRCULAR CVM/SRE Nº 01/18. Disponível em: <http://www.cvm.gov.br/legislacao/oficios-circulares/sre/OC_SRE_0118.html>. Acesso em: 12 de outubro de 2020.

[57] "Por outro lado, há ICOs que não se encontram sob a competência da CVM, por não se configurarem como ofertas públicas de valores mobiliários." *In*: OFÍCIO-CIRCULAR CVM/SRE Nº 01/18. Disponível em: <http://www.cvm.gov.br/legislacao/oficios-circulares/sre/OC_SRE_0118.html>. Acesso em: 12 de outubro de 2020.

58 Veja: Entenda a diferença entre Coins, Utility Tokens/App Coins e Security

Estes são basicamente os requisitos estabelecidos no inciso IX do artigo 2º da Lei 6385/76, que dispõe sobre o mercado de valores mobiliários e cria a Comissão de Valores Mobiliários, senão vejamos:

> Art. 2o São valores mobiliários sujeitos ao regime desta Lei:
> [...]
> IX - quando ofertados publicamente, quaisquer outros títulos ou contratos de investimento coletivo, que gerem direito de participação, de parceria ou de remuneração, inclusive resultante de prestação de serviços, cujos rendimentos advêm do esforço do empreendedor ou de terceiros.

Ainda assim, mesmo que uma determinada transação de emissão de criptoativos não se enquadre na competência regulatória da Comissão de Valores Mobiliários, é possível concluir que se está frente a um ativo financeiro, que representa determinado valor, podendo, inclusive, estar sujeito à regulação de outra autoridade ou agência reguladora, sendo que, em todos os casos, sujeitos à legislação e ao ordenamento jurídico incidente, no caso aqui estudado, o brasileiro.

Imperioso salientar que, em 03 de maio de 2019, a Receita Federal do Brasil, por meio da Instrução Normativa RFB n.º 1888, instituiu e disciplinou a obrigatoriedade de prestação de informações relativas às operações realizadas com criptoativos, apresentando manual de preenchimento da obrigatoriedade de prestação de informações relativas às operações realizadas com criptoativos à Secretaria Especial da Receita Federal do Brasil (RFB), bem como o Ato Declaratório Executivo COPES n.º 5/2019, apresentando o Manual de Orientação quanto à aparência padrão na prestação das informações.

Ademais, não há como se deixar de referir o ambiente regulatório experimental, também conhecido como *sandbox*

Tokens. *In*: Criptoeconomia, novembro de 2017. Disponível em: <https://criptoeconomia.com.br/entenda-diferenca-entre-coins-utility-tokens-app-coins-e-security-tokens/>. Acesso em: 12 de outubro de 2020.

regulatório, que vem sendo desenvolvido no Brasil. Nesse sentido, inicialmente, registre-se o Comunicado Conjunto, de 13 de junho de 2019, pelo qual a Secretaria Especial de Fazenda do Ministério da Economia, o Banco Central do Brasil, a Comissão de Valores Mobiliários e a Superintendência de Seguros Privados tornaram pública a intenção de implantar um modelo de *sandbox* regulatório no País, divulgando ação coordenada para implantação nos mercados financeiro, de capitais e securitário brasileiros. Vale frisar que tal medida é tida como resposta às transformações ocorridas notadamente pela utilização de tecnologias inovadoras, como *distributed ledger technology* – DLT, *blockchain*, *roboadvisors* e inteligência artificial,59 que ensejam o surgimento de novos modelos de negócio, com reflexos na oferta de produtos e serviços, com maior qualidade e alcance.

Justamente, tal circunstância desafia os reguladores a atuar:

> [...] com a flexibilidade necessária, dentro dos limites permitidos pela legislação, para adaptar suas regulamentações às mudanças tecnológicas e constantes inovações, de forma que as atividades reguladas mantenham conformidade com as regras de cada segmento, independentemente da forma como os serviços e produtos sejam fornecidos, principalmente sob as perspectivas da segurança jurídica, da proteção ao cliente e investidor e da segurança, higidez e eficiência dos mercados.
>
> Os reguladores que subscrevem este comunicado coordenarão suas atividades institucionais para disciplinar o funcionamento de elementos essenciais do sandbox em suas correspondentes esferas de competência, contemplando elementos comuns aos modelos observados em outras jurisdições, a exemplo da concessão de autorizações temporárias e a dispensa, excepcional e justificada, do cumprimento de regras para atividades reguladas específicas, observando critérios, limites e períodos previamente estabelecidos. Os reguladores, ademais, buscarão atuar conjuntamente sempre

