

A REGULAMENTAÇÃO DAS CRIPTOMOEDAS COMO MEIO GARANTIDOR DE SEGURANÇA JURÍDICA

Lucas Fernandes Alves dos Reis¹

Andrea Medina Coeli²

RESUMO

Neste trabalho, para solução da problemática levantada, será utilizado o método de pesquisa explicativo, como meio para analisar e abordar as matérias pertinentes às criptomoedas. O objetivo é apresentar a regulamentação como solução para a garantia da segurança jurídica dos usuários de criptomoedas e da sociedade em geral. Por fim será utilizado o método de pesquisa bibliográfica, com base na Constituição Federal, direito administrativo, instrução normativa 1.888/2019, e obras pertinentes ao trabalho.

Palavras Chaves: Criptomoedas. Regulamentação. Segurança Jurídica.

REGULATION OF CRYPTOMOEDS AS A MEANS OF LEGAL SECURITY GUARANTEE

ABSTRACT

In this article, to solve the problem introduced, the method of research explanatory will be used as a way to analyze and explain the relevant matters with the cryptocurrencies. The goal is to present regulation as a solution to guarantee the legal certainty of cryptocurrency users, and society in general. In the end, research bibliographic method will be used, based on the Federal Constitution, administrative law, normative instruction 1,888 / 2019, and another articles relevant to the work.

Key Words: Cryptocurrencies. Regulation. Legal Certainty.

¹ Acadêmico(a) da 10ª etapa do curso de Direito da Universidade de Uberaba.

² Mestre e professora da Universidade de Uberaba. *E-mail.* medinacoeli@terra.com.br

1. INTRODUÇÃO

Há alguns anos o termo Criptomoeda não seria familiar, nem compreensível, em uma primeira abordagem, para praticamente todas as pessoas no mundo, mesmo as atuantes na área tecnológica ou no mercado financeiro. Atualmente o cenário é diferente. O bitcoin, a pioneira e mais negociada Criptomoeda, por exemplo, é conhecido por uma relevante quantidade de pessoas. A grande parcela conhece pelo menos superficialmente o assunto. Diante da relevância do assunto várias questões merecem atenção quanto a conceituação da, relativamente, nova tecnologia e de suas consequências perante o Estado e a sociedade.

Para o desenvolvimento desta pesquisa serão levantados, preliminarmente, os aspectos pertinentes a definição de criptomoedas, assim como seu modo de negociação e funcionamento, através da rede blockchain, desenvolvida juntamente com a criação do Bitcoin, entre 2008-09. Em seguida serão abordados os relevantes avanços tecnológicos que as criptomoedas possibilitam para o modo como as pessoas utilizam o dinheiro, como por exemplo, menores custos e maior celeridade para as transações, dentre outras vantagens relativas à sua utilização, e que serão elencadas no corpo dessa pesquisa.

Porém, em que pese o rol de avanços tecnológicos proporcionados pelo desenvolvimento das criptomoedas, prepondera a discussão quanto ao tratamento normativo desse segmento pelo Estado, vez que, apesar de todas as vantagens proporcionadas pela tecnologia, podem ser utilizadas para fins criminosos, como a lavagem de dinheiro ou a sonegação fiscal, já que, uma das características do sistema é anonimidade, ou a possibilidade do uso de pseudônimos. Sopesa também a necessidade de regulamentação para a definição da natureza jurídica desses ativos, e assim estabelecer seu tratamento legal perante o Estado, como por exemplo, a respeito da tributação que deverá incidir sobre seus usuários.

O escopo desta pesquisa é alvitrar a regulamentação estatal como meio capaz de proporcionar segurança jurídica aos usuários desse segmento, e, a própria coletividade. Contudo, sem com isso burocratizar o setor, ou obstar o desenvolvimento tecnológico que deu vida ao sistema, e vem, constantemente, aprimorando-o. Dessa maneira serão beneficiados os usuários, e toda a sociedade, possibilitando o crescimento mais sólido e confiável desse mercado no país.

2. CRIPTOMOEDAS: DEFINIÇÃO E MODO DE FUNCIONAMENTO

As criptomoedas são moedas digitais, ou seja, dinheiro que existe apenas virtualmente, dotadas de um nível avançado de segurança e privacidade, graças as tecnologias de criptografia e, portanto, não emitidas nem controladas por nenhuma entidade financeira estatal central, como um Banco Central.

A blockchain, ou cadeia de blocos, é a tecnologia base das criptomoedas, e foi desenvolvida com a criação do Bitcoin em 2008-2009. É um grande banco de dados virtual que registra as informações de todas as transações de determinada Criptomoeda realizadas, uma espécie de livro contábil online, que pode ser acessado por qualquer usuário. A rede é espalhada por todos os computadores, o que permite que cada um tenha sua própria cópia da blockchain.

É formada, como sugere o nome, por uma cadeia de blocos interligados, cada bloco é constituído pelo registro de diversas transações financeiras de um grupo determinado de usuários e detém uma assinatura digital única, denominada hash³ (também proof of work, no caso do Bitcoin). Imagine uma corrente de blocos, as hash são os elos de cada parte da corrente. A transação obrigatoriamente deve ser aprovada pela maioria dos chamados nodes, ou mineradores, que são na realidade os computadores que efetivamente estão inscrevendo as transações no bloco. Os mineradores são os detentores dos hardwares que processam os problemas matemáticos complexos, em troca de uma recompensa financeira do sistema e com isso criam os blocos na rede. Cada transação inserida no bloco por meio do trabalho de processamento do minerador é chamada de prova de trabalho. O processamento para alcançar a prova de trabalho é aleatório e com baixa probabilidade de acerto, basicamente através de tentativas e erros, assim quanto mais poder de processamento tem o hardware menos tempo ele levará para solucionar os cálculos do bloco. Quando o minerador produz um bloco utilizando a prova de trabalho, e este bloco é aprovado por uma maioria de outros nodes mineradores, ele é recompensado com um pagamento em criptomoedas proporcional às provas de trabalho realizadas.

