UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE GESTÃO E ECONOMIA
CURSO DE ESPECIALIZAÇÃO EM GESTÃO FINANCEIRA

RICARDO VIEIRA ROSA

ANÁLISE DE VIABILIDADE DA CRIPTOMOEDA BITCOIN COMO MEIO DE PAGAMENTO

MONOGRAFIA DE ESPECIALIZAÇÃO

CURITIBA
2018

RICARDO VIEIRA ROSA

ANÁLISE DE VIABILIDADE DA CRIPTOMOEDA BITCOIN COMO MEIO DE PAGAMENTO

Monografia de Especialização apresentada ao Departamento Acadêmico de Gestão e Economia da Universidade Tecnológica Federal do Paraná como requisito para obtenção do título de “Especialista em Gestão Financeira”.

Orientador: Prof. Dr. Ricardo Lobato Torres

CURITIBA
2018

TERMO DE APROVAÇÃO

ANÁLISE DE VIABILIDADE DA CRIPTOMOEDA BITCOIN COMO MEIO DE PAGAMENTO

Esta monografia foi apresentada no dia 28 de junho de 2018, como requisito parcial para a obtenção do título de Especialista em Gestão Financeira, do Departamento Acadêmico de Gestão e Economia da Universidade Tecnológica Federal do Paraná, Câmpus Curitiba. O Ricardo Vieira Rosa apresentou o trabalho para a Banca Examinadora composta pelos professores abaixo assinados. Após a deliberação, a Banca Examinadora considerou o trabalho aprovado.

_____
Prof. Dr. Ricardo Lobato Torres
Orientador

_____
Prof. Dr. Antônio Barbosa Lemes Jr
Banca

_____
Prof. Dr. Paula Daniel de Sousa
Banca

Visto da coordenação:

_____
Prof. Dr. Antônio Barbosa Lemes Jr.

RESUMO

Desde a criação da *internet*, muitas empresas que souberam aproveitar seu potencial, tiveram destaque em seus negócios, adquirindo uma vantagem significativa sobre seus concorrentes, algumas até foram além e conseguiram mudar setores já consolidados. Muito se tem visto de pequenas organizações que se tornaram disruptivas de modelos de negócios, com mudanças que afetam diretamente a economia e a forma como a sociedade vive, alcançando até mesmo o âmbito das moedas, que até o presente momento havia sido controlado de forma centralizada e monopolista por instituições financeiras. Com o advento da tecnologia *Blockchain*, possibilitou-se a criação de uma moeda virtual, chamada *Bitcoin*, que utiliza provas criptográficas como demonstração de confiança para seus usuários em transações na plataforma, possibilitando inúmeros benefícios para os utilizadores, entre eles o baixo custo por transação, facilidade de transporte, transparência e principalmente a ausência de terceiros para o controle da moeda, permitindo que seu valor seja ajustado pelo mercado, podendo ser encarado também como um risco devido sua volatilidade Ainda que pareça muito promissor, muita resistência pode ser percebida atualmente, entendendo-se que enquanto pessoas e empresas não se aprofundarem no conhecimento dessa inovação, todo o sistema de pagamento realizado por criptomoedas poderá estar comprometido pelos próximos anos.

Palavras-chave: Bitcoin. Criptomoeda. Blockchain. Moeda virtual. Meio de pagamento.

ABSTRACT

Since the creation of the Internet, many companies that have been able to take advantage of their potential have excelled in their businesses, gaining a significant advantage over their competitors, some even went beyond and have managed to change sectors already consolidated. Much has been seen of small organizations that have become disruptive of business models, with changes that directly affect the economy and the way society lives, reaching even the scope of the currencies, which until the present moment had been centrally controlled and monopoly by financial institutions. With the advent of Blockchain technology, it was possible to create a virtual currency, called Bitcoin, which uses cryptographic evidence as a demonstration of trust for its users in transactions on the platform, allowing numerous benefits for users, including low transaction costs, ease of transportation, transparency and mainly the absence of third parties to control the currency, allowing its value to be adjusted by the market, and can be considered as a risk due to its volatility. Although it seems very promising, a lot of resistance can be perceived today, it being understood that as long as people and companies do not deepen in the knowledge of this innovation, the whole system of payment made by cryptomoedas may be compromised for the next years.

Keywords: Bitcoin. Criptomoeda. Blockchain. Virtual currency. Means of payment

SUMÁRIO

1. INTRODUÇÃO

Muitas organizações atualmente estão sendo forçadas a repensar seus modelos de negócio, pois, até as mais pequenas, estão ganhando força no mercado por se aliarem a novas tecnologias, propiciando assim um cenário mais competitivo. Devido ao fácil acesso à *internet* em amplitude global, a troca de informações entre qualquer parte do mundo atualmente se torna algo simples e de baixo custo, tornando-se um potencial para muitas categorias de empreendimentos, principalmente os que utilizam bases de dados contendo características de usuários em seus negócios. Benefício que só foi possível a partir da década de noventa com a criação da *World Wide Web,* ou somente *Web*, permitindo que muitas pessoas conseguissem de forma fácil transacionar informações, dados, arquivos, fotos etc.

Passaram-se alguns anos até as pessoas e empresas adotarem a *Web* como um instrumento usual, mesmo sendo algo muito disseminado como uma tecnologia revolucionária. Essa falta de aderência possivelmente foi afetada não só pelo desconhecimento da grande maioria da população a respeito da invenção como também pela desconfiança de um “mundo virtual”. Problema esse que foi resolvido ao longo dos anos, principalmente porque propiciava aos usuários incontáveis benefícios, possibilitando assim o crescimento da confiança na nova tecnologia.

Desde então, muitas empresas estão se tornando disruptivas de alguns padrões até então nunca questionados, mostrando ao mundo que tudo pode ser aperfeiçoado, e tudo está sob risco de desaparecer assim como começou. Não poderia ser diferente quando pensamos em uma das criações que está presente em nossas vidas por centenas de anos, sendo considerada, até então, como algo solidificado na nossa sociedade: a moeda.

Em 2008, em meio a uma das maiores crises mundiais, iniciada por práticas do sistema financeiro privado, surgiu em um *blog* uma proposta de criação de um sistema de pagamentos eletrônicos que utilizaria provas criptográficas ao invés da confiança usual dada as grandes instituições financeiras de todo o mundo, permitindo que duas partes pudessem fazer transações diretamente, sem a necessidade de um intermediador controlando o processo. Dessa forma, poucos meses depois uma das tecnologias mais promissoras na área financeira, para muitos especialistas, tinha sido criada, e foi batizada de *Bitcoin*.

A primeira criptomoeda, de muitas que surgiriam depois, tinha como premissa ser um meio de troca ideal para fugir do controle das instituições financeiras que manipulavam o dinheiro de forma, muitas vezes, inconsequente, causando inflação e consequentemente grandes períodos de crises. Ainda que na teoria a ideia de uma moeda virtual seja muito bem elaborada, na prática, é possível notar a mesma desconfiança que existia em relação à *internet*, ocasionada no início de sua criação pela falta de conhecimento tecnológico, mantendo muitas pessoas longe dessa invenção.

