UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
FACULDADE DE DIREITO
DEPARTAMENTO DE DIREITO ECONÔMICO E DO TRABALHO

Marcelo Merlo Flores

A LEGISLAÇÃO BRASILEIRA ATUAL E A DIFICULDADE DE TRIBUTAÇÃO SOBRE AS OPERAÇÕES COM CRIPTOATIVOS EM REDES P2P

Porto Alegre
2022

Marcelo Merlo Flores

A LEGISLAÇÃO BRASILEIRA ATUAL E A DIFICULDADE DE TRIBUTAÇÃO SOBRE AS OPERAÇÕES COM CRIPTOATIVOS EM REDES P2P

Monografia apresentada ao Departamento de Direito Econômico e do Trabalho da Universidade Federal do Rio Grande do Sul como requisito parcial para a obtenção de grau de Bacharel em Ciências Jurídicas e Sociais.

Orientadora: Profa. Dra. Maria Cristina Cereser Pezzella

Porto Alegre
2022

Marcelo Merlo Flores

A LEGISLAÇÃO BRASILEIRA ATUAL E A DIFICULDADE DE TRIBUTAÇÃO SOBRE AS OPERAÇÕES DE CRIPTOATIVOS EM REDES P2P

Monografia apresentada ao Departamento de Departamento de Direito Econômico e do Trabalho da Universidade Federal do Rio Grande do Sul como requisito parcial para a obtenção de grau de Bacharel em Ciências Jurídicas e Sociais. Orientadora: Profa. Dra. Maria Cristina Cereser Pezzella

Aprovado em _____ de _____ de 2022.

BANCA EXAMINADORA:

_____
Profa. Dra. Maria Cristina Cereser Pezzella – (orientadora)

_____
Prof. Dr. Éderson Garin Porto

_____
Prof. Me. Rafael Ferreira da Costa

_____
Prof. Dra. Kelly Lissandra Bruch

AGRADECIMENTOS

Agradeço a minha orientadora, Maria Cristina Cereser Pezzella, pelo apoio nas discussões do tema escolhido e pelo tempo que compartilhou comigo nesse trabalho desenvolvido.

Agradeço a minha família, a qual sempre me indicou, desde criança, que a educação é a forma mais intensa e satisfatória para o crescimento pessoal . Aos meus amigos da Defensoria Pública (estagiários, Analistas e Defensoras), por terem criado comigo o melhor ambiente de trabalho que já existiu e por terem construído as melhores memórias que levarei pro resto da vida. Trabalhar na Defensoria Pública do Partenon e conviver com todos vocês foi um verdadeiro privilégio.

.

A liberdade não é apenas um valor em particular é a fonte e condição da maioria dos valores morais. O que uma sociedade livre oferece ao indivíduo é muito mais do que ele seria capaz de fazer se apenas ele fosse livre.

— Friedrich August von Hayek

RESUMO

Ao avançar da sociedade, as novas tecnologias e construções sociais geram uma necessidade de modernização do nosso arcabouço jurídico e legislativo para acompanhar e resguardar esse dinamismo, garantindo segurança jurídica e proteção aos cidadãos. O mundo virtual das criptomoedas é muito recente (iniciou com a criação do Bitcoin em 2008) e de natureza técnica, frequentemente distante do entendimento de parte considerável da sociedade, com exceção daqueles mais habituados às tecnologias de informação e de dados. Por essa razão, diversas situações devem surgir e demorarão a ser institucionalizadas, trazidas ao formalismo jurídico da sociedade e dos governos, sob a forma de regulamentação jurídica e legislativa. O trabalho tem como objetivo estudar o cenário atual da legislação brasileira sobre criptoativos, bem como discutir sobre a dificuldade de auditar e tributar uma operação específica nesse ambiente virtual, qual seja, a transferência P2P (*peer-to-peer* / ponto-a-ponto) entre carteiras digitais (*crypto wallets*).

Palavras-chave: Criptoativos. Criptomoeda. Bitcoin. Peer-to-peer. Carteira digital. Tributação.

ABSTRACT

As society advances, new technologies and social constructions generate a need to modernize our legal and legislative framework to accompany and protect this dynamism, ensuring legal certainty and protection for citizens. The virtual world of cryptocurrencies is very recent (it started with the creation of Bitcoin in 2008) and of a technical nature, often far from the understanding of a considerable part of society, with the exception of those more accustomed to information and data technologies. For this reason, different situations must arise and will take time to be institutionalized, brought to the legal formalism of society and governments, in the form of legal and legislative regulation. The objective of this work is to study the current scenario of Brazilian legislation on crypto assets, as well as to discuss the difficulty of auditing and taxing a specific operation in this virtual environment, namely, the P2P transfer (peer-to-peer) between digital wallets (crypto wallets).

Keywords: Crypto assets. Criptocurrency. Bitcoin. Peer-to-peer. Digital wallets. Taxation.

SUMÁRIO

1 INTRODUÇÃO **8**
2 DEFINIÇÕES **10**
2.1 Criptomoeda 10
2.2 Token 12
2.2.1 *Token de pagamento (Payment Tokens)* 12
2.2.2 *Token de utilidade (Utility Tokens)* 12
2.2.3 *Token de ativo (Assets Tokens)* 12
2.3 NFTS (non- fungible tokens) 13
2.4 Criptoativo 13
2.5 Blockchain (Ledger Descentralizado Virtual) 14
2.6 Crypto Wallets (Carteiras Digitais) 16
3 BITCOIN **19**
3.1 Contexto Histórico 19
3.2 Funcionamento e operacionalização 22
3.3 Criptografia na rede Bitcoin 24
3.4 Formas de aquisição de bitcoins 26
3.5 Características desafiadoras do uso de bitcoins 28
4 LEGISLAÇÃO BRASILEIRA E O ATUAL CENÁRIO JURÍDICO **31**
4.1 Projetos de Lei 2.303/2015 e 2.060/2019 (Câmara dos Deputados) 31
4.2 Projeto de Lei 3.825/2019 (Senado Federal) – substituído pelo PL 4.401/2021 . 34
4.3 Análise sobre a regulamentação legislativa brasileira 35
4.4 A dificuldade de enquadramento jurídico dos criptoativos 36
5 AS TRANSFERÊNCIAS P2P (*PEER-TO-PEER* / PONTO-A-PONTO) ENTRE CARTEIRAS DIGITAIS **40**
5.1 Conceito e funcionamento 40
5.2 Problema jurídico – possibilidades de tributação sobre operações P2P 42
5.3 Questão operacional/instrumental – dificuldades em tributar uma operação anônima 49
5.3.1 Pontos de vazamento de privacidade na rede Bitcoin: possíveis caminhos para identificação das partes que negociam em redes P2P 51
5.3.2 Práticas que dificultam a identificação das transações em redes P2P puras ... 53
6 CONSIDERAÇÕES FINAIS **56**
REFERÊNCIAS 59
ANEXO – Projeto de Lei 4.401/2021 60

1 INTRODUÇÃO

Inicialmente, entender o que são criptoativos não é uma tarefa simplória, uma vez que a essência tecnológica das criptomoedas como Bitcoin, Ethereum e outras, é bastante inovadora e congrega conquistas de diferentes áreas do conhecimento humano. Trabalharei utilizando o Bitcoin como representante da categoria criptomoedas/criptoativos por algumas razões: ele foi o precursor desse campo; atualmente, representa em torno de 40% da capitalização total existente[1], bem como sua tecnologia de *blockchain* foi replicada para outros ativos e é base do problema enfrentado nesse trabalho.

Em razão da tecnicidade da matéria, primeiro é necessário desenvolver melhor alguns conceitos-base que permeiam esse campo do conhecimento, como *blockchain*, criptomoeda, *token*, entre outros. Após, buscarei apresentar o cenário atual da regulação desse mercado, especialmente quanto aos projetos legislativos em tramitação.

Por fim, a problemática principal que são as transferências de ativos sem instituições financeiras intermediárias, ou seja, transferências P*2P* (*peer-to-peer*) entre carteiras digitais (*crypto wallets*). De fato, essa é uma parcela ainda mais específica desse nicho (criptoativos) e que pode gerar grandes desdobramentos para a segurança jurídica e tributária dos países. Embora os sistemas de pagamentos descentralizados (os quais permitem transferências de ativos via internet, sem uma contraparte institucional e de forma rápida e barata) sejam uma notável evolução e uma resposta a deficiências conhecidas do sistema financeiro tradicional, é inegável que essa ferramenta pode ser utilizada, por exemplo, para transferir ativos sem notificação ou regulação do Estado.

Por ser recente (o primeiro bloco de Bitcoin foi minerado em janeiro de 2009, há apenas 13 anos aproximadamente), ainda não há uma construção doutrinária e jurisprudencial pátria. Em verdade, ao pensarmos globalmente, o tema permanece

[1] **Dados históricos do Bitcoin**. Disponível em: https://coinmarketcap.com/pt-br/currencies/bitcoin/ Acesso em 25.07.2022.

rodeado de controvérsia, pouco ou nenhum consenso, muita discussão política e interesses colidentes. Por exemplo, alguns países entendem as “moedas digitais” como um ativo financeiro (como ações, fundos imobiliários, entre outros ativos negociados em Bolsa de Valores); outros enxergam como moeda (assumindo regras de câmbio financeiro); e há ainda alguns que entendem as criptomoedas como propriedade, obedecendo a regulamentação comercial de bens.

A fim de regulamentar e fomentar esse sistema com o intuito de proteger os investidores, os trabalhadores do setor, bem como as empresas que investem nessa área e que geram avanços tecnológicos para a nossa sociedade, é vital que o legislador aprecie as particularidades dos criptoativos para que os enquadre apropriadamente no ordenamento jurídico.

2 DEFINIÇÕES

2.1 CRIPTOMOEDA

O bitcoin foi a primeira a surgir e é o mais capitalizado, negociado e com a rede mais testada na atualidade[2], contudo, conforme o site coinmarket.com, atualmente existem 20.719 criptomoedas, o que é um número assustador, levando em conta que, em 2019, existiam apenas 2300. Ou seja, uma multiplicação de quase 10 vezes em apenas dois anos.

A denominação criptomoeda é uma tradução do termo "*cryptocurrency*" do inglês, o qual representa a junção entre criptografia (*crypto*) e moeda (*currency*). *Currency*, mais adequadamente poderia ser traduzido por "moeda corrente", ou seja, a moeda de curso legal utilizada nos países, como o nosso Real.

Criptomoeda (espécie do gênero moedas virtuais) é um meio de troca que se utiliza de criptografia para assegurar transações e para controlar a criação de novas unidades da moeda.

O Banco Central do Brasil (BCB/BACEN), em seu Comunicado nº 25.306/2014, esclarece que as chamadas moedas virtuais ou criptomoedas não são emitidas nem garantidas por uma autoridade monetária. Algumas são emitidas e intermediadas por entidades não financeiras e outras não têm sequer uma entidade responsável por sua emissão (uma referência ao Bitcoin). Em ambos os casos, as entidades e pessoas que emitem ou fazem a intermediação desses ativos virtuais não são reguladas nem supervisionadas por autoridades monetárias de qualquer país (aqui, uma referência às *exchanges* ou corretoras estrangeiras).

Ainda, o BCB esclarece que "as chamadas moedas virtuais não se confundem com a moeda eletrônica de que trata a lei nº 12.865/2013 e regulamentação infralegal. Moedas eletrônicas, conforme disciplinadas por esses atos normativos, são recursos armazenados em dispositivo ou sistema eletrônico que permitem ao usuário final efetuar transação de pagamento denominada em moeda nacional." Em contrapartida, as moedas chamadas virtuais possuem forma própria de denominação, ou seja, são denominadas em unidade de conta distinta

[2] Bitcoin, com 'B' maiúsculo, refere-se a rede e o protocolo na qual a criptomoeda é transacionada, enquanto que bitcoin, com 'b' minúsculo, refere-se a própria unidade da criptomoeda, que é negociada com o símbolo BTC.

das moedas emitidas por governos soberanos, e não se caracterizam dispositivo ou sistema eletrônico para armazenamento em reais.

Criptomoeda, ou moeda criptografada, “é um ativo digital denominado na própria unidade de conta que é emitido e transacionado de modo descentralizado, independente de registro ou validação por parte de intermediários centrais, com validade e integridade de dados assegurada por tecnologia criptográfica e de consenso em rede.”[3]

As características mais relevantes para a diferenciação conceitual entre criptomoedas e outros valores escriturais são: i) serem denominadas na própria unidade de conta; e ii) possuírem estrutura operacional descentralizada, com governança definida primordialmente no software por meio do qual funcionam. Em relação a outras representações eletrônicas de valor, as criptomoedas são ativos digitais denominados em sua própria unidade de conta (outros exemplos são moedas de jogos eletrônicos e programas de fidelidade aérea e suas milhas), bem como possuem sua própria estrutura descentralizada e uma rede distribuída de registros para garantir a integridade de suas transações como um todo.

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

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

Quando se afirma que as criptomoedas são instrumentos que não possuem a garantia de um governo central, isso significa que tais moedas ainda não são aceitas por governos para liquidação de obrigações tributárias e não são legalmente definidas como moedas com poder liberatório de obrigações[4], nem

---

[3] Cesar Stella, Julio. Moedas virtuais no brasil: Como enquadrar as criptomoedas. Revista da PGBC – V. 11 – N. 2 – Dez. 2017. Pág. 3.

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

tampouco possuem respaldo de seguros de depósito (como ocorre com a moeda bancária).

2.2 TOKEN

Token, em inglês, pode significar um sinal, um símbolo ou uma ficha, por ser um elemento que representa outra coisa e que possui a característica de circulação. A partir de sua finalidade e forma de utilização, os *tokens* podem ser classificados de diferentes formas. Embora, como dito, ainda não haja um consenso geral nesse mundo dos criptoativos, a Comissão de Títulos e Câmbio dos Estados Unidos (em inglês, U.S. Securities and Exchange Commission, geralmente referida pela sigla SEC) e a Autoridade Financeira de Supervisão do Mercado Suíça (FINMA) têm adotado uma caracterização bastante similar.

A partir dessa classificação, os tokens são divididos em: *Payment Tokens, Utility Tokens e Asset Tokens, os quais são descritos a seguir.*

2.2.1 Token de pagamento (*Payment Tokens)*

Os *tokens* de pagamento são as próprias criptomoedas, como o Bitcoin, destinadas a serem utilizadas como meio de pagamento na aquisição de bens ou serviços, ou como uma modalidade de dinheiro ou transferência de valor.

2.2.2 Token de utilidade *(Utility Tokens)*

Os *tokens* de utilidade são aqueles destinados a prover um acesso digital a uma aplicação/serviço não financeiro. Por si só, eles não possuem valor, apenas um significado representativo para a instituição que fez sua emissão.

2.2.3 Token de ativo (*Assets Tokens*)

Por fim, os t*okens* de ativo representam ativos como a participação em uma empresa, um direito a receber dividendos ou um pagamento de juros. Sob um viés econômico, podemos fazer uma analogia às ações, títulos e derivativos. Ainda, podem representar ativos físicos que serão transacionados digitalmente, ou seja, são uma representação digital de algo que existe fisicamente.

2.3 NFTs (Non- fungible tokens)

NFTs (em inglês, non-fungible tokens) ou tokens não fungíveis são, conforme dicionário Collins, “um certificado digital único, registrado em *blockchain,* o qual é usado para registrar a propriedade de um ativo (ex: uma obra de arte ou um objeto colecionável). Portanto, um NFT é um certificado que garante propriedade sobre algo no mundo digital.

São considerados bens infungíveis, isto é, não podem ser substituídos por outros. Assim, como os criptoativos, de forma geral, ainda não possuem uma regulação específica brasileira. Os NFTs são basicamente títulos de propriedade digital que não podem ser fraudados (visto que são registrados em *blockchain* pública e distribuída), entretanto podem ser emitidos e negociados online, de forma segura e eficiente. Por exemplo, atualmente, uma das principais aplicações visualizadas para essa tecnologia, é a compra e venda de obras de arte virtuais, musicais, serviços, softwares, todos com um certificado digital que atesta a veracidade do bem/serviço.

NFTs repreentam uma nova forma de investimento pensada e criada para o mercado digital, utilizando a tecnologia *blockchain*, a qual permite uma transição de uma “internet de cópia” (copia e cola, duplicação de arquivos, “gasto duplo”) para uma internet de valor, inaugurando o conceito de escassez digital, algo antes impossível de se garantir tecnicamente[5].

2.4 CRIPTOATIVO

Criptoativos (*cryptoassets, em* inglês) são o gênero, dentro do qual existem as espécies criptomoedas, tokens e NFTs, entre outros. Frequentemente veremos a expressão criptomoeda ser utilizada como sinônimo de criptoativo, porém, tecnicamente, é mais adequado utilizar criptoativo para representar uma classe de ativos digitais. O processo regulatório desse mercado é muito recente e as próprias definições básicas de alguns termos ainda estão sendo construídas ou difundidas de forma mais uniforme.

---

[5] NFT: por que essa tecnologia vale tanto. Disponível em https://www.migalhas.com.br/quentes/350148/nft-entenda-o-que-e-e-por-que-essa-tecnologia-vale-tanto. Acesso em 14/07/2022.

Os criptoativos são representações de valores que só existem em registros digitais. A transação destas representações é feita entre indivíduos ou empresas sem a intermediação de uma instituição financeira. Eles são um ativo intangível, que não tem uma substância física. A definição da Receita Federal resume as principais características dos criptoativos:

> "A representação digital de valor denominada em sua própria unidade de conta, cujo preço pode ser expresso em moeda soberana local ou estrangeira, transacionado eletronicamente com a utilização de criptografia e de tecnologias de registros distribuídos, que pode ser utilizado como forma de investimento, instrumento de transferência de valores ou acesso a serviços, e que não constitui moeda de curso legal".

2.5 BLOCKCHAIN (ledger descentralizado virtual)

A tecnologia *blockchain* é a base dos conceitos de distribuição e descentralização das informações e traz consigo o princípio de transparência e imutabilidade dos registros, proporcionando a auditabilidade dos dados.