O valor desse pagamento é variável com o tempo, mas, no caso do Bitcoin por exemplo, é de 12,5 BTC por bloco minerado desde 2017. Esse sistema de recompensa pela mineração também propicia a constante inserção de novas criptomoedas no mercado. Esse processo por outro

³ Função matemática expressada por um código com letras e números que representa e assina os dados registrados naquele bloco, e liga um bloco a outro, assim um bloco possui sua própria hash e também a do bloco anterior

lado tem um limite, escolhido arbitrariamente: 21 milhões de bitcoins. O número de Bitcoins adicionados por bloco é reduzido pela metade a cada 4 anos, e dessa forma sua quantidade em circulação só decresce com o tempo., em outras palavras: a adição de novas criptomoedas no mercado tem um limite, estima-se até que o último bitcoin será minerado em meados de 2140.

Quando a transação é aprovada pela maioria dos nodes ela passa a integrar o núcleo do bloco. A cada 10 minutos a rede blockchain se atualiza automaticamente, e na medida em que o bloco atinge determinado número de transações registradas e aprovadas pelos nodes do bloco, ele é "selado" por uma nova hash de um novo bloco a ser formado, e assim a rede se manterá sucessivamente.

Para que alguém possa hackear o conteúdo de um bloco ele obrigatoriamente terá que encontrar todas as hash antecedentes do seu alvo, já que uma hash é indissociável da anterior. A tarefa será tecnicamente impossível, pois cada formação de blocos é criada através de cálculos matemáticos complexos, além de ser distribuída para verificação entre milhares de nodes no mundo, algo impossível para os computadores atuais. No caso de alguma informação ser alterada, o hash irá mudar, será completamente novo, e assim é possível que os nodes possam verificar a fraude e então invalidá-lo. Dessa forma é garantida a segurança, pois o sistema inviabiliza as fraudes, cópias e alterações de dados vitais aos usuários. A rede também não é passível de pane já que por ser descentralizada entre todos os nodes que a mantém e um único ente não teria como derrubá-la.

2.1. CRIPTOGRAFIA NA REDE BLOCKCHAIN

Todas as transações realizadas com criptoativos e inseridas na blockchain são seguras e privadas para quem as transaciona uma vez que estão acobertadas pela tecnologia de criptografia. Essa tecnologia é a mesma utilizada em aplicativos de mensagens, como o WhatsApp e o Telegram por exemplo, para garantir a privacidade das mensagens. No contexto das criptomoedas ela é praticamente impossível de ser quebrada. A criptografia funciona através da existência de duas chaves para cada usuário: uma pública e uma privada⁴.

⁴ A chave privada funciona como uma senha que permite a assinatura das transações feitas pelo usuário, e assim possibilita o envio ou o recebimento de criptomoedas. É a senha privada pessoal de cada usuário, e através dela é possível o acesso à conta de fundos e seu uso. Pode ser comparável a senha de uma conta bancária por exemplo. Dessa maneira, por ser única a cada um, só o seu detentor pode ter acesso a própria conta de fundos, e mais ninguém. É composta geralmente por até 78 números e/ou letras aleatórios, o que equivale a até 256 bits de informação. Quanto

A chave pública é o endereço do usuário na rede, e por meio de uma complexa função matemática, é extraído dela o “Endereço Público”⁵ Este endereço pode ser compartilhado com outros usuários caso seja de interesse do detentor da chave realizar uma operação, seja de recebimento ou transferência de criptoativos. O Endereço Público figura-se como uma carteira virtual onde serão armazenadas, recebidas ou enviadas as criptomoedas negociadas.

Estas duas chaves, pública e privada, são indissociáveis. E o procedimento para gerá-las segue uma ordem exata: primeiro é gerado uma chave privada, isto pode ser feito em diversos sites ou programas que tornam aleatórios dados e assim criam uma chave. Um exemplo destes é o site www.walletgenerator.net. Automaticamente é gerada uma chave pública relativa à chave privada pré-criada, através de uma relação matemática entre elas. Para cada chave privada sempre existirá uma chave pública única e específica correlata. A partir da chave pública advirá um endereço público, conforme mencionado anteriormente, e existirá também uma relação matemática única entre eles. Então, à semelhança da relação entre as chaves público-privada, para cada chave pública haverá associado um endereço público único.

Essa tríade de chaves e endereço constitui a base criptográfica da rede blockchain. Graças a ela os usuários não são furtados por hackers, já que a chave privada é inviolável uma vez associada a chave pública, sendo esta última possível de acesso e confirmação de legitimidade pelos demais usuários.

Esse sistema de criptografia, juntamente com sua interação com toda a cadeia de blocos e o trabalho dos mineradores, permite a correção do maior possível problema na utilização das criptomoedas: o gasto duplo. O gasto duplo é a possibilidade que um usuário utilize a mesma criptomoeda duas vezes. Em tese isso deveria ser possível por serem as criptomoedas em essência arquivos digitais, e estes últimos são passíveis de cópias e envios infinitos, como um arquivo de música mp3, por exemplo. Porém, isso é impossível na blockchain, pois para uma transação ser validada e inscrita no bloco ela necessita receber confirmações de uma maioria dos nodes

menos componentes possuir a chave menos segura ela será. Um exemplo de chave privada: 333589873763554900277288289919987. Para criá-la são utilizadas as leis da probabilidade matemática, e cada vez que uma nova chave é gerada possuirá um número único. Com até 78 dígitos o grande número de combinações prováveis será tão aleatório que é correto afirmar que ninguém no mundo possuirá uma chave idêntica à de outra pessoa.

⁵ (no caso do bitcoin é Endereço Bitcoin ou Carteira de Bitcoins) do usuário. É palpável uma analogia com o e-mail, caso alguém deseje receber uma mensagem de e-mail ela necessitará passar seu endereço de e-mail para a outra pessoa, para assim esta última localizá-la na rede e então enviar a mensagem. O Endereço Público é constituído por uma combinação de 32 letras e números, com 160 bits, e é derivado diretamente da chave pública.

mineradores atuantes no bloco, e como cada bloco na rede é adicionado por ordem cronológica e de poder de processamento (os de maior são adicionados primeiro), duas transações idênticas não serão confirmadas ao mesmo tempo, apenas uma será, e a outra será invalidada pelos mineradores.