Muito conhecimento a respeito desse ativo ainda precisa ser disseminado para que então sirva a seu propósito, até lá, cabe a sociedade, em especial as empresas, buscarem entender como essa inovação irá influenciar as dinâmicas do mercado e seus negócios.

1.1 PROBLEMA DE PESQUISA

Desde o momento que a moeda *Bitcoin* começou a ser utilizada como meio de troca em sua primeira operação, algumas empresas tentaram replicar o modelo, na maioria para inovação como experimento, mas sem abandonar as formas tradicionais de pagamento até então utilizadas. O mercado estava aberto para realizar transações de uma forma diferente do que realizara até então, pois se baseava em uma moeda pouco utilizada, complexa de entender e de baixo valor, apenas com a promessa de revolução tecnológica voltada ao sistema financeiro. Talvez este tenha sido o grande motivo impulsionador da aderência dos primeiros usuários. Alguns anos mais tarde, o conhecimento a respeito do assunto foi ganhando força, assim como novos produtos que serviriam para auxiliar as principais operações desse sistema, como, por exemplo os *softwares* e *hardwares*, capazes de gerenciar e armazenar os pagamentos e valores transacionados.

O crescimento dos locais que aceitam a moeda Bitcoin como meio de pagamento é expressivo se analisarmos os últimos 4 anos. Conforme pode ser verificado no mapa abaixo, passou de 3.287 para 12.158 estabelecimentos.

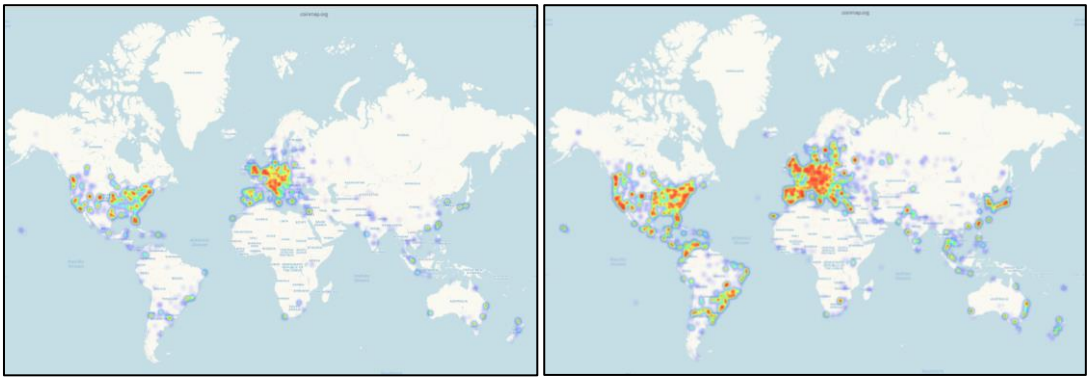

Figura 1 – Mapa utilização Bitcoin março 2014/2018

Fonte: Coinmap

Porém, se analisarmos globalmente, ainda são poucas, frente a população mundial, e principalmente de empresas que aderiram às criptomoedas como forma de pagamento, tornando-se um grande desafio de sobrevivência para o *Bitcoin*, que mesmo tendo um elevado valor tecnológico, pode não ser percebido por seus usuários, resultando assim na sua desvalorização. Visto que atualmente este ativo tem sido utilizado principalmente como especulação e não como meio de troca, traz incertezas para o mercado envolve alto risco para novos entrantes. Como pode ser verificado no gráfico abaixo, seu valor negociado no mercado nos últimos 2 anos sofreu grandes variações, tanto no caminho da valorização, quanto na desvalorização em alguns períodos. Chegando a ultrapassar a faixa dos 60k (sessenta mil) reais em dezembro/2017.

Gráfico 1 – Mapa Valorização Bitcoin abril 2016/2018

Fonte: Infomoney

Analisando o contexto histórico apresentado até o momento, assim como o cenário econômico atual da utilização da moeda virtual, a de maior destaque o *Bitcoin*,

e as diversas oportunidades e ameaças consequentes das criptomoedas, é viável para as empresas adotarem uma política de pagamentos por meio da criptomoeda como meio alternativo aos métodos convencionais?

1.2 OBJETIVOS

1.2.1 Objetivo Geral

Analisar os benefícios, riscos e desafios das empresas ao adotarem uma política de pagamento através da criptomoeda *Bitcoin*.

1.2.2 Objetivos específicos

a. Analisar características dos meios de pagamentos convencionais em comparação com o meio oferecido pela criptomoeda *Bitcoin*.
b. Analisar o comportamento do consumidor na utilização da criptomoeda
c. Examinar a legislação existente acerca de um sistema de pagamento através de criptomoedas.

1.3 JUSTIFICATIVA

Este trabalho, além de responder as questões propostas, visa contribuir para a literatura nacional sobre o tema das criptomoedas e suas utilizações, que ainda possui um conteúdo pouco difundido, e sem dúvidas, está longe de um entendimento global assertivo do que a tecnologia representa para nosso sistema financeiro e de como poderá mudar alguns padrões em nossa sociedade.

Um relatório lançado em 2017 pela Cambridge Center for Alternative Finance mostra que o número atual de usuários de criptomoedas ativos é estimado em 2,9 milhões e 5,8 milhões, e demostra que esse total nos últimos anos apenas está crescendo. Atualmente está disponível cerca de 16,9 milhões de bitcoins[1], que representa, na atual cotação[2], cerca de 150 bilhões de dólares, sem contar quantidades e valores de outras moedas digitais.

[1] informação disponível em: blockchain.info/pt/charts/total-bitcoins
[2] cotação em dólar disponível em: https://br.investing.com/crypto/bitcoin/btc-usd

Como pode ser visto, o tema escolhido representa uma grande oportunidade de expansão, tanto no campo da pesquisa acadêmica, quanto na própria utilização do bitcoin como meio de pagamento, onde existe ainda uma pequena parcela da população como usuários ativos, permitindo crescimento em dimensões globais e que possivelmente movimentarão bilhões de dólares.

1.4 ESTRUTURA DA MONOGRAFIA

A presente monografia de especialização será apresentada em quatro capítulos: Referencial Teórico – introduzindo todos as principais ideias dos autores que irão dar sustentação à monografia; Metodologia – apresentando o método realizado para as pesquisas e o local das informações; Análise de Resultados – sendo a contribuição do autor para a presente pesquisa; Conclusão – permitindo um desfecho e análise de atingimento dos objetivos e as respostas para o problema de pesquisa pré-definido.