Filippi e Wright[6] definem *blockchain* como "um banco de dados descentralizado e mantido por uma rede, sendo possível compreender o armazenamento de informações e a execução de protocolos."

Assim, cada bloco confirma a integridade do bloco anterior, garantido a integridade de todas as transações realizadas. *Block*, em inglês, significa bloco, e *chain* significa corrente, o que é bem ilustrativo, pois as transações são agrupadas em blocos, que por usa vez são encadeadas de forma criptografada aos blocos anteriores, como uma corrente, conferindo a segurança das transações e imutabilidade dos registros.

A tecnologia de livro razão distribuída ou *distributed ledger technology* (DLT) é utilizada na rede Bitcoin. Nesse sistema, todos os usuários têm acesso a todos os dados do livro razão, que consiste num histórico encadeado de todas as transações já efetivadas. Qualquer usuário que tenha capacidade computacional para tal pode se conectar para emitir moeda e validar transações. As novas transações são publicadas pelo emissor do pagamento mediante a aposição da chave privada que corresponde à sua carteira. Essa assinatura eletrônica garante a autenticidade de cada transação originada perante todos os usuários da rede. Cada transação, após

---

[6] DE FILIPPI, Primavera; WRIGHT, Aaron. **Blockchain and the Law: the Rule of Code**. Harvard University Press: Cambrige, Massachusetts: 2018.

ser confirmada, é unida a um determinado número de outras transações também confirmadas, formando um bloco. Esse bloco é, então, selado criptograficamente e registrado no *blockchain* com data e horário, sendo gravado na sequência do anterior.

O problema central resolvido pelo *blockchain* foi o gasto duplo. Qual é a questão? O dinheiro eletrônico é apenas um dado, conjunto de bits e bytes que podem ser reproduzidos, copiados. Isso faz com que uma pessoa possa transferir um arquivo a outra, porém manter uma cópia dele em seu próprio computador. Logo, na prática, haveria uma duplicação do “dinheiro” (não uma operação de crédito e débito, mas sim uma criação artificial de um valor). Na prática, seria como se alguém estivesse falsificando uma cédula monetária, imprimindo dinheiro falso.

Para que isso não ocorra, a rede descentralizada do *blockchain*, por meio de sua rede de milhares de nós, faz uma verificação após introdução de uma transação: caso essa transação não seja compatível com o registro de todos os outros nós, ela não será registrada, será descartada. Dessa forma, a rede Bitcoin mantém os seus níveis de segurança, já que para fazer uma alteração na rede, é necessária a validação de um número substancial de nós.

O que são os nós (*nodes*) em uma rede *blockchain*? Um nó é um ponto em uma rede: no campo da informática e da tecnologia de informação, nós são dispositivos conectados a uma rede de computadores que transmite, processa e armazena informações. Consistem em 2 coisas: hadware, que é a parte física necessária para executar o software, o qual é o conjunto de instruções para executar uma tarefa.

Os nossos celulares, por exemplo, são um nó da internet, logo os aplicativos instalados nele são softwares que podem se conectar à internet e receber instruções ou pedaços de informações, os quais são processados e armazenados dentro do celular e de servidores (computadores) conectados à internet. Analogamente, a rede Bitcoin funciona da mesma maneira, todavia ela é muito mais simples, uma vez que a rede e os nós do Bitcoin foram criados para transmitir e armazenar apenas um tipo de informação: dados que representam transações com a criptomoeda Bitcoin.

Os nós também podem exercer a função de mineradores, dispendendo esforço computacional para processar transações, garantir a segurança da rede e

que todo o sistema esteja sincronizado, recebendo recompensa na forma do criptoativo sendo minerado. O termo “mineração” é utilizado em analogia a mineração do ouro, pois, por meio do esforço dos mineradores, novos ativos serão disponibilizados.

Os aspectos de segurança e confiança são o que torna a *blockchain* uma tecnologia tão promissora, denominada por alguns autores como “protocolo de confiança”[7], pois asseguraria a consistência e a imutabilidade dos dados ali registrados. A cada dez (10) minutos, todas as transações efetuadas dentro do sistema são verificadas e registradas em um bloco, que é salvo concomitantemente em computadores de vários voluntários, disponibilizados para este fim, sendo o bloco vinculado ao bloco anterior, formando uma corrente (*chain)*.

A maneira como a criptografia é integrada ao sistema a fim de evitar a necessidade de validação da chave por um intermediário é o principal valor agregado pela *blockchain*, uma vez que permite que as criptomoedas circulem pelo mercado sem uma autoridade estatal para assegurar seu valor ou a sua autenticidade.

2.6 CRYPTO WALLETS (carteiras digitais)

Assim como necessitamos de uma carteira para guardar nosso dinheiro físico ou uma conta em corretora de valores para custodiar ativos como ações, fundos e títulos públicos, as *crypto wallets* são softwares (aplicativos) instalados no celular ou no computador, nos quais é possível realizar transações com criptomoedas. Ainda, as *wallets* podem ser dispositivos físicos que guardam as chaves criptográficas fora do ambiente virtual. Na prática, as carteiras virtuais são semelhantes a contas bancárias, mas com uma gigante diferença: é o dono da carteira o responsável pela posse e segurança de seus ativos, não o banco.

Uma carteira virtual é um mecanismo para administrar as senhas de acesso que possibilitam movimentar os ativos digitais. Como já mencionado, toda carteira de criptomoedas possui uma chave pública (identificadora) e uma chave privada (usada para assinar as transações) vinculadas. É importante explicar que um

---

[7] TAPSCOTT, Don; TAPSCOTT, Alex. **Blockchain revolution – how the technology behind bitcoin is changing money, business and the world**. Nova York: Penquin, 2016. E-book.

endereço de Bitcoin, por exemplo, não é compatível com outras criptomoedas, como Ethereum Chainlink, Cardano, etc. Existem carteiras digitais que custodiam diversas criptomoedas diferentes, entretanto os endereços para transferências são independentes, ou seja, para cada criptomoeda existe um endereço público próprio.

O funcionamento de uma *crypto wallet* é relativamente fácil: após ser criada, imediatamente é gerada uma *seed* (semente, em inglês), que é uma chave-mestra. Essa *seed* é uma sequência de 12 a 24 palavras em inglês, que funciona como uma senha de recuperação do sistema (essa sequência é uma representação visual da chave-mestra). É extremamente importante que ela seja guardada sem exposição, caso contrário isso poderia permitir que qualquer pessoa possa acessar essa carteira, bem como a chave privada criptografada.

Existem alguns tipos de *wallets*, divididas em 2 grupos: as *hot wallets* (carteiras quentes) e as *cold wallets* (carteiras frias). As *hot* são aquelas conectadas à internet, logo são mais práticas do que as *cold*, contudo costumam ser mais vulneráveis a ataques virtuais. Existem 3 versões de *hot wallets*: *mobile, web* e *desktop*. Mobile são carteiras de criptomoedas que podem ser baixadas em lojas de aplicativo de celular; as web são aquelas acessadas pelo próprio computador; e as desktop são aquelas que podem ser baixadas e instaladas no próprio HD do computador.

As carteiras frias são aquelas que não estão conectadas à internet e, por essa, razão, costumam ser mais seguras, embora possam sofrer dano físico (calor, umidade, etc) ou até serem perdidas. As *hardware wallets* são dispositivos físicos (pequenas e semelhantes a pen drives) em que é possível armazenar criptomoedas; já as *paper wallets* são, basicamente, um pedaço de papel impresso com as chaves pública e privada, havendo programas, como o BitAddress, em que é possível gerar uma *paper wallet*.

Figura 1 – Carteiras virtuais

Fonte: https://blog.mercadobitcoin.com.br/carteira-virtual.

3 BITCOIN

3.1 CONTEXTO HISTÓRICO

Ao final da segunda guerra mundial, em julho de 1944, o sistema financeiro internacional estava despedaçado, pois as maiores potências ainda estavam em guerra, preocupadas com os avanços bélicos, mais do que com os avanços econômicos. Nesse contexto, ocorreu o acordo (ou acordos) de Bretton Woods entre 45 países, com o intuito de definir novos parâmetros que iriam reger a economia mundial pós-guerra. Esse novo sistema financeiro seria amplamente favorável aos Estados Unidos ao implementar uma conversibilidade dólar-ouro.

O primeiro passo foi garantir uma estabilidade monetária para as nações, ao definir que cada país seria obrigado a manter a taxa de câmbio de sua moeda “congelada” ao dólar, com margem de manobra de cerca de 1%, sendo que o dólar seria ligado ao valor do ouro em uma base fixa. Assim, os bancos centrais deveriam administrar suas moedas com lastro em dólar, e a moeda norte americana seria conversível a uma taxa constante em ouro.

Além disso, foram criadas instituições para controle e gerência do acordo, como o Banco Mundial e o Fundo Monetário Internacional (FMI). Esse novo sistema liberal, o qual primava pelo livre mercado e fluxo de comércio e capitais, foi a base para o maior ciclo de crescimento da história do capitalismo.

Porém, esse lastro em ouro, no final das contas, controlava indiretamente os gastos que as Nações tinham, bem como demandava uma quantidade muito grande do metal. Assim, por conta de uma série de ataques especulativos ao dólar, e um aumento da oferta mundial dessa moeda, o governo estadunidense se viu pressionado, e, de forma unilateral, decidiu pôr fim ao lastro do dólar em ouro, ou seja, a conversibilidade do dólar em ouro deixou de existir na economia mundial. Diante disso, algumas moedas que antes estavam sendo trabalhadas em regimes de câmbio fixo passam a ser flutuantes, e o dólar se torna uma moeda de reserva internacional.

Diante desse comportamento, a economia mundial entra numa fase na qual a simetria e a rigidez de períodos anteriores deixam de ser seguidas, para que os governos tenham mais autonomia na prática de políticas visando ao mercado interno. Outrossim, a moeda passa a ser totalmente fiduciária, não havendo nenhum lastro fixo que a sustente. Essa última característica é base fundamental para

entender a política monetária desenvolvida pelos bancos centrais mundiais na década de 2000, bem como uma das principais razões para o surgimento da tecnologia *blockchain* e do Bitcoin.

A crise financeira de 2008 deixou uma marca profunda na sociedade e, possivelmente, alavancou a criação do bitcoin: foi o ano da bolha imobiliária norte-americana (a última grande crise econômica, antes da epidemia do COVID-19), o qual logo se espalhou para o resto do mundo. Gerada pelo descontrole do setor financeiro, principalmente na manipulação de derivativos e operações securitizadas com títulos altamente arriscados e frágeis, cumulado com a ineficácia das empresas de auditoria contábil e ganância excessiva dos bancos e instituições financeiras, a crise foi respondida pelos governos com expansão fiscal e monetária como nunca antes visto.

Após esse evento, a desconfiança nas grandes instituições financeiras e nas moedas emitidas pelos Estados, foi um dos catalisadores para o surgimento do bitcoin. Em verdade, não foi a crise de 2008 o ponto inicial das criptomoedas: as moedas digitais e as moedas criptografadas remetem aos movimentos anarquistas da década de 1980, período no qual ganhou importância um grupo que via na criptografia e no uso das tecnologias de informação uma forma de suplantar a supervisão e regulação dos entes governamentais, além de um caminho para aperfeiçoar a privacidade dos indivíduos. Em 1989, foi criada a primeira moeda digital amplamente conhecida, o Digicash, o qual baseava suas transações em um sistema de pagamentos centralizado (*eCash*) e no uso da criptografia para dar privacidade aos seus usuários adicionando anonimato nas transações.

Após, outras moedas digitais foram criadas, como o *e-gold* (1996) e o *b-money* (1998), as quais operavam em sistemas de pagamentos centralizados. Contudo o grande diferencial veio mesmo com o bitcoin, pois, diferentemente das outras tecnologias, ele não representava uma moeda fiduciária, era baseado em um sistema descentralizado de pagamento, utilizava criptografia para manter seguro o sistema de validação das transações e não necessitava de intermediário financeiro para validação e registro das transações (um perfeito sistema *peer-to-peer*).

Ainda, ao longo da década de 90, aprimoramentos tecnológicos deram origem ao *hashcash*. O *hashcash* não é um tipo de moeda digital, nem mesmo seu desenvolvimento inicial está atrelado ao desenvolvimento paralelo de uma

criptomoeda. No entanto, por definição, o *hashcash* é uma tecnologia de *proof-of-work* (prova de trabalho), originalmente criada para limitar o spam de e-mails e outros ataques de rede por meio da implementação de provas de trabalho que requerem uma quantidade específica de trabalho de uma CPU para realizar verificações eficientes. Essa tecnologia foi uma das bases fundamentais para a criação do Bitcoin e de outras criptomoedas, como o *b-money*. Anterior à criação do bitcoin, o *b-money*, citado por Nakamoto em seu artigo, foi uma proposta de moeda digital relacionada às possíveis implementações do *hashcash*. No sistema *B-money*, o dinheiro é transferido transmitindo a transação para todos os participantes, e os servidores (um número menor de participantes) são os responsáveis por publicar essas transações no sistema, evitando também que haja um movimento inflacionário de criação da moeda.

A evolução das moedas digitais proporcionou um cenário propício para o surgimento de sistemas de pagamentos mais ágeis e flexíveis. Nesse sentido, a idealização do bitcoin traduz não apenas o aprimoramento e as novas descobertas tecnológicas que lhe deram imenso destaque, mas a continuidade de ideias relativas ao movimento anarquista que viam a criptografia como uma forma de atingir autonomia e independência dos Estados e governos.

Desse modo, antes mesmo de aprofundar suas características e operacionalidade, deve-se salientar que, em relação ao seu aspecto tecnológico, o grande diferencial de Nakamoto ao criar o Bitcoin foi o desenvolvimento de uma moeda capaz de funcionar em um sistema de pagamentos descentralizado, diferente dos sistemas das moedas antecessoras. Alinhado a esse sistema descentralizado de pagamentos, a *blockchain* foi incorporada ao *hashcash* como tecnologia de *proof-of-work* para dar segurança nas transações, superando definitivamente o problema relacionado ao gasto duplo: “Para implementar um servidor de *timestamp* distribuído em uma base *peer-to-peer*, precisaremos usar um sistema de prova de trabalho semelhante ao Hashcash“[8]. Adicionalmente, a fim de evitar o suposto problema da espiral inflacionária, sua oferta total foi criada de forma a ser limitada em 21 milhões de bitcoins, número ao qual se espera chegar em 2140.

---

8 NAKAMOTO, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. 4. Proof of work - “to implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash”

3.2 Funcionamento e operacionalização

O problema do gasto duplo sempre foi um verdadeiro obstáculo ao efetivo uso e popularização das criptomoedas: ele se refere à possibilidade de um mesmo *token* digital ser gasto em mais de um transação, uma vez que ele é um arquivo digital que poderia facilmente e livremente ser duplicado, assim como são os arquivos digitais que enviamos a outras pessoas, mas que as cópias podem ser mantidas em nossos computadores.

Em 2008, um indivíduo ou grupo de indivíduos conhecido(os) apenas pelo nome Satoshi Nakamoto, publicou um documento de 9 páginas intitulado "Bitcoin: Um Sistema de Dinheiro Eletrônico par-a-par".[9] O software que contém o código feito por esse grupo permite a criação do Bitcoin, está disponibilizado na internet e qualquer pessoa pode ter acesso a ele, sendo assim um software de código aberto.

Até a invenção do Bitcoin em 2008, transações online sempre requereram um terceiro intermediário de confiança, o qual faria um registro histórico das transações para evitar a duplicação de saldos e o correto crédito-débito de valores entre 2 pontos. A necessidade de um terceiro agente é característica dos sistemas de pagamentos centralizados.

Com a criação do Bitcoin, eliminou-se a necessidade desse agente, dando espaço para o desenvolvimento de um sistema de pagamentos descentralizado, a *blockchain*. Nesse sistema, a responsabilidade por registrar as transações foi atribuída a todos os computadores que fizessem parte da rede, como um sistema de ponto a ponto (*peer-to-peer*) descentralizado. Além disso, o sistema é uma rede pública totalmente distribuída, ou seja, qualquer um pode ter o software instalado em seu computador e fazer parte da rede.

Nesse sistema, a validação de qualquer tipo de transação está apoiada no uso da tecnolgia do *hashcash*, o qual possibilitou a existência de uma prova de trabalho (*proof-of-work*) capaz de validar as transações por meio das CPUs que integram o sistema, e essa mesma tecnologia foi utilizada por Nakamoto na elaboração do Bitcoin. O *proof-of-work* é a resolução de problemas matemáticos de alta dificuldade que são realizados pelas CPUs, caracterizando-se por ser um

9 NAKAMOTO, Satoshi. **Bitcoin: Um Sistema de Dinheiro Eletrônico Peer-to-Peer**. Disponível em https://bitcoin.org/files/bitcoin-paper/bitcoin_pt_br.pdf. Acesso em 15.08.22.

processo custoso, tanto por necessitar equipamentos caros e de alta performance, quanto pelo tempo e gasto energético despendido na resolução desses exercícios.