Fernando Ulrich exemplifica esse processo e sua correlação com o sistema de chaves público-privada:

As transações são verificadas, e o gasto duplo é prevenido, por meio de um uso inteligente da criptografia de chave pública. Tal mecanismo exige que a cada usuário sejam atribuídas duas “chaves”, uma privada, que é mantida em segredo, como uma senha, e outra pública, que pode ser compartilhada com todos. Quando a Maria decide transferir bitcoins ao João, ela cria uma mensagem, chamada de “transação”, que contém a chave pública do João, assinando com sua chave privada. Olhando a chave pública da Maria, qualquer um pode verificar que a transação foi de fato assinada com sua chave privada, sendo, assim, uma troca autêntica, e que João é o novo proprietário dos fundos. A transação – e, portanto, uma transferência de propriedade dos bitcoins – é registrada, carimbada com data e hora e exposta em um “bloco” do blockchain (o grande banco de dados, ou livro-razão da rede Bitcoin). A criptografia de chave pública garante que todos os computadores na rede tenham um registro constantemente atualizado e verificado de todas as transações dentro da rede Bitcoin, o que impede o gasto duplo e qualquer tipo de fraude (ULRICH, 2014)

Isso permite que as criptomoedas sejam realmente funcionais, já que tudo que é inserido na rede é público, mas ao mesmo tempo, para cada usuário, existe a segurança ante possíveis fraudadores e a privacidade inerente as suas informações. O problema do gasto duplo também impossibilitaria a manutenção da moeda, pois o que garante valor ao dinheiro é sua escassez, e então, se todos pudessem multiplicar o dinheiro a seu bel prazer o sistema monetário seria impraticável. Não haveria mais necessidade em se discutir o valor e conseqüentemente a necessidade do dinheiro. As criptomoedas, desta feita, não teriam mais valor.

Para finalizar, as criptomoedas podem ser negociadas entre os usuários com a utilização da chave pública como espécie de “conta” em que serão retiradas ou recebidas as moedas, mas, podem também, e geralmente são, negociadas em corretoras de câmbio próprias: as Exchanges, ambiente no qual podem ser negociadas várias criptomoedas ao preço da moeda do país em que funcionam e são regulamentadas.

3. BREVE EXPOSIÇÃO DAS CRIPTOMOEDAS MAIS NEGOCIADAS

O Bitcoin é a criptomoeda pioneira, foi desenvolvida no interstício de 2008-2009 por um criador (ou criadores) anônimo, utilizando o pseudônimo Satoshi Nakamoto. Trata-se de uma criptomoeda, par-a-par, e, assim como todas: descentralizada, e desde sua criação até hoje é a mais utilizada. Conforme Fernando Ulrich:

Bitcoin é uma moeda digital peer-to-peer (par-a-par ou simplesmente, de ponto a ponto), de código aberto, que não depende de uma autoridade central. Entre muitas outras coisas, o que faz o Bitcoin ser único é o fato de ele ser o primeiro sistema de pagamentos global totalmente descentralizado. (ULRICH, 2014)

A proposta do Bitcoin foi levantada por seu criador, ou criadores, como opção à bolha financeira americana em 2008, modelo financeiro centralizado, regido por determinados interesses políticos e econômicos, que nem sempre se traduzem em uma situação favorável as pessoas, como exemplifica a crise. Seu conceito, bem como intuito de sua criação, é o de ser um sistema de troca monetária, nesse sentido, semelhante ao papel-moeda que utilizamos cotidianamente, porém, realizado exclusivamente por meio virtual e de forma intrinsecamente descentralizada. Não existe um órgão financeiro central, como o Banco Central Brasileiro por exemplo, que regule, emita, controle ou mesmo interfira na circulação do ativo. Esse poder é dividido entre todos os usuários da criptomoeda. Esses aspectos são pressupostos comuns a todas as criptomoedas criadas após o Bitcoin.

O protesto ao sistema financeiro vigente fica nítido no texto que foi inscrito no primeiro bloco de Bitcoin minerado por Nakamoto: “The Words 03/Jan/2009 Chanceler à beira do segundo resgate aos bancos (tradução do autor) ⁶”

Entre 2011 e 2012, o uso mais acentuado do Bitcoin foi em mercados negros na internet obscura, conhecida por darknet. Tal fato agregou inclusive uma má reputação para a novel tecnologia. O anonimato conferido as transações tornaram o Bitcoin interessante para negociantes desse submundo. Um exemplo predominante foi o site Silk Road, dedicado ao comércio de produtos ilícitos, especialmente narcóticos. Estima-se que o total de transações mensais da plataforma alcance cerca de 1,2 milhão de dólares.

⁶ O texto refere-se a uma manchete do jornal inglês The Times sobre uma das tentativas fracassadas do governo britânico em alavancar a economia, e marca também a data da mineração do bloco gênese: primordial da estrutura blockchain.

Uma característica marcante no bitcoin, e nas demais criptomoedas é a escassez. Como o protocolo impossibilita o gasto-duplo, e todas as transações são verificadas para só então serem registradas, como exposto inicialmente, um determinado bitcoin só pode existir em apenas uma carteira em dado momento, e seu detentor tem o poder de transferi-lo a quem desejar. Esse fator aliado a taxa de mineração limitada, de 21 milhões, propiciam a escassez dos ativos, nesse ponto, à semelhança dos metais preciosos, como o ouro, daí o nome “mineração”.

Outra característica comum é a volatilidade. A popularidade do Bitcoin, por exemplo, vem crescendo desde 2013 para o público em geral, e, assim seu preço tem aumentos constantes, e sofre baixas também constantes, graças as oscilações do mercado, em virtude da oferta e demanda, e da batalha especulativa, influenciada em grande medida pela ação da imprensa, conforme ressalta Ulrich:

Esses ajustes se assemelham a bolhas especulativas tradicionais: coberturas da imprensa otimistas em demasia provocam ondas de investidores novatos a pressionar para cima o preço do bitcoin. A exuberância, então, atinge um ponto de inflexão, e o preço finalmente despenca. Novos entrantes ávidos por participar correm o risco de sobrevalorizar a moeda e perder dinheiro em uma queda abrupta. (ULRICH, 2014)

Em dezembro de 2017 a moeda atingiu seu patamar máximo até hoje, com valor cambial de 20 mil dólares.

Após o bitcoin muitas outras criptomoedas foram desenvolvidas: as altcoins⁷, termo que denomina qualquer outra criptomoeda que não o Bitcoin.