2. REFERENCIAL TEÓRICO

2.1. DINHEIRO

2.1.1. A moeda na história

A moeda, desde sua concepção, sempre teve um papel fundamental na história da evolução da humanidade, sendo uma tecnologia capaz de minimizar esforços e garantir segurança nas transações comerciais. Mesmo que o seu conceito de valor seja abstrato para muitos, nunca inviabilizou as negociações, pelo contrário, assegurou que houvesse uma ordem em meio as práticas de mercado. Entretanto, nem sempre a moeda permaneceu da mesma forma por muitos anos, atualmente, com o advento das tecnologias digitais, um novo modelo foi apresentado a humanidade, assim, o *Bitcoin* nos faz questionar sobre suas aplicações e seus fundamentos como moeda.

De acordo com Ulrich (2014), a moeda digital *Bitcoin*, revisitou o conceito presente a séculos na humanidade: a intangibilidade do dinheiro. Diversos bens já desempenharam a função de meio de troca ao longo da história das civilizações, como exemplo: o tabaco, na Virgínia colonial; o açúcar, nas Índias Ocidentais; o sal, na Etiópia; o gado, na Grécia antiga; os pregos, na Escócia; o cobre, no Antigo Egito; assim como grãos, rosários, chás e outros itens. Porém, foi o ouro e a prata que permaneceram por muitos séculos como dinheiro.

Com o passar dos anos, com o desenvolvimento e intensificação da divisão do trabalho, houve a necessidade de aperfeiçoamento do dinheiro utilizado nos intercâmbios no mercado. Criou-se então o serviço de custódia do ouro, em que os depositantes recebiam um certificado por armazenar as quantias em ouro, ou qualquer outro metal monetário. Esses certificados começaram a se tornar frequentes e levaram ao crescimento e fortalecimento da confiança nos bancos da época. De forma que os clientes não precisavam transferir a cédula para quem iriam transacionar, bastava escrever uma ordem para que seu banco fizesse a transferência de uma conta para outra. A partir desse momento, os bancos perceberam que muitas pessoas não resgatavam seus depósitos com frequência, passaram então a operar com reservas fracionárias, mantendo apenas uma fração do dinheiro físico que foi depositado e emprestando o restante. Neste modelo o banco através de um registro contábil,

denominado “depósito à vista”, pode expandir o crédito, criando assim mais dinheiro (ULRICH, 2014).

> Economicamente, os depósitos à vista desempenham a mesma função que um dinheiro material. Esse novo depósito à vista criado do nada é o que denominamos de moeda bancária ou escritural (ULRICH, 2014, p.58).

Para Ulrich (2014), o conceito da moeda escritural evidencia que mesmo antes do Bitcoins, uma moeda digital, a ideia de uma moeda intangível já estava presente na sociedade. Além das movimentações bancárias que são realizadas atualmente por grande parte da população por meios digitais. Ressalta-se que a criação dessa moeda escritural pelos bancos não é ilimitada, sendo o banco central o responsável por controlar e coordenar sua produção.

Dessa forma, percebe-se que a humanidade tem buscado diversas maneiras de viabilizar a tecnologia responsável pelas negociações, desde as que envolvem menores até maiores valores. Aperfeiçoando para sistemas mais complexos, porém, mais adequados às necessidades presentes na atualidade.

2.1.2. Tipos de Moeda e Meios de pagamento

Segundo Carvalho et al. (2007), o papel-moeda (e a moeda metálica) que está em poder do público é também conhecida como moeda manual. Já os depósitos a vista nos bancos comerciais são chamados de moeda escritural. Portanto a soma dos dois tipos de moeda é igual aos meios de pagamento de uma economia. Os saldos de cartões de crédito não são considerados como meios de pagamento, pois são utilizados apenas para obter crédito, ao qual o compromisso deverá ser honrado com moeda escritural ou manual em uma data futura. Portando, nem toda criação de crédito significa criação de moeda, e o pagamento feito através de um cartão de crédito não significa a criação de moeda.

> A moeda de uma economia, ou seja, o conjunto de meios de pagamento, consiste na totalidade de ativos possuídos pelo público que pode ser utilizado a qualquer momento para a liquidação de qualquer compromisso futuro ou à vista. (CARVALHO et al. 2007, p.4)

O sistema monetário é o nome dado as instituições capazes de criar moeda em uma economia. É composta por bancos comerciais, responsáveis pela criação de moeda escritural, e pelo seu Banco Central, pela moeda manual. Para que os bancos comerciais criem moeda escritural, é necessária autorização pelo Banco Central de receber depósitos à vista. Dessa forma, quando um indivíduo toma um empréstimo junto aos bancos comerciais, através de uma operação contábil, essas instituições criam depósitos à vista. Essa operação é realizada, pois, os bancos sabem que nem todas aqueles que possuem direito de saque irão exercer simultaneamente. (CARVALHO et al. 2007).

Essa criação de dinheiro, tanto manual quanto escritural, é muito questionada, pois com o aumento da oferta monetária, poderá gerar inflação, tendo causas desastrosas na economia quando não bem administradas, trazendo menor poder de compra para o consumidor final.

2.1.3. Funções básicas da moeda

De acordo com Carvalho et al. (2007), a criação da moeda responde a uma necessidade social originada da divisão do trabalho, onde na estrutura capitalista moderna, os agentes econômicos se especializaram em suas unidades de produção, e dessa forma, a utilização da moeda surgiu para auxiliar na agilidade e facilidade das transações, evitando desgastes físicos e mentais, caso o método fosse ainda pela troca de bens excedentes ao consumo como era antigamente. Portanto, só seria possível permanecer no método antigo, de trocas diretas, no cenário ao qual indivíduos e/ou grupos familiares fossem praticamente autossuficientes, onde cada indivíduo produzisse o que necessitasse e transacionasse somente quando houvesse eventualmente um excedente não planejado da sua produção.

Na economia monetária presente, a remuneração dos agentes é feita através da moeda, permitindo que tenham planos mais flexíveis e maior liberdade de compra e venda no momento que desejarem, sem a perda de tempo e desgastes físicos e mentais. Sendo assim, depois da aceitação da moeda, a facilidade em trocar os excedentes por moeda e então transacionar por outros bens e serviços que lhe eram

oferecidos, superou o método de trocas diretas e permitiu que fosse criado um sistema de trocas indiretas.

Carvalho et al. (2007) explica que a moeda possui três funções básicas:

A. Intermediário de troca: uma função básica da moeda, portanto, ao permitir que seja realizada compras e vendas em datas diferentes, a moeda exerce a função de meio de pagamento.
B. Unidade de conta: possibilita que os contratos exercidos no processo produtivo, pelos diversos agentes econômicos, possuam uma unidade de medida monetária. Assim os contatos não poderiam existir sem uma unidade de conta que determinasse a quantidade de unidades monetárias suficientes para liquidação das obrigações, através do uso da moeda corrente. Forçando com que as duas partes em uma transação cumpram com suas obrigações, devendo assim, que a parte que recebeu a mercadoria e/ou serviço faça o pagamento de acordo com a unidade de conta estabelecida. A função da moeda-de-conta ou unidade de conta contratual, é uma representação intangível da moeda, diferente da moeda como um meio de troca, que possui uma representação concreta. Assim, a moeda-de-conta dentro do conjunto de contratos deve ser aceita em todas as transações de uma determinada economia.
C. Reserva de valor: decorrente da existência de amplos mercados futuros e à vista na economia. No momento que um agente recebe um recurso na forma monetária, ele possui o direito de reter poder de compra, teoricamente sem temer perdas, por períodos longos sem qualquer custo. Em uma economia hiperinflacionária, a moeda perde a função de reserva de valor, pois, impossibilita a manutenção do seu valor ao longo do tempo, fazendo com que o agente perca o poder de compra.