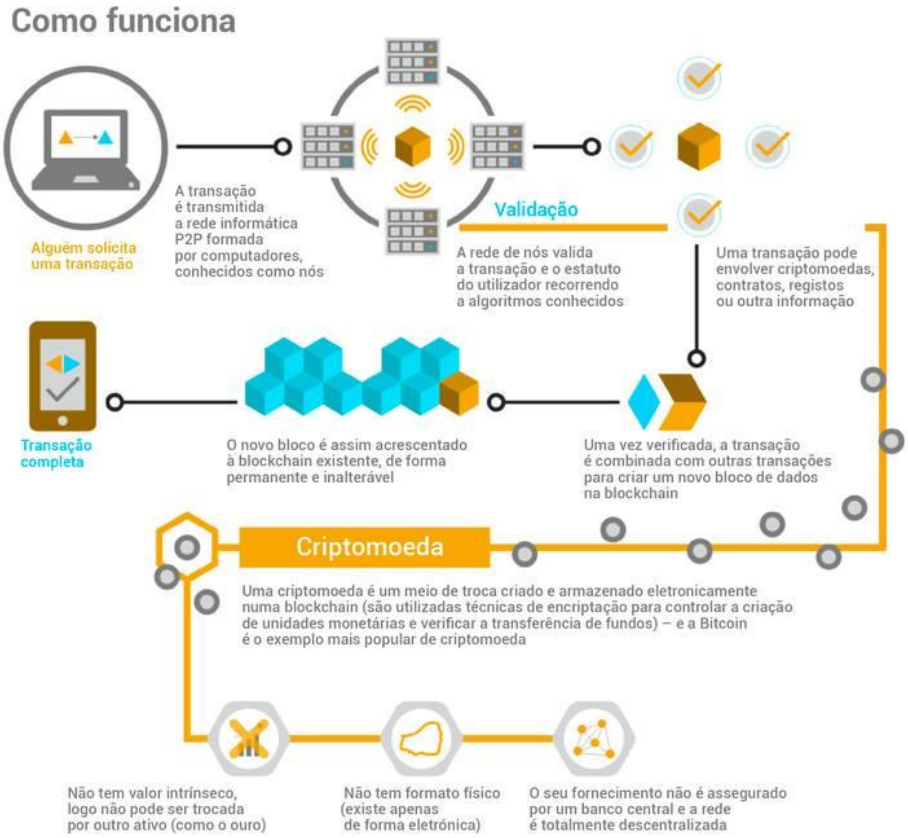
Com o passar do tempo, a dificuldade das resoluções do *proof-of-work* aumenta conforme o número de bitcoins emitidos, sendo esta dificuldade ajustada a cada 2016 blocos criados (aproximadamente duas (2) semanas). Em termos práticos, uma maior dificuldade nesse processo de mineração significa que é preciso cada vez maior potência na CPU para minerar um mesmo número de blocos, tornando a rede Bitcoin cada vez mais segura contra os ataques maliciosos.

Como dito anteriormente, a *blockchain* é a responsável por conter todas as informações relativas às transações já processadas - o histórico -, uma vez que controla constantemente os saldos de bitcoins que são inseridos no livro razão virtual (*ledger*) após os processos de mineração. O que isso permite é que qulquer pessoa que use o software possa registrar e visualizar as operações processadas pelo sistema, contribuindo com a resolução do problema do gasto duplo.

Em relação ao funcionamento da *blockchain,* o processo de validação da transação ocorre da seguinte forma: quando a ordem de transferência é feita, a transação é propagada para a rede de computadores e os mineradores incluem essa ordem nos próximos blocos que serão minerados. Os diversos computadores conectados à rede tentarão resolver esse problema matemático, o qual segue uma regra clara de protocolos requeridos pelo sistema. Esse é o chamado processo de mineração, que consiste no processo computacional de calcular um determinado *hash* e que decorre até que um dos computadores da rede tenha, de fato, resolvido a prova de trabalho. Uma vez resolvido, é criado um novo bloco contendo as informações das transações, e que é enviado aos demais participantes da rede para que se cheque a validade desse bloco por meio de um consenso algorítmico. Ao ser validado, o bloco é incluído em uma cadeia de blocos anteriores (por isso o nome *blockchain*) de maneira sequenciada, e a rede inteira é atualizada com essa nova. (Figura 2)

Cria-se, assim, um novo conjunto de informações referente às transações, e é praticamente impossível alterar qualquer tipo de registro nos blocos já criados, o que confere confiabilidade ao sistema e evita que um bitcoin seja gasto mais de uma vez por um mesmo usuário.

Figura 2 - Estrutura básica da *blockchain*



Fonte: https://www.livti.com.br/blog/blockchain-tecnologia-por-tras-da-revolucao-das-moedas-digitais/

Esse protocolo estabeleceu um conjunto de regras – na forma de cálculos distribuídos – que asseguram a integridade dos dados trocados entre bilhões de dispositivos que operam dentro da rede do blockchain, o fazendo sem a necessidade de intervenção ou participação de um terceiro de confiança.[10]

3.3 Criptografia na rede Bitcoin

A criptografia é um ramo do conhecimento estudado, principalmente, na matemática e na ciência da computação e consiste em analisar e aplicar técnicas para realizar a proteção de uma comunicação. Até o séc. XIX, o estudo da

_____
10 TAPSCOTT, DON e TAPSCOTT, ALEX. Blockchain Revolution: como a tecnologia por trás do Bitcoin está mudando o dinheiro, os negócios e o mundo. São Paulo: SENAI-SP Editora, 2016. p. 35.

criptografia consistia basicamente em analisar a aplicar técnicas de encriptação e decriptação, também chamadas de cifragem e decifragem: basicamente, escolhia-se um texto puro e se aplicava uma técnica de modo que a informação ali contida só pudesse ser lida por quem detivesse a chave ou método de decriptação.

Atualmente, com a onipresença da internet em nossa sociedade, a criptografia é utilizada em computação, redes financeiras, comunicações e diversos outros lugares e sistemas, bem como, é claro, nas criptomoedas. Na década de 1980, um tipo de criptografia muito importante foi desenvolvido e permitiu a criação do Bitcoin anos à frente: trata-se da criptografia assimétrica de chave pública e chave privada, a tecnologia básica por trás das *blockchains*.

A criptografia assimétrica é conhecida por esse nome uma vez que ela permite converter uma informação ‘A’ em informação ‘B’, porém não consigo reproduzir a operação inversa. Por exemplo, se eu sei minha chave privada da rede Bitcoin, eu consigo encontrar a minha chave pública, todavia o contrário não ocorre, ou seja, não consigo descobrir uma chave privada a partir de uma chave pública. Assim, essa característica traz segurança às transações na rede.

Como essa criptografia funciona na rede Bitcoin? A rede emite a todos os usuários uma chave privada e gera, por um método chamado *hashing*, uma chave pública vinculada. Esse *hashing* envolve o processamento de uma sequência de dados por um algoritmo, sendo praticamente impossível revertê-lo. Como as chaves estão vinculadas, a rede sabe que um determinado bitcoin pertence a você, permanecendo em sua propriedade enquanto você tiver a sua chave privada.

De uma forma simples, uma transação na rede possui os seguintes dados: entrada/*input*, é o endereço público de carteira dos quais os bitcoins estão saindo, a fim de compor o saldo total que o usuário deseja remeter a novo endereço público de carteira (i); valor, a quantidade de bitcoins que se deseja enviar por meio dessa transação (ii); e saída/*output*, que são as condições necessárias para gastar os fundos listados no *input* e, na maioria das transações, informa ainda o(s) endereço(s) que poderão gastar os bitcoins que estão sendo enviados (iii).

Logo, sendo o Bitcoin essencialmente uma rede descentralizada, para que as transações realizadas entre um dado número de partes sejam comunicadas aos demais usuários, a adoção de criptografia permite ao protocolo os seguintes atributos: autenticidade, privacidade e integridade. A transação será autêntica, uma

vez que é possível verificar matematicamente quais partes da rede estão se comunicando, ou seja, realizando uma transação de bitcoins entre si, sem que haja o risco de conflito de dados ou necessidade de um agente intermediário que atribua segurança e validade ao processo. A transação também será privada, pois a criptografia garante que, após a comunicação de transferência à rede, somente o destinatário detentor da chave privada poderá movimentar os fundos ali depositados. E, por fim, a transação tem sua integridade assegurada porque qualquer transferência é validada pelo conjunto de mineradores e nós que executam o algoritmo de consenso necessário para validação dela.[11]

3.4 Formas de aquisição de bitcoins

Em decorrência do seu caráter descentralizado e sua independência em relação a instituições financeiras, a criptomoeda não é emitida de forma semelhante às moedas fiduciárias, reguladas por Banco Centrais. A rede Bitcoin possui previsão de emissão de novos bitcoins como forma de incentivo à formação de consenso na rede, ou seja, os usuários que se dispõem a utilizar sua capacidade computacional a favor da rede, por meio da resolução dos problemas criptográficos de autenticação de transações, são recompensados com esses novos criptoativos quando os problemas são solucionados.

Ao passo que novos blocos são criados e adicionados à *blockchain*, os mineradores (usuários que solucionam os problemas matemáticos) são recompensados com os bitcoins criados. Todavia, a capacidade de mineração não é ilimitada. A fim de conter um eventual processo inflacionário decorrente do excesso de emissão, foi estabelecido o número máximo de 21 milhões de bitcoins passíveis de serem minerados.

Outrossim, conforme novos blocos são criados e bitcoins emitidos, a remuneração vai sendo reduzida progressivamente com o intuito de garantir a escassez digital da criptomoeda. Essa redução da remuneração ocorre a cada 210

_____

11 Disponível em https://blocktrends.com.br/criptografia-aplicada-a-seguranca-por-tras-do-bitcoin/ Acessado em 15/07/22.

mil blocos criados, o que acontece a cada quatro (4) anos, momento em que a remuneração é reduzida à metade, em um processo conhecido como "*halving*". [12]

Após 2140, ano em que provavelmente será minerado o último bloco da rede Bitcoin, para manter o incentivo dos mineradores, eles serão recompensados por taxas de transferência deduzidas da própria transação realizada. Desta forma, mantém-se um modelo que encoraje os mineradores a atuarem favoravelmente ao sistema, sempre buscando evitar um excesso de oferta da criptomoeda que gere um efeito inflacionário.

De acordo com Campos, o bitcoin pode facilmente se adaptar às necessidades do consumidor pós-moderno, porque pode ser quebrado em até oito decimais. Por não sofrer intervenção governamental e, também, por não estar baseada em um Estado específico, ou seja, a adesão a essa criptomoeda é voluntária, o bitcoin não estaria sujeito aos eventuais processos de desvalorização monetária por parte do Estado, como por exemplo, a inflação ocasionada por maior impressão de papel-moeda.[13]

Além de "conquistar" bitcoins por meio da mineração e das taxas de transferência, pode-se adquirir de duas outras formas: comprando em *exchanges* (instituições análogas a corretoras de valores, embora ainda não regulamentadas no Brasil) e recebendo diretamente por meio de outros usuários, a partir de transferências P2P (*peer-to-peer*) entre carteiras digitais (*crypto wallets*).

Ao abrir uma conta em uma exchange como, por exemplo, a Binance, maior exchange em *marketshare* atualmente, pode-se depositar moeda fiduciária como reais, dólares, euros, e adquirir bitcoins (BTC), ethereum (ETH) e diversas outras criptomoedas. Ainda, o que é bastante comum é utilizar algumas criptos como BTC, ETH para comprar outras criptos, uma vez que elas são utilizadas como unidade de conta também (diversas criptomoedas podem ser precificada em unidades de outras criptomoedas).

Quanto à custódia, as *exchanges* também provêm esse tipo de serviço, embora uma parte dos proprietários de criptoativos costume utilizar as *wallets* para

_____

12 Disponível em https://decrypt.co/resources/what-is-the-bitcoin-halving. Acessado em 17/08/2022.
13 CAMPOS, Gabriela Isa Rosendo Vieira. Bitcoin: consequências jurídicas do desenvolvimento da moeda virtual. Revista Brasileira de Direito, 11(2): 77-84, jul-dez. 2015. Disponível em: <https://seer.imed.edu.br/index.php/revistadedireito/article/view/769>. Acesso em: 09.10.22, p. 78.

custodiar seus próprios criptoativos com segurança, possibilitando também transacionar com outros usuários. Assim, após adquirir as criptomoedas, eles sacam da conta da exchange para a sua carteira virtual. A expressão "*not your keys, not your coins*" (se não são suas chaves, não são suas moedas) refere-se à necessidade de possuir as chaves privadas associadas aos seus fundos, por esta razão, os proprietários sempre são orientados a não deixar suas criptomoedas na corretora/*exchange*.

3.5 Características desafiadoras do uso de bitcoins

Por ser um sistema de pagamentos ainda muito recente e com seu uso ainda não massificado, o preço do bitcoin sofre alta volatilidade: somente no ano de 2022, o Bitcoin na paridade com o dólar americano (BTCUSD) já sofreu uma queda de 60% aproximadamente. Aqueles que adquirem a criptomoeda o fazem com fins especulativos ou como reserva de valor: no futuro, com o aumento da circulação e utilização do bitcoin no comércio, por exemplo, a tendência é uma redução gradual de sua volatilidade e crescimento estável de seus preços (por possuir uma natureza deflacionária).

Um outro desafio aos entusiastas das criptomoedas são as falhas de segurança, sejam elas por uso inapropriado de carteiras e contas pelos usuários, ou também pelas brechas de segurança nas redes e *blockchain* utilizadas. Algumas redes já sofreram *hacks* e foram furtadas, como a Poly Network, a qual teve 611 milhões de dólares transferidos de suas carteiras para as de um desconhecido, o maior crime desse tipo até hoje na história dos criptoativos.[14] Outra questão é o erro de uso das carteiras virtuais: elas podem ser deletadas e perdidas, ainda que não propositalmente, bem como pode haver transferência de criptomoedas para endereços errados (frequentemente uma ação conclusiva, sem a possibilidade de desfazimento da transferência) ou para redes não compatíveis (quando alguém transfere Bitcoin para uma rede que somente aceita outra criptomoeda). Enfim, todos esses erros podem culminar na perda total dos saldos em carteira ou conta, com alta probabilidade de irreversibilidade da situação, via de regra.

---

14 Disponível em <https://thehack.com.br/o-grande-assalto-de-criptomoedas-a-historia-do-roubo-de-us-611-milhoes-da-poly-network/>. Acesso em 25/07/22.

Por fim, a principal preocupação para reguladores diz respeito aos possíveis usos ilícitos das criptomoedas, principalmente quanto à lavagem de dinheiro e ao financiamento de crimes como tráfico de drogas e armas e terrorismo. Importante destacar que o bitcoin, como meio de pagamento, está sujeito aos mesmos desvios praticados com outras moedas fiduciárias no sistema financeiro tradicional, ou seja, o real, o dólar, qualquer moeda oficial de um país pode ser (e frequentemente é) usada para todos esse fins ilegais[15]. A rede Bitcoin, embora seja anônima, não é irrastreável, como se desenvolverá mais à frente neste trabalho, o que já começa a desqualificar o discurso de que as criptomoedas deveriam ser ilegais ou banidas pelos governos em razão da sua irrastreabilidade.

Ainda, como todas as transações na blockchain da rede Bitcoin são públicas e ficam registradas sem a possibilidade de alteração, não há um incentivo para que criminosos utilizem essa rede, pois há uma visibilidade considerável que os governos e instituições policiais podem explorar para identificar os atos ilegais e seus executores.

A evasão de divisas ou cambial é um possível fator para adquirir bitcoins, uma vez que a utilização da blockchain permite uma semi-anonimidade e baixo custo de transação para transferência de grandes somas, o que se apresenta como um atrativo para essas atividades ilegais. No Brasil, a evasão de divisas é regulada pela lei nº 7.492/86, a qual define os crimes contra o sistema financeiro nacional, e especifica em seu artigo 22:

> "Art. 22. Efetuar operação de câmbio não autorizada, com o fim de promover evasão de divisas do País:
> Pena - Reclusão, de 2 (dois) a 6 (seis) anos, e multa.
> Parágrafo único. Incorre na mesma pena quem, a qualquer título, promove, sem autorização legal, a saída de moeda ou divisa para o exterior, ou nele mantiver depósitos não declarados à repartição federal competente."[16]

Como o bitcoin é uma criptomoeda descentralizada e sem uma instituição responsável pela sua emissão, também existem problemas quanto à responsabilização no caso de violações a direitos do consumidor:

---

15 Uma investigação demonstrou um escândalo financeiro envolvendo grandes banco multinacionais (...). Disponível em https://einvestidor.estadao.com.br/mercado/escandalo-hsbc-bancos-globais. Acesso em 25.09.22.

16 BRASIL. Lei nº. 7.492, de 16 de junho de 1986. Define os crimes contra o sistema financeiro nacional. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L7492.htm. Acesso em: 09.10.2022.

> Há, ainda, problemas com o sistema financeiro das bitcoins no que tange a qualquer controle em relação à observância aos direitos do consumidor, já que não há órgão de defesa do consumidor ou sistema judiciário que traga eficácia às decisões, sendo esse espaço praticamente uma área cinza do Direito, pois não há autoridade central que gerencia o sistema, sendo bastante dificultoso achar um órgão apropriado, para reivindicar os direitos. Os Estados, por sua vez, devem buscar soluções para esse "não-lugar" (AUGÉ, 2000), observando os padrões estabelecidos pelo ordenamento jurídico, de forma a não prejudicar os direitos do consumidor, ferindo sua dignidade humana.[17]

Também existem questões normativas a serem enfrentadas, como, por exemplo, o enquadramento legal no Direito Penal. Outros países optaram pela proibição de uso e circulação do bitcoin, criminalizando a conduta dos usuários. As penas para a utilização do Bitcoin em transações variam desde multas, como na Islândia, até a prisão como na China e Rússia. Os países que impõem a proibição terminam por levar em consideração justamente o caráter monetário do Bitcoin. "A Rússia, por exemplo, reconhece no Bitcoin um "substituto monetário", utilizando-se da denominação para justificar sua proibição", como explica Fobe.[18]

---

17 CAMPOS, Gabriela Isa Rosendo Vieira. Bitcoin: consequências jurídicas do desenvolvimento da moeda virtual. Revista Brasileira de Direito, 11(2): 77-84, jul-dez. 2015. Disponível em: https://seer.imed.edu.br/index.php/revistadedireito/article/view/769. Acesso em 08.10.22, p. 04.

18 FOBE, Nicole Julie. O Bitcoin como moeda paralela – uma visão econômica e a multiplicidade de desdobramentos jurídicos. São Paulo: Escola de Direito de São Paulo da Fundação Getúlio Vargas, 2016. Disponível em: <http://bibliotecadigital.fgv.br/dspace/handle/10438/15986>. Acesso em 08.10.22, p. 72.

