

**UNIVERSIDADE FEDERAL DE GOIÁS
UNIDADE ACADÊMICA ESPECIAL DE CIÊNCIAS SOCIAIS APLICADAS
GRADUAÇÃO EM DIREITO**

WALDOMIRO NETO CESAR DE SOUZA

**BLOCKCHAIN, CRIPTOMOEDAS E SEGURANÇA DA INFORMAÇÃO: ANÁLISE
DA LEI Nº 14.478/2022 COMO MARCO REGULATÓRIO INICIAL NO
ORDENAMENTO BRASILEIRO**

**Cidade de Goiás
2023**



UNIVERSIDADE FEDERAL DE GOIÁS
UNIDADE ACADÊMICA ESPECIAL DE CIÊNCIAS SOCIAIS APLICADAS

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO PARA DISPONIBILIZAR VERSÕES ELETRÔNICAS DE TRABALHO DE CONCLUSÃO DE CURSO DE GRADUAÇÃO NO REPOSITÓRIO INSTITUCIONAL DA UFG

Na qualidade de titular dos direitos de autor, autorizo a Universidade Federal de Goiás (UFG) a disponibilizar, gratuitamente, por meio do Repositório Institucional (RI/UFG), regulamentado pela Resolução CEPEC no 1240/2014, sem ressarcimento dos direitos autorais, de acordo com a Lei no 9.610/98, o documento conforme permissões assinaladas abaixo, para fins de leitura, impressão e/ou download, a título de divulgação da produção científica brasileira, a partir desta data.

O conteúdo dos Trabalhos de Conclusão dos Cursos de Graduação disponibilizado no RI/UFG é de responsabilidade exclusiva dos autores. Ao encaminhar(em) o produto final, o(s) autor(a)(es)(as) e o(a) orientador(a) firmam o compromisso de que o trabalho não contém nenhuma violação de quaisquer direitos autorais ou outro direito de terceiros.

1. Identificação do Trabalho de Conclusão de Curso de Graduação (TCCG)

Nome(s) completo(s) do(a)(s) autor(a)(es)(as): **Waldomiro Neto Cesar de Souza**

Título do trabalho: **“BLOCKCHAIN, CRIPTOMOEDAS E SEGURANÇA DA INFORMAÇÃO: ANÁLISE DA LEI Nº 14.478/2022 COMO MARCO REGULATÓRIO INICIAL NO ORDENAMENTO BRASILEIRO”**

2. Informações de acesso ao documento (este campo deve ser preenchido pelo orientador) Concorda com a liberação total do documento [x] SIM [] NÃO¹

[1] Neste caso o documento será embargado por até um ano a partir da data de defesa. Após esse período, a possível disponibilização ocorrerá apenas mediante: a) consulta ao(à)(s) autor(a)(es)(as) e ao(à) orientador(a); b) novo Termo de Ciência e de Autorização (TECA) assinado e inserido no arquivo do TCCG. O documento não será disponibilizado durante o período de embargo.

Casos de embargo:

- Solicitação de registro de patente;
- Submissão de artigo em revista científica;
- Publicação como capítulo de livro.

Obs.: Este termo deve ser assinado no SEI pelo orientador e pelo autor.



Documento assinado eletronicamente por **BRUNA PINOTTI GARCIA, Professora do Magistério Superior**, em 23/08/2023, às 20:09, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Waldomiro Neto Cesar De Souza, Discente**, em 23/08/2023, às 20:12, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site https://sei.ufg.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **3958740** e o código CRC **63C3753B**.

Referência: Processo nº 23070.045367/2023-29

SEI nº 3958740

WALDOMIRO NETO CESAR DE SOUZA

**BLOCKCHAIN, CRIPTOMOEDAS E SEGURANÇA DA INFORMAÇÃO: ANÁLISE
DA LEI Nº 14.478/2022 COMO MARCO REGULATÓRIO INICIAL NO
ORDENAMENTO BRASILEIRO**

Monografia jurídica apresentada à
Unidade Acadêmica Especial de Ciências
Sociais Aplicadas da Regional Goiás da
Universidade Federal de Goiás, como
trabalho de conclusão do curso de
bacharelado em Direito, sob a orientação
da Profa. Dra. Bruna Pinotti Garcia.

**Cidade de Goiás
2023**

Ficha de identificação da obra elaborada pelo autor, através do Programa de Geração Automática do Sistema de Bibliotecas da UFG.

Souza, Waldomiro Neto Cesar de
Blockchain, criptomoedas e segurança da informação: análise da Lei nº 14.478/2022 como marco regulatório inicial no ordenamento brasileiro [manuscrito] / Waldomiro Neto Cesar de Souza. - 2023. 56 f.

Orientador: Profa. Dra. Bruna Pinotti Garcia.
Trabalho de Conclusão de Curso (Graduação) - Universidade Federal de Goiás, Unidade Acadêmica Especial de Ciências Sociais Aplicadas, Direito, Cidade de Goiás, 2023.

1. Direito digital. 2. Blockchain. 3. Criptomoedas. 4. Segurança da informação. 5. Lei nº 14.478/2022. I. Garcia, Bruna Pinotti, orient. II. Título.



UNIVERSIDADE FEDERAL DE GOIÁS
UNIDADE ACADÊMICA ESPECIAL DE CIÊNCIAS SOCIAIS APLICADAS

ATA DE DEFESA DE TRABALHO DE CONCLUSÃO DE CURSO

Aos **dezessete dias do mês de agosto do ano de dois mil e vinte e três**, iniciou-se a sessão pública de defesa do trabalho de conclusão de curso (TCC) intitulado “**BLOCKCHAIN, CRIPTOMOEDAS E SEGURANÇA DA INFORMAÇÃO: ANÁLISE DA LEI Nº 14.478/2022 COMO MARCO REGULATÓRIO INICIAL NO ORDENAMENTO BRASILEIRO**”, de autoria de **Waldomiro Neto Cesar de Souza**, do curso de **Direito**, da Unidade Acadêmica Especial de Ciências Sociais Aplicadas da UFG. Os trabalhos foram instalados pela **presidenta, professora doutora Bruna Pinotti Garcia** com a participação dos demais membros da Banca Examinadora: **professora doutora Maria Carolina Carvalho Motta (UAECSA/UFG)** e **professora doutora Renata Botelho Dutra (UAECSA/UFG)**.

Após a apresentação, a banca examinadora realizou a arguição do(a) estudante. Posteriormente, de forma reservada, a Banca Examinadora deliberou, tendo sido o TCC considerado **aprovado**.

Proclamados os resultados, os trabalhos foram encerrados e, para constar, lavrou-se a presente ata que segue assinada pelos Membros da Banca Examinadora.



Documento assinado eletronicamente por **BRUNA PINOTTI GARCIA, Professora do Magistério Superior**, em 23/08/2023, às 20:08, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Maria Carolina Carvalho Motta, Professor do Magistério Superior**, em 23/08/2023, às 20:18, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Renata Botelho Dutra, Professora do Magistério Superior**, em 24/08/2023, às 09:32, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site https://sei.ufg.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **3958731** e o código CRC **E42A6B25**.

AGRADECIMENTOS

Sou grato a Deus por me conceder força, sabedoria e saúde para prosseguir durante esses anos de estudos.

Quero agradecer aos meus pais, Adail Ferreira de Souza e Telma Maria Cesar de Souza, por serem minha base e facilitarem toda minha experiência discente, me apoiando sempre nas minhas decisões e confiando na minha capacidade.

A comunidade Quilombola São Felix, a qual eu faço parte e que não mediram esforços para me apoiar no início desta jornada acadêmica.

A Universidade Federal de Goiás, Regional Goiás, na Unidade de Ciências Sociais Aplicadas, com sua excelente equipe docente, em especial a Profa. Dra. Bruna Pinotti Garcia, que aceitou participar deste desafio.

Aos componentes da banca examinadora pela disponibilidade de leitura do texto e direcionamentos dos caminhos a serem seguidos.

Por fim, a todos aqueles que, de forma direta ou indireta, fizeram parte desta caminhada.

“A primeira regra de qualquer tecnologia utilizada nos negócios é que a automação aplicada a uma operação eficiente aumentará a eficiência. A segunda é que a automação aplicada a uma operação ineficiente aumentará a ineficiência”.
(Bill Gates)

RESUMO

O presente trabalho de conclusão de curso (TCC) aborda o tema "Blockchain, criptomoedas e segurança da informação: análise da lei nº 14.478/2022 como marco regulatório inicial no ordenamento brasileiro". O objetivo principal é explorar as diversas aplicações e benefícios da tecnologia blockchain além do âmbito das criptomoedas, sendo o mesmo estudado pela ótica do Direito. O blockchain, originalmente desenvolvido para sustentar o funcionamento das criptomoedas, é uma tecnologia inovadora que permite o registro de dados de forma descentralizada, transparente e imutável. Neste TCC, será analisado como essa tecnologia tem sido regulamentada pelo ordenamento jurídico brasileiro. A pesquisa terá como foco os desafios da adoção do blockchain em setores financeiros sob a égide da regulamentação jurídica, bem como sua capacidade de melhorar a eficiência, segurança e transparência de processos financeiros. Lado outro serão analisados também os mecanismos necessários para impedir a prática de crimes e fraudes utilizando-se das criptomoedas, bem como o comportamento legislativo brasileiro acerca de tais problemas. Por meio desta pesquisa, espera-se fornecer uma visão abrangente sobre o potencial disruptivo do blockchain e como essa tecnologia pode transformar a maneira como interagimos e realizamos negócios em diversos campos. Além disso, o estudo visa contribuir para uma compreensão mais ampla da importância do blockchain como uma ferramenta poderosa para impulsionar a inovação tecnológica financeira.

Palavras-chave: Direito digital. Blockchain. Criptomoedas. Segurança da informação. Lei nº 14.478/2022.

ABSTRACT

The present undergraduate thesis addresses the theme "Blockchain, Cryptocurrencies, and Information Security: Analysis of Law No. 14.478/2022 as the initial regulatory framework in the Brazilian legal system." The main objective is to explore the various applications and benefits of blockchain technology beyond the scope of cryptocurrencies, examining it from a legal perspective. Originally developed to support the functioning of cryptocurrencies, blockchain is an innovative technology that allows decentralized, transparent, and immutable data recording. In this thesis, we will analyze how this technology has been regulated by the Brazilian legal system. The research will focus on the challenges of adopting blockchain in financial sectors under the umbrella of legal regulation, as well as its ability to enhance the efficiency, security, and transparency of financial processes. Additionally, we will examine the necessary mechanisms to prevent crimes and frauds involving cryptocurrencies, as well as the Brazilian legislative approach to such issues. Through this research, we aim to provide a comprehensive view of the disruptive potential of blockchain and how this technology can transform the way we interact and conduct business in various fields. Moreover, the study aims to contribute to a broader understanding of the importance of blockchain as a powerful tool to drive financial technological innovation.

Keywords: Digital law. Blockchain. Cryptocurrencies. Information security. Law n. 14.478/2022.

SUMÁRIO

INTRODUÇÃO	09
CAPÍTULO 1 – EVOLUÇÃO DOS ATIVOS FINANCEIROS NA SOCIEDADE	12
1.1 O surgimento do dinheiro.....	14
1.2 A emergência dos ativos financeiros virtuais: criptomoedas e bitcoin.....	17
CAPÍTULO 2 – BLOCKCHAIN E SEGURANÇA DA INFORMAÇÃO	20
2.1 Segurança da informação: brechas sob o ponto de vista dos ativos financeiros virtuais.....	21
2.2 Blockchain: conceito e importância da segurança para as transações de ativos financeiros virtuais.....	24
CAPÍTULO 3 – A LEI Nº 14.478/2022 E A REGULAMENTAÇÃO DOS ATIVOS FINANCEIROS VIRTUAIS NO BRASIL	37
3.1 Discussões no entorno da emergência da Lei nº 14.478/2022.....	37
3.2 Criminalização das fraudes que envolvem ativos financeiros virtuais.....	37
3.3 Criminalização das fraudes que envolvem ativos financeiros virtuais.....	42
3.3 Segurança da informação e a evitabilidade das fraudes envolvendo ativos financeiros virtuais com uso de blockchain: um olhar a partir dos princípios regentes da Lei nº 14.478/2022.....	44
CONSIDERAÇÕES FINAIS	48
REFERÊNCIAS	51

INTRODUÇÃO

Nesta monografia, será explorado o potencial da tecnologia blockchain além das criptomoedas. Serão abordados casos de uso em diferentes setores, bem como os desafios e as limitações da implementação dessa tecnologia. Além disso, serão discutidas as perspectivas para o futuro do blockchain e seu impacto na sociedade e na economia.

Para compreendermos melhor a tecnologia blockchain e suas aplicações além das criptomoedas, é preciso entender como ela funciona. De maneira simplificada, blockchain é um registro digital descentralizado, que permite que informações sejam armazenadas e compartilhadas de forma segura e transparente. Essa tecnologia é baseada em um sistema de consenso distribuído, no qual cada transação é validada por uma rede de participantes, tornando praticamente impossível a manipulação ou alteração dos dados.

No entanto, apesar de todo o seu potencial, a adoção do blockchain ainda enfrenta alguns desafios, como a falta de padronização, a complexidade da implementação e a necessidade de uma regulamentação clara. Mas, mesmo diante desses obstáculos, muitas empresas e organizações já estão explorando as possibilidades do blockchain e desenvolvendo soluções inovadoras.

Diante desse cenário, o objetivo desta monografia é oferecer uma visão mais ampla sobre o potencial da tecnologia blockchain, indo além do seu uso em criptomoedas. Ao explorar suas aplicações em diferentes setores e abordar seus desafios e perspectivas futuras, esta pesquisa tem como objetivo contribuir para a compreensão e o desenvolvimento dessa tecnologia disruptiva e revolucionária.

Este trabalho é uma pesquisa de revisão bibliográfica, o método consiste em analisar criticamente e de forma detalhada publicações sobre um determinado tema. A análise permite explicar e discutir o tema partindo de referências publicadas em trabalhos acadêmicos como artigos, livros, dissertações, teses, dentre outros. Os artigos e periódicos disponíveis em base de dados são fontes amplamente utilizadas e que permitem aprofundar ainda mais o estudo (MARTINS; PINTO, 2001).