Entre os benefícios das criptomoedas, elencadas na obra de Fernando Ulrich, base desta pesquisa, destaca-se o baixo custo e a celeridade das transações, uma vez que não dependem de terceiros intermediários para serem concretizadas como as redes de pagamento convencionais. Este fator incentiva a existência dos micropagamentos e suas inovações.

Também pesa a possibilidade de serem utilizadas como reserva de valor, possibilitada pela característica da escassez, o que permite por exemplo um escape a pessoas vivendo em nações com controle de capital estrito.

O número total de bitcoins que podem ser minerados é limitado e não pode ser manipulado. Não há autoridade central que possa reverter transações e impedir trocas de bitcoins entre países. O bitcoin dessa forma, proporciona uma válvula

⁷ Mais de 1.369 foram criadas, e o número cresce a cada dia, mesmo porque as configurações comuns a todas as criptomoedas estão sempre presentes, quais sejam a estrutura Blockchain e o sistema de Criptografia. As mais predominantes, a título de exemplo: Ethereum, Ripple, Dash, Litecoin, Monero, Nxt, Synereo, Siacoin, dentre muitas outras.

de escape para pessoas que almejam uma alternativa à moeda depreciada de seu país ou a mercados de capital estrangulados. (ULRICH, 2014)

De outra sorte, existe a possibilidade de seu uso para fins criminosos, como por exemplo a lavagem de dinheiro, ou a compra e venda de produtos ilícitos já que o sistema apesar de registrar e tornar públicas as transações, não vincula estas informações a dados pessoais dos usuários, permitindo inclusive o uso de pseudônimos. Isto já ocorreu na utilização do Bitcoin no mercado negro da DarkNet, conforme já mencionado. Este fator, principalmente, levanta questionamentos sobre a necessidade de sua regulamentação perante os governos, tal ponto será apresentado adiante.

4. A REGULAMENTAÇÃO DAS CRIPTOMOEDAS

O Estado historicamente figura como o detentor constituído da prerrogativa de elaboração das normas reguladoras das atividades humanas de um determinado território, e quando se volta a atenção para o próprio conceito de atividade humana é indissociável sua relação com a economia. A economia é regida tradicionalmente pela atividade regulamentadora do Estado, tal regramento seja em menor ou maior escala, abre a possibilidade de se perseguir a diminuição da desigualdade, através da mais justa distribuição de renda, bem como pela melhor e mais eficaz utilização das riquezas do território abrangido pela regulamentação, e aliado a isso propiciar o incentivo à livre iniciativa e concorrência, gerando dessa maneira mais empregos para as pessoas e assim almejando cada vez mais alcançar padrões de vida melhores para a coletividade. A leitura do artigo 170 da Carta Magna brasileira fundamenta esse entendimento: A ordem econômica, fundada na valorização do trabalho humano e na livre iniciativa, tem por fim assegurar a todos existência digna, conforme os ditames da justiça social [...]

O dinheiro é o instrumento base que constitui o sistema financeiro de praticamente todas as economias mundiais, e esse meio é regulado pela conveniência da política monetária de cada Estado. No Brasil a competência para emitir moeda é da União, através do Banco Central, conforme o art. 164 da Constituição Federal de 1988.

As criptomoedas, em que pese a discussão de sua natureza como moeda ou ativo, podem ser utilizadas como meio de troca à semelhança do dinheiro tradicional, mesmo que não

universalmente aceito por todos, inclusive como investimento e reserva de valor, mesmo que revestidos de volatilidade, então como confrontar sua regulamentação perante o Estado?

Abaixo uma apertada exposição de como está avançando essa discussão a respeito da regulamentação no cenário mundial:

4.1. EXPOSIÇÃO EXEMPLIFICATIVA DA REGULAMENTAÇÃO EM ÂMBITO MUNDIAL

Nos Estados Unidos a regulamentação é tema conturbado. O inspetor do Tesouro Americano, Steven Mnuchin afirmou, em Novembro de 2017, que iria rever as práticas do FinCen (The Financial Crimes Enforcement Network)- agência que coleta e analisa informações relativas a movimentações financeiras com o intuito de combater crimes financeiros - em relação as criptomoedas, perante a existência de seu uso para crimes como lavagem de dinheiro e financiamento ao terrorismo, e que não são um meio de pagamento legítimo perante nenhum Estado americano. A SEC (Securities and Exchange Commission) órgão semelhante a CVM do Brasil, indeferiu projetos de produtos financeiros relacionados às criptomoedas, como ETFs de Bitcoin. ACFTC (U.S Commodity Futures Trading Commission), de outra maneira, classificou o Bitcoin como uma commodity e anunciou que qualquer atividade criminosa relacionada com seu uso sob sua jurisdição estará sob sua autoridade. A entidade permitiu também que a CME (Bolsa de Chicago) e a CBOE (Chicago Board Options Exchange) elaborassem futuros de Bitcoin.

Na China, em setembro de 2017, o governo proibiu todas as instituições financeiras e empresas de soluções de pagamento de fazerem uso ou aceitarem criptomoedas. Proibiu também o funcionamento de todas as Exchanges do país. Esse episódio em específico ficou conhecido com ChinaBan. Essas medidas constituíram um duro golpe para o criptomercado, vez que a China era o maior mercado desse setor no mundo, e concentrava 80% e toda a atividade de mineração global.

Na Coreia do Sul por sua vez, em 2017, os reguladores propuseram uma alteração na lei de transações financeiras eletrônicas vigente (Electronical Financial Transaction Act) que passaria a regulamentar negócios envolvendo criptomoedas, como por exemplo a atividade das corretoras, dos negociantes, emissores e gestores. Já em dezembro de 2017 a comissão de serviços financeiros do país proibiu a negociação de futuros do Bitcoin. As Exchanges por outro lado não sofreram limitações.

O Japão foi a nação que mais evoluiu em termos de regulamentação específica de criptomoedas: em maio de 2016 foi aprovada uma lei que regulamentava as moedas digitais e em abril de 2017 a Agência de Serviços Financeiros (FSA) regulamentou as criptomoedas como meio de pagamento, colocando-as na mesma configuração jurídica do dinheiro tradicional. Essas políticas foram importantíssimas para o crescimento desse setor no país, que hoje concentra o maior número de transações com bitcoins, por exemplo. Em setembro de 2017 a FSA concedeu as primeiras licenças, sob exigências severas de transparência e aprimoramento do sistema computacional, a 11 corretoras de criptomoedas.