4 LEGISLAÇÃO BRASILEIRA E O ATUAL CENÁRIO JURÍDICO

4.1 Projetos de Lei 2.303/2015 e 2.060/2019 (Câmara dos Deputados)

O primeiro projeto de lei a tratar do assunto foi o PL nº 2.303/2015, de autoria do deputado Aureo Ribeiro (Solidariedade/RJ). O PL dispunha sobre a inclusão das moedas virtuais e programas de milhagem aéreas na definição de “arranjos de pagamento” sob a supervisão do Banco Central do Brasil (BCB). O relatório especial do Banco Central Europeu (BCE) de 2012, chamado de “Virtual Currency Schemes”[14], publicado em 2012 e atualizado em 2015, foi utilizado como base para a confecção do PL 2.303/2015 (conforme justificação do projeto). Por essa razão, foi utilizada a expressão “moedas virtuais”, bem como exemplificadas as moedas dos programas de milhagem das companhias aéreas.

Contudo, essas duas figuras, criptoativos e milhas aéreas, são muito diferentes e o projeto, além de não introduzir os conceitos básicos a serem utilizados, misturou ativos com propriedade de formação e negociação muito diversos. Por fim, um escopo mais reduzido e focado nos criptoativos seria necessário, o que veio no segundo projeto do mesmo deputado.

O segundo projeto de lei do deputado Aureo Ribeiro a tratar do assunto, o PL nº 2.060/2019, foi juntado ao primeiro (mantida a numeração do 2.303), e evoluiu em alguns conceitos. Em seu primeiro parágrafo, ele estatui que o PL dispõe sobre o regime jurídico de criptoativos, sendo que o artigo 1º vai além:

> "Art. 1º Esta lei dispõe sobre Criptoativos, que englobam ativos utilizados como meio de pagamento, reserva de valor, utilidade e valor mobiliário, e sobre o aumento de pena para o crime de “pirâmide financeira”, bem como para crimes relacionados ao uso fraudulento de Criptoativos.".

Neste primeiro artigo, o deputado cita quatro utilidades para criptoativos: meio de pagamento, reserva de valor, valor imobiliário e utilidade. Além disso, ele se preocupa com os tipos penais relativos aos usos fraudulentos das criptomoedas.

Diferentemente do PL 2.303/15, o primeiro, o projeto de lei 2.060/19 conceituou os criptoativos e os dividiu em três grupos no artigo 2º:

> "Art. 2º Para a finalidade desta lei e daquelas por ela modificadas, entende-se por criptoativos:
> I – **Unidades de valor** criptografadas mediante a combinação de chaves públicas e privadas de assinatura por meio digital, geradas por um sistema

> público ou privado e descentralizado de registro, digitalmente transferíveis e que não sejam ou representem moeda de curso legal no Brasil ou em qualquer outro país;
> II – **Unidades virtuais representativas de bens, serviços ou direitos**, criptografados mediante a combinação de chaves públicas e privadas de assinatura por meio digital, registrados em sistema público ou privado e descentralizado de registro, digitalmente transferíveis, que não seja ou representem moeda de curso legal no Brasil ou em qualquer outro país;
> III – **Tokens Virtuais** que conferem ao seu titular acesso ao sistema de registro que originou o respectivo **token de utilidade** no âmbito de uma determinada plataforma, projeto ou serviço para a criação de novos registros em referido sistema e que não se enquadram no conceito de valor mobiliário disposto no art. 2° da Lei no 6.385, de 7 de dezembro de 1976;
> Parágrafo único. Considera-se intermediador de Criptoativos a pessoa jurídica
> prestadora de serviços de intermediação, negociação, pós- negociação e custódia de Criptoativos. (grifou-se).".

Dado o conteúdo do PL nº 2.060/2019, é possível observar que o deputado Aureo buscou trazer termos mais atualizados e conceitos melhor definidos em relação ao PL 2.303/2015. Ainda, os programas de milhagem aérea foram retirados do escopo do projeto e a definição de tipos penais se manteve presente.

O terceiro e o quarto artigo do projeto tratam das operações com criptoativos. Neles, reconhece-se a circulação e a emissão de criptoativos, que poderá ser realizada inclusive por pessoas jurídicas de direito público ou privado estabelecidas no Brasil. Destaca-se que o projeto não restringe a emissão dos criptoativos a entidades brasileiras, mas declaradamente estipula tal possibilidade. Ou seja, o PL busca conferir expresso status legal aos investimentos em criptoativos.

Todavia, o PL nº 2.060/2019 ainda carece de uma melhor pontuação sobre a competência regulatória e fiscalizatória, pois o único Órgão ou entidade governamental citada no textos é a Comissão de Valores Mobiliários (CVM). Ainda que cite a CVM, é importante ressaltar que o PL não esclarece suas competências relacionadas à matéria dos criptoativos. Ainda assim, o projeto avançou consideravelmente nas definições necessárias para melhor entendimento da temática e segurança jurídica do setor.

De acordo com o texto, serão consideradas prestadoras de serviços de ativos virtuais as pessoas jurídicas que executam serviços como troca, em nome de terceiros, de moedas virtuais por moeda nacional ou estrangeira; troca entre um ou mais ativos virtuais; transferências deles; custódia ou administração, mesmo que de instrumentos de controle; e participação em serviços financeiros e prestação de

serviços relacionados à oferta por um emissor ou venda de ativos virtuais.

O projeto considera ativo virtual “a representação digital de valor que pode ser negociada ou transferida por meios eletrônicos e utilizada para realização de pagamentos ou com propósito de investimento”.

Ficam de fora as moedas tradicionais (nacionais ou estrangeiras), as moedas estrangeiras (recursos em reais mantidos em meio eletrônico que permitem ao usuário realizar pagamentos por cartões ou telefone celular), pontos e recompensas de programas de fidelidade, e valores mobiliários e ativos financeiros sob regulamentação já existente.

O PL cria uma órgão fiscalizador, a ser apontado pelo Poder Executivo, que será responsável por autorizar e controlar o funcionamento das corretoras de criptoativos. Além disso, caso aprovado, o texto acrescenta, no Código Penal, um novo tipo penal de estelionato, atribuindo reclusão de 4 a 8 anos e multa para quem "organizar, gerir, ofertar ou distribuir carteiras ou intermediar operações envolvendo ativos virtuais, valores mobiliários ou quaisquer ativos financeiros com o fim de obter vantagem ilícita em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil ou qualquer outro meio fraudulento".

O texto também estabelece os critérios para enquadramento de empresas na categoria de corretoras de criptoativos (ou "exchanges") e lista uma série de deveres e condições que esse tipo de empresas será obrigada a cumprir. Empresas ligadas a este mercado também deverão compartilhar um número maior de informações com órgãos do governo e terão seis meses para se adequar às novas regras.

O PL2303/15 também cria diretrizes para o mercado cripto, que deverá ser baseado em boas práticas de governança e abordagem baseada em riscos; segurança da informação e proteção de dados pessoais; proteção e defesa de consumidores e usuários; e prevenção à lavagem de dinheiro, ao financiamento do terrorismo e ao financiamento da proliferação de armas de destruição em massa, em alinhamento com os padrões internacionais.

4.2 Projeto de Lei 3.825/2019 (Senado Federal) – substituído pelo PL 4.401/2021

O PL nº 3.825/2019, de autoria do senador Flávio Arns (Rede-PR), foi à votação no dia 26 de abril de 2022 e foi aprovado o substitutivo apresentado pelo relator, senador Irajá (PSD/TO). Assim, o substitutivo PL 4.401/2021[19] voltou à Câmara dos Deputados para análise, uma vez que ele incorporou ideias de outros projetos sobre o mesmo tema, como o PL 3.825/2019, do sen. Flávio Arns, o PL 3.949/2019, do sen. Styvenson Valetim (Podemos/RN) e o PL 4.207/2020, da sen. Soraya Thronicke (União/MS). O texto original permanece sendo do PL 4.401/2021, o qual é de iniciativa do dep. Federal Aureo Ribeiro.

Os senadores observaram em discussão que o mercado de criptoativos, no Brasil, em 2021, movimentou aproximadamente R$215 bilhões e, especificamente o mercado como método de pagamento, teve crescimento de 6% nesse mesmo ano. O crescimento acelerado desse mercado tem gerado preocupação mundialmente, principalmente quanto ao seu possível uso para lavagem de dinheiro diante da insuficiência de regulamentação.

O PL 3.825/2019, agora 4.401/21, dispõe sobre diretrizes a serem observadas na prestação de serviços de ativos virtuais e na regulamentação das prestadoras de serviços de ativos virtuais, não se aplicando o disposto no PL aos ativos representativos de valores mobiliários sujeitos ao regime da Lei nº 6.385/76, bem como não alterando competências da CVM.

Para os efeitos dessa lei, considera-se ativo virtual a representação digital de valor que pode ser negociada ou transferida por meios eletrônicos e utilizada para realização de pagamentos ou com propósito de investimento. Todavia, não estão incluídos nesse elenco, as moedas nacionais e estrangeiras (ex: real, dólar, euro); a moeda eletrônica nos termos da lei nº 12.865/2013, art. 6, VI (“VI - moeda eletrônica - recursos armazenados em dispositivo ou sistema eletrônico que permitem ao usuário final efetuar transação de pagamento.”; instrumentos que provejam ao seu titular acesso a produtos ou serviços especificados ou a benefício proveniente desses produtos ou serviços; e representações de ativos cuja emissão,

---

19 Disponível em <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=1555470>. Acesso em 09.10.22.

escrituração, negociação ou liquidação esteja prevista em lei ou regulamento.

Uma das críticas que o setor de criptomoedas brasileiro está fazendo ao projeto é o fato de o Legislativo ter deixado a ser definido posteriormente por ato do Executivo a escolha de com qual Órgão ou entidade da Administração Pública Federal ficará a responsabilidade de estabelecer quais ativos financeiros serão regulados. Ainda, quais as diretrizes e parâmetros terão que ser obedecidos pelas prestadoras de serviços virtuais.

Ainda assim, o PL do senador Arns é bem detalhado, principalmente no que se refere ao funcionamento das instituições intermediadoras de compra e venda de criptoativos (as *exchanges*). Outrossim, o projeto estabelece a competência do Banco Central brasileiro para autorizar o funcionamento e fiscalizar estas *exchanges*. Quanto à preocupação com os ilícitos penais relacionados aos criptoativos, é demonstrada na submissão do setor às medidas de prevenção e combate à lavagem de dinheiro previstas na Lei nº 9.613/1998, bem como na criação de um tipo penal direcionado às exchanges, quanto à prática de crimes de pirâmide financeira.

4.3 Análise sobre a regulamentação legislativa brasileira

Como mencionado, por ser uma temática bastante técnica, recente (apenas 13 anos se passaram da primeira transferência utilizando a rede Bitcoin) e, principalmente, disruptiva dos sistemas tradicionais de nossa sociedade, os projetos de lei ainda em votação (não sabemos necessariamente se e quando serão aprovados, bem como se o conteúdo permanecerá esse aprovado no Senado) buscam trazer uma base jurídica para melhor desenvolver o mercado e a indústria criptofinanceira. Entretanto, mais do que regularizar um mercado em ascensão, os PLs focam em garantir os direitos dos investidores e tratar dos controles internos das instituições financeiras intermediadoras, a fim de evitar fraudes e crimes contra o sistema financeiro, tributário e contra os próprios investidores.

De fato, os deputados e senadores não indicaram diretamente os Órgãos e entidades administrativas que farão a fiscalização e regularização do mercado de criptoativos, embora alguns detalhes como autorização para funcionamento das exchanges e lançamento de valores mobiliários criptos já tenham o BCB e a CVM, respectivamente, como responsáveis nos projetos de lei.

Provavelmente, com o avanço das instituições financeiras de criptoativos, com a modernização dos instrumentos financeiros como derivativos, contratos futuros, ETFs, fundos de criptomoedas, etc, e com a popularização do uso dos criptoativos, veremos a legislação se expandir e, especialmente, uma atuação maior do Executivo com atos normativos mais dinâmicos e que possam se adequar à realidade diariamente construída, sempre imbuído de um espírito empreendedor, de inovação, com fundamento nos valores sociais e da livre iniciativa, como prega a Constituição Federal, em seu art. 1º, inciso IV.

De fato, uma grande preocupação do legislador é e será regularizar o mercado de criptoativos para trazer segurança aos trabalhadores do setor, empresas, investidores e o fisco, contudo sempre sopesando e ponderando os alcances das legislações para não asfixiar este mercado tão inovador e que trará benefícios a todos os setores da economia, uma vez que sua principal tecnologia, a *blockchain*, possui um leque de aplicações que extrapolam demasiadamente o mercado cripto.

4.4 A dificuldade de enquadramento jurídico dos criptoativos

Como o regime jurídico dos criptoativos não foi adequadamento definido, visto que os projetos de lei ainda estão em tramitação e não há garantia de aprovação, o que existe atualmente são opiniões doutrinárias (ainda que não coesas) e posicionamentos de alguns órgãos regulatórios, os quais foram obrigados a apresentar alguns entendimentos técnicos, dada a inexistência de regulação legislativa formal.

A partir da doutrina, diversas naturezas jurídicas são apresentadas ao direito brasileiro, tratando as criptomoedas como mercadorias ou commodities, títulos, valores imobiliários, ativos financeiros[20], moeda estrangeira/mercadoria, moeda natural[21]. Ainda, há um estudo (dissertação de Mestrado de Nicole Julie Fobe) que aponta a existência de, pelo menos, 13 classificações jurídicas em 29 países que já se manifestaram sobre o tem, o que cristaliza a dificuldade de enquadramento jurídico único dos criptoativos também nos outros países.

---

20 SILVA, Luiz Gustavo Doles. Bitcoins & outras criptomoedas – Teoria e prática à luz da legislação brasileira. Curitiba: Juruá, 2018. p. 51 a 66.

21 ULRICH, Fernando. São Paulo: Instituto Ludwig von Mises Brasil, 2015. P. 96-98.

Em relação às autoridades brasileiras, a Receita Federal do Brasil, em seu Perguntas e Respostas da Declaração de Imposto de Renda Pessoa Física 2022[22], equiparou os investimentos em criptomoedas (ou moedas virtuais) como “ativos financeiros. Respondendo à questão 455 (Como os criptoativos devem ser declarados?), a RFB esclarece: (Figura 3)

Figura 3 – Reposta à pergunta 455

CRIPTOATIVOS - COMO DECLARAR

455 — Como os criptoativos devem ser declarados?

Os criptoativos não são considerados moeda de curso legal nos termos do marco regulatório atual. Entretanto, podem ser equiparados a ativos sujeitos a ganho de capital e devem ser declarados pelo **valor de aquisição** na Ficha Bens e Direitos (Grupo 08 – Criptoativos), considerando os códigos específicos a seguir (01, 02, 03, 10 e 99), quando o valor de aquisição **de cada tipo de criptoativo** for igual ou superior a R$ 5.000,00 (cinco mil reais):

Código do bem	Descrição	Conteúdo do campo “Discriminação”
01	Criptomoeda Bitcoin - BTC	Quantidade e onde está custodiada (nome da empresa com CNPJ ou custódia própria).
02	Outras criptomoedas, conhecidas como altcoins.	Tipo, quantidade e onde está custodiada (nome da empresa com CNPJ ou custódia própria). Tipos de criptoativos diferentes devem constituir itens separados na declaração. Por exemplo, Ether (ETH), Binance Coin (BNB), XRP (Ripple), Bitcoin Cash (BCH), Litecoin (LTC), Cardano (ADA), Solana (SOL), Dogecoin (DOGE), entre outros.
03	Stablecoins	Tipo, quantidade e onde está custodiada (nome da empresa com CNPJ ou custódia própria). Exemplos: Tether (USDT), Brazilian Digital Token (BRZ), USDC, Binance dólar (BUSD), TrueUSD (TUSD), DAI, Paxos Gold (PAXG), Gemini dólar (GUSD), entre outros.
10	NFTs (Non-Fungible Tokens)	Tipo, quantidade e onde está custodiado (nome da empresa com CNPJ ou custódia própria). Exemplos: Tokens representativos de direitos sobre bens digitais ou físicos, como colecionáveis, obras de arte e imóveis.
99	Outros criptoativos não incluídos nos códigos 1, 2, 3 ou 10.	Tipo, quantidade e onde está custodiado (nome da empresa com CNPJ ou custódia própria). Exemplos: Fan Tokens, Tokens de Precatório, Tokens de Consórcio, Tokens de Crédito de carbono, recebíveis, entre outros.

Fonte: https://www.gov.br/receitafederal/pt-br/centrais-de-conteudo/publicacoes/perguntas-e-respostas/dirpf/pr-irpf-2022.pdf/view.

---

22 Disponível em https://www.gov.br/receitafederal/pt-br/centrais-de-conteudo/publicacoes/perguntas-e-respostas/dirpf/pr-irpf-2022.pdf/view. Acesso em: 08.09.2022.

Além da obrigação de declarar, a RFB esclareceu que as alienações de criptomoedas se submetem à tributação do imposto de renda sobre os eventuais ganhos de capital, tal como ocorre com as alienações de ativos financeiros. Essa resposta é fundamentada no art. 118 do Código Tributário Nacional (lei nº 5.172/66), o qual determina que “a definição legal do fato gerador é interpretada abstraindo-se: [I] da validade jurídica dos atos efetivamente praticados pelos contribuintes, responsáveis, ou terceiros, bem como da natureza do seu objeto ou dos seus efeitos; [II] dos efeitos dos fatos efetivamente ocorridos.”

No Ofício Circular 1/2018/CVM/SIN, a CVM também se posicionou quanto a operações com criptomoedas (especificamente quanto à possibilidade de investimento em criptos pelos fundos de investimento regulados pela Instrução CVM nº 555/14), manifestando entendimento oposto de que os criptoativos não são ativos financeiros:

> "Como sabido, tanto no Brasil quanto em outras jurisdições ainda tem se discutido a natureza jurídica e econômica dessas modalidades de investimento, sem que se tenha, em especial no mercado e regulação domésticos, se chegado a uma conclusão sobre tal conceituação.
> Assim e baseado em dita indefinição, 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."