Marconi e Lakatos (2017) afirmam que essa metodologia coloca os pesquisadores em contato direto com as publicações acerca do tema. O objetivo dessa metodologia não é replicar o que já foi escrito anteriormente e sim, apresentar

outra visão crítica sobre o assunto, introduzindo uma nova abordagem e outro enfoque ao tema, enriquecendo a bibliografia sobre o tema.

A revisão bibliográfica é uma metodologia de pesquisa que permite a identificação, seleção e análise crítica de trabalhos anteriores relevantes para a compreensão do problema em estudo. Segundo Bardin (2011), a revisão bibliográfica é um método que tem por objetivo fazer o levantamento e o exame crítico da literatura existente sobre determinado tema, a fim de identificar os principais conceitos, teorias e resultados alcançados por outros pesquisadores.

A revisão bibliográfica é uma ferramenta importante para a pesquisa científica, pois permite que o pesquisador conheça as principais contribuições já realizadas sobre o tema em questão, evitando que sejam cometidos erros metodológicos ou que sejam realizadas pesquisas já realizadas anteriormente. Além disso, a revisão bibliográfica também é importante para a construção de uma base teórica sólida, que fundamentará a pesquisa a ser realizada, assim como para a identificação de lacunas e novas oportunidades de pesquisa.

Para que a revisão bibliográfica seja efetiva, é necessário que seja realizada de forma sistemática e organizada, com a utilização de técnicas de pesquisa que permitam a identificação e seleção dos trabalhos mais relevantes e a análise crítica dos resultados apresentados por esses trabalhos. A revisão bibliográfica pode ser realizada por meio de diferentes abordagens, tais como a revisão narrativa, a revisão sistemática e a meta-análise, cada uma delas com características e objetivos específicos.

O primeiro capítulo do presente trabalho irá tratar da evolução dos ativos financeiros na sociedade, demonstrando como esses evoluíram e como saímos dos feitos rudimentares de negociação para a vivência atual com moedas digitais que tem se mostrado o presente e o futuro das negociações por todo o globo.

O segundo capítulo trará uma explicação detalhada de como funciona a nova tecnologia de moedas, a partir do conceito de Blockchain e como essa tecnologia tem aplicabilidade na vida atual, ademais, perpassara também sobre os pontos de segurança da informação, e de falhas dessa segurança, demonstrando como tal tecnologia pode ser usada tanto para a melhora, quanto para a piora do cenário mundial em todos os temas que envolvem ativos financeiros.

O terceiro capítulo se ocupará de demonstrar os acontecimentos e princípios envolvendo criptomoedas sob a égide da Lei nº 14.478/2022, conhecida como “Marco

Legal das Criptomoedas”, demonstrando seus pontos “fortes” e seus pontos “fracos” na tentativa de coibir as fraudes e utilizações ilegais das criptomoedas no Brasil.

Há como justificativa para o presente trabalho, que ao estudar a Lei nº 14.478/2022 como marco regulatório inicial no ordenamento jurídico brasileiro, surge uma necessidade de compreender o impacto da regulamentação no desenvolvimento desse mercado em rápida expansão no Brasil. A lei pode fornecer insights sobre a postura do governo em relação às criptomoedas, bem como suas implicações para empresas, investidores e usuários.

A análise da lei permitirá identificar aspectos positivos e desafios relacionados à regulamentação, abordando questões como a proteção dos investidores, prevenção de atividades ilícitas, estabilidade financeira e incentivo à inovação. Além disso, examinará como a legislação aborda a segurança da informação e a proteção dos dados em um ambiente digital cada vez mais complexo e suscetível a ataques cibernéticos.

CAPÍTULO 1 – EVOLUÇÃO DOS ATIVOS FINANCEIROS NA SOCIEDADE

A evolução dos ativos financeiros na sociedade é um processo que se estende por séculos e está intrinsecamente ligado ao desenvolvimento das instituições financeiras, tecnologia e mudanças nas práticas comerciais.

Nas sociedades primitivas, a troca direta era a forma predominante de comércio. As pessoas trocavam bens e serviços uns com os outros sem a necessidade de moedas ou ativos financeiros intermediários.

Esse método de troca direta, que predominava nas negociações era conhecido como escambo. Nesse sistema, bens e serviços eram trocados diretamente, o que limitava a complexidade das transações. A evolução para formas mais sofisticadas de dinheiro foi um processo gradual, com a adoção de objetos valiosos, como conchas, metais preciosos e gado, como meio de facilitar as trocas. Nesse sentido:

Como características básicas, o escambo se apresenta como uma troca de produtos em estado natural, que variam de acordo com as condições do lugar onde se dão as trocas, as atividades desenvolvidas pelo grupo, e suas respectivas necessidades. Neste sistema, a própria mercadoria torna-se moeda, passando a representar também, medida de valor e de riqueza, assim como acontece em civilizações mais simples. Seguindo esta mesma lógica, algumas mercadorias passarão a ter uma procura maior que outras, tornando-se involuntariamente a moeda daquele grupo. (SANTIAGO, 2023, p.1)

Com o tempo, a troca direta mostrou-se limitada, pois exigia a coincidência de necessidades mútuas entre as partes envolvidas. Para superar essa limitação, surgiram as formas iniciais de dinheiro, como conchas, grãos e metais preciosos, que eram utilizados como meio de troca e unidade de conta.

Porém, tal método ainda necessitava evoluir, para atender as demandas, desse modo, com a evolução da civilização, a cunhagem de moedas de metal se tornou comum, facilitando as transações comerciais e permitindo a acumulação de riqueza.

As primeiras moedas, tal como conhecemos hoje, peças representando valores, geralmente em metal, surgiram na Lídia (atual Turquia), no século VII A. C. As características que se desejava ressaltar eram transportadas para as peças através da pancada de um objeto pesado (martelo), em primitivos cunhos. Foi o surgimento da cunhagem a martelo, onde os signos

monetários eram valorizados também pela nobreza dos metais empregados, como o ouro e a prata. (GONÇALVES, 1985, p.37)

Após esse período, e com o exponencial crescimento das atividades comerciais, as pessoas começaram a buscar formas mais seguras de guardar seus recursos e emprestar dinheiro. Surgiram então as primeiras instituições financeiras, como bancos e casas de câmbio.

O acúmulo de capital chegou a tal ponto, que mesmo as moedas cunhadas e gravadas geravam um volume muito alto para manter. Assim, as instituições financeiras começaram então a emitir títulos, como notas promissórias e obrigações, que representavam dívidas a serem pagas no futuro. Esses títulos permitiam que as pessoas investissem em projetos e governos e recebessem juros ou dividendos em troca.

Outra evolução acerca dos ativos financeiros ocorreu no século XVII, quando surgiram as primeiras companhias com ações negociadas publicamente, como a Companhia das Índias Orientais. Com o tempo, a ideia de comprar e vender ações em uma bolsa de valores se tornou uma prática comum, proporcionando aos investidores uma forma de participar do crescimento de empresas e setores econômicos.

Fechando um pouco o espectro para o Brasil, temos que o país ainda se encontrava no período colonial quando as relações comerciais começaram a se acentuar devido ao fluxo de mercadorias entre o Brasil e o mercado europeu.

Com esse aumento e com a vinda da família Real para o Brasil, ocorreu uma valorização do mercado financeiro nacional, a ponto que ainda no século XIX foi inaugurada a primeira bolsa de valores do Brasil. Vejamos:

Na Bolsa de Valores do Rio de Janeiro, primeira bolsa de valores de grande importância a ser fundada no país, as operações ainda não formais foram iniciadas em 1820, para auxiliar nos negócios de fretes de navios e transações referentes à importação e exportação. Nessa época, os pregões eram realizados ao ar livre e os corretores eram conhecidos como “zangões”. A necessidade de se ter uma bolsa de valores no país surgiria com a vinda da Família Real Portuguesa, na primeira metade do século XIX, quando foram implementadas as primeiras tentativas de organização do mercado, época do surgimento da Praça do Comércio onde os primeiros pregões de rua eram realizados (INFOESCOLA, 2013, s.p.).

Ao passar de alguns anos criou-se a bolsa de valores de São Paulo como um reflexo da importância da capital paulista para a economia brasileira.

Em São Paulo foi criada a Bolsa Livre por Emílio Rangel Pestana, no ano de 1890. Essa bolsa não durou muito na capital paulista encerrando as suas atividades já no ano seguinte, 1891. O problema enfrentado pela Bolsa Livre foi uma crise que aconteceu no Brasil causada pela política do encilhamento. Somente no ano de 1895 é que começaram a ser realizadas as atividades de negociação da Bolsa de Fundos Públicos de São Paulo. Após quase quatro décadas de atuação essa bolsa passou a ser chamada de Bolsa Oficial de Valores de São Paulo. Quando apareceram as sociedades corretoras, no ano de 1967, o nome mudou para Bolsa de Valores de São Paulo. Uma curiosidade é que nesse tempo a bolsa funciona como grandes quadros negros em que se marcava as cotações. O período ficou sendo conhecido como Idade da Pedra, em nada se parecia com os painéis que não param de mudar as cotações dos dias de hoje (CULTURA MIX, 2013, s.p.).

No século XX, o avanço da tecnologia da informação transformou radicalmente os mercados financeiros. A negociação de ativos financeiros tornou-se mais rápida, acessível e global, com a introdução de plataformas de negociação eletrônica e sistemas financeiros interconectados.

Com a evolução dos mercados, surgiram inúmeros tipos de ativos financeiros, como títulos de dívida, ações, commodities, moedas estrangeiras, derivativos e muitos outros. Essa diversificação permitiu que os investidores construíssem portfólios mais equilibrados e adaptados aos seus objetivos financeiros.

Mais recentemente, a digitalização dos ativos financeiros e o surgimento das criptomoedas (como o Bitcoin) trouxeram novas oportunidades e desafios para a sociedade. As criptomoedas são ativos digitais descentralizados, que utilizam a tecnologia blockchain e representam uma forma alternativa de investimento e meio de pagamento.

Essa é apenas uma breve visão geral da evolução dos ativos financeiros na sociedade. A história é complexa e continua em constante mudança, impulsionada por avanços tecnológicos, regulamentações e as necessidades econômicas e financeiras das pessoas e empresas ao redor do mundo.

1.1 O surgimento do dinheiro

Atualmente, compreendemos que o dinheiro é um elemento crucial para o funcionamento das sociedades humanas. Sua evolução ao longo dos séculos reflete as transformações culturais, econômicas e tecnológicas da humanidade. Desde a

antiguidade até os dias atuais, o dinheiro desempenhou um papel vital nas trocas comerciais e na facilitação das transações econômicas.

Conforme vimos, com o desenvolvimento de civilizações antigas, como os gregos e romanos, as moedas metálicas começaram a ser cunhadas. Esse marco foi um avanço significativo na evolução do dinheiro, pois proporcionava um meio mais padronizado e aceito de troca. A regulamentação sobre a cunhagem, peso e autenticidade das moedas foi estabelecida por leis e governos, buscando garantir a confiança dos participantes das transações comerciais. Vejamos:

Pedaços de metal podiam ser menos volumosos e, portanto, mais fáceis de manipular, e eram também mais duráveis, divisíveis em peças ainda menores e virtualmente não perecíveis. Podiam também ser fundidos, remoldados ou trabalhados para outras utilizações práticas. A partir do momento em que certos povos desenvolveram sistemas de pesos de ampla aceitação e garantidos ou estabelecidos por uma autoridade central, difundiu-se a utilização de metais como unidade de referência e meio de pagamento, ou seja, com algumas das funções modernas da moeda. (LAGO, 2004, p. 6)

Após as moedas metálicas, e ao longo dos séculos, o papel-moeda ganhou destaque como forma de dinheiro. Seu uso foi facilitado por instituições financeiras e governos, que emitiam notas promissórias lastreadas em reservas de ouro ou prata. O papel-moeda trouxe a possibilidade de transferências financeiras mais convenientes e seguras, impulsionando o comércio e a economia em escala global.

Os primeiros registros da utilização do papel como moeda remontam do ano 89. As matrizes para a impressão eram confeccionadas em tabuleiros de madeira ou de bambu, sobre as quais era aplicada uma pasta especial, feita de polpa vegetal amolecida e batida. A madeira recebia tinta e os desenhos e textos gravados eram passados para o papel. Essa invenção permaneceu escondida durante séculos; sua importância pode ser exemplificada pelo fato de os chineses terem erguido um templo em homenagem ao inventor dessa técnica. (BRASIL, 2023, p.1)

Com a revolução tecnológica, surgiu o conceito de dinheiro digital e a proliferação de transações eletrônicas. Cartões de crédito, transferências bancárias e pagamentos eletrônicos transformaram a forma como as pessoas interagem com o dinheiro. No entanto, essa evolução trouxe desafios jurídicos, especialmente relacionados à segurança cibernética, privacidade financeira e responsabilidade legal em caso de fraudes.

Com o dinheiro digital e as criptomoedas ganhando popularidade, as legislações precisam se adaptar para abordar questões específicas, como proteção de dados, cibersegurança, regulamentação das exchanges de criptomoedas e tributação desses ativos. A criação de um ambiente jurídico adequado é fundamental para promover a inovação e, ao mesmo tempo, proteger os interesses dos cidadãos.

A evolução do dinheiro sob o prisma jurídico tem sido um processo contínuo e desafiador. Desde as formas primitivas de troca até as criptomoedas modernas, a regulação financeira teve que se adaptar para acompanhar as mudanças tecnológicas e sociais.

À medida que a sociedade continua a evoluir, as questões jurídicas relacionadas ao dinheiro continuarão a surgir, exigindo uma abordagem flexível e atualizada das leis e regulamentos para garantir um sistema financeiro seguro, justo e eficiente para todos os envolvidos.

Conforme o jurista Silva (2018), "o dinheiro, como um sistema de troca de valores, é um fenômeno histórico que se desenvolveu ao longo dos séculos para atender às necessidades das transações comerciais e econômicas".

Em relação à regulamentação do papel-moeda, Souza e Santos (2015) explicam que "a emissão de cédulas e moedas por entidades governamentais foi uma resposta às demandas do mercado, buscando estabelecer um meio confiável e padronizado de troca".

Sobre a emergência das criptomoedas, Oliveira (2019) afirma que "as moedas digitais baseadas em blockchain representam um desafio único para a legislação financeira, uma vez que operam em um ambiente descentralizado e muitas vezes transpassam fronteiras jurisdicionais".