4.2. A REGULAMENTAÇÃO NO BRASIL

Inexistia regulamentação específica no Brasil até o advento da Instrução Normativa Nº 1.888 da Receita Federal, com importantes alterações feitas pela Instrução Normativa 1899 de 10 de julho de 2019. A novel legislação abarcou expressamente a definição para fins jurídicos do que é configurado como Criptoativo e Exchange de Criptoativos, conforme depreende-se da leitura de seu 5º artigo:

Art. 5º Para fins do disposto nesta Instrução Normativa, considera-se:

I - Criptoativo: 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; e

II - Exchange de criptoativo: a pessoa jurídica, ainda que não financeira, que oferece serviços referentes a operações realizadas com criptoativos, inclusive intermediação, negociação ou custódia, e que pode aceitar quaisquer meios de pagamento, inclusive outros criptoativos.

Parágrafo único. Incluem-se no conceito de intermediação de operações realizadas com criptoativos, a disponibilização de ambientes para a realização das operações de compra e venda de criptoativo realizadas entre os próprios usuários de seus serviços.

A norma avançou ainda mais ao obrigar todas as Exchanges a prestarem informações à Receita Federal de todas as transações de seus usuários: nome dos negociantes, quantia movimentada, datas e taxas de operação pagas, dentre outras. Tal previsão está expressa no artigo 7º e incisos da aludida norma:

Art. 7º Deverão ser informados para cada operação:

I - Nos casos previstos no inciso I e na alínea “b” do inciso II do caput do art. 6º:

a) a data da operação;

b) o tipo da operação, conforme o § 2º do art. 6º;

- c) os titulares da operação;
- d) os criptoativos usados na operação;
- e) a quantidade de criptoativos negociados, em unidades, até a décima casa decimal;
- f) o valor da operação, em reais, excluídas as taxas de serviço cobradas para a execução da operação, quando houver;
- g) o valor das taxas de serviços cobradas para a execução da operação, em reais, quando houver; e

II - No caso previsto na alínea “a” do inciso II do art. 6º:

- a) a identificação da exchange;
- b) a data da operação;
- c) o tipo de operação, conforme o § 2º do art. 6º;
- d) os criptoativos usados na operação;
- e) a quantidade de criptoativos negociados, em unidades, até a décima casa decimal;
- f) o valor da operação, em reais, excluídas as taxas de serviço cobradas para a execução da operação, quando houver;
- g) o valor das taxas de serviços cobradas para a execução da operação, em reais, quando houver; e

§ 1º Em relação aos titulares da operação, devem constar das informações a que se refere este artigo:

I - O nome da pessoa física ou jurídica;

II - O endereço;

III - O domicílio fiscal;

IV - O número de inscrição no Cadastro de Pessoas Físicas (CPF) ou no Cadastro Nacional da Pessoa Jurídica (CNPJ), conforme o caso, ou o Número de Identificação Fiscal (NIF) no exterior, quando houver, no caso de residentes ou domiciliados no exterior; e

V - As demais informações cadastrais.

§ 2º Caso os titulares das operações sejam residentes ou domiciliados no Brasil, a prestação da informação relativa ao número de inscrição no CPF ou no CNPJ, conforme o caso, é obrigatória a partir da data da entrega do primeiro conjunto de informações, prevista no § 1º do art. 8º.

§ 3º Caso os titulares das operações sejam residentes ou domiciliados no exterior, a prestação das informações relativas ao país do domicílio fiscal, endereço e NIF no exterior é obrigatória a partir da entrega de informações a ser efetuada em janeiro de 2020, referentes às operações realizadas em dezembro de 2019.

§ 4º A entrega das informações relativas ao endereço da wallet de remessa e de recebimento, se houver, é obrigatória apenas na hipótese de recebimento de intimação efetuada no curso de procedimento fiscal.

Essa obrigação de prestação de informações estende-se às pessoas físicas investidoras de forma independente nesse mercado, sem recorrerem às Exchanges, ou quando utilizadas Exchanges domiciliadas no estrangeiro, no caso de extrapolarem 30.000 reais de criptomoedas transacionadas mensalmente, nos termos do art. 6º, inciso II, “a” e “b”:

Art. 6º Fica obrigada à prestação das informações a que se refere o art. 1º:

I - A exchange de criptoativos domiciliada para fins tributários no Brasil;

II - A pessoa física ou jurídica residente ou domiciliada no Brasil quando:

- a) as operações forem realizadas em exchange domiciliada no exterior; ou
- b) as operações não forem realizadas em exchange.

§ 1º No caso previsto no inciso II do caput, as informações deverão ser prestadas sempre que o valor mensal das operações, isolado ou conjuntamente, ultrapassar R\$ 30.000,00 (trinta mil reais)

A partir da mencionada Instrução Normativa, para além da obrigação tributária com o fisco, está acrescido o dever de prestar todas as informações relativas às movimentações financeiras realizadas, determinadas no art. 7º, inciso I, grafado anteriormente.

A nova legislação trouxe uma enormidade de aspectos positivos para o usuário do setor, vez que em primeiro momento contempla as definições para fins do direito do que é Criptoativo, que agora afasta seu tratamento como moeda legal, e Exchange, e também obriga as pré-definidas Exchanges a prestar todas as informações pessoais e relativas as transações financeiras feitas pelos usuários, o que acarreta uma maior transparência da utilização desses ativos, dificultando assim a ação de usuários para fins ilegais, como a lavagem de dinheiro e a sonegação fiscal.

Por outro lado, a maior preocupação do mercado é que a medida poderá dificultar as inovações possíveis de serem desenvolvidas no setor, como por exemplo através do aumento de custos operacionais para poderem obedecer a regra de registro de toda e qualquer operação, o que poderia prejudicar a sobrevivência de muitas pequenas empresas novas no setor, que ainda possuem limitação de recursos disponíveis para adequação.