No mesmo ofício, a CVM ressalta que futura legislação “poderia restringir, impedir ou até mesmo criminalizar a negociação de criptoativos” e, por esta razão, era prudente aos gestores de fundos de investimento aguardarem manifestações posteriores da própria CVM, bem como as aprovações de legislações futuras em discussão nas Casas Legislativas federais.

Ainda, o BCB, por meio do Comunicado nº 31.379 de 2017[23], alertou sobre os riscos decorrentes de operações de guarda e negociação das denominadas moedas virtuais. Embora não tenha expressado o seu entendimento sobre a natureza jurídica desses bens, o BACEN frisou que as criptomoedas “não são emitidas nem garantidas por qualquer autoridade monetária, por isso não têm garantia de conversão para moedas soberanas, e tampouco são lastreadas em ativo real de qualquer espécie, ficando todo o risco com os detentores”.

---

23 Disponível em https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Comunicado&numero=31379.. Acesso em: 15.08.22.

Quanto à regulação das exchanges, o BCB esclareceu, no ponto 4, que a atividade de compra e venda desses bens está fora de seu controle:

> "4. As empresas que negociam ou guardam as chamadas moedas virtuais em nome dos usuários, pessoas naturais ou jurídicas, não são reguladas, autorizadas ou supervisionadas pelo Banco Central do Brasil. Não há, no arcabouço legal e regulatório relacionado com o Sistema Financeiro Nacional, dispositivo específico sobre moedas virtuais. O Banco Central do Brasil, particularmente, não regula nem supervisiona operações com moedas virtuais."

Percebe-se que as manifestações dos órgãos oficiais, no que tange o enquadramento jurídico das criptomoedas, são apenas provisórias e não há uma posição unificada estatal. A própria Receita Federal, a qual orientou os contribuintes a classificar os criptoativos como ativos financeiros, fez uma equiparação expressa e, ao tratar da incidência de IRPF sobre os ganhos de capital auferidos com a alienação de criptomoedas, fundamentou a sua posição em artigo do Código Tributário que, entre outras coisas, determina que a incidência tributária prescinde da validade dos negócios jurídicos e da natureza de seus objetos. Entretanto, a própria natureza dos objetos em questão (criptoativos) não é consenso na discussão legislativa e não consta em nenhum ordenamento legislativo vigente.

É possível concluir que, devido à grande incerteza sobre a natureza jurídica das criptomoedas, à falta de coesão dos pronunciamentos oficiais sobre o tema, bem como à ausência de legislação que positive o tema no quadro normativo infraconstitucional atual, ainda não deveria haver qualquer tributação nas operações de compra e venda de criptomoedas, dada a insegurança jurídica que ainda permeia essa temática.

5 AS TRANSFERÊNCIAS P2P (*PEER-TO-PEER* / PONTO-A-PONTO) ENTRE CARTEIRAS DIGITAIS

5.1 Conceito e funcionamento

A tecnologia P2P (*peer-to-peer*, ponto-a-ponto, par-a-par) precede a invenção dos criptoativos. No contexto tecnológico, o P2P é basicamente uma rede de computadores que compartilham arquivos por meio da internet sem a necessidade de um servidor central (um computador para armazenar dados). Assim, os usuários fazem download (“baixam”, recebem) e upload de arquivos (transferem, enviam) e os disponibilizam para outros usuários, e assim por diante. Desta forma, cada computador funciona como um servidor, o qual disponibiliza o arquivo a ser baixado e, ao mesmo tempo, é cliente, pois consome o arquivo também. Atualmente, tecnologias como torrents funcionam exatamente dessa forma.

Existiram duas grandes motivações para o desenvolvimento de aplicações P2P: o desejo por mais privacidade e anonimato na internet e o uso da capacidade ociosa de processamento e armazenamento dos computadores conectados à internet. Quanto a esta última, o modelo cliente-servidor necessita de nós centrais com um grande poder de processamento, devido a sempre crescente demanda por novos sistemas e aplicações. Assim, as aplicações que rodam em redes P2P podem fazer uso destes recursos ociosos para suportar um grande número de usuários acessando um mesmo sistema, sem a necessidade de nós centrais de processamento (servidores centrais). Como exemplo bem interessante desta sistemática, existe a possibilidade de se doar poder computacional para pesquisas, via redes P2P, a partir de sites como o “*World Community Grid*”[24]: ele permite que qualquer pessoa com um computador, smartphone ou tablet doe seu poder de computação não utilizado para avançar em pesquisas científicas de ponta, em tópicos relacionados à saúde, pobreza, sustentabilidade, entre outros temas. É como se fosse uma comunhão de esforços, via hardware e software, para executar algo que demandaria de diversos computadores ou supercomputadores, mas que pode ser executado com um pedacinho de cada computador participante.

Dito isso, a principal razão pela qual foram criadas as redes P2P foi a busca

---

24 Disponível em < https://www.worldcommunitygrid.org/ >. Acesso em: 25.08.22.

por mais privacidade e anonimato na internet. É importante lembrar que as discussões sobre criptografia, sistemas independentes de pagamento e desenvolvimento de moedas que pudessem unificar a economia virtual, iniciaram com matemáticos e cientistas de computação que, já na década de 1980, não concordavam com a falta de regulação dos mercados financeiros, com o descontrole monetário dos governos soberanos, com a leniência com a inflação e perda do poder de compra dos cidadãos, bem como com o excesso de informação pessoal que circulava entre as empresas e setores do governo, os quais não tratavam esses dados pessoais com o devido cuidado, sigilo e segurança necessários.

A *blockchain* do Bitcoin é basicamente um protocolo P2P, uma vez que a rede não possui um servidor central: cada computador que roda o software é um nó (ou *node*) desta rede, funcionando como um servidor próprio. Assim, as criptomoedas, como o bitcoin, podem ser negociadas e transferidas de maneira independente de qualquer entidade ou órgão central. Por essa razão, as criptomoedas fazem parte de um sistema denominado de finanças descentralizadas, visto que a partir da tecnologia *blockchain*, foi possível descentralizar diversos serviços financeiros, sendo o principal deles o envio de dinheiro de um lado para outro, sem precisar de um órgão intermediário (ou mais de 1) para fazer a transferência.

Todavia, dentro do universo dos criptoativos, o P2P se apresenta como um outro conceito um pouco diferente da tecnologia em si: utiliza-se esse termo para se referir a transações que ocorrem com criptomoedas diretamente de um usuário para o outro. São os *trades* (negociações) que são realizados fora das plataformas das exchanges, nos quais o comprador negocia preço e quantidade diretamente com o vendedor e não há intermediação da transação pela empresa. Este modelo já estava, inclusive, previsto no white paper do Bitcoin de Satoshi Nakamoto, documento base da rede que explica seu funcionamento e conceito. Para fazer transferência de bitcoins ou outras criptomoedas, é possível fazer via *crypto wallets* ou via contas em *exchanges*.

No primeiro caso, basta um usuário baixar uma carteira digital, a qual gerará uma chave pública – endereço que identifica essa carteira – e uma chave privada – chave que criptografa a transação. Após, basta que ele digite a chave pública da carteira para a qual deseja transferir os valores e inserir sua chave privada. Assim,

em poucos minutos (ou segundos, dependendo de qual rede se utiliza) e por um baixo custo, esses valores são transferidos de A para B. Note que essa transação, embora validada e registrada publicamente na *blockchain* por mineradores, não passa por nenhuma empresa intermediadora, no que se poderia chamar de “P2P puro”.

No caso das transferências de criptomoedas via conta em uma *exchange*, a forma de transferência poderia ser entendida como um P2P híbrido (em verdade, de característica *peer-to-peer* apenas a *blockchain* utilizada), pois o que ocorre é que as exchanges disponibilizam ferramentas para salvaguardar as negociações. Como funciona? As partes negociam seus preços, o vendedor transfere as criptomoedas para a conta da exchange que as reterá por um período X (minutos ou horas) até que haja confirmação de recebimento de pagamento. Após essa confirmação, as criptomoedas são enviadas para a conta do comprador, finalizando a negociação, ou são devolvidas ao vendedor caso o comprador não efetue o pagamento na janela de tempo delimitada. Esse tipo de serviço é oferecido pela maioria das grandes exchanges (Binance, FTX, Coinbase, Kucoin, entre outras) como uma forma de mitigar os riscos de fraude nos trades P2P puros, em transferências diretas.

5.2 Problema jurídico – possibilidades de tributação sobre operações P2P

O que se pode perceber é que o Bitcoin e as outras criptomoedas estão sendo introjetados nos diferentes sistemas jurídicos dos países, majoritariamente, pela via tributária. Permanece um debate entre os Órgãos técnicos que flutua entre a necessidade de regular o sistema para desenvolvimento da economia que o rodeia e a possibilidade de tornar ilegal algumas transações, como as P2P que não possuem registro em exchanges ou outras instituições financeiras, apenas na *blockchain*, com a alegação de que não há como controlá-las e, portanto, há uma inclinação para as práticas de crimes com esse tipo de *trade*.

Como vimos, a normatização jurídica brasileira – lei *stricto sensu* – permanece tímida, quanto ao Bitcoin e às outras criptomoedas, existem apenas orientações, comunicados e instruções normativas emitidas pelo BACEN, RFB e CVM. No Comunicado 25.306/2014, o Banco Central alerta sobre os riscos inerentes às criptomoedas, especialmente quanto a sua utilização e à volatilidade dos preços,

esta última derivada “do baixo volume de transações, baixa aceitação como meio de troca e da falta de percepção clara sob sua fidedignidade”.

Esse comunicado é de 2014, portanto 8 anos já se passaram e o mercado de criptoativos avançou a passos largos[25], inclusive com apoio recente instituicional, ou seja, antes um mercado movimentado apenas por pessoas físicas, após o início da pandemia do COVID-19, houve a criação de instrumentos financeiros mais modernos que permitiram a entrada de enorme fluxo institucional[26], bem como foram aceleradas as conversas sobre a regulação do setor. Todavia, o BACEN não propõe a regulamentação do mercado, reservando-se a adotar medidas no âmbito de sua competência. Em agosto de 2019, o BACEN passou a reconhecer as criptomoedas como bens (“ativos não financeiros produzidos”) – e indiretamente como meio de pagamento – e qualificar a atividade de mineração de criptomoedas como “processo produtivo”, seguindo as recomendações de um texto do FMI (Fundo Monetário Internacional) chamado *Treatment of Crypto Assets in Macroeconomics Statistics*[27].

A Comissão de Valores Mobiliários, por sua vez, emitiu nota em outubro de 2017 relativamente às ICOs (*Initial Coin Offerings*, veículos parecidos com os IPOs), conceituando-as como “(...) captações públicas de recursos, tendo como contrapartida a emissão de ativos virtuais, também conhecidos como ‘tokens’ ou ‘ coins ’ junto ao público investidor”. De acordo com a CVM, os ICOs, “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 6.835/76”, impondo ao seu ofertante obediência à regulamentação específica do registro da oferta pública na CVM, sob pena das sanções aplicáveis. Entretanto, em 12 de janeiro de 2018, o Órgão emitiu Ofício Circular 1/2018/CVM/SIN pelo qual deixa claro que moedas digitais “não podem ser qualificadas como ativos financeiros” e, por essa razão, sua aquisição direta pelos fundos de investimento regulados na instrução CVM 555/14 não é permitida.

_____

25 Disponível em < https://livecoins.com.br/o-bitcoin-superou-o-mercado-de-acoes-por-8-anos-na-ultima-decada/ > e < https://cointelegraph.com.br/news/417-growth-boosts-cryptocurrencies-and-accelerates-creation-of-real-digital-and-regulation-in-brazil >. Acesso em: 10.09.22.

26 Disponível em < https://www.infomoney.com.br/colunistas/blog-do-cunha/derivativos-de-cripto-um-mercado-muito-maior-do-que-o-de-criptoativos/ >. Acesso em: 01.09.22.

27 Disponível em < https://www.imf.org/external/pubs/ft/bop/2019/pdf/Clarification0422.pdf >. Acesso em 18.09.22.

A Secretaria da Receita Federal do Brasil, dentro de suas competências, estabeleceu a obrigatoriedade da declaração no Imposto de Renda, para pessoas físicas e jurídicas (investidores e *exchanges*/corretoras de criptomoedas), dos criptoativos e das moedas virtuais, ao editar a Instrução Normativas 1.888 de 03 de maio de 2019. Esta IN gerou obrigações acessórias para exchanges de criptoativos, as quais são obrigadas a relatar quaisquer movimentações que ocorram em suas plataformas.

Como já mencionado, a RFB incluiu em seu Manual de Perguntas e Respostas sobre a Declaração de IRPF, pergunta 445, a informação de que “os criptoativos não são considerados moeda de curso legal nos termos do marco regulatório atual, entretanto podem ser equiparados a ativos sujeitos a ganho de capital e devem ser declarados pelo valor de aquisição (...)”. Também refere que não há cotação oficial para esses ativos e as operações devem ser comprovadas com documentação legítima.

Quanto a decisões de Tribunais Superiores que possam evidenciar algum caminho alternativo, a 3ª Turma do Superior Tribunal de Justiça, ao julgar mérito do Recurso Especial 1.696.214/SP (2017/0224433-4), em 09 de outubro de 2018, proferiu decisão colegiada (transitada em julgado em 09.11.2018), por maioria de votos, vencida a Ministra Nancy Andrighi, reconhecendo a legalidade do ato de fechamento unilateral de conta corrente de criptomoedas de titularidade da empresa Mercado Bitcoin Serviços Digitais Ltda, corretora de moedas digitais Bitcoin, Bitcoin Cash e Litcoin, pela instituição financeira Itaú Unibanco S.A.

Nesse processo, foi analisada a autonomia de contratação em serviços bancários no caso de moedas digitais, afastando a aplicação do Código de Defesa do Consumidor (CDC), uma vez que os bancos são partes interessadas no setor financeiro, onde atuam as *exchanges*, e são detentores de um serviço fundamental à prática comercial de qualquer agente econômico. Todavia, ainda que o STJ tenha analisado sob o viés contratual, sem dúvidas, há uma relação com o próprio funcionamento das *exchanges*, pois sem uma atividade bancária legítima não há como operar no mercado financeiro brasileiro.

Um dos argumentos utilizados pelo banco para o fechamento unilateral da referida conta-corrente foi o de “que as instituições financeiras não sabem se aquele fluxo de dinheiro provocado pelas contas das corretoras de criptomoedas é lícito ou

não". É importante destacar que tal argumento da instituição financeira foi utilizado como fundamento de tal decisão judicial colegiada.[28]

Assim, pode-se constatar que a regulamentação sobre criptomoedas e criptoativos vem sofrendo modificações frequentemente, porém apenas no escopo da instrumentalização tributária e na delimitação de alguns conceitos base relativos a criptoativos e moedas virtuais. Quanto à jurisprudência superior, o próprio Superior Tribunal de Justiça reconhece a inexistência de legislação brasileira que regulamente de forma específica as criptomoedas.

Diante da ausência de legislação, a incidência de tributação sobre as operações com criptoativos dependerá necessariamente da relação jurídica entre as partes envolvidas, o que evidencia que não há apenas um tributo apto a incidir sobre a relação jurídica material tributária.

Quando a operação for uma alienação de criptomoedas (venda e compra de "moedas virtuais" por moeda corrente de curso legal) pertencente à pessoa física ou jurídica e, ocorrendo acréscimo patrimonial, entende-se que deve ser pago o imposto de renda sobre o ganho de capital[29]. Caso a operação de venda gere lucro, deve-se pagar o imposto como ocorre com todo bem e qualquer outra moeda, sem ressalvas aqui por se tratar de moeda digital. Contudo, caso se adquire bitcoins ou outras criptomoedas com moeda de curso forçado (real-R$), o resultado da operação é um novo bem (moeda virtual), ao qual a RFB qualifica como "ativo financeiro" e ele deve ser declarado na ficha "Bens e Direitos" e registrado pelo valor de aquisição (conforme art. 5º da IN SRF 84/2001).

Situação diferente ocorre quando há a aquisição de mercadorias ou serviços utilizando-se bitcoin. O contribuinte possui a criptomoeda, devidamente declarada por um dado valor, e a utiliza como meio de pagamento para compra de outros bens ou serviços ou, especulativamente, troca-a por outra criptomoeda. Nesse caso, entende-se que a relação jurídica tributária se caracteriza por meio de uma permuta (contrato de permuta), uma vez que o bitcoin não pode ser considerado moeda

---

28 STEFFENS, Luana; TESSARI, Cláudio. A tributação das operações com criptomoedas no Brasil: o caso da Bitcoin. Revista de Direito Tributário Contemporâneo/ vol. 30/2021. P. 269-296. Acesso em: 10.09.22.

29 Instrução Normativa 118, de 28/12/2000, da SRF: Art. 2º Na hipótese de bens e direitos adquiridos e aplicações financeiras realizada em moeda estrangeira com rendimentos auferidos originariamente em reais, o ganho de capital corresponderá à diferença positiva, em reais, entre o valor de alienação, liquidação ou resgate e o custo de aquisição do bem ou direito ou o valor original da aplicação financeira.

corrente nacional, assim não possui curso legal forçado e não é emitido por um Estado soberano. Caso haja ganho de capital, deverá ser tributado pelo IR o ganho de capital, nos termos do art. 128, § 4º, II do Regulamento do IR (Decreto 9.580/18).

A aplicação da disposição legal parece clara sempre que houver a troca de bitcoin por bens e serviços, assim como a utilização da moeda virtual como meio de pagamento. Havendo diferença entre o valor de aquisição declarado e o bem adquirido é impositivo o recolhimento do IR sobre ganho de capital, lembrando que, nos termos do art. 22, II, da lei 9.250/95, o ganho de capital advindo de alienações e investimentos em criptomoedas, realizadas a cada mês, que não ultrapasse R$ 35.000,00 (trinta e cinco mil reais), é isento do imposto de renda.

Da mesma forma, a operação anterior (aquisição de bens ou serviços utilizando-se bitcoin como meio de pagamento) poderá dar ensejo à tributação pelo ICMS, no caso de aquisição de mercadoria (obrigação de dar) ou, então, pelo ISS, no caso de pagamento pela realização de um serviço (obrigação de fazer). Ainda, se houver a utilização da criptomoeda para a aquisição de um imóvel poderá haver a incidência do ITBI de competência municipal.