2.1.4 Características da moeda

Carvalho et al. (2007) ressalta que para as moedas desempenharem suas funções de meio de troca, unidade de conta, e reserva de valor, algumas

características, físicas e econômica, devem lhe ser atribuídas. As características econômicas são: custo de estocagem e custo de transação próximos de zero. Alguns exemplos de moedas podem ser destacados como falhos nessas características caso viessem a serem eleitas socialmente, como exemplo, o trigo, o sal e a soja. Assim, os dois custos, estocagem e transação, seriam elevados demais tornando ineficiente seu uso como moeda.

Carvalho et al. (2007) também elenca as características físicas como aspectos fundamentais na competência da moeda. Deve ser divisível, durável, difícil de falsificar, manuseável e transportável.

a) Divisível – essencial, pois a moeda deve poder ser fracionada em múltiplos e submúltiplos, para que transações de valor fracionado ou de grande valor seja realizado sem custos adicionais;
b) Durável – conservar as características físicas para que continue servindo na sua condição disseminada e não traga prejuízos a seu último detentor;
c) Difícil de falsificar – serve o propósito de aumentar a confiança do público de que não está sendo feita reprodução indevida da moeda, consequentemente auxiliando a aceitação da mesma;
d) Manuseável e transportável – evita com que o detentor tenha custos de transação, viabilizando assim, a função meio de troca.

2.1.5 Sistema monetário

Segundo Carvalho et al. (2007) o Banco Central possui algumas funções específicas, como: emissor de papel-moeda e controlador da liquidez da economia, banqueiro dos bancos, regulador do sistema financeiro e depositário de reservas internacionais do país.

1. Emissor de Papel-moeda e Controlador de Liquidez: o Banco Central possui o monopólio de emissão de papel-moeda e da cunhagem de moedas metálicas. Também possui o controle da quantidade de papel-moeda em circulação, isto é, o tamanho da base monetária. Assim

como pode impedir a criação de moeda pelos bancos comerciais. Controlando assim a liquidez na economia.

2. Banqueiro dos Bancos: o Banco Central tem como responsabilidade compensar os cheques, realizar o transporte de cédulas e moedas metálicas aos bancos, manter parte das reservas dos bancos entre outras tarefas que auxiliam o sistema bancário. Também deve socorrer os bancos comerciais e instituições financeiras em dificuldade, concedendo liquidez aos mesmos através de empréstimos ou redescontando títulos.
3. Regulador do Sistema Monetário e Financeiro: O Banco Central é responsável por regular as operações dos bancos comerciais e instituições financeiras. Supervisionam essas instituições com o objetivo de proteger os depósitos dos clientes e garantir a solvência de cada banco e impedir possíveis crises sistêmicas. Também pode agir como limitador de certas operações que se exponham a situações excessivas de risco, assim como intervir em instituições mal administradas.
4. Depositário de Reservas internacionais: O Banco Central pode deter grande parte de reservas nacionais do país, visando controlar a taxa de câmbio através de operações de compra ou venda no mercado de divisas internacionais. Boa parte dessas reservas em posse do Banco Central, são investidas em títulos do Tesouro Americano, com objetivo de obter juros e aumentar a quantidade total de divisas.

2.2 PROPULSORES TECNOLÓGICOS DO BITCOIN

Algumas tecnologias, criadas anteriormente ao *Bitcoin*, são fundamentais para o funcionamento da moeda virtual. Entre as mais importantes, a internet, que sem ela, não seria possível ter a comunicação entre todos os usuários e nem as transações das informações. A criptografia, que também se torna fundamental para a segurança das informações geradas e transacionadas por toda a rede, pois impossibilita que ataques ao sistema se tornem um empecilho ao funcionamento.

Outra tecnologia, referente a arquitetura de rede, conhecida como *peer-to-peer*, torna as informações descentralizadas, substituindo o formato de servidor central, dificultando ainda mais o ataque de invasores. E para que todo o sistema continue funcionando e as transações permaneçam acontecendo, a tecnologia conhecida como *proof-of-work* possibilita que cada transação passe por uma verificação, através de esforço computacional.

2.2.1 Internet

Na década de 1970, o conceito da internet surgiu como uma revolução na rede de computadores. Diferente de como é conhecida atualmente, já passou por diversas melhorias desde sua criação, e a assim como grande maioria das inovações, teve seu processo de adaptação e aceitação de maneira lenta e gradativa até a utilização plena de seus usuários.

> A internet é formada pela interconexão de múltiplas redes de comutação de pacotes. O funcionamento da Internet é substancialmente mais poderoso do que o de uma tecnologia simples de rede, porque o enfoque permite que novas tecnologias sejam incorporadas ao mesmo tempo sem exigir a substituição das tecnologias antigas como um todo (COMER, 2016, p.7).

Comer (2016) acredita que o crescimento contínuo da Internet global é um dos fenômenos mais interessantes em redes. Pode-se entender como rede a infraestrutura que liga computadores de todo o mundo, alcançando milhões de pessoas, permitindo um sistema de comunicação entre todos os países. É utilizada também para aspectos de negócios, incluindo propagandas, produção, transporte, planejamento, faturamento e contabilidade. Consequentemente a maioria das organizações possui múltiplas redes, e está sendo utilizada em várias dimensões, incluindo instituições acadêmicas, militares e órgãos governamentais.

Segundo Comer (2016) A World Wide Web (WWW) é um dos serviços mais utilizados na internet e devido à complexidade da rede, alguns padrões de protocolos foram criados para especificar aspectos e detalhes. São eles:

A. *HyperText Markup Language* (HTML) – Representação padrão usada para especificar os conteúdos de uma página da Web;

B. *Uniform Resource Locator* (URL) – Representação padrão especificando o formato e o significado dos identificadores da página Web;
C. *HyperText Transfer Protocol* (HTTP) – Protocolo de transferência especificando como um *browser* (navegador) interage com o servidor web para transferir dados.

Mougayar (2017) afirma que a internet trouxe importantes “mini revoluções” desde 1994, como no campo das comunicações pessoais, auto publicações, comércio eletrônico e as redes sociais. Desatendendo funções e serviços já existentes como os correios, as mídias impressas, as lojas físicas e o mundo real. E assim como a Web precisa da internet para seu funcionamento, o *blockchain* - tecnologia responsável pelo *Bitcoin* - também necessita. Dessa forma a internet se faz importante, pois sem ela nenhuma das duas aplicações seria possível.