59 Acresceríamos, *big data, machine learning, deep learning*, entre outras.

> que as atividades perpassem mais de um mercado regulado. Espera-se que a implantação desse regime regulatório seja capaz de promover o desenvolvimento de produtos e serviços mais inclusivos e de maior qualidade e possa fomentar a constante inovação nos mercados financeiro, securitário e de capitais.60

Nesse contexto, frise-se a iniciativa do Conselho Monetário Nacional que, por meio da Resolução CMN n.º 4.865, de 26 de outubro de 2020, estabeleu as diretrizes para funcionamento do ambiente controlado de testes para inovações financeiras e de pagamento (*sandbox* regulatório) e as condições para o fornecimento de produtos e serviços no contexto desse ambiente no âmbito do Sistema Financeiro Nacional; assim como, por parte do Banco Central do Brasil, a Resolução BCB n.º 29, de 26 de outubro de 2020, que igualmente estabeleceu as diretrizes para funcionamento do ambiente controlado de testes para inovações financeiras e de pagamento (*sandbox* regulatório) e as condições para o fornecimento de produtos e serviços no contexto desse ambiente no âmbito do Sistema Financeiro Nacional e do Sistema de Pagamentos Brasileiro.

De forma semelhante, no âmbito da Comissão de Valores Mobiliários, a Instrução CVM n.º 626, de 15 de maio de 2020, que dispôs sobre as regras para constituição e funcionamento de ambiente regulatório experimental (*sandbox* regulatório), inclusive tendo ora iniciado o processo de admissão de participantes. No tocante, importante também mencionar a PORTARIA/CVM/PTE/n.º 75, de 29 de junho de 2020, por meio da qual se dispôs sobre a composição e o funcionamento do Comitê de *Sandbox* ("CDS") de que trata o art. 2º, inciso III, da Instrução CVM n.º 626, antes referida.

---

60 Comunicado Conjunto, de 13 de junho de 2019, da Secretaria Especial de Fazenda do Ministério da Economia, do Banco Central do Brasil, da Comissão de Valores Mobiliários e da Superintendência de Seguros Privados. Disponível em: <http://www.cvm.gov.br/noticias/arquivos/2019/20190613-1.html>. Acesso em: 13 de novembro de 2020.

No âmbito da Superintendência de Seguros Privados – SUSEP, importante salientar a Resolução n.º 381, de 4 de março de 2020, que estabeleceu as condições para autorização e funcionamento, por tempo determinado, de sociedades seguradoras participantes exclusivamente de ambiente regulatório experimental (*sandbox* regulatório), que desenvolvam projetos inovadores, mediante o cumprimento de critérios e limites previamente estabelecidos; assim como a Circular n.º 598, de 19 de março de 2020, que dispôs sobre autorização, funcionamento por tempo determinado, regras e critérios para operação de produtos, transferência de carteira e envio de informações das sociedades seguradoras participantes exclusivamente de ambiente regulatório experimental (*sandbox* regulatório), que desenvolvam projetos inovadores, mediante o cumprimento de critérios e limites previamente estabelecidos; além do Edital eletrônico n.º 2/2020/SUSEP, de seleção de interessados em participar exclusivamente de ambiente regulatório experimental (*sandbox* regulatório).

Ainda, outra discussão que se observa intensa é quanto à possibilidade ou não de encerramento, por parte dos bancos, de contas bancárias de empresas que operam com criptoativos, notadamente as *exchanges*, como ocorreu no âmbito do Superior Tribunal de Justiça, por meio do Recurso Especial n.º 1.696.214 - SP (2017/0224433-4), o qual restou assim ementado:

> RECURSO ESPECIAL. AÇÃO DE OBRIGAÇÃO DE FAZER. PRETENSÃO EXARADA POR EMPRESA QUE EFETUA INTERMEDIAÇÃO DE COMPRA E VENDA DE MOEDA VIRTUAL (NO CASO, BITCOIN) DE OBRIGAR A INSTITUIÇÃO FINANCEIRA A MANTER CONTRATO DE CONTA-CORRENTE. ENCERRAMENTO DE CONTRATO, ANTECEDIDO POR REGULAR NOTIFICAÇÃO. LICITUDE. RECURSO ESPECIAL IMPROVIDO.