5. A REGULAMENTAÇÃO COMO MEIO GARANTIDOR DA SEGURANÇA JURÍDICA

A regulamentação, entre muitos fatores, propicia a segurança jurídica, pois, com leis pré-estabelecidas, garantimos o instituto do direito adquirido, o dever de cumprimento pelo Estado de suas funções estabelecidas em lei, com a indissociável junção ao princípio da legalidade, e como finalidade é alcançada a paz jurídica, consistente na confiabilidade dos cidadãos de que suas condutas, quando permitidas ou não expressamente proibidas pela norma, estarão garantidas pelo Estado Democrático de Direito. Conforme Moreira Neto (2006, p. 285 apud Wagnacker, 2016):

O Estado é instrumento da sociedade e sua existência só tem sentido se estiver a serviço de todos e de cada um. Por isso, justifica-se a confiança que legitimamente os membros da sociedade nele depositam, não se admitindo que os agentes públicos possam desempenhar suas funções traíndo essa confiança.

Ao tratar a temática do mercado das criptomoedas é imperioso se discutir sua posição em relação à segurança jurídica. As criptomoedas são descentralizadas, o que significa não estarem obrigadas a nenhum ente central, nenhum órgão estatal as controla ou supervisiona, tal função é distribuída entre seus usuários. Desta feita sem lei expressa que as normatize, e assim confira proteção jurídica às pessoas que as utilizem, o manto da segurança jurídica é retirado, para não dizer atacado.

A fragilidade que acarreta a falta desse princípio é constatada no campo da utilização das criptomoedas para a prática de crimes, como o branqueamento de capitais, financiamento do terrorismo, compra e venda de produtos ilícitos, dentre outros. Isso ocorre graças ao anonimato no qual as transações estão inseridas. O próprio Bitcoin como já mencionado anteriormente já foi amplamente utilizado para compra de drogas no mercado negro da internet obscura (deep web) através do site Silk Road, entre 2011-2012. Segundo Mariana Dionísio de Andrade:

Há muitas questões quanto à ausência de regulamentação e suas implicações. Há um justificável temor de que as moedas digitais tornem mais fáceis os crimes como lavagem de dinheiro, pirâmides financeiras, invasão de sistemas bancários, evasão de divisas, estelionato e demais delitos relacionados ao uso ilícito da tecnologia. As facilidades de acesso às transações via bitcoins podem atrair usuários que pretendem transgredir no ambiente real limites estabelecidos pelo que a lei ainda prevê apenas no mundo real. (ANDRADE, 2018, p. 51)

Além dessa utilização criminosa, as corretoras e os possuidores individuais de criptomoedas, estão sujeitos ao furto do patrimônio por ataques de hackers. A corretora Binance, umas das maiores do mundo, foi alvo de um ataque hacker, no dia 07/05/2019, onde foram movimentados em uma única movimentação fraudulenta 7 mil Bitcoins, avaliados em cerca de 160 milhões de reais à época.

O Estado tem entre suas atribuições a garantia da segurança pública, desta maneira é sua obrigação a efetivação desta segurança no território de abrangência de sua chancela, sob pena de inobservância a manutenção da segurança jurídica, e assim tais crimes devem ser alvo da persecução penal do Estado, consoante expressa o artigo 144 da Constituição Federal: A segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio, (...).

As criptomoedas, sob esta perspectiva, devem possuir regulamentação específica, vez que, como já mencionado, possuem maior facilidade em serem utilizadas maliciosamente.

Outro aspecto positivo no estabelecimento de regulamentação específica para o tema, reside na possibilidade de o Estado tributar as criptomoedas, dessa forma possibilitando a arrecadação de recursos que podem e devem ser utilizados na ampla gama de serviços públicos fornecidos à população, como saúde, segurança, educação etc. Esse terreno já é alvo de algum regramento no Brasil. As Exchanges, como sendo pessoas jurídicas já estão obrigadas ao pagamento das obrigações fiscais à Receita Federal. As pessoas físicas devem autodeclarar suas criptomoedas no Imposto de Renda, caso os investimentos superem 35 mil reais, conforme o tópico 607 do Documento de Perguntas e Respostas da Receita Federal.

De outra sorte, de acordo com a pesquisa do autor, as críticas levantadas a respeito do estabelecimento de regulamentações próprias para este campo estão relacionadas ao cerne da própria da ideia de criptomoeda: descentralização e liberdade financeira, conforme perseguidas por Nakamoto com a criação do bitcoin. A partir do momento em que o Estado cria normas para a limitação do uso das criptomoedas passa a existir a figura de um terceiro ente, regulamentador e controlador do sistema, e assim não haveria que se falar mais em descentralização.

A Escola Austríaca de Economia, conforme Molyneux (2011, p.13), levanta a Teoria do Interesse Privado, como crítica ao gradativo aumento do intervencionismo do Estado, considerando as regulações como fruto de interesses privados e não para o bem do interesse público: “Quando surge um problema, a demanda (para soluções do governo) não vem mais do povo, mas preferencialmente de grupos que irão beneficiar-se do aumento de regulação”.

Desta proposição, infere-se que o aumento de políticas intervencionistas sobre as criptomoedas traduzir-se-iam como mecanismos de salvaguarda de interesses privados de quem controla e se beneficia do poder do Estado, na contramão assim dos aspectos originais de descentralização e do total controle dos usuários das criptomoedas sobre seu uso.

Outra crítica levantada consiste na premissa de que o ambiente virtual do qual existem e dependem as criptomoedas deveria ser ambiente livre de normas jurídicas estatais, por não deter limitação territorial e dessa forma, qualquer tentativa de regulamentação feita pelos Estados estará determinadamente destinada ao fracasso. Assim, dada a falta de limite territorial, nenhum Estado conseguiria deter o controle normativo das atividades intrínsecas de seu ambiente.

No entanto tal posicionamento é extremamente falho, vez que considera o ambiente virtual como um fim, porém, sua configuração como meio para a realização de atividades ilícitas, como a venda de drogas, que acarretam efeitos materiais no território físico dos países. Desta feita, é

preponderante o posicionamento de que os países devem possuir leis próprias para regulação do ambiente virtual. De tal sorte, cada Estado exerce sua jurisdição, e estabelece normas para regulação da vida civil dos usuários em seu território e para punição de ilícitos civis, penais e administrativos que possam eventualmente ser cometidos por meio do ciberespaço. E é nesse sentido que reside a busca pela segurança jurídica pelo Estado.