Quanto às operações com as exchanges, as empresas podem (i) não comprar e vender criptomoedas, apenas fornecer uma plataforma para que essas negociações ocorram. Nesse exemplo, as criptomoedas não são custodiadas em uma carteira de propriedade da exchange. Podem as empresas também (ii) comprar e vender bitcoins (e outras criptomoedas) que circulam pelas carteiras de titularidade da exchange.

No primeiro caso, no qual as *exchanges* apenas fazem a intermediação de venda e compra, há uma prestação de serviço em favor de vendedores e compradores, o que seria tributável pelo ISS/ISSQN (Imposto Sobre Serviços), de competência dos municípios, desde que a lista anexa da Lei Complementar 116/2003 apresente expressamente essa previsão, em atenção ao princípio da tipicidade/legalidade tributária. Atualmente, a lista traz o item 10.02 (“agenciamento, corretagem ou intermediação de títulos em geral, valores mobiliários e contratos quaisquer), entretanto o item não apresenta expressamente a atividade de *exchange*. Assim, em atendimento ao que definiu o Supremo Tribunal Federal no

tema 296[30], a ausência da previsão expressa da atividade de exchange na lista anexa poderia impossibilitar a cobrança do imposto pelos municípios.

No segundo caso, quando a *exchange* não apenas intermedeia, mas também aliena criptomoedas de sua própria carteira em troca de moeda fiduciária de curso legal, poderia incidir ICMS e IOF, a depender de como será a regulamentação ainda em votação no Congresso Nacional. Dito isso, atualmente não há legislação equiparando as exchanges de moedas virtuais a casas de câmbio, assim não há que se cogitar em tributação pelo IOF. Quanto ao ICMS, as criptomoedas são bens incorpóreos: poderiam elas serem compreendidas como “mercadoria”? Caso esse seja o entendimento da regulamentação a ser votada, após a alienação de criptoativos, poder-se-ia identificar a ocorrência de uma transmissão de direito de propriedade e, portanto, uma circulação jurídica de “mercadoria”, o que poderia ensejar ao Estado, em tese, o direito de cobrar ICMS.

Quanto ao Imposto sobre Operações de Câmbio (IO-Câmbio), a União tem competência tributária para instituir imposto sobre operações de câmbio, conforme art. 153, inciso V da Constituição Federal/88, e art. 21, inciso VIII, o qual esclarece que “compete à União administrar as reservas cambiais do País e fiscalizar as operações de natureza financeira, especialmente as de crédito, câmbio e capitalização, bem como as de seguros e de previdência privada”. Algumas legislações infraconstitucionais, como as Leis 4.131/62 e 4.595/64, também disciplinam a aplicação do capital estrangeiro e as remessas de valores para o exterior. Percebe-se que a atividade de câmbio é bastante regulada e, teoricamente, somente pode envolver operações que sejam submetidas a uma estrita regulação de natureza cambial.

Com efeito, as operações de compra e venda de moeda estrangeira são formalizadas, no direito brasileiro, por meio de “contratos de câmbio”, que são contratos típicos nos quais a moeda brasileira representa o preço e a estrangeira, a mercadoria a ser adquirida[31]. Como possui cláusulas preestabelecidas pelo BCB e

---

30 Tese: É taxativa a lista de serviços sujeitos ao ISS a que se refere o art. 156, III, da Constituição Federal, admitindo-se, contudo, a incidência do tributo sobre as atividades inerentes aos serviços elencados em lei em razão da interpretação extensiva.

31 Circular 3.691/2013 (BACEN) - Contrato de câmbio é o instrumento específico firmado entre o vendedor e o comprador de moeda estrangeira, no qual são estabelecidas as características e as condições sob as quais se realiza a operação de câmbio.

deve respeitar forma especial para a sua celebração, o contrato de câmbio, além de típico, é contrato de adesão solene e formal.

O CTN também define as operações de câmbio como a "entrega de moeda nacional ou estrangeira, ou de documento que a represente, ou sua colocação à disposição do interessado em montante equivalente à moeda estrangeira ou nacional entregue ou posta à disposição por este" (art. 63, inciso II), o que parece condizente com o conceito de contrato de câmbio advindo do direito privado.

Dadas essas definições, a legislação não autoriza a compra e venda de moeda estrangeira se tais operações não se realizem por meio de contratos de câmbio firmados com as instituições autorizadas para tanto. Desse modo, qualquer operação que esteja à margem das reguladas pelo BCB não estaria incluída pelo campo material de incidência do imposto.

Assim, embora existam aqueles que defendem o enquadramento das criptomoedas no conceito de "moeda", dado o nosso direito interno, ainda não é possível juridicamente admitir essa ideia. Dada a pluralidade de conceitos que a noção de moeda vem desenvolvendo durante a história humana, em termos gerais, é importante ressaltar que as funções comumente atribuídas ao dinheiro (moeda) são as de servir como meio de troca(i), reserva de valor (ii) e unidade de conta (iii). Contudo, as três funções não emergem instantaneamente no momento em que um bem passa a ser utilizado como meio de troca. Na verdade, facilitar as trocas, desempenhar a função de meio de troca é a função principal da moeda e é como a moeda deve ser definida.

Como Fernando Ulrich bem ensina, "um bem que ganha crescente liquidez no mercado tende a ser estocado, ou entesourado, como reserva de valor, de riqueza, para ser usado no comércio futuramente, quando será, então, empregado como meio de troca" Assim, a moeda também é usada para preservar o poder de compra futuro, o que se consubstancia na função primordial de meio de troca manifestando-se no tempo e no espaço. Logicamente, a moeda não é o único bem escolhido como reserva de valor: outros ativos podem desempenhar essa função como imóveis, metais preciosos, obras de arte, etc. Entretanto, os graus de liquidez são distintos. Ulrich ressalta que "o que uma pessoa decidir entesourar como reserva de valor dependerá de suas necessidades monetárias frente aos seus dispêndios futuros e da liquidez e expectativa de valor das diferentes moedas e ativos disponíveis no

mercado."[32] Portanto, servir como reserva de valor é uma função secundária do dinheiro (moeda).

A terceira função atribuída à moeda – ser uma unidade de conta – é derivada de seu uso como meio de troca: à medida que a liquidez de um bem monetário aumenta, este passa a circular como a principal moeda em uma economia, a sociedade tende a precificar os produtos e serviços e realizar cálculos econômicos em função dessa moeda. Ulrich entende que essa característica poderia ser a que marca uma moeda amplamente aceita e desenvolvida: ser usada não somente como meio de troca, mas também como unidade geral de conta.

Com o passar do tempo e com a maior complexidade das relações sociais, a noção de moeda foi alterada ao ponto de haver uma enorme evolução das moedas cunhadas até as atuais moedas eletrônicas. Por conta disso, nada impede que as moedas virtuais, após passarem por mais testes durante alguns anos ou décadas, não sejam amplamente aceitas pela comunidade internacional a ponto de serem consideradas moedas de fato, assim como as moedas fiduciárias o são. Por enquanto, parece não ser possível enquadrar as criptomoedas ainda como moedas de fato, com todas as consequências jurídico-financeiras que isso resulta.

5.3 Questão operacional/instrumental – dificuldades em tributar uma operação anônima

Pesquisa recente da ANBIMA (Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais)[33], realizada em novembro/2021, revelou que 2% da população brasileira investe em criptoativos, ou seja, um pouco mais de 4 milhões, quase o mesmo número de CPFs registrados na Bolsa brasileira, a B3[34], em junho de 2022 (4,4 milhões). Ou seja, o volume de transações que ocorrem nas diversas *blockchains* existentes já representa um valor considerável e proporcional aos mercados financeiros mais tradicionais.

---

32 ULRICH, Fernando. Bitcoin: a moeda na era digital. São Paulo: Instituto Ludwig von Mises, 2014, p.93-94.

33 Disponível em https://portaldobitcoin.uol.com.br/pesquisa-da-anbima-revela-quantos-brasileiros-investem-em-criptomoedas-e-qual-a-geracao-mais-entusiasta/. Acesso em 28.08.22.

34 Disponível em https://www.b3.com.br/pt_br/market-data-e-indices/servicos-de-dados/market-data/consultas/mercado-a-vista/perfil-pessoas-fisicas/perfil-pessoa-fisica/. Acesso em 04.09.22.

Como demonstrado, a RFB esclareceu que as alienações de criptomoedas se submetem à tributação do imposto de renda sobre os eventuais ganhos de capital, tal como ocorre com as alineações de ativos financeiros. Ainda, em sua Instrução Normativa nº 1.888/2019, ela institui e disciplina a obrigatoriedade de prestação de informações relativas às operações realizadas com criptoativos à Secretaria Especial da Receita Federal do Brasil. A obrigatoriedade se refere (i) à *exchange* de criptoativos domiciliada para fins tributários no Brasil; (ii) à pessoa física ou jurídica residente ou domiciliada no Brasil quando as operações forem realizadas em exchange domiciliada no exterior; (iii) e à pessoa física ou jurídica residente ou domiciliada no Brasil quando as operações não forem realizadas em exchange.

Na primeira e segunda obrigatoriedade (i e ii), a dinâmica é muito parecida com uma corretora de valores mobiliários, a qual possui os registros de transações dos clientes e nutre a Secretaria da Receita Federal e outros órgãos com dados para checagem de movimentações financeiras e para batimento da declaração do Imposto de Renda de Pessoa Física. A grande questão é a terceira obrigatoriedade (iii): pessoa física ou jurídica ficam obrigados a declarar informações quando as operações não forem realizadas em *exchanges*. Essa alínea no artigo 6º da IN 1.888 está relacionada com as operações P2P puras, aquelas nas quais as partes fazem negociações diretamente entre si, sem a intermediação de uma *exchange*, ficando, portanto, o registro público na *blockchain* da rede do criptoativo negociado, mas sem a identificação das partes, uma vez que a rede é pública, porém anônima.

As transações puras P2P são o ponto mais frágil para as auditorias e checagens de transações pelos Órgãos públicos, uma vez que as exchanges não possuem registros dessas transações e elas somente poderiam ser indicadas pelos usuários que participam da negociação. Via de regra, a Receita Federal, por exemplo, teria que acatar os dados informados pelos usuários, o que facilita a prática de crimes de “lavagem” ou ocultação de valores (regrados pela Lei nº 9.613/98). Os usuários mal-intencionados podem simplesmente deixar de reportar negociações e/ou reportá-las com valores adulterados, passando o ônus da verificação para o setor público, o qual terá grande dificuldade técnica em identificar os corretos aspectos das operações financeiras, bem como cobrar os eventuais tributos incidentes.

5.3.1 Pontos de vazamento de privacidade na rede Bitcoin: possíveis caminhos para identificação das partes que negociam em redes P2P

ENDEREÇO IP - Existem alguns pontos de fragilidade na privacidade da rede Bitcoin e que possibilitariam uma identificação das partes em negociação. O primeiro deles é o IP (*Internet protocol* ou Protocolo da Internet). Esse termo é utilizado para duas coisas: descrever os protocolos de comunicação entre dispositivos, dentre os quais existem os modelos TCP/IP (*Transmission Control Protocol*) e OSI (*Open System Interconnection*); e também é o número de identificação de um dispositivo conectado à internet (também conhecido como Endereço IP ou *IP Address*.

Basicamente, o número de endereço IP é o CPF do seu computador, celular, tablet, TV, enfim, dos aparelhos eletrônicos (hardwares). É um número atribuído ao dispositivo no momento em que ele é ligado, chamado IP interno. Porém, assim que o gadget se conecta à internet, ele recebe um segundo número de registro, o IP externo: ambos servem para identificação, o interno serve para identificar uma máquina em uma rede interna (ambientes corporativos ou domiciliares, por exemplo). Já o externo é sua identidade na internet: esse número único, porém dinâmico, permite que você se conecte à rede. O endereço IP é uma identidade digital, portanto, e permite que outras pessoas tenham acesso a arquivos que se queira compartilhar.

Assim, teoricamente, seria possível que alguns nós (nodes) pudessem guardar informações referentes ao IP de usuários que executassem um *trade* em rede P2P, possibilitando a identificação das partes negociantes, uma vez que, como explicado, todos os aparelhos que se conectam à internet estão identificados com endereços IP. Contudo, percebe-se que há, no mínimo, custos e diligências a serem feitas por órgãos públicos, no processo de auditoria e verificação de uma negociação, para que sejam identificadas as partes anônimas, a fim de serem autuadas para o pagamento dos tributos devidos.

Caso o percentual de negociações anônimas se torne muito alto, o que pode trazer insegurança ao sistema jurídico tributário nacional, prejudicando a eficiência arrecadatória e o planejamento estatal, os Estados passarão a desenvolver tecnologias cada vez mais avançadas de processamento de dados, inteligência artificial e criptografia para identificação dessas partes e correto adimplemento dos

tributos devidos. Ou, em uma ação mais radical, caso entendam impossível identificar os negócios em P2P, poderão tornar ilegal esse tipo de *trade*.

CARTEIRA DIGITAL WEB (*crypto wallet*) – Caso o usuário faça suas transferências via uma *crypto wallet* online (uma carteira virtual WEB que é executada diretamente em navegadores como Internet Explorer, Google Chrome ou Mozilla Firefox, por exemplo), utilizando-se de smartphone ou computador pessoal, por estar utilizando um serviço de internet, as empresas e os governos podem ter acesso ao endereço IP do dispositivo utilizado (via sistema de administração das prestadoras de serviço online, ainda que após autorização judicial). Cruzando dados da transação (valores, data, endereços públicos) com os recolhidos pelas empresas operadoras de internet, é possível identificar quem executa as negociações P2P.

SERVIÇOS P2P DENTRO DAS PLATAFORMAS DE EXCHANGES (*crypto wallet*) – Como as negociações P2P puras possuem um risco associado ao se negociar com pessoas diferentes (e não entre carteiras de propriedade da mesma pessoa ou empresa), as *exchanges*, como a Binance, oferecem plataformas de negociação direta entre as partes com uma fase extra: as partes negociam os valores e forma de pagamento diretamente entre si, e a empresa utiliza seu ecossistema para adicionar uma camada de garantia e segurança.

Como funciona a Binance P2P, por exemplo? Ela é uma plataforma que permite a transação de bitcoins e outras criptomoedas: a diferença para o P2P puro é que, além de estabelecer a exchange como um intermediário, o que não ocorre nas operações diretas, o criptoativo permanece custodiado na carteira da Binance até que o vendedor confirme que recebeu o dinheiro, com o intuito de reduzir o potencial de fraudes que podem ocorrer nesse tipo de transação sem um terceiro garantidor.

Nesse caso, por se utilizar de um sistema que se encontra dentro da plataforma de uma *exchange*, esta possui acesso a todos os dados que identificam aqueles que negociam, sejam os dados mais básicos utilizados para fazer cadastro na plataforma, sejam os endereços públicos e valores utilizados na negociação. Caso todas as transações P2P fossem feitas dessa forma, não existiriam problemas na auditoria e verificação de transações financeiras pelos órgãos públicos, assumindo um cenário de futura regulamentação das corretoras que operam criptoativos, e que seriam vinculadas por lei a um arcabouço jurídico-administrativo

parecido com as atuais corretoras de valores mobiliários.

5.3.2 Práticas que dificultam a identificação das transações em redes P2P puras

Atualmente, os usuários da rede Bitcoin já desfrutam de um certo nível de privacidade, uma vez que, embora sua *blockchain* seja pública, ela não identifica por nome e CPF os seus integrantes, e sim por um endereço também público sem vinculação direta com as partes. Como visto no ponto 5.4.1, existem alguns caminhos que podem identificar as supostas negociações anônimas e futuras tecnologias certamente serão desenvolvidas para facilitar essa revelação pelos Estados, comprovando que as negociações em uma rede Bitcoin não são irrastreáveis. Logo, os órgãos públicos podem fazer uso de novas tecnologias para poderem identificar as partes dentro de um *trade*.

A questão é que também existem ferramentas para tentar aumentar a privacidade das negociações P2P, adicionando camadas de sigilo e tornando mais difícil a identificação dos *traders*. Algumas tecnologias de aprimoramento de anonimato conhecidas são:

VPN (*Virtual Private Network* ou Rede Privada Virtual) – uma rede virtual privada criptografa seu tráfego de internet e disfarça sua identidade online, ocultando o endereço IP do dispositivo onde está instalada, fazendo com que a rede atue a partir de um servidor remoto. Isso significa que quando se navega online com essa conexão, o servidor VPN se tornará a fonte de seus dados, fazendo com que provedores de internet e terceiros não tenham acesso a quais sites estão sendo acessados, quais dados estão sendo baixados, protegendo a privacidade do usuário.

Esses serviços são muito utilizados para poder acessar redes Wi-Fi públicas (como de cafés, shoppings, aeroportos, etc) aumentando substancialmente a segurança e buscando evitar ataques virtuais, furtos de senhas e dados, entre outros problemas frequentes em conexões públicas. As VPNs também são utilizadas por usuários que desejam acessar serviços só disponíveis em outros países, uma vez que a rede identifica o usuário pelo local onde o servidor está instalado (ex: desejo assistir um filme que somente passa na Netflix da Espanha; assim, basta eu utilizar uma VPN espanhola para poder assisti-lo). Por fim, muitas

empresas disponibilizam sua própria VPN para funcionários acessarem a rede empresarial de qualquer lugar do mundo de forma mais segura, aumentando a proteção contra crimes cibernéticos.[35]

TOR (Navegador) – o tor Project Inc. é uma organização sem fins lucrativos que desenvolveu o navegador Tor[36], um software gratuito cujo objetivo é retransmitir suas comunicações em uma rede distribuída de relés (servidores aleatórios), rodada por pessoas voluntárias ao redor do mundo, evitando que alguém esteja observando sua conexão com a internet e saiba os sites que visita, sua localização física, etc. O objetivo final, portanto, é manter uma web sem censura e privada ao rotear o tráfego por múltiplos servidores e criptografá-los a cada passo do caminho.