2.2.2 Criptografia

Segundo Mougayar (2017), a ciência da criptografia é usada em múltiplos lugares para garantia da segurança, em redes ela repousa sobre três conceitos fundamentais: chaves, *hashing* e assinaturas digitais.

Comer (2016) afirma que a criptografia é uma ferramenta essencial na segurança de informações, permitindo a confidencialidade de dados, autenticação de mensagens e integridade de dados, além de evitar ataques de repetição. Dessa forma, o remetente aplica criptografia para codificar a mensagem de tal maneira que somente o destinatário poderá decodifica-la. Um interceptador dessa mensagem, através de uma cópia, não é capaz de extrair a informação.

A terminologia utilizada para criptografia se divide em quatro itens:

A. Texto aberto – mensagem original antes de ser criptografada
B. Texto cifrado – mensagem após ser criptografada
C. Chave de criptografia – conjunto curto de bits utilizado para criptografar uma mensagem
D. Chave de descriptografia- conjunto curto de bits utilizado para descriptografar uma mensagem.

As tecnologias de criptografia podem ser divididas em dois grandes grupos, definida pela forma como elas são utilizadas:

- Chave privada – Em um sistema de chave privada, cada par de entidades partilha uma única chave, sendo usado como chave de criptografia e descriptografia. Portanto, deve ser mantida em segredo, caso contrário, se um terceiro obtiver uma cópia dela, poderá decifrar a mensagem que passa entre o par. Sistemas de chave privada são *simétricos*, ou seja, cada lado pode enviar e receber mensagens, tanto o transmissor quanto o receptor utilizam a mesma chave.
- Chave pública – Em um sistema de chave pública, para cada entidade é atribuído um par de chaves. Não havendo necessidade de ser mantida em segredo, podendo ser publicada junto ao nome do usuário, pois uma mensagem de texto aberto criptografada com a chave pública não pode ser descriptografada, exceto pela chave privada. O sistema de chave pública é *assimétrico*, pois possui a propriedade de sentido único. Dessa forma, revelar a chave pública é seguro, já que não permite alguém falsificar uma mensagem criptografada com a chave privada.

Para Comer (2016), um esquema de *hashing* se baseia na confiança de uma chave secreta conhecida apenas pelo emissor e receptor. Fornecendo um código de autenticação de mensagens a prova de quebra ou falsificação.

> O emissor recebe a mensagem para transmitir, utiliza a chave para calcular um hash, H, e transmite H juntamente com a mensagem. H é uma sequência curta de bits, e o comprimento de H é independente do tamanho da mensagem. O receptor usa a chave para calcular um hash da mensagem e compara o hash com H. Se os dois forem iguais, a mensagem chegou intacta. Um atacante, que não tem a chave secreta, não conseguirá modificar a mensagem sem a introdução de um erro. Assim, H fornece a autenticação da mensagem porque um receptor sabe que uma mensagem com um hash válido é autêntica. (COMER, 2016, p.450)

Um dos mecanismos conhecidos da criptografia é conhecido como assinatura digital, que de acordo com Mougayar (2017, p.12) significa “[..] uma computação matemática usada para provar a autenticidade de uma mensagem ou documentos (digitais).”.

Conforme a explicação de Comer (2016) para assinar uma mensagem, o remetente precisa criptografar usando uma chave conhecida somente por ele (chave privada) e para verificar a assinatura, o destinatário olha somente para a chave pública do remetente e utiliza para descriptografar. Dessa forma, o remetente sabe quem enviou a mensagem original, podendo conter a hora e data que foi criada, uma vez que somente o remetendo tem a chave capaz de efetuar a criptografia daquelas informações.

2.2.3 Proof of Work

No campo da criptografia, a ideia do protocolo *Proof of Work* (em português, Prova de trabalho), surgiu pela primeira vez em 1993 em um artigo publicado por Cynthia Dwork e Moni Naor, como sugestão ao combate de ataques cibernéticos como DDOS e SPAM. Dessa forma, para os usuários realizarem uma ação, eles devem provar que realizaram determinada tarefa. Porém, foi somente no ano de 1999, com um artigo publicado por Markus Jakobsson e Ari Juels, que o termo “Prova de Trabalho” foi utilizado.

De acordo com Juels e Jakobsson (1993), conforme tradução livre, protocolos de prova servem como pilar para maioria dos algoritmos de segurança de dados. Em um cenário convencional, uma parte, o provador, visa convencer a outra parte, o verificador, de que há um segredo de uma certa forma, ou que certa afirmação matemática é verdadeira. Assim, o *Proof of Work* (POW), é o protocolo no qual o provador demonstra para o verificador que gastou um certo nível de esforço computacional em um determinado intervalo de tempo.

Ainda que seja um sistema eficaz, possui alguns apontamentos na sua eficácia, conforme descrito abaixo por Mougayar (2017).

> Um dos inconvenientes do algoritmo de POW é que ele não é ecologicamente correto, porque requer grandes quantias de poder de processamento de máquinas especializadas que geram energia excessiva. Um forte competidor para a Prova-de-trabalho (POW) será o algoritmo Prova-de-participação (POS), que depende do conceito de mineração virtual e voto baseado em token, um processo que não requer a mesma intensidade de processamento computacional que a Prova-de-trabalho e que promete alcançar a segurança de uma maneira mais efetiva, financeiramente falando (Mougayar, 2017 p. 2017)

2.2.4 Peer-to-peer (P2P)

De acordo com Comer (2016) a partir de 1990, vários grupos do ramo da computação, experimentaram aumentar a velocidade de carga de arquivos, substituindo o processo de buscar um arquivo completo em um servidor central preestabelecido, pelo processo de busca em pedaços individuais em vários servidores espalhados na internet. Dessa maneira, sempre que um cliente precisava de um pedaço do arquivo, ele escolhia o servidor mais próximo que possui a cópia. Para que o número de locais disponíveis a serem encontrados esses pedaços fosse maior, cada cliente concordava em agir como um servidor e fornece-lo para outros clientes. Essa abordagem é conhecida como *peer-to-peer* (p2p) *architecture*. Alguns sistemas ficaram conhecidos por utilizarem essa tecnologia para permitir o compartilhamento de arquivos de música.

Uma forma de evitar gargalos em relação ao tráfego de arquivos entre os clientes e os servidores, é a utilização da arquitetura *peer-to-peer* (ou par-a-par), evitando manter os dados em um servidor central. Dessa forma, os dados são distribuídos igualmente por N servidores, e cada solicitação de cliente é enviada para o servidor mais próximo. Como cada servidor fornece 1/N dos dados, o tráfego entre cada servidor e internet será de 1/N. A ideia principal com o software que possibilita isso é a de que se cada um concordar em localizar 1/N dos dados do computador, não serão necessários servidores especiais (COMER, 2016, p. 32).