A evolução do dinheiro sob o prisma jurídico é um tema complexo e multifacetado, que abrange tanto aspectos históricos quanto desafios contemporâneos. Desde as formas rudimentares de troca até as inovações digitais, o dinheiro tem desempenhado um papel fundamental na organização da sociedade e das atividades econômicas. No entanto, a adaptação das normas e regulamentações financeiras às mudanças tecnológicas tem sido uma tarefa desafiadora para governos e juristas.

A busca por soluções que promovam a inclusão financeira, garanta a segurança das transações e protejam os direitos dos cidadãos continua sendo um objetivo primordial. Para alcançar esses resultados, é fundamental que os legisladores

trabalhem em conjunto com especialistas em tecnologia e economia, a fim de criar um ambiente jurídico favorável à inovação, sem comprometer a estabilidade e a segurança do sistema financeiro.

Nesse sentido, é imprescindível que os estudos e pesquisas sobre a evolução do dinheiro e suas implicações jurídicas sejam ampliados, permitindo o desenvolvimento de políticas públicas mais eficientes e adequadas às necessidades da sociedade moderna. Ao olharmos para o futuro, é certo que o dinheiro continuará a evoluir, e, portanto, os marcos jurídicos devem ser flexíveis e adaptáveis para acompanhar essas mudanças, garantindo a integridade e a estabilidade do sistema financeiro em todos os momentos.

1.2 A emergência dos ativos financeiros virtuais: criptomoedas e bitcoin

A adoção de criptomoedas tem se expandido de forma notável, impulsionada por diversos fatores. Primeiramente, a tecnologia blockchain que sustenta essas moedas oferece um nível de segurança e transparência inédito, eliminando a necessidade de intermediários financeiros, como bancos, em muitas transações.

Além disso, as criptomoedas permitem transações internacionais mais rápidas e acessíveis, com taxas reduzidas em comparação com os sistemas tradicionais. Isso tem sido particularmente benéfico para pessoas que não têm acesso a serviços bancários convencionais e para remessas de dinheiro entre países.

Nas últimas décadas, testemunhamos a emergência das criptomoedas, como o Bitcoin e o Ethereum, que introduziram um novo paradigma no sistema financeiro. As criptomoedas funcionam em uma tecnologia descentralizada chamada blockchain, que registra todas as transações de forma transparente e imutável.

Blockchain é uma tecnologia de registro de dados que permite o armazenamento seguro, transparente e imutável de informações em uma rede descentralizada. O termo "blockchain" é composto por duas palavras: "block" (bloco) e "chain" (cadeia). Essa tecnologia é a base das criptomoedas, como o Bitcoin, mas possui aplicações muito mais amplas em diversas áreas além do universo financeiro.

Em um sistema blockchain, as informações são agrupadas em blocos, e cada bloco contém um conjunto de transações ou dados. Cada bloco é vinculado ao anterior, formando uma cadeia de blocos, daí o nome "blockchain". Cada bloco possui um identificador exclusivo, conhecido como "hash", que é gerado através de uma

função criptográfica que leva em consideração os dados do bloco anterior, o conteúdo do bloco atual e um número chamado "nonce".

Como falado, o funcionamento do blockchain é descentralizado, o que significa que não é controlado por uma única entidade central, como um banco ou governo. Em vez disso, a rede blockchain é mantida por uma rede distribuída de computadores, conhecidos como "nós" ou "nodos", que validam e armazenam as transações.

Essa descentralização traz vantagens importantes, como maior segurança, resistência a falhas únicas e eliminação da necessidade de confiar em uma autoridade central.

Um dos principais princípios do blockchain é a imutabilidade dos dados. Uma vez que um bloco é adicionado à cadeia, não pode ser alterado sem afetar todos os blocos subsequentes, o que torna praticamente impossível modificar ou apagar transações anteriores de forma não autorizada.

As transações são validadas na rede por meio de consenso, onde os nós da rede concordam que uma transação é legítima antes de ser adicionada ao blockchain. Existem diferentes algoritmos de consenso, como o Proof-of-Work (PoW) e o Proof-of-Stake (PoS), que variam em sua abordagem para alcançar esse acordo.

A tecnologia blockchain tem sido amplamente discutida nos últimos anos, principalmente em relação às criptomoedas como o Bitcoin. No entanto, essa tecnologia tem muito mais a oferecer do que apenas transações financeiras. Como afirmou Tapscott e Tapscott (2016), "o blockchain é uma tecnologia fundamentalmente disruptiva que pode transformar a forma como as empresas e as economias operam".

Dentre as inúmeras possíveis aplicações do blockchain, pode-se citar: contratos digitais auto executáveis (Smart contracts), novos sistemas de governança, registro de ativos de diversas naturezas e registros públicos (WRIGHT; DE FILIPPI, 2015; YERMACK, 2017).

Essa série de possibilidades acarreta falta de compreensão sobre os potenciais usos da "cadeia de blocos" (MORABITO, 2017). E ainda: "Por ser uma tecnologia recente, possui ainda um baixo nível de maturação, o que pode comprometer seu uso em larga escala no sentido de substituir as soluções tradicionais no curto prazo". (FERREIRA et al., 2017, p.116)

De fato, a tecnologia blockchain tem o potencial de revolucionar setores como o de saúde, logística, governança, energia e muito mais. Por meio da

descentralização, transparência e segurança, a tecnologia blockchain pode oferecer soluções inovadoras para problemas complexos e melhorar significativamente a eficiência e a confiança em diversos processos. Nesse diapasão:

Assim como o real ou o dólar, o bitcoin é uma moeda. A diferença é que ela é exclusivamente digital e baseada em criptografia. Além disso, ela não pertence a nenhum país e não é submetida à regulação de sistemas financeiros ou do governo. As criptomoedas são geradas e reguladas por meio de código. Programadores e pessoas ligadas ao mundo cibernético desenvolvem atividades para angariar as criptomoedas, atividade que ficou conhecida como “mineração digital”. Por outro lado, uma cadeia de codificadores em blocos (blockchain), composto por programadores que usam softwares para validar a moeda, garantem a sua integridade e validade. (CAPUCIO, 2017, s.p.)

Essa inovação levantou questões sobre a regulamentação e o status legal das criptomoedas, já que muitos governos ainda não estabeleceram uma estrutura legal clara para lidar com esses ativos digitais.

As leis financeiras têm como objetivo proteger os consumidores e garantir a integridade do sistema financeiro. Regulamentações sobre instituições financeiras, taxas de juros, proteção contra fraudes e lavagem de dinheiro são essenciais para manter a estabilidade econômica e a confiança dos participantes do mercado.

CAPÍTULO 2 – BLOCKCHAIN E SEGURANÇA DA INFORMAÇÃO

Conforme vergastado nos tópicos anteriores, nos últimos anos, a tecnologia blockchain emergiu como uma das mais promissoras inovações na área da segurança da informação. Com suas características revolucionárias de descentralização, imutabilidade e transparência, o blockchain tem o potencial de transformar a forma como lidamos com dados e transações digitais, garantindo uma maior proteção e integridade das informações.

O blockchain é uma estrutura de dados distribuída que funciona como um livro-razão público, onde todas as transações são registradas em blocos e interligadas de forma cronológica. Cada novo bloco é conectado ao anterior, criando uma cadeia de blocos que não pode ser alterada ou adulterada sem que isso seja evidente para toda a rede. Essa característica torna o blockchain praticamente imune a manipulações e fraudes, tornando-o altamente seguro para o armazenamento e compartilhamento de informações sensíveis.

A segurança da informação é uma preocupação crescente em um mundo cada vez mais digitalizado, onde ataques cibernéticos e violações de dados se tornaram uma ameaça constante para indivíduos e organizações. A tecnologia blockchain oferece uma abordagem inovadora para a proteção de dados, permitindo a criação de sistemas confiáveis e transparentes sem depender de uma entidade central de controle.

Quando corroboramos blockchain e segurança da informação, seus princípios de segurança e como essa tecnologia pode ser aplicada em diversos setores, desde serviços financeiros até governança e cadeias de suprimentos, vemos que ele está pronto para corresponder as demandas atuais, porém, não se pode afirmar que essa tecnologia é invulnerável, vejamos:

Toda essa complexidade expõe a blockchain a riscos cibernéticos, já que não existem tecnologias, pessoas, equipamentos ou processos que estejam imunes a ameaças e vulnerabilidades cibernéticas no ambiente de rede. Por isso, é mister envidar esforços para que a segurança cibernética na organização seja tratada em âmbito estratégico e não apenas no nível tático, isto é, aquilo que se refere a questões relacionadas à unidade organizacional de TIC. Ainda que a blockchain seja reconhecidamente uma tecnologia revolucionária, ela não é impenetrável e não está livre de ataques cibernéticos. Em razão da garantia do anonimato, é conferido um baixo risco ao atacante cibernético e uma alta recompensa associada aos fatores de sucesso. Por essa razão, são crescentes os esforços para a exploração de

quaisquer vulnerabilidades no ambiente de blockchain. (SILVEIRA, 2022, s. p.)

O blockchain, mesmo com suas falibilidades, representa uma promessa de maior confiança e segurança nas operações digitais, oferecendo uma infraestrutura sólida para proteger a integridade das informações em uma era onde a segurança da informação é uma das maiores prioridades para a sociedade como um todo.

2.1 Segurança da informação: brechas sob o ponto de vista dos ativos financeiros virtuais

As brechas de segurança são vulnerabilidades e falhas que podem ser exploradas por atacantes maliciosos para obter acesso não autorizado a sistemas e informações sensíveis. No contexto dos ativos financeiros virtuais, essas brechas podem ter consequências graves, resultando em perdas financeiras significativas para indivíduos e organizações.

Algumas das principais brechas de segurança enfrentadas pelos ativos financeiros virtuais incluem, os ataques a Exchanges de criptomoedas, “Phishing” e as mais variadas formas de golpes aplicadas

As exchanges de criptomoedas são plataformas onde os usuários podem comprar, vender e armazenar ativos digitais. Nesse sentido:

Desde que o Bitcoin (BTC) foi criado, no final de 2008, uma indústria bilionária se formou ao redor da criptomoeda. Surgiram novas empresas, produtos, empregos e modelos de negócio até então nunca vistos. E na lista de participantes desse novo mundo criptográfico, um dos destaques são as exchanges. Também chamadas de corretoras, elas têm a função de intermediar as negociações entre vendedores e compradores de ativos digitais. Por esse serviço, claro, elas cobram taxas, e é assim que sobrevivem. (INFOMONEY, 2022, s. p.)

Uma das maiores ameaças é o ataque cibernético direcionado a essas exchanges. Casos de hackers comprometendo exchanges e roubando grandes quantidades de criptomoedas têm sido frequentes, o que destaca a importância de práticas rigorosas de segurança por parte dessas plataformas. Temos exemplos de ataques que podem ser citados, dentre eles:

Em 2014, a Mt. Gox era uma das maiores exchanges de Bitcoin do mundo, mas sofreu um ataque cibernético massivo que resultou no roubo de

aproximadamente 850.000 Bitcoins, avaliados em bilhões de dólares na época. O incidente levou à falência da empresa e causou um grande impacto na comunidade de criptomoedas.

Ocorreu também que em janeiro de 2018, a exchange japonesa Coincheck sofreu um ataque cibernético em que mais de 500 milhões de NEM (uma criptomoeda) foram roubados, totalizando cerca de 530 milhões de dólares na época. Esse ataque foi considerado um dos maiores da história das criptomoedas.

Em maio de 2019, a Binance, uma das maiores exchanges de criptomoedas do mundo, relatou um ataque cibernético em que hackers obtiveram acesso a informações de contas de usuários e roubaram 7.000 Bitcoins, equivalente a mais de 40 milhões de dólares na época. A exchange reembolsou os fundos afetados aos usuários.

Dentre outras formas destacadas de práticas que podem violar a segurança das criptomoedas, devemos elencar também os golpistas e hackers que frequentemente utilizam técnicas de “phishing” para obter informações confidenciais dos usuários, como senhas e chaves privadas.

Phishing é uma forma de ataque cibernético que busca enganar os usuários, levando-os a divulgar informações pessoais, como senhas, números de cartão de crédito, informações de contas bancárias ou outras informações confidenciais. O objetivo do phishing é obter acesso não autorizado a contas e dados sensíveis para fins maliciosos, como roubo de identidade, fraude financeira ou acesso a sistemas protegidos.

O termo "phishing" deriva da palavra "fishing" (pesca, em inglês) e reflete a natureza do ataque: os cibercriminosos lançam "iscas" virtuais, geralmente na forma de e-mails, mensagens de texto, redes sociais ou sites falsos, para atrair vítimas desavisadas e obter suas informações pessoais. Ariane Gonçalves explica:

Phishing é um crime virtual no qual pessoas comuns são contactadas através de email, telefone ou mensagens de texto (SMS) por uma outra pessoa ou empresa. O contato se faz de maneira genuína, para atrair e induzir o contactado a fornecer informações sigilosas dados bancários, cartão de crédito, senhas e outras informações confidenciais ao compartilhar estas informações, as pessoas têm sua conta e cartão violados, e podem ser vítimas de crimes de falsa identidade ou perder dinheiro através de transações financeiras indesejadas. (GONÇALVES, 2023, s. p.)

Outras vulnerabilidades utilizadas por criminosos são os “Malwares”, como cavalos de Troia, ransomware e keyloggers, pode infectar computadores e dispositivos móveis para roubar chaves privadas ou interceptar informações confidenciais durante transações de ativos financeiros virtuais.

Malware é uma abreviação de "software malicioso" (do inglês "malicious software"). É um termo geral usado para descrever qualquer tipo de software projetado com o propósito de causar danos, roubar informações, infectar sistemas ou realizar atividades indesejadas em um dispositivo ou rede de computadores, sem o conhecimento ou consentimento do usuário.

Existem vários tipos de malwares, cada um com suas características e métodos de propagação. Os malwares podem ser distribuídos de várias maneiras, incluindo downloads de sites não confiáveis, anexos de e-mails maliciosos, links em mensagens instantâneas ou por meio de vulnerabilidades em sistemas não atualizados.

Devemos ainda destacar, outro método comum para explorar falhas quanto as transações envolvendo criptomoedas, qual seja, as vulnerabilidades em carteiras digitais. As carteiras digitais são usadas para armazenar chaves privadas e, portanto, são um alvo atraente para hackers. Vulnerabilidades em carteiras podem permitir que terceiros acessem os ativos de seus proprietários.