Misturadores de criptomoedas – um misturador de moedas, como o Blender.io ou o Tornado Cash, é um recurso especial projetado pela comunidade cripto para permitir que usuários misturem suas criptomoedas com as de outros usuários, buscando melhor privacidade e anonimato. Após agregar todas as criptomoedas de diversas transações em uma carteira apenas (a fim de ocultar os detalhes de sua origem), os valores são devolvidos às contas indicadas por seus donos em diversas transações que somam os valores inicialmente remetidos pelas partes, porém com um desconto de uma taxa pelo serviço dos mineradores e da plataforma.

Nesse serviço, as criptomoedas depositadas pelos usuários não são as mesmas que retornam a eles “após a mistura”, quebrando a relação original entre 2 endereços Bitcoin diferentes e ofuscando a relação de propriedade pública derivada da *blockchain*. Como vantagem nesse tipo de serviço, há o aumento de privacidade para empresas e proprietários de grandes quantidades de criptomoedas, os quais desejam reduzir os riscos de serem alvos de extorsão ou de hacks/furtos virtuais de seus ativos; impedir que organizações e/ou governos rastreiem fundos e saibam o quanto alguém possui e de que forma usa (principalmente em regimes não-democráticos, essa função apresenta elevado valor social); garantir o direito à privacidade e ao anonimato em transações financeiras entre usuários de qualquer lugar no mundo.

---

35 Disponível em <https://www.techtudo.com.br/listas/2020/05/como-funciona-uma-vpn-veja-cinco-perguntas-e-respostas.ghtml > Acesso em 17.08.22.
36 Disponível em <https://www.torproject.org/pt-BR/about/history/ > Acesso em 20.08.22.

Como principal argumento contrário aos serviços de misturadores de criptomoedas, está, principalmente, o fato de que ele possa ser utilizado para desvincular a origem de dinheiro/ativos oriundos de atos ilegais, o que facilitaria a lavagem de dinheiro, o financiamento de atos terroristas, do tráfico de drogas, de pessoas, enfim, de atos criminosos em geral. Inclusive, recentemente a secretária assistente do Departamento de Tesouro norte-americano, Elizabeth Rosenberg, sugeriu que “sancionar misturadores de criptomoedas poderia ajudar a fortalecer a resposta do governo a entidades estrangeiras que procuram usar ativos digitais para meios ilícitos.” Ela também ressaltou que “tecnologias de aprimoramento de anonimato, como misturadores [...] são de fato uma preocupação para entender o fluxo de financiamento ilícito e ir atrás dele.”[37]

De acordo com dados de um levantamento da Chainalysis, estima-se que apenas 8% dos fundos transferidos para esses serviços de misturadores provêm de atividades ilegais. Ou seja, a maior parte dos usuários desses serviços realmente são empresas ou pessoas que desejam mais privacidade ao lidar com suas riquezas e seus ativos. Todavia, sabemos da dificuldade que os governos possuem para identificar as origens de fundos ilegais, uma vez que o próprio sistema financeiro tradicional é utilizado por criminosos para lavagem de dinheiro, como já informado, e esse formato não seria diferente se tratando de criptoativos, os quais, por natureza, já possuem uma essência mais reservada e anônima, o que atrai fundos de origem ilegal também.

Dito isso, essas ferramentas que aumentam o anonimato dos usuários de criptomoedas existem e são utilizadas tanto de forma legal, quanto ilegal. Assim, os Estados e os órgãos técnicos devem permanecer em discussão para trazer uma regulamentação que consiga abraçar o potencial econômico dessas medidas, sem deixar de lado o combate ao crime financeiro.

---

37 Disponível em https://cointelegraph.com.br/news/us-treasury-official-says-crypto-mixers-are-a-concern-in-enforcing-sanctions. Acesso em 21.09.22.

6. CONSIDERAÇÕES FINAIS

O Direito é uma ciência social que reflete as realidades da sociedade, porém frequentemente apresenta um descompasso. Isso ocorre porque a velocidade com que as mudanças acontecem não é amparada nos ordenamentos jurídicos, visto que as inovações tecnológicas e de padrões de comportamento demoram a ser percebidas e até compreendidas pelo Estado e seus agentes.

O surgimento do Bitcoin e dos outros criptoativos que o seguiram trouxeram uma ruptura normativa que ainda não foi preenchida pelo Estado brasileiro. De fato, o que se pode observar atualmente é uma lacuna legislativa que não ampara o mundo virtual e o universo digital das criptomoedas. Em verdade, o Brasil não é o único país atrasado quanto à regulação dessa temática e ainda não há uma legislação mundial que acolha a totalidade do universo cripto.

Essa ausência normativa e legislativa, a qual ocorre também em relação a outros fatos sociais, infelizmente é característica comum ao Legislativo brasileiro, contudo os números apresentados no trabalho quanto ao montante negociado no Brasil (R$215 bilhões no ano de 2021), bem como ao número de investidores brasileiros de criptomoedas (mais de 4 milhões), exigem dos legisladores uma maior atenção para o enquadramento jurídico desse mercado, a fim de trazer segurança aos brasileiros, sejam eles investidores, empresas que atuam no segmento e/ou administração pública.

A pandemia do COVID-19 acelerou a digitalização do mundo, uma vez que uma parte substancial da população foi segregada e por um bom tempo fomos obrigados a viver e trabalhar de nossas casas, pela internet. Essa transformação digital que ainda está ocorrendo também virtualizou a circulação do próprio capital, a partir dos investimentos, sejam eles no mercado de criptoativos, sejam no mercado financeiro tradicional, por meio da Bolsa de Valores e corretoras de valores mobiliários.

Como visto, a criação dos criptoativos foi derivada do descontentamento de uma parcela da população quanto à qualidade dos serviços financeiros da época; quanto à desvalorização anual da renda das pessoas, via inflação das moedas fiduciárias; quanto ao controle excessivo de informações pessoais que eram e são comercializadas por empresas e estados sem a autorização de seus donos. Enfim, todas essas realidades foram questionadas e o fenômeno do Bitcoin foi criado, e

uma sucessão de novos ativos surgiram posteriormente.

Os criptoativos ainda não possuem uma natureza jurídica definida, havendo diversas possibilidades para seu uso: como visto, eles são usados como investimento especulativo; para fazer trocas entre ativos dentro das plataformas de negociação; para pagar por bens e serviços (ainda que o número de empresas que oferecem essa possibilidade ainda é incipiente).

Sem a aprovação de robusta normativa pelo legislativo brasileiro a respeito dos criptoativos, os órgãos fazendários e o Judiciário buscaram construir uma regulamentação mínima, a fim de possibilitar visibilidade a uma correta tributação das negociações envolvendo criptoativos, optando por aproximar a natureza deles a ativos financeiros e implementando, portanto, a tributação quanto ao ganho de capital. Atualmente, a Instrução Normativa nº 1.888/2019, emitida pela RFB, esclarece os caminhos aos contribuintes brasileiros para declaração de bitcoins e outros criptoativos.

Dito isso, esse estudo veio para alertar que há um nicho de mercado - as negociações P2P puras -, o qual gerará uma dificuldade técnica muito maior à administração pública brasileira, no sentido de auditar as negociações, identificar as partes que realizam os *trades* e garantir que os tributos devidos sejam adimplidos corretamente. Foi demonstrado que, da mesma forma que os órgãos públicos possuem ferramentas para rastrear e melhor identificar valores e partes negociais (a partir da identificação dos endereços IP utilizados nos trades, por exemplo), também há ferramentas que aumentam o anonimato dos usuários, com o intuito de resguardar sua privacidade, e que podem impossibilitar essa mesma identificação necessária para o sistema tributário brasileiro.

É importante sempre lembrar que o mundo das criptomoedas foi desenvolvido imbuído de uma natureza semi-anarquista, com um propósito de eliminar o controle governamental ou a centralização desmedida nas negociações financeiras, transferências de valores entre cidadãos, etc. Como uma resposta às excrescências de alguns governos e Bancos Centrais que ainda não fazem o melhor trabalho em resguardar o valor do dinheiro dos cidadãos, a internet desejava construir uma moeda virtual que fosse universal, produzida de uma forma isenta, matemática e sem influência de terceiros, e que pudesse ser utilizada sem fronteiras de fato. Foi assim que o Bitcoin foi criado e iniciou o mercado de criptoativos.

Por enquanto, como ainda não há uma legislação robusta aprovada e em vigor, as negociações P2P puras continuam a ser executadas e podem ser combinadas com as ferramentas que aumentam o anonimato dos usuários de criptomoedas (utilizadas tanto de forma legal, quanto ilegal), o que, por fim, inviabilizam o conhecimento dos detalhes de negociações financeiras e origem de fundos transferidos. Sem algum tipo de registro formal dessas negociações, no futuro, esse pode ser o novo caminho pelo qual as grandes ações ilegais para "lavagem" de dinheiro ocorrerão. Inclusive, é opinião do autor que esse tipo de ausência total de controle estatal não sobrevive a novas regulações e pode ser chancelado como ilegal em diversos Estados, em razão da grande dificuldade da administração pública em conhecer todos os aspectos desse tipo de negociação.

Assim, para resguardar o planejamento financeiro-tributário dos Estados e para facilitar a fiscalização criminal-financeira no mundo, os governos e seus órgãos técnicos devem permanecer em ampla discussão conjunta para trazer uma regulamentação que consiga abraçar o potencial econômico dessas medidas, sem deixar de lado o combate aos crimes financeiros, garantindo o correto fluxo tributário necessário para execução dos serviços e projetos públicos no país.

REFERÊNCIAS

BRITO, M.S.H. D. **Manual de Direito Tributário**, 11ª edição. São Paulo: Grupo GEN, 2019.

CAMPOS, Gabriela Isa Rosendo Vieira. **Bitcoin: consequências jurídicas do desenvolvimento da moeda virtual.** Revista Brasileira de Direito, 11(2): 77-84, jul-dez. 2015.

BRASIL. Lei nº 5.172/66. Dispõe sobre o Sistema Tributário Nacional. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l5172compilado.htm >. Acesso em 14.08.22.

BRASIL. Lei nº 8.078/90. Dispõe sobre a proteção do consumidor. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l5172compilado.htm. Acesso em 15.08.22.

BRASIL. Lei nº 12.865/2013. Dispõe sobre os arranjos de pagamento e as instituições de pagamento integrantes do Sistema de Pagamentos Brasileiro (SPB). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12865.htm. Acesso em 17.08.22.

BRASIL. Lei nº 9.069/2013. Dispõe sobre o Plano Real, o Sistema Monetário Nacional [...]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9069.htm. Acesso em 14.08.22.

BRASIL. Lei nº 8.880/1994. Dispõe sobre o Programa de Estabilização Econômica e o Sistema Monetário Nacional, institui a Unidade Real de Valor (URV) [...]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8880.htm. Acesso em 10.08.22.

BRASIL. Lei nº 6.385/1976. Dispõe sobre o mercado de valores mobiliários e cria a Comissão de Valores Mobiliários. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L6385compilada.htm. Acesso em 12.08.22.

BRASIL. Lei nº 9.613/1998. Dispõe sobre os crimes de “lavagem” ou ocultação de bens, direitos e valores [...]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9613.htm. Acesso em 23.08.22.

BRASIL. Lei nº 9.250/1995. Altera a legislação do imposto de renda das pessoas físicas. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9250.htm. Acesso em 21.08.22.

BRASIL. Lei nº 6.404/1976. Dispõe sobre as Sociedades por Ações. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l6404consol.htm. Acesso em 19.08.22.

BRASIL. Lei nº 10.406/2002. Intitui o Código Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em 18.08.22.

DE FILIPPI, Primavera; WRIGHT, Aaron. **Blockchain and the Law: the Rule of Code**. Harvard University Press: Cambrige, Massachusetts: 2018.

FOBE, Nicole Julie. **O *Bitcoin* como moeda paralela – uma visão econômica e a multiplicidade de desdobramentos jurídicos.** Dissertação de Mestrado apresentada ao Programa de Mestrado Acadêmico da Escola de Direito de São Paulo da Fundação Getulio Vargas (FGV Direito SP), na área de concentração Direito e Desenvolvimento, para obtenção do título de Mestre em Direito. São Paulo: 2016

GOMES, Daniel de Paiva. ***Bitcoin*: a tributação de investimento em criptomoedas.** Dissertação de Mestrado apresentada ao Programa de Mestrado Acadêmico da Escola de Direito de São Paulo da Fundação Getulio Vargas (FGV Direito SP), na área de concentração Direito Tributário, para obtenção do título de Mestre em Direito. São Paulo: 2019

GONÇALVES. Gabriel de Souza. **Regulação de criptoativos: Uma Análise das Propostas Legislativas Nacionais diante do Ordenamento Jurídico Brasileiro e da visão de outros países**. Monografia apresentada ao Curso de Direito da Universidade do Sul de Santa Catarina como requisito parcial à obtenção do título de Bacharel em Direito. 2019

MARTINS, Ronaldo Corrêa. **Imposto de Renda: noção teórica de renda. O conceito de renda na legislação brasileira. Imposto de renda de pessoas física**, in Revista Interesse Público, n. 26, 2004

MELLO, Fernando Figueiredo.**Tributação e segurança jurídica: a importância para o Brasil de uma eficiente rede de proteção** / Fernando Figueiredo Mello, Oscar Pilagallo. – São Paulo, SP: ETCO, 2019

MOSQUERA, Roberto Quiroga. **Tributação no mercado financeiro e de capitais**. São Paulo: Dialética, 1999.

NAKAMOTO, Satoshi. **Bitcoin: A Peer-to-Peer Electronic Cash System**. Disponível em https://bitcoin.org/bitcoin.pdf. Acesso em 15.08.22.

SHIRKY, Clay. Prestando atenção ao Napster. In: ORAM, Andrew. **Peer-to-peer: o poder transformador das redes ponto a ponto.** São Paulo, Brasil, Editora Berkeley, 2001.

SILVA, Luiz Gustavo Doles. **Bitcoins & outras criptomoedas – Teoria e prática à luz da legislação brasileira.** Curitiba: Juruá, 2018. p. 51 a 66.

STELLA, Julio Cesar. **Moedas virtuais no brasil: Como enquadrar as criptomoedas**. Revista da PGBC – V. 11 – N. 2 – Dez. 2017.

STEFFENS, Luana; TESSARI, Cláudio. **A tributação das operações com criptomoedas no Brasil: o caso da Bitcoin.** Revista de Direito Tributário Contemporâneo/ vol. 30/2021. P. 269-296. Acesso em: 10.09.22.

TAPSCOTT, Don; e TAPSCOTT, Alex. **Blockchain revolution: como a tecnologia por trás do Bitcoin está mudando o dinheiro, os negócios e o mundo**. São Paulo: Editora SENAI-SP, 2016

ULRICH, Fernando. **Bitcoin: a moeda na era digital.** 1a edição. São Paulo: Instituto Ludwig Von Mises Brasil, 2014.

Zilveti, Fernando Aurelio. Nocetti, Daniel Azevedo. **Blockchain e Criptomoedas: um Desafio para o Sistema Tributário Internacional.** 7º Congresso Brasileiro de Direito Tributário Internacional, 22, 23, 24 de agosto de 2018 em São Paulo: FDUSP, SP. – São Paulo, IBDT, 2018

ANEXO – Projeto de Lei 4.401/2021 – Senado Federal (substitutivo ao PL nº 2.303/2015)

COMPLEMENTAÇÃO DE VOTO AO RELATÓRIO APRESENTADO NO PLENÁRIO SOBRE O PROJETO DE LEI Nº 3825/2019

PARECER Nº 126, DE 2022-PLEN/SF

De PLENÁRIO, sobre o Projeto de Lei no 3.825, de 2019, que disciplina os serviços referentes a operações realizadas com criptoativos em plataformas eletrônicas de negociação; e o Projeto de Lei nº 4.401, de 2021, que dispõe sobre a prestadora de serviços de ativos virtuais; e altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), e as Leis nºs 7.492, de 16 de junho de 1986, e 9.613, de 3 de março de 1998, para incluir a prestadora de serviços de ativos virtuais no rol de instituições sujeitas às suas disposições.

RELATOR: Senador IRAJÁ

Na sessão do dia 19 de abril de 2022, apresentamos relatório perante este Plenário, oferecendo emenda substitutiva ao Projeto de Lei nº 3.825, de 2019.

Consideramos ponderações e sugestões de aprimoramento apresentadas pelos nobres pares, instituições governamentais e setores organizados da sociedade, encaminhamos as seguintes complementações de voto:

1 – Com o acolhimento total das emendas de nºs 7, 11, 13, 14 e 18 ao Projeto de Lei nº 3.825, de 2019, e da emenda nº 5 ao Projeto de Lei nº 4.401, de 2021, nos termos do substitutivo.

2 – Com o acolhimento parcial das emendas de plenário nºs 4 e 19 ao Projeto de Lei nº 3.825, de 2019, nos termos do substitutivo.

3 – Nova redação ao art. 11, acolhendo sugestões de aprimoramento da Associação Nacional dos de Procuradores da República - ANPR.

Ante o exposto, pronunciamo-nos pela constitucionalidade, juridicidade, regimentalidade e boa técnica legislativa dos Projetos de Lei nº 3.825, de 2019, e no 4.401, de 2021, e das Emendas de Plenário apresentadas.

No mérito, votamos pela aprovação do Projeto de Lei nº 4.401, de 2021, na forma

do Substitutivo, restando prejudicado o Projeto de Lei no 3.825, de 2019, com a incorporação total das Emendas nos 5, 7, 11, 13, 14 e 18 e parcial das Emendas nos 4 e 19, e rejeição das demais Emendas de Plenário ao Projeto de Lei no 3.825, de 2019, e ao Projeto de Lei no 4.401, de 2021.

EMENDA Nº 6 - PLENÁRIO (SUBSTITUTIVO)

PROJETO DE LEI Nº 4.401, DE 2021

Dispõe sobre diretrizes a serem observadas na prestação de serviços de ativos virtuais e na regulamentação das prestadoras de serviços de ativos virtuais; e altera as Leis no 7.492, de 16 de junho de 1986, que define crimes contra o sistema financeiro nacional, e no 9.613, de 3 de março de 1998, que dispõe sobre lavagem de dinheiro, para incluir essas entidades no rol de suas disposições.