> Ao contrário das redes usuais, em que há um servidor central e os computadores (clientes ou nós, nodes, em inglês) se conectam a ele, uma rede *peer-to-peer* não possui um servidor centralizado. Nessa arquitetura de redes, cada um dos pontos ou nós de rede funciona tanto como cliente quanto como servidor – cada um dos nós é igual aos demais (*peer* traduz-se como “par” ou “igual”) -, o que permite o compartilhamento de dados sem a necessidade de um servidor central. Por esse motivo, uma rede *peer-to-peer* é considerada descentralizada, em que a força computacional é distribuída. (ULRICH, 2014, p.44)

2.3 A MOEDA BITCOIN

2.3.1 Criação da Moeda digital

É importante entender o contexto mundial ao qual a moeda virtual Bitcoin surgiu, pois teve início em meio a Grande Crise Econômica do século XXI, logo após o anúncio da quebra do banco Lehman Brothers, em setembro de 2008, marcando na história econômica dos Estados Unidos e posteriormente do mundo.

Para o autor Ulrich (2014) o arranjo monetário atual do Ocidente é uma antítese ao livre mercado, uma vez que está estruturado em dois pilares “1) Monopólio da emissão de moeda com leis de curso legal forçado; e 2) banco central, responsável por organizar e controlar o sistema bancário. ”. Demonstrando assim, a interferência governamental no âmbito monetário, verificado na maioria dos países. Além das moedas emitidas hoje pelos governos não possuírem lastro físico, como eram utilizados o ouro e a prata antigamente, restando nos dias atuais somente a confiança em seus governos.

> Desde 1971, quando o então presidente Richard Nixon suspendeu a conversibilidade do dólar em ouro, vivemos na era do papel-moeda fiduciário, em que bancos centrais podem imprimir quantidades quase ilimitadas de dinheiro, salvo o risco de que os cidadãos percam toda a confiança na moeda, recusando-se a usá-la em suas transações, como costuma ocorrer em episódios de hiperinflação. (ULRICH, 2014, p.36)

O mecanismo chamado de reservas fracionárias, permite que os bancos possam guardar uma parte do dinheiro que foi depositado e emprestar o restante ao público, concedendo aos bancos o poder de criar depósitos bancárias através de expansão de crédito. Esses depósitos constituem parte da oferta monetária, já que tem a mesma função que a moeda física. Resultando em inflação, devido à quantidade de moeda na economia, elevando os preços, fazendo com que o poder de compra diminuía com cada unidade monetária. Como citado por Ulrich (2014, p.43) “Nesse contexto, o projeto *Bitcoin*, vinha a ser uma tentativa de resposta à instabilidade financeira causada por décadas de monopólio estatal da moeda e por um sistema bancário de reservas fracionárias”. Até o ano 2008, as transações online eram sempre feitas através de um terceiro intermediário de confiança. Depois desse ano, o mundo

conheceu por meio de um programador, denominado Satoshi Nakamoto, a invenção *Bitcoin*.

A proposta do criador foi a criação de um sistema de pagamentos eletrônicos através de provas criptográficas ao invés de confiança, possibilitando que as duas partes dispostas façam transações diretamente entre si sem a necessidade de um terceiro para intermediar (NAKAMOTO, 2008).

No dia 31 de outubro de 2008, um *paper* chamado "*Bitcoin: a Peer-to-Peer Eletronic Cash System*" foi publicado em um blog de criptografia. Neste arquivo estava presente as principais ideias de um sistema descentralizado e *peer-to-peer*, sem a necessidade de um terceiro fiduciário. Era revolucionário porque, pela primeira vez, pode resolver um problema chamado de "gasto duplo", sem a necessidade de um terceiro. Esse problema é conhecido em ciência da computação quando um usuário consegue gastar as mesmas moedas mais de uma vez. Sendo assim, o usuário do *Bitcoin* não enfrenta esse problema, pois emprega os registros históricos das transações de todos os usuários do sistema em uma rede *peer-to-peer* (ULRICH, 2014).

Atualmente, existe uma grande quantidade de criptomoedas em circulação, dentre as mais conhecidas estão a *Litecoin*, com o foco em realizar transações com alta velocidade, a *Etherum*, que permite a criação de contratos inteligentes através do *Blockchain*, e a *Ripple*, que resolver manter seu foco no mercado financeiro. Todas projetadas e implementadas utilizando o sistema do *Blockchain* da *Bitcoin* (SILVA, 2018, p.31)

Resumidamente pode-se concluir que o *Bitcoin* é uma forma de dinheiro, que se diferencia das demais moedas, como o real, dólar ou euro, pelo fato de ser digital, e não ser emitido por um governo. Tem seu valor determinado livremente pelos indivíduos no mercado e apresenta uma maneira ideal de pagamento online, sendo mais rápido, barato e seguro. Possui algumas peculiaridades que precisam ser entendidas para se realizar uma análise do *Bitcoin*, como a ausência de lastro, a intangibilidade, a oferta inelástica e a ausência de um emissor central (ULRICH, 2014).

2.3.2 Blockchain

De acordo com Mougayar (2017), o "*Blockchain*" é a invenção tecnológica por trás do *Bitcoin*, tornando-o possível. Pode ser entendido tecnicamente como um banco de dados de *back-end*, que mantém registros distribuídos e disponibilizados abertamente para inspeção. O modelo de negócios do *blockchain* é baseado em uma rede de troca para movimento de transações, valores, ativos, sem a assistência de intermediários. Substituindo entidades consideradas confiáveis pela maioria. Sendo assim, é um sistema descentralizado, pois transfere a autoridade e a confiança para uma rede virtual descentralizada, permitindo através da estrutura *peer-to-peer*, que seus nós - cada computador que contribui para o sistema - registrem transações contínuas e sequenciais em um "bloco" público. Cada bloco sucessivo contém um "*hash*" (impressão digital única) do código anterior, dessa forma, a criptografia através de códigos de *hash* é utilizada para garantir a autenticação da fonte de transação e remover a necessidade de um intermediário centralizado.

> Todas as transações que ocorrem na economia Bitcoin são registradas em uma espécie de livro-razão público e distribuído chamado de Blockchain (corrente de bloco, ou simplesmente um registro público de transações), o que nada mais é do que um grande banco de dados público, contendo o histórico de todas as transações realizadas. (ULRICH, 2014, p.18)

Conforme descrito por Mougayar (2017) o blockchain é uma metatecnologia pois, afeta outras tecnologias, sendo ele próprio feito de várias delas.