Para elucidar, carteiras digitais, também conhecidas como wallets ou carteiras virtuais, são aplicativos, programas ou serviços que permitem armazenar, gerenciar e interagir com ativos financeiros digitais, como criptomoedas e moedas virtuais. Essas carteiras funcionam como uma espécie de interface entre os usuários e o blockchain, permitindo que eles realizem transações, recebam ou enviem ativos digitais de forma segura e eficiente.

Após explanação das mais comuns brechas exploradas pelos criminosos para burlar a efetividade da segurança das criptomoedas, compreendemos que para mitigar essas brechas de segurança, é fundamental que os usuários, exchanges e outras entidades envolvidas em ativos financeiros virtuais adotem práticas sólidas de segurança da informação. Isso inclui o uso de autenticação de dois fatores, adoção de carteiras de hardware seguras, educação dos usuários sobre phishing e outras ameaças, atualização regular de softwares e sistemas, além da implementação de medidas de criptografia e monitoramento constante de atividades suspeitas.

Em um cenário em constante evolução, a segurança da informação deve ser tratada como uma prioridade máxima para garantir a confiança e a viabilidade dos ativos financeiros virtuais em nossas vidas diárias. A colaboração entre governos, empresas e usuários é essencial para enfrentar esses desafios de forma proativa e eficaz, garantindo um ecossistema financeiro digital mais seguro e resiliente.

2.2 Blockchain: conceito e importância da segurança para as transações de ativos financeiros virtuais

Conforme melhor definição, o blockchain é uma tecnologia de registro distribuído e descentralizado que permite a criação e manutenção de um registro seguro e imutável de transações e informações. É a tecnologia por trás das criptomoedas, como o Bitcoin, mas suas aplicações vão muito além disso, abrangendo uma ampla gama de setores e casos de uso.

O conceito básico do blockchain pode ser resumido em três pilares fundamentais: Registro distribuído; Segurança criptográfica; Imutabilidade e consenso. Sobre esses pilares vejamos:

O conceito de registro distribuído, implica dizer que em vez de manter um registro centralizado de transações, o blockchain é uma rede de computadores (nós) conectados que compartilham uma cópia idêntica do mesmo livro-razão digital. Cada nó possui uma cópia completa do blockchain, atualizada constantemente por meio de um consenso entre os participantes da rede. Isso significa que não há uma única autoridade ou intermediário controlando o sistema, tornando-o resistente a falhas e ataques.

A segurança é garantida por meio de técnicas criptográficas. Cada transação no blockchain é protegida por uma assinatura digital única e verificável, gerada por uma chave privada. Além disso, os blocos são conectados uns aos outros por meio de uma função matemática complexa chamada de hash. Qualquer alteração em um bloco resultaria em mudanças em todos os blocos subsequentes, tornando impraticável a modificação de dados passados sem o consenso da maioria dos nós na rede.

A imutabilidade é uma das principais características do blockchain. Uma vez que uma transação é registrada em um bloco e adicionada à cadeia, ela se torna permanentemente gravada e não pode ser alterada ou apagada. Isso garante a

integridade do histórico de transações. O consenso é alcançado por meio de algoritmos de consenso, como Proof-of-Work (PoW) ou Proof-of-Stake (PoS), que garantem que a maioria dos nós concorda sobre a validade das transações antes de serem registradas no blockchain.

Com esses três pilares, o blockchain se torna uma plataforma segura e transparente para realizar transações e manter registros. Além das criptomoedas, o blockchain pode ser aplicado em diversos setores, como logística, cadeia de suprimentos, votação eletrônica, gerenciamento de identidade, registros médicos, tokenização de ativos, entre outros.

Sua capacidade de criar um ambiente confiável, transparente e descentralizado torna o blockchain uma tecnologia promissora com potencial para transformar a forma como interagimos, realizamos negócios e compartilhamos informações em um mundo cada vez mais digitalizado.

A expressão Peer-to-peer (ponto-a-ponto) é uma arquitetura de redes de computadores onde cada um dos pontos ou nós da rede, funcionam tanto como cliente quanto como servidor, permitindo compartilhamentos de serviços e dados sem a necessidade de um servidor central.

Podemos vencer uma grande batalha na corrida armamentista e ganhar um novo território de liberdade por vários anos. Governos são bons em cortar a cabeça de redes centralmente controladas, como o Napster, mas redes puramente P2P, como Gnutella e Tor, parecem seguir em frente inabaladas. (NAKAMOTO apud ULRICH, 2014, p. 42)

Conforme Nakamoto (2008) a utilização de rede P2P possibilita operações sem a necessidade estrita de terceiros, as operações são registradas cronologicamente e as informações permanecem disponíveis.

Aparentemente surgido do nada, o Bitcoin é, em realidade, resultado de mais de duas décadas de intensa pesquisa e desenvolvimento por pesquisadores praticamente anônimos. No seu âmago, o sistema é um avanço revolucionário em ciência da computação, cujo desenvolvimento foi possibilitado por 20 anos de pesquisa em moedas criptográficas e 40 anos de pesquisa em criptografia por milhares de pesquisadores ao redor do mundo (ULRICH, 2014, p. 44).

Segundo relatório do European Central Bank (2012), as raízes teóricas do Bitcoin podem ser encontradas na teoria econômica da Escola Austríaca, sobretudo

nos trabalhos de Friedrich A. Hayek (2011), Eugen von Böhm-Bawerk e Ludwig von Mises. Hayek defende em seu trabalho que o governo não deve ter o monopólio da emissão de moeda, assim, os bancos privados poderiam emitir certificados sem juros, que seriam como moedas privadas transacionadas no livre mercado. Assim, as moedas mais estáveis sobreviveriam, e o sistema monetário se tornaria mais estável: “Governos não podem inflacionar bitcoins. Governos não podem apropriar-se da rede Bitcoin. Governos tampouco podem corromper ou desvalorizar bitcoins. E também não podem proibir-nos de enviar bitcoins a um comerciante no Maranhão ou no Tibete” (ULRICH, 2009, pag. 105).

Conforme Ulrich (2014), o Bitcoin foi projetado de modo a reproduzir a extração de ouro ou outro metal precioso da Terra – somente um número limitado e previamente conhecido de Bitcoins poderá ser minerado.

Franco e Bazan (2018) identificam vários aspectos importantes do sistema. Evidenciam o fator da descentralização, ou seja, a independência de uma instituição central para gerir o sistema financeiro. O mesmo não possui um servidor único e central que faça as operações, pelo contrário, o servidor está disponível em milhares de pontos da rede (rede peer-to-peer, ou ponto-a-ponto em português), de forma com que uma só entidade ou pessoa não consiga controlar o sistema inteiro a bel prazer.

Nakamoto (2008) e Ulrich (2014) destacam a prova de trabalho, as transações em blocos e a criptografia como um dos principais fatores que asseguram ao detentor de Bitcoins um risco reduzido de perdê-lo, uma vez que nenhum ativo é livre de riscos. As medidas cautelares se resumem em armazenar a senha da melhor forma possível, e evitar o contato com vírus e sites maliciosos.

Segundo Fonseca (2009), Bitcoin é uma moeda emitida por uma entidade não governamental de uma comunidade, diferente da moeda nacional, de modo a desenvolver economias locais. Deve ser encarada como uma “moeda-comunidade” dentro da lei:

As leis e regulações atuais não preveem uma tecnologia como o Bitcoin, o que resulta em algumas zonas legais cinzentas. Isso ocorre porque o Bitcoin não se encaixa em definições regulamentares existentes de moeda ou outros instrumentos financeiros ou instituições, tornando complexo saber quais leis se aplicam a ele e de que forma (ULRICH, 2014, p. 33).

Considerada a pioneira das criptomoedas, entre as características que a diferenciam estão a descentralização e a preservação do anonimato nas transações.

Pode-se concluir que, apesar de ter sido criada anonimamente, dado o crescimento do número de transações efetuadas por meio das moedas virtuais, mormente pelo sistema Bitcoin, é de se esperar que haja uma regulação, ou pelo menos uma regulamentação por parte das autoridades.

A Bitcoin é criada por meio de um programa open source (ou “código aberto” em português) com base peer-to-peer, ou seja, diretamente de usuário para usuário. Permite a sua constante modificação e atualização pelos usuários. Ou seja, caso haja uma falha no sistema de um antivírus open source, os próprios usuários podem tentar consertá-la por meio de sua experiência e habilidade. Conforme Dequech (2007), um aumento do desenvolvimento de programas open source, ou seja, programas de computador desenvolvidos com seu código aberto a quem quiser reproduzi-lo ou modificá-lo, tem tido uma participação importante no desenvolvimento tecnológico e econômico no mundo. O desenvolvimento do protocolo Bitcoin ocorre exatamente através de um processo open source, onde qualquer pessoa pode analisar o seu código, propor melhorias ou desenvolver outras coisas a partir dele.

A Bitcoin é uma moeda que não depende de nenhuma terceira parte para o seu funcionamento. Comenta Ulrich (2014) que ela funciona sem uma autoridade central responsável pelo suprimento de dinheiro, sem uma câmara de compensação central (clearing house), sem instituições financeiras envolvidas nas transações, na qual os próprios usuários desempenham todas as funções necessárias para transacionar os recursos como por exemplo, um banco. abre um novo paradigma para o futuro dos sistemas de pagamentos, pois é uma inovação financeira nascida da necessidade de superar a lacuna tecnológica que existia entre o universo digital e o sistema financeiro.

O sistema da Bitcoin é um sistema de pagamentos inteiramente virtual que independe de um ente central que garanta seu lastro ou organize seu funcionamento. Trata-se de um sistema criptográfico – baseado em códigos informáticos – que contém códigos não “monetários” e códigos “monetários”, - correspondendo esses últimos aos Bitcoins. Usa um banco de dados distribuído pelos diferentes nós da rede que, com o uso de criptografia, garantem o funcionamento e a criação da Bitcoin. A criptografia é um conjunto de regras que visa codificar a informação de forma que só o emissor e o receptor consigam decifrá-la. O funcionamento do seu sistema de pagamentos processa as transações e emite unidades através de Proof-of-work (Prova de

trabalho), executada por subcontratados, ao invés de confiança em um agente terceiro (NAKAMOTO, 2008).

O sistema Bitcoin utiliza a prova de trabalho como um mecanismo para validar as transações e garantir a segurança da rede. A prova de trabalho envolve a resolução de problemas computacionais complexos, exigindo poder de processamento e consumo de energia. Os usuários que contribuem com seu poder de computação para resolver esses problemas são recompensados com novas unidades de Bitcoin, um processo conhecido como mineração.

Essa abordagem descentralizada e baseada em criptografia garante que as transações sejam transparentes e seguras. Cada transação é registrada em um bloco, que é posteriormente adicionado a uma cadeia de blocos, formando assim a blockchain. A blockchain é um registro público e distribuído de todas as transações já realizadas na rede Bitcoin. Essa transparência e imutabilidade tornam extremamente difícil modificar transações passadas ou falsificar novas transações.

Além disso, a criptografia é fundamental para garantir a segurança das transações e a proteção dos dados dos usuários. As chaves criptográficas são utilizadas para autenticar e assinar as transações, garantindo a identidade dos envolvidos e a integridade das informações. As carteiras digitais, que são utilizadas para armazenar e gerenciar os Bitcoins, são protegidas por chaves privadas, que devem ser mantidas em segurança pelo usuário. Nesse sentido:

A criptografia é a parte essencial desses contratos, garantindo confiança entre as partes que querem realizar esse tipo de contrato, além de ser prático por poder ser implementado com segurança em uma rede pública. Ademais, as normas e obrigações já ficam pré-programadas no sistema do contrato, com as cláusulas contratuais escritas no software e sendo executadas automaticamente após as condições estabelecidas serem atendidas, não sendo permitido mudanças no contrato após sua realização, trazendo assim segurança jurídica para as partes envolvidas. (ZANINI, 2023, p.31)

No entanto, o Bitcoin também enfrenta desafios e críticas. Sua volatilidade de preço é uma preocupação para muitos, já que o valor da criptomoeda pode flutuar significativamente em curtos períodos de tempo. Além disso, a falta de regulamentação e supervisão governamental levanta questões sobre a proteção dos usuários e a prevenção de atividades ilícitas, como lavagem de dinheiro e financiamento ao terrorismo.

Entre os ganhos e sim também podem haver perdas, uma delas acontece por ser uma moeda volátil, que já enfrentou grandes períodos de baixa nos preços. A procura pela moeda vem aumentando com o passar dos anos e a aceitação no mercado financeiro como meio de troca, a demanda aumenta, inflação crescente também afeta o preço da bitcoin, quando as moedas tradicionais se desvalorizam, mais a bitcoin aumenta a demanda. (DALL'AGNOL; GUTH, 2023, p.06)

Apesar desses desafios, o Bitcoin continua a crescer em popularidade e a atrair a atenção de investidores, empresas e governos ao redor do mundo. Seu potencial para transformar o sistema financeiro tradicional, oferecendo maior autonomia e liberdade financeira, tem despertado interesse e debate em diversos setores.

Não restam dúvidas de que em qualquer setor da economia que se observe, dado o crescente nível de concorrência, exigência por eficiência e melhores resultados, verifica-se também um aumento proporcional no risco de fraudes, desvios, irregularidades, descumprimento de normas regulatórias, corrupção, enfim, qualquer meio que se encontre para se atingir os próprios objetivos.

Para uma análise do patamar em que o mercado de moedas digitais se encontra, em outubro de 2018, a capitalização de mercado das criptomoedas, de acordo com a Coin Market Cap, era de US\$ 212 bilhões. Isoladamente o Bitcoin representa 52% de todo o mercado de criptomoedas.

São valores relativamente pequenos quando se pensa no sistema financeiro global. Mas, apenas uma fração desse montante, se usado para fins escusos, pode representar um problema e tanto para autoridades e para a segurança mundial.

Afinal, como ninguém controla o fluxo de criptomoedas, é possível que, ao menos uma parte desse montante, pertença a organizações criminosas e grupos terroristas.

O Banco Central não trata as criptomoedas como uma moeda oficial, a exemplo do real ou de outras moedas estrangeiras e, por isso, não oferece nenhum tipo de segurança ou garantia oficial, ficando o investidor exclusivamente por sua própria conta e risco (COHEN,2004).