O CONGRESSO NACIONAL decreta:

Art. 1º Esta Lei dispõe sobre diretrizes a serem observadas na prestação de serviços de ativos virtuais e na regulamentação das prestadoras de serviços de ativos virtuais.

Parágrafo único. O disposto nesta Lei não se aplica aos ativos representativos de valores mobiliários sujeitos ao regime da Lei nº 6.385, de 7 de dezembro de 1976, e não altera nenhuma competência da Comissão de Valores Mobiliários.

Art. 2º As prestadoras de serviços de ativos virtuais somente poderão funcionar no país mediante prévia autorização de órgão ou entidade da Administração Pública Federal.

Parágrafo único. Ato do órgão ou da entidade da administração pública federal a que se refere o caput estabelecerá as hipóteses e os parâmetros em que a autorização de que trata o caput deste artigo poderá ser concedida mediante procedimento simplificado.

Art. 3º Para os efeitos desta Lei, considera-se ativo virtual a representação digital de valor que pode ser negociada ou transferida por meios eletrônicos e utilizada para realização de pagamentos ou com propósito de investimento, não incluídos:

I - moeda nacional e moedas estrangeiras;

II - a moeda eletrônica, nos termos da Lei nº 12.865, de 9 de outubro de 2013;

III - instrumentos que provejam ao seu titular acesso a produtos ou serviços especificados ou a benefício proveniente desses produtos ou serviços; e

IV - representações de ativos cuja emissão, escrituração, negociação ou liquidação esteja prevista em lei ou regulamento.

§ 1º Competirá a órgão ou entidade da Administração Pública Federal definido em ato do Poder Executivo estabelecer quais serão os ativos financeiros regulados, para fins desta Lei.

§ 2º Fica autorizada a abertura de conta em prestadoras de serviços de ativos virtuais e a realização de operações com ativos virtuais e seus produtos derivados por órgãos e entidades da administração pública, nas hipóteses previstas em regulamento a ser editado por ato do Poder Executivo.

Art. 4º A prestação de serviço de ativos virtuais deve observar as seguintes diretrizes, segundo parâmetros a serem estabelecidos pelo órgão ou pela entidade da Administração Pública Federal definido em ato do Poder Executivo:

I - livre iniciativa e livre concorrência;

II - controlar e manter de forma segregada os recursos aportados pelos clientes;

III - boas práticas de governança, transparência nas operações e abordagem baseada em riscos;

IV - segurança da informação e proteção de dados pessoais; V - proteção e defesa de consumidores e usuários;
VI - proteção à poupança popular;

VII - solidez e eficiência das operações; e

VIII - prevenção à lavagem de dinheiro, ocultação de bens, direitos e valores, combate à atuação de organizações criminosas, ao financiamento do terrorismo e ao financiamento da proliferação de armas de destruição em massa, em alinhamento com os padrões internacionais.

Art. 5º Considera-se prestadora de serviços de ativos virtuais a pessoa jurídica que executa, em nome de terceiros, pelo menos um dos serviços de ativos virtuais, entendidos como:

I - troca entre ativos virtuais e moeda nacional ou moeda estrangeira; II - troca entre um ou mais ativos virtuais;
III - transferência de ativos virtuais;

IV - custódia ou administração de ativos virtuais ou de instrumentos que

possibilitem controle sobre ativos virtuais; ou

V - participação em serviços financeiros e prestação de serviços relacionados à oferta por um emissor ou venda de ativos virtuais.

Parágrafo único. O órgão ou a entidade da Administração Pública Federal indicado em ato do Poder Executivo poderá autorizar a realização de outros serviços que estejam, direta ou indiretamente, relacionados à atividade da prestadora de serviços de ativos virtuais de que trata o caput deste artigo.

Art. 6º Ato do Poder Executivo atribuirá a um ou mais órgãos ou entidades da Administração Pública Federal a disciplina do funcionamento e a supervisão da prestadora de serviços de ativos virtuais.

Art. 7º Compete ao regulador indicado em ato do Poder Executivo federal:

I - autorizar funcionamento, transferência de controle, fusão, cisão e incorporação da prestadora de serviço de ativos virtuais.

II - estabelecer condições para o exercício de cargos em órgãos estatutários e contratuais em prestadora de serviço de ativos virtuais e autorizar a posse e o exercício de pessoas para cargos de administração.

III - supervisionar a prestadora de serviço de ativos virtuais e aplicar as disposições da Lei nº 13.506, de 13 de novembro de 2017, em caso de descumprimento desta Lei ou de sua regulamentação;

IV – cancelar ou suspender, mediante processo administrativo com o devido processo legal, as autorizações de que se trata os incisos I e II deste artigo, ressalvadas as garantias constitucionais de todos os envolvidos.

V - dispor sobre as hipóteses em que as atividades ou operações de que trata o art. 3º desta Lei serão incluídas no mercado de câmbio ou em que deverão se submeter à regulamentação de capitais brasileiros no exterior e capitais estrangeiros no País.

Parágrafo único. O órgão ou a entidade da Administração Pública Federal de que trata o caput deste artigo definirá as hipóteses que poderão provocar o cancelamento previsto no inciso IV do caput deste artigo e o respectivo procedimento.

Art. 8º As instituições autorizadas a funcionar pelo Banco Central do Brasil poderão prestar exclusivamente o serviço de ativos virtuais, ou cumulá- lo com outras atividades, na forma da regulamentação a ser editada por órgão ou entidade da Administração Pública Federal indicada em ato do Poder Executivo Federal.

Art. 9º O órgão ou a entidade da Administração Pública Federal de que trata o

caput do art. 2º desta Lei estabelecerá condições e prazos, não inferiores a 6 (seis) meses, para adequação das prestadoras de serviços de ativos virtuais que estiverem em atividade às disposições desta Lei e às normas por ele estabelecidas.

Parágrafo único. As prestadoras de serviços de ativos virtuais que estiverem em atividade na data da publicação desta Lei poderão continuar a exercê-la enquanto não proferida decisão final acerca do processo de autorização pelo órgão ou pela entidade da Administração Pública Federal definido em ato do Poder Executivo, desde que estejam regularmente cadastradas no Sistema de Controle de Atividades Financeiras, para fins de cumprimento da Lei nº 9.613, de 3 de março de 1998, e no Cadastro Nacional de Pessoas Jurídicas (CNPJ), da Secretaria da Receita Federal do Brasil, cumprindo a legislação fiscal brasileira, sob pena de indeferimento da autorização a que se refere este artigo.

Art. 10. O Decreto-Lei nº 2.848, de 07 de dezembro de 1940 (Código Penal) passa a vigora acrescido do seguinte artigo 171-A:

“Fraude em prestação de serviços de ativos virtuais, valores mobiliários ou ativos financeiros

Art. 171-A. Organizar, gerir, ofertar carteiras ou intermediar operações envolvendo ativos virtuais, valores mobiliários ou quaisquer ativos financeiros com o fim de obter vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento.
Pena – reclusão, de 4 (quatro) a 8 (oito) anos e multa.”

Art. 11. O parágrafo único do art. 1º da Lei no 7.492, de 16 de junho de 1986, passa a vigorar com a seguinte redação:

“Art. 1º .....
Parágrafo único. .....
.....
II – a pessoa jurídica que oferece serviços referentes a operações com ativos virtuais, inclusive intermediação, negociação ou custódia.

III - a pessoa natural que exerça quaisquer das atividades referidas neste artigo, ainda que de forma eventual. “(NR)

Art. 12. A Lei no 9.613, de 3 de março de 1998, passa a vigorar com a seguinte redação:

“Art. 1º .....
.....
§ 4º A pena será aumentada de 1/3 (um terço) a 2/3 (dois terços) se os crimes definidos nesta Lei forem cometidos de forma reiterada, por

intermédio de organização criminosa ou por meio da utilização de ativo virtual .....” (NR)

“Art. 9º
.....
Parágrafo Único. .....
.....
XIX – as prestadoras de serviços de ativos virtuais.” (NR)

“Art.10. .....
.....
II - manterão registro de toda transação em moeda nacional ou estrangeira, títulos e valores mobiliários, títulos de crédito, metais, ativos virtuais, ou qualquer ativo passível de ser convertido em dinheiro, que ultrapassar limite fixado pela autoridade competente e nos termos de instruções por esta expedidas;
.....” (NR)

Art. 13. Aplicam-se às operações conduzidas no mercado de ativos virtuais, no que couber, as disposições da Lei no 8.078, de 11 de setembro de 1990, e suas alterações.

§ 1º As prestadoras de serviços de ativos virtuais deverão manter a segregação patrimonial dos recursos financeiros, ativos virtuais e respectivos lastros de titularidade própria daqueles detidos por conta e ordem de terceiros.

§ 2º Os recursos financeiros, ativos virtuais e respectivos lastros detidos por conta e ordem de terceiros não respondem, direta ou indiretamente, por nenhuma obrigação das pessoas jurídicas mencionadas no caput, não podem ser objeto de arresto, sequestro, busca e apreensão ou qualquer outro ato de constrição judicial em função de débitos de responsabilidade destas últimas.

§ 3º Os recursos financeiros, ativos virtuais e respectivos lastros detidos por conta e ordem de terceiros não integrarão o patrimônio das pessoas jurídicas mencionadas no § 1º e:

I – não podem ser dados em garantia de obrigações assumidas por elas;

II - não compõem o ativo das prestadoras de serviços de ativos virtuais e não se sujeitam à arrecadação nos regimes especiais das instituições autorizadas a funcionar pelo Banco Central do Brasil, à recuperação judicial e extrajudicial, à falência, à liquidação judicial e extrajudicial ou a qualquer outro regime de recuperação ou dissolução a que seja submetida; e

III – deverão ser restituídos na hipótese de decretação de falência, ou qualquer regime de concurso de credores, na forma prevista no art. 85, da Lei no 11.101, de 9 fevereiro de 2005.

Art. 14. A Lei nº 9.613, de 03 de março de 1998, passa a vigorar acrescida do seguinte art. 12-A:

“Art. 12-A. Ato do Poder Executivo Federal regulamentará a disciplina e o funcionamento do Cadastro Nacional de Pessoas Expostas Politicamente (CNPEP), disponibilizado pelo Portal da Transparência.

§ 1º Os órgãos e as entidades de quaisquer Poderes da União, dos Estados, do Distrito Federal e dos Municípios deverão encaminhar ao gestor CNPEP, na forma e na periodicidade definida no regulamento de que trata o caput, informações atualizadas sobre seus integrantes ou ex- integrantes classificados como pessoas expostas politicamente (PEP) na legislação e regulação vigentes.

§ 2º As pessoas referidas no art. 9º desta Lei incluirão consulta ao CNPEP entre seus procedimentos para cumprimento das obrigações previstas nos arts. 10 e 11 desta Lei, sem prejuízo de outras diligências exigidas na forma da legislação.

§ 3º O órgão gestor do CNPEP indicará em transparência ativa, pela rede mundial de computadores, órgãos e entidades que deixem de cumprir a obrigação prevista no § 1º deste artigo.

.....” (NR)

Art. 15. Até 31 de dezembro de 2029, ficam reduzidas a 0 (zero) as alíquotas dos seguintes tributos, devidos sobre a importação, a industrialização ou a comercialização de máquinas (hardware) e ferramentas computacionais (software) utilizadas nas atividades de processamento, mineração e preservação de ativos virtuais desenvolvidas por pessoas jurídicas de direito privado:

I - Contribuição para o PIS/PASEP;

COFINS;

III - Imposto de Importação - II; e

IV - Imposto sobre Produtos Industrializados - IPI.

§ 1º As reduções de alíquotas previstas no caput deste artigo aplicam- se exclusivamente às máquinas e ferramentas destinadas a empreendimentos que utilizarem em suas atividades 100% (cem por cento) de sua necessidade de energia elétrica de fontes renováveis e que neutralizem 100% (cem por cento) das emissões de gases de efeito estufa (GEE) oriundas dessas atividades.

§ 2º A alienação dos bens adquiridos nos termos do caput deste artigo que ocorrer no período de 3 (três) anos, contado da data de sua aquisição, a pessoas que não satisfaçam as condições e os requisitos estabelecidos para a fruição do benefício previsto neste artigo acarretará o pagamento pelo alienante do tributo dispensado, atualizado na forma prevista na legislação tributária.

§ 3º A inobservância do disposto no § 2º deste artigo sujeita ainda o alienante ao pagamento de multa e juros moratórios previstos na legislação em vigor para a

hipótese de fraude ou falta de pagamento do tributo devido.

§ 4º Ato do Poder Executivo atribuirá a um ou mais órgãos ou entidades da Administração Pública Federal a competência para autorizar e fiscalizar a concessão do benefício de que trata o caput deste artigo.

§ 5º Ato do Poder Executivo atribuirá a um ou mais órgãos ou entidades da Administração Pública Federal a competência para autorizar e fiscalizar a concessão da isenção de que trata o caput deste artigo.

Art. 16. Esta Lei entra em vigor após decorridos 180 (cento e oitenta) dias de sua publicação oficial, exceto no que tange ao disposto no parágrafo único do art. 9 º, que passa a vigorar na data de sua publicação.

Sala das Sessões,

, Presidente

, Relator

TRECHO DAS NOTAS TAQUIGRÁFICAS DA SESSÃO DELIBERATIVA ORDINÁRIA – SEMIPRESENCIAL, REALIZADA EM 26/04/2022, REFERENTE A ADEQUAÇÕES DE TEXTO À EMENDA Nº 6-PLEN, SUBSTITUTIVO DO PL Nº 4401/2021, E AO SEU ACATAMENTO EM PLENÁRIO PELO RELATOR DO PROJETO, SENADOR IRAJÁ.

……..

O SR. IRAJÁ (Bloco Parlamentar PSD/Republicanos/PSD - TO. Para proferir parecer.) – (...)

Mas para os esclarecimentos, Presidente, devidos, eu gostaria de destacar primeiramente as ponderações do Senador Portinho, que, no art. 3º, leia-se:

> Para os efeitos desta lei, considera-se ativo virtual a representação digital de valor que pode ser negociada ou transferida por meios eletrônicos e utilizada para a realização de pagamentos ou com propósito de investimentos, não incluídos (...).
>
> O §2º, onde fica expressamente, textualmente contemplado que:
>
> Fica autorizada a abertura de conta em prestadoras de serviços de ativos virtuais e a realização de operações com ativos virtuais e seus produtos derivados por órgãos e entidades da administração pública, nas hipóteses previstas em regulamento a ser editado por ato do Poder Executivo.

Acatando assim, parcialmente, a emenda apresentada, e muito bem-vinda, pelo Senador Portinho.

No que se refere à NFT, que é uma espécie de certidão digital de um serviço, muitos conhecem até como uma espécie de fundo, que pode inclusive ser utilizada para lançar, por exemplo, uma NFT de produção de soja, da safra de um ano

futuro, que essa matéria poderá ser, sim, regulada pelo Executivo em ato posterior à aprovação e caso essa lei seja sancionada pelo Presidente da República, ou seja, não ficando prejudicada a sua sugestão. Mas nós não podemos fazê-lo neste momento. Portanto, acatada parcialmente a sua emenda.

Em relação às considerações do Senador Flávio Arns a quem eu quero aqui novamente agradecer pela contribuição que deu a esta Casa, apresentando essa matéria na condição de autor, e que eu tive honrosamente o trabalho de relatar essa matéria, que no art. 10:

O Decreto-Lei nº 2.848, de 07 de dezembro de 1940 (Código Penal) passa a vigorar acrescido do seguinte artigo 171-A:

Fraude em prestação de serviços de ativos virtuais, valores mobiliários ou ativos financeiros

> Art. 171-A. Organizar, gerir, ofertar carteiras ou intermediar operações envolvendo ativos virtuais, valores mobiliários ou quaisquer ativos financeiros com o fim de obter vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento.

A pena inicialmente prevista no substitutivo é de reclusão, de 4 a 8 anos, e multa. Por sugestão do Presidente Rodrigo Pacheco, que acolho como complementação de voto, nós iremos adequá-la estabelecendo como marco temporal de 2 a 6 anos de reclusão mais multa. Não é isso, Presidente? É uma proposta razoável, factível, e que, na condição de Relator, acolho na complementação de voto.

Inclusive, também há a tipificação – que é uma preocupação parece-me do Senador Flávio Arns –, para que nós não sejamos nem um pouco complacentes com crimes que são recorrentes, como as chamadas pirâmides financeiras. São golpes financeiros promovidos em todo o país. Infelizmente, segundo dados oficiais, esses golpes chegaram ao patamar de R$2,5 bilhões, só no ano de 2021, e precisam ser punidos com todo o rigor da lei. É por isso que estamos aqui tipificando esse crime que não estava previsto no Código Penal brasileiro, muito menos nos crimes de colarinho branco. Seria o crime denominado e conhecido popularmente como crime de pirâmide financeira.

Com relação às ponderações da Senadora Rose, eu queria tranquilizá-la. Na Emenda 16 já está contemplado o seu pedido, no próprio relatório. Nós tivemos o cuidado, Senadora Rose, de checar de novo o texto. Se puder, por gentileza, durante a discussão, valide o que estou dizendo, mas parece-me que a Emenda 16 já está contemplada no próprio relatório, o seu teor, o seu mérito.

Com relação à Emenda 17, nessa sim, nós poderíamos atender o pedido não na votação presente, mas na regulação pelo Poder Executivo. Essa foi a orientação da nossa equipe técnica, sem nenhum demérito à sua sugestão, à sua contribuição, que, V. Exa. sabe, é sempre muito bem-vinda, especialmente para me ajudar no trabalho legislativo.

Então são essas, Presidente, as minhas considerações, pedindo o apoiamento, fazendo um apelo de ajuda para que os colegas Senadores e Senadoras possam votar e aprovar essa matéria tão necessária e urgente para o país.

Obrigado.