> É um conjunto de computadores e redes construídos em cima da internet. Ao examinar as camadas arquitetônicas de um blockchain, descobre-se que ele é constituído de diversos pedaços: um bando de dados, uma aplicação de software, um conjunto de computadores conectados uns aos outros, clientes para acessá-lo,

> um ambiente de software para desenvolvê-lo, ferramentas para monitorá-lo e outras partes [...]. (MOUGAYAR, 2017, p.10)

Segundo Mougayar (2017), assim como a internet foi introduzida como um fenômeno multifuncional, o *blockchain* também possui multiplicidade das suas funções, sendo classificadas simultaneamente em dez propriedades:

1. Criptomoeda digital – é o elemento mais visível em um *blockchain*, especialmente se ele for público, sendo um estímulo econômico que viabiliza as operações e a segurança do *blockchain*. Tendo como grande desafio a volatilidade de preço das criptomoedas.
2. Infraestrutura Computacional – o *blockchain* possui um design de software capaz de unir diversos computadores ao mesmo tempo, obedecendo ao mesmo processo de “consenso” de liberação e gravação das informações através da criptografia. Promovendo uma estrutura robusta de rede.
3. Plataforma de Transação – A rede do *blockchain* consegue validar transações de diversos valores em relação a dinheiro digital ou ativos. As informações são gravadas em “blocos”, que representa um espaço de armazenamento. Mantendo sempre o controle sobre todas as transações já realizadas, independentes do valor.
4. Banco de dados descentralizado – o *blockchain* quebra o paradigma do processamento de transações através de bases de dados. É um lugar capaz de armazenar semipublicamente qualquer dado em um espaço linear (o bloco) e qualquer pessoa que desejar verificar a alteração da informação.
5. Registro Contábil Distribuído – tem a característica de mostrar a data e hora que foi registrado o ativo, permitindo que cada usuário possa verificar e validar cada transação, evitando assim, o problema da dupla contagem.
6. Plataforma de Desenvolvimento- é uma nova maneira de construção de aplicações pois inclui tecnologias destinadas à construção de novos tipos de funcionalidades, sendo descentralizadas e criptografadas
7. Software de Código Aberto – os *blockchains* que são públicos, possuem o código do software aberto, possibilitando a inovação de maneira colaborativa em cima do software inicial. Por esse fator se torna uma caraterística poderosa, pois, fortalece o ecossistema da rede.

8. Mercado de Serviços Financeiros – os *blockchains* oferecem um ambiente de inovação no campo dos serviços financeiros da atualidade. Quando a volatilidade da criptomoeda reduzir, elas se popularizarão. Possibilitando que instrumentos tradicionais como derivativos, *swaps*, instrumentos sintéticos, investimentos, empréstimos e outros tenham uma versão em criptomoeda.
9. Rede *Peer-to-peer* – o *blockchain* não possui uma rede centralizada, dessa forma, seu processamento ocorre através de computadores independentes, cada um chamado de nó, que são responsáveis por validar as transações.
10. Camada de Serviços Confiáveis – todos os *blockchain* possuem como serviço a confiança oferecida pela rede com todas essas características, não se limitando apenas as transações, se estendendo para todos os dados, serviços, processos, identidade, lógica de negócios, termos de um acordo e até mesmo objetos físicos. Ou seja, se aplica a praticamente qualquer coisa que seja digitalizada como um ativo, com um valor envolvido.

2.3.3 Funcionamento Bitcoin

De acordo com Ulrich (2014) para que as transações dentro do *blockchain* sejam feitas, e o gasto duplo prevenido, é utilizado criptografia de uma “chave pública”. Dessa forma, cada usuário possui duas “chaves”, uma privada, que é mantido em segredo pelo proprietário e utilizada para assinar a transação, e uma pública que pode ser compartilhada com todos e que serve de referência para alguém que queira realizar um depósito nesta conta. Todas essas transações são gravadas com data e hora e expostas em um “bloco” do *blockchain*. Todas as transações já efetuadas na história da economia do *Bitcoin*, podem ser visualizadas no *blockchain*.

> A criptografia de chave pública garante que todos os computadores da rede tenham um registro constantemente atualizado e verificado de todas as transações dentro da rede Bitcoin, o que impede o gasto duplo e qualquer tipo de fraude. (ULRICH, 2014, p.19)

Segundo Ulrich (2014) a criptografia aplicada ao *Bitcoin*, desempenha duas funções essenciais: impossibilitar que usuários gastem bitcoins da carteira de outros usuários (autenticação e veracidade das informações) e impedir que o *blockchain* seja

violado e corrompido (integridade das informações), dessa forma, evitando o gasto duplo. Também é utilizada para encriptar uma carteira, sendo definida por uma senha escolhida pelo usuário.

O *Bitcoin* pode ser formado por uma rede *peer-to-peer* e não possuir uma autoridade central destinada a criar unidades monetárias nem de verificar as transações. Porém, a rede necessita de usuários que disponibilizem sua força computacional para realizar os registros das transações. As pessoas que disponibilizam essa força para o funcionamento da rede são chamadas de “mineradores”, sendo remunerados assim pelo seu trabalho, com *bitcoins* que acabam de ser criados, ou “minerados”, como é conhecido pelos usuários. A mineração, é feita através de milhares de computadores ao redor do mundo, cada um constituindo um nó na rede *peer-to-peer*, realizando através de problemas matemáticos complexos a verificação das transações no *Blockchain*. A dificuldade também aumenta conforme a descoberta de mais *bitcoins*, fazendo com que seja computacionalmente mais difícil de encontrar uma solução para os problemas matemáticos. Os mineradores são remunerados com um prêmio em *Bitcoin* e uma taxa de serviço, também em *Bitcoin*. Sendo assim, os efeitos da dificuldade de obtenção de novos *bitcoins* e a taxa de serviço empregado a eles, faz com que se assemelhe ao sistema de *commodity*, como o ouro (ULRICH,2014)

Assim, o protocolo que foi projetado com todas as informações das funcionalidades, prevê que seu funcionamento referente a extração de novos *bitcoins* imite a metais preciosos. Somente um número limitado previamente de *bitcoins* será disponibilizado, sendo uma quantidade arbitrada em 21 milhões. Segundo Ulrich (2014, p.20) “Estima-se que os mineradores colherão o último “satoshi”, ou 0,00000001 de um *bitcoin*, no ano de 2140”. Tornando assim um desafio grande para os mineradores das últimas moedas. Depois que todos os *bitcoins* tiverem sido minerados, a força computacional irá se voltar somente para o processamento das transações e compensados com as taxas de serviço, garantindo que os mineradores ainda tenham um incentivo para continuar operando o sistema. Assim, pode-se concluir que o *Bitcoin* trouxe escassez autêntica e intangível ao mundo dos bens digitais não escassos.

Muita polêmica se levantou com a ausência de vinculação das chaves públicas com a identidade dos usuários, impossibilitando a identificação dos

responsáveis pelas transações no *blockchain*. Entretanto é possível através da chave pública identificar todas as transações já realizadas, rastreando as informações de quantidade e endereços destinados. Ou seja, o *Bitcoin* não permite anonimato, mas sim a possibilidade de utilizar um pseudônimo. Ainda que seja possível em alguns casos, vincular a identidade ao pseudônimo utilizado, como nas transações de *bitcoins* em páginas web ou casas de cambio sem a utilização de softwares que forneçam o anonimato do endereço IP. Mesmo com tudo isso, os usuários desfrutam de uma quantidade muito maior de privacidade que outros meios de movimentações online, entretanto essa natureza descentralizada também apresenta oportunidades para atividades criminosas, sendo um desafio desenvolver processos que reduzam essas atividades e mantenham os demais benefícios que o *Bitcoin* oferece (ULRICH, 2014).