Três caminhos básicos de regulamentação das criptomoedas são sintetizados por David Chau (2017): a liberdade completa, com nenhuma regulamentação estatal; a liberdade de propriedade, porém com a regulamentação dos serviços de intermediação e operação, como por exemplo através de normas de fiscalização, como as estabelecidos na Instrução Normativa nº 1.888 da Receita Federal; e por fim a proibição total da propriedade, mineração e negociação, como o exemplo das anteriormente citadas medidas do governo da China para extinção desse mercado em seu território.

Conforme a pesquisa do autor, a proibição total mitiga as possibilidades positivas do setor em relação à economia, como exemplo da tributação, e da inovação tecnológica, além de obviamente restringir pesadamente a liberdade de propriedade e livre iniciativa das pessoas, esculpidas respectivamente nos artigos 5º, caput e 1º, IV da Constituição Federal de 1988. A liberdade completa, por outro lado, em nada previne o mau uso dos criptoativos, como no caso do cometimento de ilícitos, e ocasiona deficiência de proteção específica aos usuários do setor sobre seu patrimônio. O que gera muito mais prejuízo do que benefício ao Estado e a coletividade

Assim, a que prepondera em relação ao dever do Estado em garantir a segurança jurídica dos usuários de criptomoedas seria a segunda, com a garantia do direito de propriedade das criptomoedas a quem interessar, e, assim, em consonância ao elencado no caput do art. 5º da Constituição Federal de 1988. Porém, com o dever do Estado em fiscalizar a utilização desse capital digital, através de legislação específica, visto a complexidade da matéria, objetivando a proteção legal dos usuários, prevenção de atividades criminosas e, ou, prejudiciais aos interesses da coletividade.

6. CONSIDERAÇÕES FINAIS

No momento vigora apenas a instrução normativa supracitada no Brasil, que justamente disciplina os conceitos básicos do mercado, a exemplo da definição expressa de criptoativo e Exchange e o dever de prestação de informações, o que acarreta o entendimento de que o sistema jurídico brasileiro adotou esse caminho na direção a regulamentação, pelo menos neste primeiro momento.

A partir da revisão bibliográfica realizada foi possível abordar a relação entre a regulamentação das criptomoedas e a efetivação do princípio da segurança jurídica, princípio fundamental a manutenção de todo Estado Democrático de Direito. Afinal, é dever do Estado, sob a égide desse basilar princípio, a garantia das tutelas e pressupostos constitucionais vitais a sociedade, a exemplo da segurança pública e da ordem econômica e tributária. Nesse sentido, em que pese as inúmeras vantagens que as criptomoedas oferecem, como os baixos custos para a realização de transações, ou a sua utilização como salvaguarda de valor para pessoas residentes em países em crise econômica, não pode-se ignorar a possibilidade de sua utilização para fins ilícitos, como a prática de crimes, a exemplo da lavagem de dinheiro, sonegação tributária e negociação de produtos ilegais, graças a anonimidade presente nas transações. É fato lógico que estes delitos agredem violentamente as tutelas e pressupostos constitucionais supramencionados.

Portanto, se o uso livre da incidência de normas das criptomoedas possibilita o cometimento de infrações que coloquem em risco os interesses da coletividade e atentem contra os bens jurídicos protegidos por nosso ordenamento, é dever do Estado efetivar a garantia da segurança jurídica de seus cidadãos através de normas regulamentadoras.

Neste sentido, ao ser estabelecida legislação específica quanto a natureza e tratamento jurídico dessa tecnologia, é possível determinar a forma de tributação adequada para a matéria, e, assim, propiciar inúmeros benefícios a sociedade através da arrecadação de impostos sobre os usuários do setor, como por exemplo pelo incremento de recursos destinados ao setor público, a serem revertidos na saúde, educação, segurança, dentre vários outros segmentos necessários. Consequentemente os próprios usuários serão beneficiados: pelo manto de legalidade que estarão revestidos; pela chancela do Estado para com o setor, fator que pode impulsionar o mercado, através da maior solidez e confiabilidade proporcionada pelo reconhecimento do setor pelo Poder

Público, incentivando, assim, a adesão de novos usuários; e, claro, pelo crescimento econômico do país.

Porém, regulamentar não se traduz unicamente em proibir esse mercado, ou de estabelecer normas burocráticas e sufocantes em demasiado, obstando a inovação tecnológica, a ponto de forçar seus usuários a buscarem formas ilícitas de utilizarem suas criptomoedas.

A regulamentação menos combativa aos interesses dos usuários de criptomoedas, e que mantém observância ao dever de garantir a segurança jurídica pelo Estado, se daria pela implementação de normas de definição dos elementos do mercado, fiscalização e tributação do setor. A exemplo da instrução normativa supramencionada.

Assim, ante a pesquisa realizada, demonstra-se imperiosa a ação do Estado frente a esse mercado em crescimento, no sentido de estabelecer normas mais específicas, com vistas a garantir a segurança jurídica para seus usuários, e, conseqüentemente, para toda a coletividade.

REFERÊNCIAS

AMARAL, Antônio José Rodrigues. **Relação entre bitcoin, altcoins e moedas convencionais: uma análise quantitativa**. 2018. 61 f. Tese (Doutorado) - Curso de Economia, Departamento de Economia, Gestão, Engenharia Industrial e Turismo, Universidade de Aveiro, Aveiro, 2018. Disponível em: <https://ria.ua.pt/>. Acesso em: 22 out. 2019.

ANDRADE, Mariana Dionísio de. **TRATAMENTO JURÍDICO DAS CRIPTOMOEDAS: A DINÂMICA DOS BITCOINS E O CRIME DE LAVAGEM DE DINHEIRO**. *Revista Brasileira de Políticas Públicas*, [s.l.], v. 7, n. 3, p.45-59, 6 fev. 2018. Centro de Ensino Unificado de Brasília. Disponível em: <<https://www.publicacoesacademicas.uniceub.br/RBPP/article/view/4897/3645> >. Acesso em 04 out. 2019.