No Âmbito do Conselho Administrativo de Defesa Econômica (CADE), tal discussão se estabeleceu no Processo

n.º 8700.003599/2018-95, cuja ementa e conclusão restaram assim consignadas:61

> Inquérito Administrativo. Recusa de contratar. Discriminação. Empresas ou corretoras de "criptoativos". Prorrogação de Inquérito Administrativo nos termos do art. 66, §9º, da Lei nº 12.529, de 30 de novembro de 2011.
> II. CONCLUSÃO
> Diante do exposto, entende-se pela necessidade de avaliar pormenorizadamente as questões mencionadas, em virtude do volume de informações em análise e das novas informações trazidas aos autos recentemente, sendo as circunstâncias do caso concreto justificativas para a prorrogação do presente Inquérito Administrativo, com fundamento no art. 66, §9º, da Lei nº 12.529, de 2011.

Embora tal questão certamente ainda será aprofundada com o passar do tempo, certamente aqui se faz inarredável o seu registro.

Portanto e de qualquer forma, reitera-se, apresentando as características antes ressaltadas, tratam-se os criptoativos de ativos financeiros, passíveis de avaliação econômica e, desta forma, passíveis de se enquadrarem em objeto de regulação e supervisão de autoridade reguladora setorial, caso preencham os requisitos para tanto, sendo que, em todos os casos, sujeitos à legislação e ao ordenamento jurídico incidente, sendo que, no caso aqui estudado, o brasileiro.

VI – NECESSIDADE DE MARCO REGULADOR UNIVERSAL

As movimentações em torno do tema da regulação dos criptoativos ao redor do mundo têm sido intensas ao longo dos últimos meses. O que se tem identificado até o presente momento são posições um tanto distintas nas diferentes jurisdições. Em alguns países se avança rápido em direção a uma aceitação com um bom grau de liberdade, ao passo que em

61 Sendo que a discussão continua a se desenvolver junto ao CADE.

outros países têm havido inclusive a proibição expressa, seja de aceitação dos criptoativos, seja de transações levadas a cabo pelas chamadas *exchanges*, agentes responsáveis por intermediar a compra e venda de tais ativos.

Como regra geral, pode-se dizer que há uma posição de observação e cautela quanto à evolução destes mercados. Isso pode ser creditado ainda ao grau de desconhecimento das efetivas consequências dessas novas realidades e do relativo baixo volume que as transações em criptoativos representam até o momento, se comparados aos ativos financeiros tradicionais. Em março de 2018, o volume de transações correspondia a um pouco menos de 1% do PIB mundial. Os 100 maiores criptoativos do tipo *coin* representavam, em 26 de março de 2018, pouco mais de 300 bilhões de dólares, ao passo que o PIB mundial, em 2017, foi estimado em cerca de 79 trilhões de dólares.

No lado dos países que têm adotado uma postura mais liberal se destacam a Estônia[62] e o Japão.[63] Mais recentemente, Alemanha[64] e França[65]. Nos Estados Unidos, aos poucos, os estados estão avançando no tema da regulação. O mesmo se

62 Na Estônia, Fundador do *e-Residency* planeja criptomoeda oficial, *in*: <https://www.tecmundo.com.br/mercado/125864-estonia-fundador-residency-planeja-criptomoeda-oficial.htm>. Acesso em: 02 de novembro de 2020.

63 Japão pretende se tornar um líder mundial no mercado de criptomoedas, *in* <https://guiadobitcoin.com.br/japao-pretende-se-tornar-um-lider-mundial-no-mercado-de-criptomoedas/>. Acesso em: 02 de novembro de 2020.

64 Alemanha legaliza criptomoedas e reconhece bitcoin como meio de pagamento, *in* <http://www.infomoney.com.br/mercados/bitcoin/noticia/7313971/alemanha-legaliza-criptomoedas-reconhece-bitcoin-como-meio-pagamento>. Acesso em 02 de novembro de 2020.