Os contextos econômico, político e social estão imersos em modificações constantes. Inclusa nessa evolução encontra-se a fraude a qual se aprimora a cada mudança. A atualidade trouxe consigo a necessidade do mecanismo de prevenção e regulação no cenário das atividades econômicas, a conformidade que é o compliance.

Sob o olhar de (COLARES, 2014), o termo compliance advém do verbo em inglês *to comply*, que a tradução significa cumprir, exercer, desempenhar. A tradução mais adequada para esse termo provavelmente seria conformidade.

Pode ser definido também, conforme Manzi (2008), como sendo o ato de cumprir, de estar em conformidade e executar regulamentos internos e externos, impostos às atividades da instituição, buscando mitigar o risco atrelado à reputação e ao regulatório/legal. Desse modo, busca-se um relacionamento mais ético, transparente e honesto entre pessoas jurídicas, seja interno ou externo a essas.

Os autores (CANDELORO et. al., 2012), elucidam o termo como: um conjunto de regras, padrões, procedimentos éticos e legais que, uma vez determinados e implementados, será o norte de orientação do comportamento da instituição no mercado em que possui atuação, bem como seus funcionários irão receber essas mudanças implantadas.

É, portanto, um instrumento capaz de controlar o risco de imagem e o risco legal, os chamados 'riscos de compliance', a que se sujeitam as instituições no curso de suas atividades (CARVALHO, 2012, p. 30).

Aferimos então, que o compliance é um conjunto de regras, padrões, procedimentos éticos e legais que, uma vez definido e implantado, será a linha mestra que orientará o comportamento da instituição no mercado em que atua, bem como as atitudes de seus funcionários.

Para Duarte (2014), o termo compliance significa colocar as pessoas jurídicas na mesma sintonia das leis. Enquadrar as organizações na lei, fazer com que essas evitem a prática de atos lesivos à Administração Pública e dessa forma cooperem para um mercado mais íntegro. Com o compliance, busca-se um relacionamento mais ético, transparente e honesto entre pessoas jurídicas, seja interno ou externo a essas.

No cenário mundial o compliance se mostra cada vez mais necessário e presente. Uma vez que a inclinação é a de buscar um cenário econômico mais seguro, transparente, justo e ético. Principalmente no tocante a confiança das relações negociais e segurança das informações (BONOMA, 2005)

A atuação do compliance é de extrema relevância no vigente contexto, devido à constatação de que o Estado por si só não consegue deter um controle absoluto das entidades econômicas e por isso necessita do auxílio do mecanismo de conformidade, que serve como um assessor privado do Estado. Exerce, por exemplo, a função de fiscalização das entidades financeiras e possui caráter de prevenção.

Além disso deve-se ter em mente que não se pode ter um Estado que não faça nenhuma intervenção, pois nenhum dos extremos funciona, nem a intervenção total, tão pouco a falta dessa. Para os autores (RIOS; ANTONIETTO, 2015, p. 346):

[...] modelos extremos se mostraram falhos, primeiro porque o Estado com suas limitações estruturais não consegue regular e controlar as especificidades de cada empresa e o incremento do risco gerado no âmbito de suas atividades, segundo porque as empresas possuem outros interesses econômicos que se sobressaem ao da autorregulação, não conferindo a atenção demandada pelos mecanismos de prevenção dos perigos provenientes de sua atividade.

Conforme Reale (2002), o Comitê da Basileia Tem destacado a alta relevância dos riscos de compliance e de sua função nos bancos. A expressão risco de compliance é definida como risco legal, ou de sanções regulatórias, de perda financeira ou de reputação que um banco pode sofrer como resultado de falhas no cumprimento de leis, regulamentações, códigos de conduta e das boas práticas bancárias.

Para entender perda de reputação, parte-se do pressuposto que está se baseia na síntese de como os clientes e acionistas veem a organização. Essa avaliação fundamenta-se na identidade da organização, inclusive nas informações fornecidas pela empresa sobre sua visão estratégica, assim como nas ações no decorrer do tempo.

Na percepção da organização por parte de pesquisadores de opinião e terceiros com credibilidade, e no desempenho, como lucratividade e responsabilidade social.

O risco atrelado à reputação é, portanto, a perda em potencial na reputação, que poderia levar a publicidade negativa, perda de rendimento, litígios caros, declínio na base de clientes e falência.

Uma ampla avaliação desse tipo de risco é uma estimativa da atual posição da organização por seus clientes e acionistas e de sua capacidade de operar com sucesso no mercado.

Risco regulatório, ou seja, de sanções regulatórias, relaciona-se à não conformidade com leis, regulações e padrões de compliance que englobam matérias como gerenciamento de segregação de função, conflitos de interesse, adequação na venda dos produtos (código do consumidor), prevenção à lavagem de dinheiro, entre

outras. Esse arcabouço regulatório tem como fonte: as normativas de órgãos reguladores como Banco Central e Comissão de Valores Mobiliários, leis, convenções do mercado, códigos e padrões estabelecidos por associações de bancos e códigos de conduta internos aplicáveis aos profissionais dos bancos (MARX, 2008, p.39).

Quando tratamos da segurança das moedas digitais, o mercado e os Estados não escondem que o principal medo são as fraudes relacionadas a falta de segurança de rede, e a lavagem de dinheiro.

A declaração polêmica do CEO da Siemens, Joe Kaeser (2017) à revista *Época Negócios* é sinal claro desta inquietação, ele inicia falando que Bitcoins é maior ferramenta de lavagem de dinheiro da Internet, e ainda cita o sistema do Blockchain como “facilitador” de tais fraudes, ou seja, não é à toa que ainda haja muita insegurança por parte do mercado, visto que por mais tecnológica que seja o momento em que estamos vivendo, a presença de organismos físicos e aparatos físicos mercadológicos são responsáveis diretos pela credibilidade dos ativos.

Se por um lado, o blockchain proporciona uma avançada criptografia que impedia fraudes nas operações, por outro a tamanha segurança nas transações com as criptomoedas concedeu aos investidores uma condição de anonimato quase absoluto.

A falta de necessidade de identificação no sistema criou um campo fértil para ações criminosas, como a lavagem de dinheiro. Agregando assim o uso do compliance que se tornou necessário para atrair os investidores idôneos interessados nesse mercado. Aliás, virou um aliado da tecnologia blockchain para garantir de volta uma boa reputação do setor.

O conceito de estar em conformidade ganha uma importância ainda maior após anúncio de que o Banco Central, a Comissão de Valores Mobiliários (CVM) e a Superintendência de Seguros Privados anunciaram a intenção de implantar um modelo de sandbox (máquina virtual) regulatório no Brasil, com a meta de aumentar a segurança desses processos digitais.

O ordenamento jurídico brasileiro enfrenta desafios significativos no que diz respeito às criptomoedas. Com o crescimento do mercado e a falta de regulamentação específica. A ausência de controle centralizado sobre o fluxo das criptomoedas possibilita que organizações criminosas e grupos terroristas utilizem esses ativos para seus próprios fins.

A questão mais complexa em relação às criptomoedas é justamente o fato de não haver um ente central oficial que intermedeie ou supervisione as transações.

Comentam Narayanan et. al., (2016) que há quem defina as criptomoeda como um meio alternativo de pagamento e neste caso até como um meio experimental, que tem suas vantagens, como as baixas taxas de uso, mas também tem desvantagens, como serem utilizadas para comprar coisas ilegais e realizar lavagem de grande quantia de dinheiro, além de poder ser facilmente roubado através de ataques virtuais.

Todavia, tais desvantagens não se traduzem como exclusividade deste instrumento, tendo em vista que as moedas oficiais também podem ser roubadas, inclusive através de ataques virtuais, mas quanto à lavagem de dinheiro e a compra de algo ilícito há um agravante, tendo em vista que as transações deste instrumento não são rastreáveis.

Para entender o que a inexistência de um ente central implica, consideremos a seguinte hipótese: se uma pessoa compra um livro pela internet e realiza o pagamento com cartão de crédito, a empresa de cartão de crédito retirará o valor correspondente da conta dessa pessoa e depositará o mesmo valor na conta de quem vendeu o livro.

Sem a existência desse intermediário, o dinheiro virtual poderia ser gasto várias vezes: ao enviar o dinheiro da minha “carteira” virtual para outra pessoa, uma cópia desse arquivo dinheiro continua no meu computador. É como um anexo de e-mail – ao enviar um documento, o documento original continua comigo. Sem que haja alguém para controlar quem enviou o quê e “excluir” o arquivo-dinheiro da minha conta, as margens para fraude são significativas.

O Bitcoin foi o primeiro sistema a impedir que isso acontecesse, por meio de um esquema conhecido como blockchain. Comenta Ulrich (2014), que o blockchain nada mais é do que um grande banco de dados público, contendo o histórico de todas as transações realizadas.

Novas transações são verificadas contra o *blockchain* de modo a assegurar que os mesmos *Bitcoins* não tenham sido previamente gastos, eliminando assim o problema do gasto duplo. A rede global *peer-to-peer*, composta de milhares de usuários, torna-se o próprio intermediário (ULRICH, 2014, p.18).

Blockchain é um banco de dados público, distribuído pela Internet entre os mineradores. Nele são registradas todas as transações realizadas com a criptomoeda.

Ressalta Thomson (2017) que o blockchain tem as informações completas sobre endereços e balanços desde o bloco gênese (as primeiras transações realizadas) até o mais recente e completo bloco.

Os blocos são adicionados a blockchain em ordem cronológica linear. O significado do nome vem de sua implementação: estruturas de dados em que um bloco de dados “aponta” (possui um ponteiro) para o bloco anterior, “seu bloco pai”, formando uma cadeia de blocos.

Esse ponteiro é implementado utilizando o hash do bloco anterior, mantendo assim a integridade dos dados na cadeia, pois qualquer modificação em dados anteriores mudará o valor do hash do ponteiro. Cada bloco contém um conjunto de transações que é acessível por meio de uma árvore de dados que também implementa ponteiros hash (Merkle Tree).

Conforme Almeida (2016) a função hash é uma função matemática, ou de outra forma, que leva a uma sequência de entradas de comprimento variável e converte para uma saída de comprimento fixo, que geralmente são menores do que a entrada.

Através das funções hash as informações enviadas são verificadas, quando a mensagem digital provê autenticação, integridade e a não rejeição, pode-se denominar assim de assinatura digital. Há três possibilidades de se obter esta assinatura, utilizando algoritmos simétricos, funções hash ou através de uma terceira parte de confiança. A Bitcoin utiliza tanto a função hash, como algoritmos simétricos.

O processo de mineração incrementa essa cadeia adicionando um novo bloco no final (append-only). Logo, todas as transações contidas nesse bloco são salvas e quanto mais mineradores consentirem que determinado bloco faz parte da blockchain, mais efetivamente as transações desse bloco estão confirmadas.

Todas as movimentações financeiras estão gravadas no blockchain desde que a primeira transação com Bitcoin, com data e hora impossibilitando que ocorram falsificações. Afirma César (2019) que:

A segurança da Bitcoin depende do processo de conectar todas as transações. Imagine se uma nota de um dólar fosse rastreada todas as vezes que foi usada desde que foi impressa até ser retirada de circulação. Todo refrigerante, pacote de balas, flor ou brinquedo que foi comprado com esse dólar seria gravado. Se um falsificador fizesse uma cópia desse dólar ele

estaria registrado em posse do dono verdadeiro e quando o criminoso fosse tentar gastá-lo não conseguiria, porque a segurança interna não aprovaria a transação (CÉSAR, 2019, p.12).

A blockchain é formada pela união de blocos que compreendem o processamento e confirmação de cada transação. Atualmente, para cada novo bloco inserido na blockchain, o minerador ganha 25 unidades de bitcoin (cerca de R\$ 41.125,00) e por definição esse valor diminui pela metade a cada 210.000 blocos (cerca de 4 anos).

Essa recompensa representa a emissão de novas unidades de moeda e é realizada por meio de uma transação especial, chamada coinbase transaction, criada pelo próprio minerador e atribuída a um endereço de sua escolha. Devido ao protocolo em que blocos são adicionados à blockchain a um intervalo conhecido, sua capacidade máxima de transações é limitada pelo tamanho máximo do bloco e por esse intervalo.

O tamanho máximo de um bloco é de 1 MB (1 000 000 bytes) e esse valor é uma constante hardcoded no software padrão que foi introduzida por Nakamoto em julho de 2010. Considerando que uma transação tem em média 250 bytes e lembrando que é esperado em média 1 novo bloco a cada 10 minutos (600 segundos), tem-se: $1\ 000\ 000 / 250\ \text{bytes} = 4\ 000$ transações (tx) por bloco e então $4\ 000 / 600\ \text{s} = 6.6$ tx/s.

Pode-se dizer que os mineradores executam quatro funções: Armazenam e propagam a blockchain; validam novas transações; emitem novas unidades da criptomoeda e votam em um consenso com seu poder computacional.

Conforme Narayanan et al., (2016), para cada novo bloco ser agregado é preciso resolver um problema matemático de alta complexidade, formulado a partir dos dados de toda a blockchain e das novas se dá através de *Proof-of-work*, evitando gastos duplos e ação mal intencionada. Ter poder para redirecionar a *blockchain*, ou seja, atribuir blocos com transações ilegítimas, exigira mais potência em computação que toda a rede *bitcoin*.

É, ainda, uma plataforma para que todos saibam o que é verdadeiro, pelo menos no que diz respeito à informação estruturada gravada. No seu aspecto mais básico, é um código-fonte aberto: qualquer um pode, gratuitamente, baixá-lo, executá-lo e usá-lo para desenvolver novas ferramentas para o gerenciamento de transações on-line. Como tal, ele tem potencial para desencadear inúmeras novas aplicações, além da capacidade iminente de transformar muitas coisas (KEVIN, 2017, p. 36).

É possível inferir, que mesmo com as possibilidades de falha explicitadas, o Blockchain, e por consequência, as criptomoedas que dele derivam, são efetivamente seguras no ponto de vista tecnológico, uma vez que não há que se falar em segurança absoluta em nenhuma das formas de transações financeiras, desde o escambo, até atualmente nas moedas digitais, existem possibilidades de fraudes, o que não impede, dentro de um certo limiar, de considerarmos essa tecnológica monetária segura para o uso.