ASSAF, Alexandre. **O Banco Central e a Constituição Federal: uma análise contemporânea**. *Mega Jurídico*, 21 set. 2018. Disponível em: < <https://www.megajuridico.com/o-banco-central-e-a-constituicao-federal-uma-analise-contemporanea/> >. Acesso em: 05 out. 2019.

BRASIL. **Constituição da República Federativa do Brasil**. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.> Acesso em 21 out. 2019.

_____. Ministério da Fazenda. Secretaria da Receita Federal do Brasil. **Imposto sobre a renda-pessoa física. Perguntas e Respostas. Exercício de 2019, ano-calendário de 2018**. Disponível em: <<http://receita.economia.gov.br/interface/cidadao/irpf/2019/perguntao/perguntas-e-respostas-irpf-2019.pdf>.> Acesso em 16 out. 2019.

CHAU, David. **Bitcoin One Step Closer To Being Regulated In Australia Under New Antimoney Laundering Laws**. 22 out. 2017. Disponível em: <<http://mobile.abc.net.au/news/2017-10-23/bitcoin-one-step-closer-to-being-regulatedin-australia/9058582>>. Acesso em 23 out. 2019.

COINTELEGRAPH Brasil. **Como funciona a tecnologia Blockchain**. Guia para Iniciantes. Disponível em: <<https://br.cointelegraph.com/bitcoin-for-beginners/how-blockchain-technology-works-guide-for-beginners>.> Acesso em 04 out. 2019.

COSTA, Cynara de Barros. O sistema Bitcoin, as criptomoedas e o desafio de sua regulamentação pelo Direito. In: CARVALHO, Thomaz Jefferson; SILVA, Felipe Rangel da. **Temas avançados de direito eletrônico**. 23. ed. Belo Horizonte: Arraes Editores, 2018. cap. 3, p. 84-103. ISBN: 978-85-8238-364-3. Disponível em: <<https://docplayer.com.br/81389973-Temas-avancados-de-direito-eletronico.html>. > Acesso em: 21 out. 2019.

HENRIQUE, Matheus. **A história do Bitcoin – Como tudo começou**. Disponível em: <<https://guiadobitcoin.com.br/a-historia-do-bitcoin-como-tudo-comecou/>.> Acesso em 04 out. 2019.

HUMBERT, George Louis Hage; VALADARES, Murilo Cercato. **Criptomoedas transnacionais e o marco regulatório no Brasil:** Opções e Consequências. 2017. 22 f. TCC (Graduação) - Curso de Direito, Unijorge, Curitiba, 2017. Disponível em: <<https://m.migalhas.com.br>>. Acesso em: 20 out. 2019.

LIMA, João Rômulo Pereira. **Criptomoedas: regulação e oportunidades.** 2018. 51 f. Monografia (Especialização) - Curso de Economia, Departamento de Economia, Pontifícia Universidade Católica do Rio de Janeiro- PUC-rio, Rio de Janeiro, 2018. Disponível em: <http://www.econ.puc-rio.br/biblioteca.php/?titulo=Criptomoedas%3A+regula%C3%A7%C3%A3o+e+oportunidades&ano_inicial=&autor=&ano_final=&tipo=0&numero=>> Acesso em: 13 out 2019

MOLYNEUX, Stefan. **Practical Anarchy.** The Freedomain Library, Volume 6 Version 1.0, June 25, 2008. Disponível em: <https://freedomainradio.com/oldfree/books/FDR_5_PDF_Practical_Anarchy_Audiobook.pdf>. Acesso em 20 set. 2015.

NAKAMOTO, Satoshi. **Bitcoin:** A Peer-to-Peer Electronic Cash System. 2008. Disponível em <https://bitcoin.org/bitcoin.pdf>. Acesso em 22 out. 2019.

PORTAL DO BITCOIN. **Chave pública e privada do Bitcoin:** entenda o que são e como funcionam. Disponível em <https://portaldobitcoin.com/chave-publica-e-privada-do-bitcoin-entenda-o-que-sao-e-como-funcionam/>. Acesso em 04 set. 2019.

PORTAL DO BITCOIN. **Há um ano o Bitcoin atingia o maior preço da história.** Disponível em: <<https://portaldobitcoin.com/ha-um-ano-atras-o-bitcoin-atingia-o-maior-preco-da-historia/>>. Acesso em 04 out. 2019.

REVOREDO, Tatiana. **Quadro geral sobre tributação de criptoativos no Brasil.** Disponível em: <<https://www.migalhas.com.br/dePeso/16,MI300175,31047-Quadro+geral+sobre+tributacao+de+criptoativos+no+Brasil> > Acesso em: 04 out. 2019.

RFB. **Instrução normativa RFB N° 1888,** de 03 de maio de 2019. Disponível em <<http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=10059>>. Acesso em: 11 out. 2019.

ROHR, Altieres. **Corretora de Bitcoin Binance sofre ataque hacker que desvia US\$ 41 milhões.** [S. l.], 9 maio 2019. Disponível em: <<https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2019/05/09/corretora-de-bitcoin-binance-sofre-ataque-hacker-que-desvia-us-41-milhoes.ghtml>>. Acesso em: 16 out. 2019

SOUZA, Ranidson Gleyck Amâncio. **Território das criptomoedas:** limites à regulamentação estatal quanto à circulação de moedas no ciberespaço e possíveis alternativas. Revista Brasileira de Políticas Públicas, [s.l.], v. 7, n. 3, p.62-77, 6 fev. 2018. Centro de Ensino Unificado de Brasília.

Disponível em: < <https://www.publicacoesacademicas.uniceub.br/RBPP/article/view/4902>>
Acesso em: 04 out. 2019.

TAKAR, Téo. **Receita quer informação até de café pago com bitcoin, reclamam corretoras.**
Disponível em: <<https://economia.uol.com.br/noticias/redacao/2019/05/08/norma-receita-federal-criptomoedas-bitcoin.amp.htm>.> Acesso em: 04 out. 2019.

ULRICH, Fernando. **Bitcoin: A moeda na era digital.** 1. ed. São Paulo: Mises Brasil, 2014.

WAGMACKER, Lea. **O princípio da segurança jurídica no Direito Administrativo Brasileiro.**
Disponível em: <<https://jus.com.br/artigos/50302/o-principio-da-seguranca-juridica-no-direito-administrativo-brasileiro>> Acesso em: 15 out. 2019.