65 :França criará estrutura legal para ofertas de criptomoedas, *in*: <https://www.reuters.com/article/us-france-cryptocurrencies/france-to-create-legal-framework-for-cryptocurrency-offerings-idUSKBN1GY0YE>. Acesso em: 02 de novembro de 2020. No mesmo País, Governo Francês criará uma estrutura flexível e segura para ICOs, *in*: <https://www.financemagnates.com/cryptocurrency/news/cryptocurrencynews-french-government-implement-flexible-yet-safe-ico-framework/>. Acesso em: 02 de novembro de 20202.

diga quanto às discussões em nível federal daquele País.[66]

Já no lado dos países que vêm tentando frear o avanço dos criptoativos, o destaque é para a China,[67] pelo menos no que diz respeito à emissão de forma mais independente por parte da iniciativa privada.

Como se vê, há uma tendência no caminho da regulação do tema. As dissonâncias dizem respeito quanto à extensão e limites do que deverá ser regulado. O desafio não é pequeno, ainda mais se tendo em conta as características da lógica computacional que suporta tanto os criptoativos do tipo *coin* quanto os demais ativos que já têm sido comercializados por meio das ICOs.

Todo o sistema é concebido para funcionar sem a necessidade de uma autoridade central. Mesmo as disputas que eventualmente possam surgir em função das transações que ocorrem nestes mercados e com tais ativos possuem a possibilidade de serem dirimidas, algumas vezes mesmo com vantagens, pela própria plataforma e pela comunidade que integra um determinado ecossistema de *blockchain*.

Dadas as características transnacionais das transações possibilitadas pela aplicação dos criptoativos, muito tem se falado na necessidade de se estabelecer um marco regulatório para o tema, que justamente transcenda as fronteiras dos países.

Discussões multilaterais já têm se desenvolvido neste

66 Mais estados dos EUA podem implementar regulamentos de criptomoeda, *in*: <https://www.investopedia.com/news/majority-us-states-are-still-acknowledge-cryptocurrencies/>. Acesso em 02 de novembro de 2020. Estados Unidos devem analisar potenciais regulamentos para cripotomoedas, *in*: < https://www.coinstaker.com/united-states-cryptocurrency-regulations/>. Acesso em: 02 de novembro de 2020.

67 China planeja acabar com as últimas transações com criptomoedas, *in*: <https://exame.abril.com.br/mercados/china-planeja-acabar-com-as-ultimas-transacoes-com-criptomoedas/>. Acesso em: 02 de novembro de 2020. Outrossim, China está cortando acesso à negociação de criptomoedas fora do País, *in*: <https://portaldobitcoin.com/china-esta-cortando-acesso-negociacao-de-criptomoedas-fora-do-pais/>. Acesso em: 02 de novembro de 2020.

sentido. Uma das principais iniciativas foi protagonizada pela reunião do G20, que ocorreu nos dias 19 e 20 de março de 2018, em Buenos Aires, na Argentina. Por ocasião desta reunião, os líderes que se fizeram presentes acordaram em estabelecer iniciativas uniformes para a regulação dos criptoativos, reconhecendo-se também a necessidade de se coletar maiores informações antes de se formular uma proposta de regulação.

Há preocupação com os impactos que um universo de criptoativos não regulado pode causar no aumento de atividades criminosas, bem como prejuízos aos eventuais investidores. As conversações preliminares apontam para a definição de um conjunto de regras gerais que todos os países teriam condições de tornar obrigatórias, sendo que, contudo, até o momento, não foram efetivadas medidas nesse sentido. Um documento público foi divulgado, onde se afirma que a tecnologia por trás dos criptoativos possui o potencial de promover inclusão financeira, mas também assinalou os possíveis impactos na estabilidade financeira, e que seu potencial uso para evasão de tributos e a prática de atividades ilegais necessitam ser melhor compreendidos.

Como quer que seja, o fato é que já se percebe uma evolução no tratamento da questão, sendo que o interesse a seu respeito, bem como os correspondentes avanços regulatórios, tenderão a se fazer cada vez mais presentes na medida em que tais mercados sigam crescendo em importância e em volume de negócios.

Conforme se teve a oportunidade de demonstrar anteriormente, está em curso um crescimento exponencial das operações de ICOs, pelo que a ação dos órgãos reguladores tenderá a acompanhar esta rápida evolução.

De todo o exposto, considerando que o fenômeno é verdadeiramente transnacional, sendo facilmente migrável, permitindo mesmo se falar em desterritorialização destes

respectivos mercados em desenvolvimento, evidente se faz a conformação de um marco regulador universal, sob pena apenas de se gerarem graves externaidades negativas, as quais sequer se fazem possível efetivamente mensurar.