Entretanto, essa a solução apresentada pela bitcoin, abrange tão somente a questão da segurança tecnológica, não abrangendo os demais cenários de utilização indevida e até ilegal que a moeda possa vir a ter.

Por isso, é especialmente importante estudar as suas consequências jurídico-econômicas e compreender, assim, que hipóteses seriam mais apropriadas, por parte do Estado, para lidar com essa tendência econômica e com a sua respectiva criação de valor e adoção pelo mercado.

CAPÍTULO 3 – A LEI Nº 14.478/2022 E A REGULAMENTAÇÃO DOS ATIVOS FINANCEIROS VIRTUAIS NO BRASIL

Em 21 de dezembro de 2022, foi publicada a Lei nº 14.478/2022, também conhecida como “Marco Legal das Criptomoedas”, que tem como objetivo regulamentar a prestação de serviços de ativos virtuais. De acordo com o art. 3º da lei, ativo virtual é definido como a representação digital de valor que pode ser negociada e transferida por meios eletrônicos, sendo utilizada para pagamentos ou investimentos, incluindo criptomoedas e tokens não fungíveis.

A prestação de serviços relacionados a ativos virtuais somente será permitida mediante autorização de órgão ou entidade da Administração Pública Federal, a ser definido pelo Poder Executivo. Além disso, esses serviços devem obedecer a diretrizes de livre iniciativa e concorrência, seguir boas práticas de governança, garantir transparência, segurança da informação, proteção de dados pessoais e dos consumidores, e atender às medidas de prevenção à lavagem de dinheiro e ao financiamento do terrorismo, entre outras regulamentações.

O Código Penal também foi modificado para incluir o crime de fraude envolvendo a utilização de ativos virtuais, valores mobiliários ou ativos financeiros, sujeitando os infratores a penas de 4 a 8 anos de prisão, além de multa.

3.1 Discussões no entorno da emergência da Lei nº 14.478/2022

Primariamente, a discussão existente está dentro das questões da natureza jurídica da moeda digital, inicialmente, para tratamos sobre as questões jurídicas aplicáveis as criptomoedas dentro do nosso arcabouço jurídico brasileiro, devemos entender qual sua natureza jurídica, para então passarmos as disposições aplicáveis.

A natureza jurídica refere-se à classificação ou categoria legal de um determinado objeto, entidade ou fenômeno sob a perspectiva do Direito. É o entendimento sobre a natureza ou essência jurídica de algo, ou seja, como a lei o reconhece e trata.

No universo do Direito, a questão da natureza jurídica das criptomoedas tem sido debatida repetidamente, especialmente por entusiastas das tecnologias de informática. Essa pluralidade de formas assumidas pelas criptomoedas pode resultar

em diversas classificações jurídicas para o mesmo fenômeno, o que pode ser intimidante para muitos profissionais que ainda não estão totalmente familiarizados com as novas tecnologias.

A primeira discussão relevante, acerca da natureza jurídica das criptomoedas está entre considera-la uma ICO (Da sigla em inglês, ICO significa Initial Coin Offering, traduzido como oferta inicial de ativos virtuais ou oferta inicial de moedas) ou se ela seria uma moeda propriamente dita.

De fato, um token virtual pode facilmente ser considerado uma moeda, caso seja usado em uma determinada localidade como unidade de conta, reserva de valor e meio de pagamento, além de atender aos critérios teóricos adotados pela comunidade para definir uma moeda.

Além disso, o mesmo token pode ser considerado um valor mobiliário, especialmente se se assemelhar a uma Initial Coin Offering (ICO), com características próprias de um título ou contrato de investimento coletivo que oferece direitos de participação, parceria ou remuneração sobre um empreendimento, cujos rendimentos provêm do esforço de terceiros, conforme a Medida Provisória 10.198/2001 no Brasil.

Outra possibilidade é que o token seja considerado um bem incorpóreo, com poucas especificações, como a Receita Federal brasileira faz para fins de tributação. Diante dessa vasta gama de classificações, é inevitável pensar em uma verdadeira mudança de paradigma jurídico imposta pelos ventos da inovação tecnológica. As criptomoedas desafiam os sistemas jurídicos existentes e requerem uma abordagem cuidadosa para garantir que a regulamentação acompanhe o ritmo acelerado das novas tecnologias.

O estudo sobre as hipóteses mais apropriadas deve ocorrer através da análise de questões pontuais e das leis vigentes em outros ordenamentos jurídicos. Um dos aspectos essenciais, para regular a moeda refere-se à classificação tributária dada pelo Estado. Essa sistematização é importante tanto no sentido de evitar evasão fiscal quanto, para dar uma noção mais exata ao Estado dos investimentos dos cidadãos.

É seguro afirmar, por isso que a positivação de normas tributárias com relação ao dinheiro virtual deve ser prioritária. A moeda, nesse aspecto, lança questionamentos sobre o Direito de propriedade, pois serve não somente como sistema de pagamento, mas foi classificada pelo Internal Revenue Service dos Estados Unidos (órgão tributário nos Estados Unidos) como uma propriedade (IRS, 2014).

Da mesma forma, o Canadá também considerou a moeda como propriedade e obrigou as empresas a declararem as vendas efetuadas por meio de bitcoins e os lucros com a especulação da moeda (DESCÔTEAUX, 2014). Ademais:

No plano internacional, despertou especial atenção a regulação da Canadian Securities Administrators no que se refere às ICO's[2]. O órgão do Canadá, que faz as vezes de uma Comissão de Valores Mobiliários (CVM) no país, além de ter deixado claro que cada ICO é única do ponto de vista jurídico e precisa ser avaliada por suas características próprias, estabeleceu um método composto por quatro regras básicas para se definir quando a ICO se reveste de aspectos típicos de valores mobiliários. Segundo o órgão executivo, a ICO adquire característica de contrato de investimento do gênero quando (1) se caracterizar como um investimento de dinheiro (2) aplicado a um empreendimento conjunto e (3) que apresente expectativa de lucro (4) que advenha significativamente do esforço de terceiros. (CUNHA FILHO; VAINZOF, 2023, s. p.)

A maioria dos países provavelmente evitará classificar a bitcoin como dinheiro virtual, devido às consequências desconhecidas de tal ação, preferindo se ater a termos mais seguros, contrariamente ao que foi feito pela Alemanha, que classificou a moeda como dinheiro privado e não como propriedade.

O Brasil tem adotado uma postura de conciliação e apoio às moedas locais, porém ainda não apresentou nenhuma medida que as regulou e gere maior segurança para as pequenas comunidades que geralmente as usufruem.

Conforme (MARTINS, 2016), embora haja, no campo econômico, forte tendência para se admitir as moedas criptografadas como moedas de fato ou moedas em processo de formação, há uma grande dificuldade de categorização do instrumento na categoria jurídica de moeda, tendo em vista a não existência de autoridade responsável pela sua emissão.

Nesse sentido, a não categorização como moeda faz com que as transações em moedas criptografadas não sejam vedadas pelo curso forçado da moeda (art. 43 da Lei de Contravenções Penais); os contratos com moedas criptografadas não seriam de compra e venda, com obrigação de pagar, mas sim um contrato de troca ou permuta, ou seja, um escambo de bens, que forma obrigações de dar coisa certa.

A regulamentação que existe atualmente no ordenamento jurídico brasileiro, diz respeito tão somente as empresas que negociam as moedas digitais, a lei que regulamenta o mercado de criptomoedas, lei 14.478/2022 com definição de ativos virtuais, prestadoras e do crime de fraude com utilização de criptoativos e suas penas.

De acordo a lei 14.478/2022, as prestadoras de serviços de ativos virtuais somente poderão funcionar no país mediante prévia autorização de órgão ou entidade da administração pública federal.

Outra discussão sobre o tema, é quanto a demora ou ineficiência de sua aplicabilidade, isso porque, a Lei 14.478/2022, que disciplina a prestação de serviços de ativos virtuais, foi promulgada em 21/12/2022, trazendo uma cláusula de *vacatio legis* de 180 dias a contar de sua publicação. Desse modo, considerando a regra do artigo 8º, caput e § 1º da Lei Complementar nº 95/1998, a nova lei de ativos virtuais no Brasil passará a vigorar a partir de 19/06/2023.

O Brasil ao promulgar a referida lei, entendeu as criptomoedas como mercadorias e não como um ativo financeiro (moeda) em si, isso porque ficou destacado, talvez dentre as únicas regras passíveis de aplicação imediata, a incidência expressa do Código de Defesa do Consumidor e as disposições penais: a equiparação das prestadoras de serviços de ativos virtuais a instituições financeiras para fins de aplicação da lei de crimes contra o Sistema Financeiro Nacional (Lei nº 7.492/1986) e a criação do artigo 171-A no Código Penal, um estelionato com uso de ativos virtuais, valores mobiliários ou ativos financeiros, cuja pena varia de quatro a oito anos de reclusão.

A lei define ativo virtual como 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 desse enquadramento moedas tradicionais (nacionais ou estrangeiras); recursos em reais mantidos em meio eletrônico; pontos e recompensas de programas de fidelidade; e valores mobiliários e ativos financeiros sob regulamentação já existente.

Na prática, essa regulamentação influencia em diversos aspectos na comercialização e circulação de criptomoedas no Brasil. Em primeiro lugar, a prestação de serviços de ativos virtuais, incluindo serviços de intermediação e custódia, só poderá ser exercida mediante autorização estatal prévia.

Porém, ainda não foi definido o órgão ou entidade da administração pública federal responsável por esta autorização, suas hipóteses e parâmetros. Tampouco o rito de autorização foi detalhado, o que só ocorrerá após a edição de regulamentos infralegais que serão realizados muito provavelmente por resoluções do Banco Central.

Em outros termos, qualquer empresa que esteja atuando no setor não sofrerá nenhum tipo de sanção imediata. Nesse contexto, uma vez definido o regulador, deverá ser realizado procedimento de consulta pública com apresentação de uma proposta de norma, colhendo manifestações de todos os agentes de mercado, tal como ocorreu, por exemplo, com a regulamentação do novo marco legal de câmbio pelo Banco Central no passado recente.

Nessas hipóteses, diante de casos concretos, o Ministério Público e o Poder Judiciário poderão se valer das definições de ativo virtual e de serviço de ativo virtual na Lei nº 14.478/2022 para imputar condutas ao novo delito. Essa possibilidade é preocupante, dada a recorrente dificuldade enfrentada, mesmo pelos reguladores específicos do Sistema Financeiro Nacional, de diferenciar ativos virtuais de valores mobiliários, tornando ainda mais complexa a solução do conflito de normas entre pirâmide financeira (artigo 2º, IX, da Lei nº 1.521/1951) e de oferta irregular de valores mobiliários (artigo 5º, II, da Lei nº 7.492/1986). Assim temos:

Mesmo considerada um avanço, a lei – aprovada depois de sete anos de discussões – se omite sobre aspectos como a competência de órgãos sobre a gestão do sistema de ativos digitais. A aposta de Thiago Sombra, sócio de Tecnologia e Compliance do escritório Mattos Filho, é que haja uma atribuição conjunta entre o Banco Central, a Comissão de Valores Mobiliários (CVM) e o Conselho de Controle de Atividades Financeiras (Coaf). (SOUZA, 2023, s. p.)

Necessitamos também tratar do aspecto sob a égide da legislação tributária que depende da descrição legal dada para o bem, para que seja feita a adequação normativa para sua cobrança, tal ponto ainda é objeto de discussão quanto as criptomoedas.

A legislação brasileira ainda é silente quanto aos aspectos fiscais específicos das criptomoedas e da atividade de mineração. Em tom de prenúncio à normatização tributária, a Receita Federal, em seu manual “Perguntas e Respostas – IRPF/2018”, equiparou as moedas virtuais a ativos financeiros, orientando os contribuintes a declararem tais ativos na Ficha Bens e Direitos pelo valor de sua aquisição para, assim, serem tributados quando apurado ganho de capital na sua alienação. (PADILHA; CHAMAS, 2018, s. p.)

Outra questão que pode ser suscitada dentro da discussão sobre criptomoedas é se a competência envolvendo o artigo 171-A do Código Penal, que foi adicionado pela lei 14.478/2022 é da Justiça comum ou da Justiça Federal, isso porque os ativos financeiros podem estar alocados nas mais variadas

geolocalizações, e suas exchanges também, devendo ser feita uma profunda análise sob a ótica do direito penal no tempo e no espaço por parte dos operadores do Direito de doutrinadores da área.

Fato é, que a discussão acerca da nova legislação, e das características das criptomoedas está em sua fase embrionária, necessitando de respostas para as mais variadas questões que são levantadas na prática do uso desses ativos financeiros.

3.2 Criminalização das fraudes que envolvem ativos financeiros virtuais

As fraudes que envolvem ativos financeiros virtuais podem assumir diversas formas, como esquemas de pirâmide, ICOs (Ofertas Iniciais de Moedas) fraudulentas, phishing, hacks em exchanges e roubo de chaves privadas. Essas práticas visam enganar os investidores e usurpar seus fundos ou informações pessoais, causando prejuízos financeiros significativos e comprometendo a segurança dos usuários.

A preocupação com tal prática criminosa se baseia no fato de que as fraudes envolvendo ativos financeiros virtuais podem resultar em perdas financeiras substanciais para os investidores, além de prejudicar a imagem e a credibilidade do mercado de criptomoedas como um todo. A falta de confiança pode afastar potenciais investidores e limitar o desenvolvimento saudável e sustentável do setor. Temos:

A necessidade de regulamentação entende-se porque as operações por meio das moedas digitais são de difícil identificação dos usuários, o que propicia espaço para pessoas com objetivo de práticas delitivas. A capacidade de promover estabilidade monetária associada à vantagem da privacidade financeira a seus usuários, e a não incidência de controle do Banco Central, faz com que o uso deste tipo de moeda se materialize como uma forte tendência para as operações eletrônicas realizadas via ciberespaço, o que apresenta um desafio para a compreensão em termos políticos, econômicos e jurídicos, devido às incertezas quanto ao seu futuro, uma vez que é impossível falar sobre a conduta humana sem abordar possíveis desvios de comportamento que devam ser previstos pela norma jurídica. (SILVA; OLIVEIRA, 2023, p. 14)

A legislação que regulamenta a operação de criptomoedas no território nacional, inovou em alguns sentidos, com a finalidade de penalizar práticas relacionadas ao uso indevido, como fim ou como meio, das criptomoedas de forma ilícita.