VII – A EFICIÊNCIA ECONÔMICA DOS CRIPTOATIVOS

É conhecimento público e até mesmo intuitivo que a indústria de prestação de serviços financeiros movimenta enormes somas de recursos ao redor do mundo. Dentre destes serviços, o de movimentação de ativos, de acordo com estimativa do Boston Consulting Group (BCG), em estudo conduzido em 2017, é de que, em 2016, tenha circulado pelo mundo a cifra de US$ 420 trilhões de dólares, ou o equivalente a 5,5 (cinco vírgula cinco) vezes o PIB global.[68]

O mesmo estudo estima que as instituições financeiras e as empresas do segmento de cartões tiveram receita, em 2016, de US$ 1,2 (um vírgula dois) trilhões de dólares com o sistema de pagamentos global. A cifra representa entre 20% a 25% do total gerado pela atividade bancária.

Esta receita decorre em grande medida da função de intermediação que as instituições financeiras exercem. Ora, na medida em que as transações com criptoativos se viabilizam, tendo por base a arquitetura de *blockchain*, conforme os atributos que foram detalhados na primeira parte deste trabalho, se não desaparece, pelo menos é mitigada a necessidade da figura do intermediador, o qual confere certeza e confiança às transações e, consequentemente, reduz-se também a necessidade de se incorrer nas correspondentes despesas.

Uma função primordial desempenhada pelo intermediário de uma transação financeira é o de verificação dos

68 Jornal Valor. A Nova Arte de Fazer Dinheiro. Janeiro de 2018. Disponível em: <http://www.valor.com.br/cultura/5266749/nova-arte-de-fazer-dinheiro?>. Acesso em: 12 de outubro de 2020.

atributos vinculados àquela determinada transação. É preciso verificar e atestar a identidade daqueles que transacionam. Garantir que determinada pessoa (física ou jurídica) realmente é quem diz ser quem é.

Para além disso, é necessário ainda atestar que a pessoa que está realizando determinada transação está autorizada a assim fazê-lo. Ou seja, detém o poder (jurídico, fundamentalmente) para transferir fundos, ou para se obrigar, em nome próprio ou de terceiros, a realizar determinado ato jurídico no momento presente ou em determinado momento futuro.

É necessário, ainda, que o intermediário faça a verificação da existência dos ativos, sejam eles tangíveis ou creditícios, que determinado integrante da transação afirma ser o titular.

De outra banda, a atividade de verificação também se direciona ao destinatário da transação. É necessário verificar, em primeiro lugar, sua identidade. Ou seja, que aquele que afirma ser o beneficiário realmente o seja. Ao depois, é necessário verificar se o destinatário detém o poder liberatório da obrigação, se detém o poder de receber e dar quitação da obrigação que seja objeto de determinada transação.

Aqui vale invocar o milenar princípio do Direito Privado segundo o qual quem paga mal, paga duas vezes. Tal princípio está positivado em normas do nosso Código Civil, dentre as quais a mais explícita talvez seja o artigo 310:

> Art. 310. Não vale o pagamento cientemente feito ao credor incapaz de quitar, se o devedor não provar que em benefício dele efetivamente reverteu.

O tema está pacificado na jurisprudência pátria. A título de exemplo, invoca-se Decisão do Superior Tribunal de Justiça, prolatada já há quase 30 anos, da lavra do Ministro Athos Gusmão Carneio:

> O devedor que paga a quem não é o detentor do título, contentando-se com simples quitação em documento separado, corre o risco de ter de pagar segunda vez ao legítimo portador. Quem paga mal paga duas vezes. (Resp 596/RS, Rel.

Min. Athos carneiro, Quarta Turma, REPDJ 6.11.1989).

Por fim, ainda é necessário garantir que a transação, uma vez efetuada, não seja duplicada. É necessário evitar o duplo gasto, e isso se dá com a indisponibilização do recurso a seu detentor original, até que este passe a integrar a esfera do destinatário.

Todos estes processos de verificação são tradicionalmente performados pelos intermediários financeiros, as instituições financeiras,69 que cobram (legitimamente, diga-se de passagem) por tais serviços – como já registrado anteriormente, receita estimada de US$ 1,2 trilhão com o sistema de pagamentos global, em 2016, conforme o referido estudo.