Entre os avanços trazidos pela nova lei está a regulamentação de crimes praticados com as criptomoedas, entre os quais estão o estelionato e a lavagem de

dinheiro. A lei insere novos tipos penais em leis já existentes – como o Código Penal e a Lei de Lavagem de Dinheiro –, com aumento de pena caso crimes sejam praticados por meio dos criptoativos.

Entre outros pontos, a lei acrescenta no Código Penal (Decreto-lei 2.848, de 1940) um novo tipo de estelionato, com pena de reclusão de quatro a oito anos e multa. Será enquadrado no crime de fraude com a utilização de ativos virtuais quem organizar, gerir, ofertar ou distribuir carteiras ou intermediar operações envolvendo criptomoedas para obter vantagem ilícita em prejuízo alheio, induzindo ou mantendo alguém em erro. Assim restou a nova redação do Código Penal em seu artigo 171-A:

171-A: Organizar, gerir, ofertar ou distribuir carteiras ou intermediar operações que envolvam 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. (BRASIL, 1940, s. p.)

Quanto ao objeto material da norma penal incriminadora, o legislador utilizou o termo "carteiras" no tipo penal para referir-se às conhecidas carteiras digitais ou e-wallets. Em linhas gerais, uma carteira digital é um programa de computador que proporciona acesso aos ativos virtuais armazenados na blockchain. Entretanto, a fim de estabelecer claramente o que pode ser considerado como carteira digital, é necessário complementar a norma penal com um ato normativo que forneça a definição adequada, ausente no mencionado tipo penal.

É essencial lembrar que, de acordo com o Princípio da Taxatividade, a lei penal deve ser precisa e compreensível, possibilitando que o cidadão comum a entenda adequadamente. É irrealisticamente esperar que todos tenham conhecimento sobre novas tecnologias e criptoativos. A nova lei poderia ter empregado e definido o termo "carteira digital", assim como fez no art. 3º ao definir o conceito de "ativo virtual". É aguardado que o assunto seja abordado no ato normativo regulamentador a ser promulgado pela entidade indicada pelo Poder Executivo federal.

Outra regulamentação de possível uso ilícito que o legislador sabiamente se preocupou em contemplar foi o do uso de criptomoedas não como finalidade do crime, mas como meio, isso porque o mesmo poderia ser utilizado para a lavagem de dinheiro devido a sua complexidade para rastreamento.

Pensando nisso, na Lei de Lavagem de Dinheiro (Lei 9.613, de 1998), a norma inclui os crimes cometidos por meio da utilização de ativo virtual entre aqueles com agravante de um terço a dois terços de acréscimo na pena de reclusão de três a dez anos, quando praticados de forma reiterada.

O texto também determina que as empresas deverão manter registro das transações para fins de repasse de informações aos órgãos de fiscalização e combate ao crime organizado e à lavagem de dinheiro.

O endurecimento da legislação penal e processual penal ocorre em um momento no qual as fraudes envolvendo criptoativos têm aumentado no país. Em pesquisa realizada pela Comissão de Valores Mobiliários (CVM) no ano de 2020, as criptomoedas foram o produto de investimento mais citado pelas vítimas de golpes financeiros, sendo mencionadas por 43,3% dos respondentes. (BLUM, 2023, s. p.)

Depreende-se, então, que a recém-aprovada Lei nº 14.478/2022 possui o propósito de promover uma maior segurança no âmbito dos ativos virtuais, ao mesmo tempo em que busca "atualizar" o Direito Penal em relação a essa contemporânea realidade.

3.3 Segurança da informação e a evitabilidade das fraudes envolvendo ativos financeiros virtuais com uso de blockchain: um olhar a partir dos princípios regentes da Lei nº 14.478/2022

Os princípios que regem a lei 14.478/2022 estão elencados no artigo quarto da referida lei, essas diretrizes norteiam a elaboração e a aplicação do diploma legal, os princípios trazidos são: livre iniciativa e livre concorrência; boas práticas de governança, transparência nas operações e abordagem baseada em riscos; segurança da informação e proteção de dados pessoais; proteção e defesa de consumidores e usuários; proteção à poupança popular; solidez e eficiência das operações; e prevenção à lavagem de dinheiro e ao financiamento do terrorismo e da proliferação de armas de destruição em massa, em alinhamento com os padrões internacionais.

A segurança da informação é um aspecto crucial quando se trata de ativos financeiros virtuais e blockchain. O uso de blockchain como tecnologia subjacente

para criptomoedas e outros ativos digitais introduziu mecanismos avançados de segurança, mas também trouxe desafios adicionais.

A partir dessa gama de diretrizes, o marco legal das criptomoedas, lei 14.478/2022, segue uma tendência mundial que visa regulamentar juridicamente campos da vida que são afetados pelas novas tecnologias, incluindo as emergentes e em desenvolvimento, como é o caso da IA (Inteligência Artificial) e da Blockchain. Muitos países já implementaram regulação sobre o assunto ou possuem projetos em discussão, como é o caso dos Estados Unidos, Canadá, Espanha, Alemanha, Estônia, China, Índia e Austrália.

No Brasil, a legislação teve uma preocupação maior em burocratizar uso de criptomoedas, do que propriamente criar definições e proteções jurídicas e regulamentações negociais e tributárias para esses ativos.

Podemos inferir, que tal medida se demonstrou em caráter repreensivo dos golpes e crimes que ocorrem por intermédio dessas moedas e não com o intuito de organizar o mercado financeiro ou tributário. Tal afirmação vem também do contexto de ampla divulgação das fraudes que tem se tornado corriqueiras com o uso desses ativos financeiros.

A exemplo temos o caso Faraó de Bitcoins. Glaydson Acácio que é suspeito de cometer crimes contra o sistema financeiro. De acordo com as investigações, ele e a esposa teriam um esquema de pirâmide financeira com a fachada de investimento em bitcoins.

Outro caso de grande repercussão foi do jogador de futebol Gustavo Scarpa. Ele teve um prejuízo de R\$ 6,3 milhões ao investir em uma empresa que operava com criptomoedas, indicada por um ex-colega de equipe. A empresa, em questão, não tinha autorização para operar no mercado.

Desse modo, observamos que o “Norte” que rege o marco legal das criptomoedas, é majoritariamente burocrático, exceto pelas rasas definições que traz quanto as criptomoedas e os ativos digitais. Como é o caso do Art. 3º:

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 - 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, a exemplo de pontos e recompensas de programas de fidelidade; e IV -

representações de ativos cuja emissão, escrituração, negociação ou liquidação esteja prevista em lei ou regulamento, a exemplo de valores mobiliários e de ativos financeiros. Parágrafo único. 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. (BRASIL, 2022, s. p.)

Outra questão que deixou espaços vagos na legislação diz respeito aos artigos 6º e 7º da Lei nº 14.478/2022 abordam a questão da entidade reguladora responsável por supervisionar e disciplinar os serviços de ativos virtuais. O artigo 7º detalha as atribuições desse órgão, incluindo a definição das situações em que as atividades ou operações com ativos virtuais serão consideradas no mercado de câmbio ou estarão sujeitas à regulamentação de capitais brasileiros no exterior e estrangeiros no país.

O objetivo do legislador ao estabelecer essa regra pode não estar totalmente claro, uma vez que as criptomoedas, por sua própria natureza, têm a característica de serem facilmente convertidas em moedas fiduciárias de diferentes países do mundo (apesar de serem proibidas em algumas jurisdições).

Isso torna difícil a distinção de operações que devem ser incluídas no mercado de câmbio ou estar sujeitas à regulamentação de capitais estrangeiros. Por exemplo, um investimento realizado por um estrangeiro no Brasil, utilizando reais obtidos através da conversão de criptomoedas, sem a realização de um contrato de câmbio, não deveria ser considerado capital estrangeiro sujeito a registro no Banco Central, uma vez que não afeta as reservas internacionais de divisas do país.

Conclui-se, portanto, que a lei 14.478/2022, trouxe pouco avanço dentro do espectro jurídico no que tange a proteção contra violabilidades e fraudes, uma vez que mesmo com a criação de um novo tipo penal e adequação da Lei de Lavagem de Dinheiro, em pouco houve inovação para que de fato haja maior proteção contra fraudes e crimes envolvendo as criptomoedas.

A nova legislação burocratizou transações criando formas regulatórias, porém, essa burocratização, em tese, produzirá pouco ou nenhum efeito prático na ocorrência de atos ilícitos utilizando-se como meio as criptomoedas.

Por outro lado, válido é destacar que essa burocratização, e a regulamentação primária realizada pela lei 14.478/2022, pode atrair mais usuários para o mercado de criptomoedas, isso porque, a regulamentação das criptomoedas pode trazer diversos

benefícios para o mercado, proporcionando maior segurança, transparência e confiança para os participantes.

A regulamentação pode estabelecer requisitos para as empresas e plataformas que operam com criptomoedas, garantindo que elas adotem medidas para proteger os investidores contra fraudes, golpes e práticas abusivas.

Conforme vimos, mesmo que de forma simplificada, a nova lei traz regulamentações adequadas que exige que as exchanges e outras instituições que trabalham com criptomoedas implementem medidas de prevenção à lavagem de dinheiro e cumpram com obrigações de reporte de atividades suspeitas, ajudando a evitar o uso das criptomoedas para fins ilegais.

Ao regulamentar as atividades relacionadas às criptomoedas, os governos podem reduzir os riscos sistêmicos e proteger a estabilidade financeira, evitando situações de crises ou colapsos que possam afetar negativamente o mercado financeiro como um todo.

E essas regras claras e previsíveis podem atrair mais investidores e empreendedores para o setor de criptomoedas, fomentando a inovação e o desenvolvimento de novas tecnologias e aplicações.

Regulamentações adequadas podem também abrir caminho para a integração das criptomoedas com o sistema financeiro convencional, permitindo, por exemplo, que bancos ofereçam serviços relacionados a ativos digitais, ou até mesmo uma integração com o recente descoberto PIX que tem sido uma ferramenta bancária extremamente útil na realidade brasileira.

Em suma, a regulamentação das criptomoedas pode trazer uma série de vantagens ao mercado, criando um ambiente mais seguro, confiável e propício para o desenvolvimento dessa inovadora classe de ativos digitais. E em outro diapasão a lei 14.478/2022 foi assertiva, porém, insuficiente na tentativa de impedir golpes e fraudes com uso de criptomoedas.

CONSIDERAÇÕES FINAIS

Após uma análise aprofundada sobre a necessidade de regulamentação jurídica das criptomoedas, conclui-se que a falta de um quadro normativo claro pode representar riscos e desafios significativos tanto para os usuários quanto para a sociedade em geral.

A regulamentação jurídica é essencial para garantir a proteção dos direitos e interesses dos usuários de criptomoedas, especialmente em casos de fraudes, roubos e disputas comerciais. A ausência de uma estrutura legal pode dificultar a resolução de conflitos e expor os investidores a maiores riscos.

Ainda, a regulamentação adequada pode contribuir para a prevenção e detecção de atividades ilícitas, como lavagem de dinheiro, financiamento ao terrorismo e evasão fiscal, que possam estar associadas ao uso do Bitcoin. A implementação de medidas de controle e monitoramento pode ajudar a mitigar esses riscos.

A normatização ainda irá ajudar a integrar as criptomoedas ao sistema financeiro tradicional de forma segura, garantindo a estabilidade do mercado e a proteção dos investidores. Isso também pode incentivar o desenvolvimento de tecnologias blockchain e criptomoedas mais confiáveis e ampliar a adoção em diversos setores.

Já no espectro oposto, a falta de regulamentação pode criar incertezas no tratamento tributário das transações com criptomoedas, dificultando a arrecadação de impostos e o cumprimento das obrigações fiscais. Uma legislação clara nesse sentido é fundamental para garantir a justiça fiscal e a sustentabilidade das finanças públicas.

A regulamentação das criptomoedas também pode ser uma oportunidade para o desenvolvimento de políticas inovadoras, que incentivem a inovação tecnológica e a competitividade no setor, sem comprometer a segurança e a proteção dos usuários.

Portanto, a conclusão é de que a regulamentação jurídica das criptomoedas é necessária para criar um ambiente mais seguro, estável e confiável para o seu uso, protegendo os direitos dos usuários, prevenindo atividades ilícitas e garantindo a integração responsável dessa criptomoeda no sistema financeiro e na sociedade como um todo. No entanto, essa regulamentação deve ser elaborada de forma

equilibrada, buscando fomentar a inovação e o desenvolvimento tecnológico, ao mesmo tempo em que se preserva a segurança e a proteção dos interessados.

As criptomoedas já trouxeram inúmeros reflexos para o mundo jurídico e, por isso sua regulamentação é necessária, ao menos, para proibir com que condutas ilícitas sejam realizadas com o auxílio das características próprias da moeda.

A maior parte dos Estados tem decidido dar passos iniciais, como reconhecer a legalidade da moeda ou informar aos seus usuários sobre a cobrança de impostos relacionados ao seu uso e propriedade (GAO, 2013). Por isso, mantêm-se que a posição ideal é a regulamentação, inicialmente, por meio de leis nacionais mais amplas (VELDE, 2013), especialmente sobre questões tributárias e de licença por parte das casas de câmbio.

As regulamentações seguintes, certamente, serão mais restritas e específicas, pois o quadro da moeda criptográfica será mais bem delimitado através de mais análises e de um maior tempo para o desenvolvimento de suas consequências no mundo econômico e jurídico e envolverão questões jurídicas ainda enevoadas ou que não podem ter uma eficácia aparente, como, por exemplo, o respeito ao Direito do Consumidor.

Não é necessário, portanto, que se crie uma legislação extensiva sobre a moeda, pois há o risco de atrofiar essa nova tecnologia, mas o Estado deve reconhecer o seu uso lícito, buscando proteger as pessoas que usam a moeda de maneira legítima e lidar com questões pontuais, como é feito em outros países, inclusive, em razão de benefícios econômicos.

O Brasil com a criação da lei 14.478/2022, deu seu primeiro passo normativo para a regulamentação das transações envolvendo as criptomoedas, nesse sentido, ainda temos muito a evoluir para uma criação eficaz de regras que delimitem as aplicações e uso das moedas digitais.

Conclui-se, portanto, que a regulamentação jurídica das criptomoedas é um desafio relevante e necessário para garantir a segurança e o bom funcionamento desse novo ecossistema financeiro. É preciso considerar as peculiaridades das criptomoedas e as inovações que elas trazem, buscando sempre o equilíbrio entre a proteção dos usuários e a promoção da inovação e do desenvolvimento tecnológico.

Dessa forma, o Brasil poderá aproveitar os benefícios das criptomoedas de forma responsável e segura, posicionando-se de maneira adequada diante das transformações e oportunidades que essa tecnologia oferece para a sociedade

moderna. A legislação, as políticas públicas e a atuação do poder judiciário são fundamentais nesse processo de adaptação e construção de um futuro financeiro mais inclusivo e eficiente.

Por outro lado, o poder judiciário terá que se utilizar dos recursos disponíveis para a interpretação das normas, tal qual os princípios, costumes e doutrinas disponíveis, para evitar um envelhecimento precoce dos dispositivos aplicáveis, e cumprindo assim com o dever do Direito em acompanhar as evoluções sociais.

Sabe-se que as modificações trazidas pelo software ainda não foram totalmente descobertas, mas é de extrema relevância o estudo da moeda e de suas consequências jurídico-econômicas, para compreender a Pós-Modernidade. Espera-se, portanto que a apresentação propedêutica do assunto pelo artigo tenha contribuído para o debate jurídico sobre o tema.

REFERÊNCIAS

ALMEIDA, P. B. A moeda descentralizada na sociedade contemporânea: O caso da Bitcoin P2P digital Currency. Florianópolis. Trabalho de conclusão de curso (Graduação) - Curso ciencias Econômicas, Universidade Federal de Santa Catarina, 2016.

ANTONPOULOS, A. M. (2014). Mastering Bitcoin: Unlocking Digital Cryptocurrencies. O'Reilly Media.

BARDIN, L. (2011). Análise de conteúdo. Edições 70. Blockchain. Revista Gestão.Org, v. 15, Edição Especial, 2017. p. 108-117.

BLUM, Renato Opice. Lei nº. 14.478/2022: uma análise do novo tipo penal do art. 171-A do Código Penal. 2023. Disponível em: <https://pt.linkedin.com/pulse/lei-n-144782022-uma-an%C3%A1lise-do-novo-tipo-penal-art-171-a-opice-blum>. Acesso em: 06 ago. 2023.

BONOMA, J. Compliance: o crescimento da responsabilidade social empresarial. 2005. Dissertação (Mestrado em Direito) - Pontifícia Universidade Católica de São Paulo, São Paulo, 2005.

BONOMA, Thomas V. - Case Research in Marketing: Opportunities, Problems, and Process. Journal of Marketing Research, Vol XXII, May ,2005.

BRASIL. Congresso. Senado. Lei nº 1, de 21 de dezembro de 2022. Lei Nº 14.478, de 21 de dezembro de 2022.

BRASIL. Decreto-Lei 2.848, de 07 de dezembro de 1940. Código Penal. Diário Oficial da União, Rio de Janeiro, 31 dez. 1940.

CAPUCIO, Ricardo. Moeda eletrônica: é vital entender o que está acontecendo. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/moeda-eletronica-e-vital-entender-o-que-esta-acontecendo-25052017>. Acesso em: 05 ago. 2023.

CARVALHO, F. J. C. Moeda, produção e acumulação: Uma perspectiva pós keynesiana. Editora Universidade de Brasília, p. 163-194, 2012.

CARVALHO, Luiz A.P.S. de. Manual de compliance: estrutura, planejamento e implantação. São Paulo: Atlas, 2012.

CÉSAR Luiz. Prática da pesquisa jurídica – idéias e ferramentas úteis para o pesquisador do direito. 8. ed. rev. atual. amp. Florianópolis: OAB/SC Editora, 2019. 243 p.

COHEN, Benyamin. Bitcoin Regulation: Securities, Derivatives, Prediction Markets, and Gambling. SSRN Electronic Journal, 2004.

COHEN, P.. Virtual currency schemes. Frankfurt Am Main:European Central Bank, 2004 . Disponível em:<
<https://www.lume.ufrgs.br/bitstream/handle/10183/116267/000953619.pdf>>

CULTURA MIX. História da bolsa de valores no Brasil. Disponível em:
<https://www.culturamix.com/dinheiro/historia-da-bolsa-de-valores-do-brasil/> . Acesso em: 04 ago. 2023.

CUNHA FILHO, Marcelo de Castro; VAINZOF, Rony. A natureza jurídica “camaleão” das criptomoedas. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/a-natureza-juridica-camaleao-das-criptomoedas-21092017>. Acesso em: 05 ago. 2023.

DALL’AGNOL, Nádia de Almeida; GUTH, Sergio Cavagnoli. BITCOIN: ESTUDO SOBRE CONHECIMENTO E PERCEPÇÃO DA MOEDA VIRTUAL DOS ALUNOS DO CAMPUS VACARIA-CAMVA DA UNIVERSIDADE DE CAXIAS DO SUL. Disponível em:
<https://repositorio.ucs.br/xmlui/bitstream/handle/11338/11598/Artigo%20Nadia%20de%20Almeida%20Dall%27%20Agnol.pdf?sequence=1&isAllowed=y>. Acesso em: 29 jul. 2023.

DEQUECH, Nikolei M. Nerdy Money: Bitcoin, the Private Digital Currency, and The Case Against its Regulation. Loyola Consumer Law Review, Vol. 25:1 no 111, 2012-2007

DUARTE, George. Primitive Money. In: G. Dalton (org) Tribal na peasant economies. Readings in economy anthropology. New York Press, 2014 pp.254-81. URL
http://www.bylany.com/kvetina/kvetina_etnoarcheologie/literatura_eseje/5_literatura_obchod.pdf. Acesso em: 23 de junho de 2023.

DUARTE, P.C. Compliance e governança corporativa. Revista Eletrônica Direito Informático. Porto Alegre, vol. 4, n. 1, 2014.

ÉPOCA NEGÓCIOS. Bitcoin é maior ferramenta de lavagem de dinheiro da Internet, diz CEO da Siemens. Disponível em:
<https://epocanegocios.globo.com/Empresa/noticia/2017/07/bitcoin-e-maior-ferramenta-de-lavagem-de-dinheiro-da-internet-diz-ceo-da-siemens.html>. Acesso em: 19 de junho de 2023.

FAMA, E. Banking in the theory of finance. Journal of Monetary Economics, vol. 6, p. 39-57, 2018

FAMA, Rubens. Compliance: a nova aposta do mercado. São Paulo: Lura Editorial, 2018.

FERREIRA et al. Estudo De Mapeamento Sistemático Sobre As Tendências E Desafios Do

FONSECA, Brian. The Bitcoin big bang: how alternative currencies are about to change the world. New Jersey: Wiley, 2009

FRANCO, M, BAZAN, A. Metodologia Científica. Porto Alegre: Editora Atlas, 2018.

GAO (UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE), Virtual economies and currencies: Taxation of Virtual Economies and Currencies, mai. 2013.

GONÇALVES, Cleber Baptista. Casa da Moeda do Brasil, 290 anos de história, 1694-1984 Rio de Janeiro, 1985.

GONÇALVES., Ariane. O Que é Phishing? Dicas para Evitar Golpes na Internet. 2023. Disponível em: <https://www.hostinger.com.br/tutoriais/o-que-e-phishing-e-como-se-proteger-de-golpes-na-internet>. Acesso em: 04 ago. 2023.

HAYEK, Melanie. Blockchain: blueprint for a new economy. Sebastopol: O'Rilley Media Inc., 2011.

INFOESCOLA. História da bolsa de valores no Brasil. Disponível em: <https://www.infoescola.com/economia/bmf-bovespa/> . Acesso em: 04 ago. 2023.

INFOMONEY. Exchange de criptomoedas: o que são e como escolher uma? 2022. Disponível em: <https://www.infomoney.com.br/guias/exchange-de-criptomoedas/>. Acesso em: 04 ago. 2023.

JOE , K. Desestatização do Dinheiro: Uma análise da teoria e prática das moedas simultâneas. São Paulo. Instituto Ludwig von Mises. Brasil, 2017.

KEVIN , T. MEREDITH, Michael W. Rethinking virtual currency regulation in the Bitco in age. Washington.2017.

KSHETRI, N. (2018). Blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management*, 39, 80-89.

LAGO, Luiz Aranha Corrêa do. A MOEDA METÁLICA EM PERSPECTIVA HISTÓRICA : NOTAS EM TORNO DE UMA EXPOSIÇÃO. 2004. 86 f. TCC (Graduação) - Curso de Economia, Puc, Rio de Janeiro, 2004. Disponível em: <https://www.econ.puc-rio.br/uploads/adm/trabalhos/files/td481.pdf>. Acesso em: 22 jul. 2023.

MANZI, V. M. R. O compliance como estratégia de gestão da qualidade. 2008. Tese (Doutorado em Engenharia de Produção) - Universidade Federal de Santa Catarina, Florianópolis, 2008.

MARCONI, M.A. ;LAKATOS, E.M. Metodologia Científica. São Paulo. Editora Atlas, 2017

MARTINS, G. A. & Pinto, R.L. Manual para elaboração de trabalhos acadêmicos, São Paulo: Atlas, 2001.

MARTINS, Armando Nogueira da Gama Lamela. Quem tem medo do bitcoin? ofuncionamento das moedas criptografadas e algumas perspectivas de inovações institucionais. *RJLB*, Ano 2 (2016), nº 3, 137-171. Disponível em: <http://www.cidp.pt/publicacoes/revistas/rjlb/2016/3/2016_03_0137_0171.pdf>. Acesso em: 15 de junho de 2023.

MARX, Marcia Carla Pereira Ribeiro. O compliance no combate à lavagem de dinheiro nos bancos. 2008. Dissertação (Mestrado em Direito) - Pontifícia Universidade Católica de São Paulo, São Paulo, 2008.

MARX, P. . Opinion on 'virtual currencies'. 2008. Disponível em: <<http://www.ucs.br/etc/conferencias/index.php/mostraucsppga/xviiiimostrappga/paper/viewFile/5965/1969>>.

MORABITO, V. Business Innovation Through Blockchain. Springs, 2017. Disponível em:

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Disponível em: <https://bitcoin.org/bitcoin.pdf>

NAKAMOTO, Satoshi, Bitcoin: a peer-to-peer electronic cash system. (2008). Disponível em:< <https://bitcoin.org/bitcoin.pdf>>.

NARAYANAN, A., BONNEAU, J., FELTEN, E., MILLER, A., and Goldfeder, S. (2016). Bitcoin and cryptocurrency technologies. Princeton University Press

OLIVEIRA, F. S. (2019). Criptomoedas: uma análise das questões regulatórias e jurídicas. *Revista de Finanças Digitais*, 42(3), 212-228.

PADILHA, Maria Ângela Lopes Paulino; CHAMAS, Henrique Nimer. Incertezas na tributação de mineração de criptomoedas pelo imposto sobre a renda. 2018. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/incertezas-na-tributacao-de-mineracao-de-criptomoedas-pelo-imposto-sobre-a-renda-24122018>. Acesso em: 06 ago. 2023.

REALE, Mário. *Direito Bancário*. 16ª edição. São Paulo: Saraiva, 2002.

REALE, Miguel. *Teoria tridimensional do direito*. 5 ed. Ver. E aum. - São Paulo, Editora Saraiva, 2002. 161p

RIOS, Rodrigo; ANTONIETTO, Caio. Prevenção e minimização de riscos na gestão da atividade empresarial. *Revista Brasileira de Ciências Criminais*, São Paulo, v.23, n. 114, p.346, maio/jun. 2015.

ROTHER, E. T. (2007). Revisão sistemática X revisão narrativa. *Acta Paulista de Enfermagem*, 20(2), v-vi.

SANTIAGO, Emerson. ESCAMBO. Disponível em: <https://www.infoescola.com/economia/escambo/>. Acesso em: 21 jul. 2023.

SILVA, A. B. (2018). Evolução histórica do dinheiro: do escambo às criptomoedas. *Revista de Direito Econômico*, 35(2), 78-94.

SILVA, Kairo Freire da; OLIVEIRA, Sara Beatriz Pereira de. LAVAGEM DE CAPITALS ATRAVÉS DE CRIPTOMOEDAS E SUA REGULAMENTAÇÃO NO DIREITO BRASILEIRO. 2023. 21 f. TCC (Doutorado) - Curso de Direito, Pontifícia Universidade Católica, Natal, 2023.

SILVEIRA, Mariana da. A relação entre a tecnologia blockchain e a segurança cibernética. 2022. Disponível em: <https://www.brasiliano.com.br/a-relacao-entre-a-tecnologia-blockchain-e-a-seguranca-cibernetica-newsletter>. Acesso em: 04 ago. 2023.

SOUZA, C. L., & Santos, M. R. (2015). A regulamentação do papel-moeda e a evolução do sistema financeiro. *Anais do Congresso Nacional de Economia*, 20, 154-166.

SOUZA, Mazé de. O que muda com a entrada em vigor do Marco Legal das Criptomoedas? Disponível em: <https://www.jota.info/coberturas-especiais/regulamentacao-criptoativos/o-que-muda-com-a-entrada-em-vigor-do-marco-legal-das-criptomoedas-16022023>. Acesso em: 06 ago. 2023.

SWAN, M. (2015). Blockchain: blueprint for a new economy. O'Reilly Media.

TAPSCOTT, D., & Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. Penguin.

THOMSON, R. Understanding Modern Money, Eduard Elgar, 2017

ULRICH Eitan ;RON, L Transforming Command: the pursuit of Mission Command in the U.S., British and Israeli Armies. Stanford Security Studies. Standford University Press. California, USA, 2014.

ULRICH, FERNANDO. Bitcoin, A Moeda Na Era Digital, 1º edição, Instituto Ludwig Von Mises Brasil, São Paulo, 2008. Pags. 95 e 96.

VELDE, François R.. Bitcoin: A primer, Chicago Fed Letter. The Federal Reserve Bank, n. 317, dez. 2013.

WRIGHT, A.; DE FILIPPI, P. Decentralized Blockchain Technology and the Rise of Lex Cryptographia. New York: Social Science Research Network, 2015.

ZANINI, Ana Julia. BLOCKCHAIN E O DIREITO NA ÁREA DIGITAL. 2023. 78 f. TCC (Graduação) - Curso de Direito, Centro Universitário Curitiba Faculdade de Direito de Curitiba, Curitiba, 2023.