Ora, as estruturas de *blockchain* que suportam os diversos criptoativos hoje já em curso pelo mundo estão habilitadas a executar todas as funções inerentes ao processo de verificação aqui sucintamente descrito. E com vantagem, na medida em que suas transações contam com a segurança da criptografia assimétrica, sendo registradas nos blocos de informação dos livros-razão distribuídos pela rede, com selo de tempo (*time stamping*, certificação de data e hora da ocorrência das transações, assegurando a anterioridade).[70]

---

69 Importante registrar que também é a análise de crédito e o risco que justificam a remuneração dos agentes financeiros tradicionais, especialmente no mercado de crédito, por meio do *spread* bancário, o que não é alterado, pelo menos por ora e pelas utilizações aqui descritas, com a tecnologia de *blockchain*.

70 "We identify two key costs that are affected by distributed ledger technology: 1) the cost of verification; and 2) the cost of networking. Markets facilitate the voluntary exchange of goods and services between buyers and sellers. For an exchange to be executed, key attributes of a transaction need to be verified by the parties involved at multiple points in time. blockchain technology, by allowing market participants to perform costless verification, lowers the costs of auditing transaction information, and allows new marketplaces to emerge. Furthermore, when a distributed ledger is combined with a native cryptographic token (as in bitcoin), marketplaces can be bootstrapped without the need of traditional trusted intermediaries, lowering the cost of networking. This challenges existing revenue models and incumbents's market power, and opens opportunities for novel approaches to regulation, auctions and the provision of public goods, software, identity and reputation systems.", *in*: CATALINI, Christian; GANS, Joshua S. *Some Simple Economics of the blockchain.* Working Paper

E aqui vem uma questão chave, qual seja, todas as funções tradicionalmente exercidas pelo intermediário passam a ser efetuadas pelos próprios integrantes da rede, e a custos infinitamente menores do que os regularmente incorridos. [71]

Vale dizer, os custos de verificação, em realidade, decorrem da assimetria de informações que se afigura entre os diversos agentes econômicos ao realizarem suas transações. Então, fazer face a esta assimetria representa um custo, o que justamente proporciona o surgimento e o espetacular desenvolvimento da indústria de prestação de serviços financeiros. Já a tecnologia de *blockchain*, por sua vez, possui a virtude de reduzir a assimetria de informação, reduzindo, assim também, consequentemente, os custos de transação daí decorrentes, justamente emergidos para fazer face aos mencionados problemas de assimetria informacional. Já não é mais necessário confiar no intermediário que assegurara a lisura da transação. Ou melhor, sequer se faz mais necessário o intermediário. Passa-se a confiar no processo, na rede. E isto se faz a um custo infinitamente menor.[72]

IX – CONCLUSÕES

22952, National Bureau of Economic Research 1050, Cambridge, dezembro de 2016, p. 2. Disponível em: http://www.nber.org/papers/w22952. Acesso: 16 out. 2020.

71 "The cost of intermediation is one of the transaction costs buyers and sellers incur when they cannot efficiently verify all the relevant attributes of a specific transaction by themselves", *in*: CATALINI, Christian; GANS, Joshua S. *Some Simple Economics of the blockchain.* Working Paper 22952, National Bureau of Economic Research 1050, Cambridge, dezembro de 2016, p. 5. Disponível em: http://www.nber.org/papers/w22952. Acesso: 16 out. 2020.

72 "[…] bitcoin appeals to two distinct clienteles. One group consists of technology enthusiasts who embrace bitcoin for online commerce. As more and more routine business transactions migrate online, these users believe bitcoin's value should increase due to transaction demand, and they also cite its cost advantages over credit cards and other payment systems for routine bricks and mortar retail shopping", *in*: YERMACK, David. *Is bitcoin a real currency?* An economic appraisal. Working Paper 19747, NATIONAL BUREAU OF ECONOMIC RESEARCH 1050, Cambridge (MA), dezembro 2013, p. 9. Disponível em: <http://www.nber.org/papers/w19747>. Acesso em: 07 de set. 2020.

Tendo em conta os aspectos técnicos, matemáticos e lógicos envolvidos no funcionamento dos criptoativos, é possível afirmar que estes detêm o potencial não se de funcionarem como efetivos meios de troca, reserva de valor e unidades de conta (enquanto *coins* ou criptomoedas), inclusive superando os benefícios hoje outorgados pelas moedas tradicionais; como também funcionar como ativos financeiros à semelhança dos valores mobiliários (*security tokens*); além de serem utilizados como outorgantes de utilidades para os seus titulares (*utility tokens*); tudo com grande potencial de ganhos de eficiência econômica, haja vista os menores custos de transação daí observados, tanto diretos, como também indiretos, considerando a eficácia com que lidam com o problema da assimetria informacional e a respectiva eliminação dos consequentes gastos que justamente se fazem presentes em razão da necessidade da existência de intermediários, como ocorre no sistema financeiro tradicional; e isso não só no mercado bancário, porquanto também possível no mercado de capitais, em que o terceiro figura como prestador de serviços.

Tais fundamentos técnicos de fato viabilizam a eliminação de uma entidade intermediadora, e com vantagens de eficiência econômica em relação ao sistema tradicional. Contudo, dado o profundo grau de transformação que os criptoativos representam, é natural esperar que a comunidade em geral reclame por um período de adaptação, por uma transição que possibilite aos mercados e à comunidade em geral irem aos poucos compreendendo toda a filosofia que está por trás das arquiteturas de *blockchain*.

Assim, o presente trabalho se propõe justamente a contribuir para este processo de esclarecimento e contínuo aprendizado sobre tal temática. Há sem dúvida uma curva de aprendizado que necessita ser percorrida. Quanto mais rápido e eficiente for este percurso de aprendizado, mais a coletividade

poderá se beneficiar.

Para tanto, buscou-se em primeiro lugar demonstrar os fundamentos da arquitetura de *blockchain*. Viu-se que o fato de esta fazer uso da criptografia assimétrica, e por contar com o atributo da descentralização, e com mecanismos de incentivo à verificação coletiva por parte dos próprios integrantes das redes onde ocorrem as transações, faz com que todo o sistema oferte atributos de segurança e de redução de custos de transação de maneira inédita e muito poderosa. No limite, a sua aplicação sistemática e consistente tende a mudar radicalmente os paradigmas sobre os quais está assentada a civilização ocidental. As formas de gerar e de circular a recursos encontram nas estruturas de *blockchain* o sustentáculo para uma verdadeira reinvenção.

De qualquer forma, imperioso reconhecer que se trata de tema que está em constante evolução, o que faz com que o presente trabalho, além de estabelecer alguns conceitos basilares para o entendimento da temática, procura refletir o estágio atual das discussões. Sem dúvida, faz-se necessário o constante acompanhar da temática.

No entanto, apesar da intensidade e da dinâmica da evolução, alguns aspectos dão sinais de estabilidade e consistência. Estes dizem com a viabilidade e a inexorabilidade da adoção de soluções que utilizem organizações distribuídas autônomas, suportadas por tecnologias de *blockchain*. A tarefa que se impõe a todos quantos que em alguma medida estão envolvidos com o assunto é seguir acompanhando atentamente os seus desdobramentos, sobretudo para que a regulação destes mercados se dê de modo a promover eficiência econômica e o bem-estar da sociedade em geral.

Outrossim, como antes ponderado, há que se reconhecer a necessidade de um marco regulador mínimo, de modo a ensejar segurança sobretudo jurídica, sendo que a regulação deve se dar, preferencialmente, de modo universalmente

padronizado, tendo em vista o caráter transfronteiriço que tais tecnologias ensejam, possibilitando a fácil migração e mesmo a ocorrência do fenômeno da desterritorialização.

E, ao se construírem regulações, é importante se ter em mente que tais respectivos custos de conformidade não podem se constituírem maiores que os ganhos de eficiência econômica que se observam por meio da adoção dessas novas tecnologias, a fim de que não se desincentive a inovação e, dessa forma, retraía o crescimento e o desenvolvimento econômico. Ou seja, ao se normatizar e regular qualquer fenômeno, sobretudo tais avanços que vão no sentido de se reduzirem custos de transação, deve-se cuidar para que os custos de conformidade não suplantem os ganhos propiciados pelas próprias inovações.

Por fim, importante considerar o arcabouço jurídico já existente, sendo que, como no caso aqui estudado, o brasileiro, que pode já perfeitamente incidir sobre tais realidades, a depender do enquadramento aos suportes normativos existentes, como antes detalhadamente demonstrado.

IX – REFERÊNCIAS BIBLIOGRÁFICAS

BAROSSI-FILHO, Milton; SZTAJN, Rachel. *Natureza Jurídica da Moeda e Desafios da Moeda Virtual.* Revista Jurídica Luso-Brasileira, Ano 1 (2015), nº 1, p. 1669-1690. Disponível em: <https://www.cidp.pt/revistas/rjlb/2015/1/2015_01_1669_1690.pdf>. Acesso em: 12 de outubro de 2020.

Cardozo Blockchain Project. Research Report #1. *Not So fast—Risks Related to The Use of a "Saft" for Token Sales*, November, 21, 2017, p. 2. Disponível em:

https://cardozo.yu.edu/programs- centers/blockchain-project. Acesso em: 12 de outubro de 2020.

CRUZ E TUCCI, José Rogério. *Eficácia probatória dos contratos celebrados pela Internet. In:* DE LUCCA, Newton (Coordenador). *Direito & Internet.* Bauru: Ed. Edipro, 2000.

KADAMAI, Rosine. *Criptos, Brasil e as chances que se vão... rápido*. *In*: Linkedin. Disponível em: <https://www.linkedin.com/pulse/criptos-brasil-e-chances-que-se-v%25C3%25A3o-r%25C3%25A1pido-rosine-kadamani/>. Acesso em: 25 de outubro de 2020.

LOYOLA, Gustavo. *Bitcoin: criptomoeda ou pseudomoeda. Disponível em:* <http://www.valor.com.br/opiniao/5305917/bitcoin-criptomoeda-ou-pseudomoeda?utm_source=Facebook&utm_medium=Social&utm_campaign=Compartilhar>. Acesso em 07 de set. 2020.

MAEHARA ALIAGA, Yoshitomi Eduardo. *Estudo sobre mecanismos de consenso de baixo custo para Blockchain*. Dissertação de mestrado. Universidade Estadual de Campinas. Faculdade de Engenharia Elétrica e de Computação. Campinas, 2019. Disponível em: <http://repositorio.unicamp.br/bitstream/REPOSIP/335887/1/Aliaga_YoshitomiEduardoMaehara_M.pdf>. Acesso em: 07 de set. 2020.

MOUGAYAR, Willian. *The Business blockchain. Promise, practice and application of the next internet technology*. New Jersey: John Willey & Sons. Inc, 2016.

NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System.* Disponível em: <https://bitcoin.org/bitcoin.pdf. Acesso em: 07 de set. 2020.

QUEIRÓZ, Régis Magalhães Soares de. *Assinatura Digital e o Tabelião Virtual. In:*

DE LUCCA, Newton (Coordenador). Direito & Internet. Bauru: Ed. Edipro, 2000.

REZENDE, Pedro Antonio Dourado de. *Carta aberta ao Dr. Renato Opice Blum. Proposta de Debate na 1ª Conferência Internacional de Direito na Internet e na Informática*. São Paulo, 6 e 7 de novembro de 2000. Disponível em: < https://www.cic.unb.br/~rezende/trabs/gesso.htm>. Acesso em: 07 de set. 2020.

Thomson Reuters. *Are you ready to blockchain?* Disponível em: <https://www.thomsonreuters.com/en/reports/blockchain.html>. Acesso em: 07 de set. 2020.

TRINDADE, Manoel Gustavo Neubarth Trindade. Economia de Plataforma (ou tendência à bursatilização dos mercados): Ponderações Conceituais Distintivas em relação à Economia Compartilhada e à Economia Colaborativa e uma Abordagem de Análise Econômica do Direito dos Ganhos de Eficiência Econômica por meio da Redução Severa dos Custos de Transação. *Revista Jurídica Luso-Brasileira*, Ano 6 (2020), n.º 4. Disponível em: <https://www.cidp.pt/publicacao/revista-juridica-luso-brasileira-ano-6-2020-n-4/209>. Acesso em: 07 de set. 2020.

YERMACK, David. *Is bitcoin a real currency? An economic appraisal.* Working Paper 19747, NATIONAL BUREAU OF ECONOMIC RESEARCH 1050, Cambridge (MA), dezembro 2013, p. 8. Disponível em: <http://www.nber.org/papers/w19747>. Acesso em: 07 de set. 2020.