2.3.4 Wallets

Segundo o site Blockgeeks (2017), conforme tradução livre, para a utilização das criptomoedas é necessário entender o conceito das *Cryptocurrency Wallets*, que são as carteiras digitais responsáveis por receber e enviar essas moedas, interagindo com vários *softwares, hardwares* e até mesmo na forma de papel físico.

Ao contrário das carteiras tradicionais, as carteiras digitais não armazenam a moeda, na verdade as moedas não são armazenadas em um único lugar, ou existem em forma física, tudo o que existe são registros de transações armazenados no *blockchain.* As carteiras de criptomoedas armazenam na verdade as chaves públicas e privadas, interagindo com vários *blockchains*, fazendo com que os usuários possam monitorar o saldo, enviar dinheiro e outras operações. Assim, a transação significa meramente um registro de transação no *blockchain*, que resulta em uma mudança no saldo do usuário que enviou e recebeu. Para isso, a chave privada armazenada na carteira deve corresponder ao endereço público ao qual a quantia foi destinada pelo remetente, só então o destinatário poderá usufruir das novas moedas.

Conforme as definições do Blockgeeks (2017), entre as *Softwares Wallets* também existem as distinções entre desktop, mobile e online.

A. *Desktop* – Carteiras baixadas e instaladas em um PC ou Laptop. Acessíveis somente a partir de um único computador, ao qual foi baixado. Oferecem o nível alto de segurança, porém se o computador for hackeado, existe a possibilidade de perder todos os fundos.
B. *Online* – Carteiras são executadas na nuvem, acessíveis de qualquer dispositivo em qualquer lugar. Ainda que sejam mais convenientes para o acesso de vários lugares, se torna o alvo mais vulnerável para ataques, uma vez que é administrada por terceiros.
C. *Mobile* – Carteiras são executadas através de um aplicativo, são úteis porque podem ser usadas em qualquer lugar, inclusive nas lojas de varejo.

Os demais tipos de carteira, conforme as definições da Blockgeeks (2018), são as *Hardwares* e *Papers Wallets*

- *Hardware* – São carteiras diferentes das Softwares pois as chaves são armazenadas em um dispositivo de *Hardware*, como um pendrive. Embora elas sejam capazes de efetuar transações *online*, elas são armazenadas *offline*, sendo assim, mais seguras. Os usuários simplesmente conectam seu dispositivo em qualquer computador e interagem com alguma aplicação *Web*.
- *Paper* – São carteiras fáceis de usar, e possuem grau elevado de segurança, nada mais são do que a impressão de suas chaves, pública e privada. É relativamente simples de usar, devendo realizar a transferência para uma *Software Wallet* caso queira sacar ou gastar a moeda. O processo de identificação da chave pode ser realizado manualmente, ou através da leitura de um código QR, presente na carteira de papel.

2.3.5 Volatilidade

Entende-se o conceito de volatilidade, como a indicação da intensidade e frequência das oscilações no preço de um ativo. A volatilidade é certamente um dos pontos que mais gera incertezas em relação ao futuro do *Bitcoin*, pois em poucos anos teve grandes oscilações tanto positivas quanto negativas. Saindo de um preço de aproximadamente 14 mil reais por *bitcoin* (outubro/2017) para 63 mil reais (dezembro/2017), um salto de 450% em dois meses. Um aumento significativo para quem decide investir na moeda.

Para Ulrich (2014) um dos desafios enfrentados pela moeda *Bitcoin* é a volatilidade, que na sua série histórica teve diversos ajustes de preço significativos. São explicadas pela semelhança de bolhas especulativas tradicionais ocasionadas pela cobertura de imprensa otimista em excesso, impulsionando “ondas” de novos investidores, pressionando o preço do *bitcoin* para cima e para baixo. O valor flutuante ocasiona um ceticismo na população, causando incertezas quanto ao futuro da moeda. Principalmente quando são utilizadas somente nas funções de reserva de valor ou unidade de conta, se tornando inviável guardar economias se o preço de mercado oscila descontroladamente. Já para a função de meio de troca, a volatilidade não se torna um problema tão expressivo pois os comerciantes podem precificar seus produtos pela moeda tradicional e aceitar o equivalente em *bitcoin*, não importando tanto como será o câmbio no dia seguinte, pois estão focados em reduzir os custos das transações presentes. Acredita-se que para o *bitcoin* apresentar uma volatilidade menor, é preciso que as pessoas se familiarizem mais com a tecnologia e desenvolvam expectativas realistas a respeito do futuro da moeda. Ulrich (2014, p.47) também explica que “boa parte do ceticismo em relação à moeda digital resina na complexidade tecnológica intrínseca ao Bitcoin”.

2.3.5 Benefícios da utilização

Alguns benefícios do Bitcoin se destacam das demais moedas, como dólar ou real. Mesmo que ainda não seja aceita por muitos comerciantes, sendo algo experimental para muitos usuários, Ulrich (2014, p.23) destaca que para melhor

entendimento “ajuda se pensarmos que ele não é necessariamente um substituto às moedas tradicionais, mas sim um novo sistema de pagamentos”.

Três benefícios são destacados pelo autor:

a) Menores custos de transação – seu custo é reduzido em transações, mesmo com um terceiro intermediário para certificar as operações, pois, as taxas são mais baratas que as encontradas em meios tradicionais, como cartões de crédito. Permitindo que seja um grande benefício principalmente para pequenos comerciantes, com margens apertadas de lucratividade, e também para remessas de dinheiro globais. Utilizar o Bitcoin como meio de pagamento ao invés de cartões de crédito evita também estornos fraudulentos ou falsas alegações de que o produto não foi entregue. Perdendo assim, o pagamento, o item, e pagando ainda o custo de estorno.
b) Potencial armar contra pobreza e a opressão – permite o acesso a serviços financeiros básicos para áreas mais afastadas e pobres, em uma escala global, uma vez que as instituições financeiras não estão presentes em algumas regiões por motivos de custos. Sendo também uma alternativa para pessoas que procuram “fugir” da depreciação das moedas de seu pais. Assim como indivíduos que estejam em alguma situação de opressão e que necessitem de anonimato.
c) Estímulo à inovação financeira – O protocolo *Bitcoin* possui o modelo de referência digital para uma série de serviços financeiros, legais e úteis, em que programadores podem sugerir melhorias incrementais ao protocolo existente, permitindo ser uma plataforma colaborativa entre os programadores.

3. METODOLOGIA

Uma pesquisa científica objetiva o conhecimento científico de um ou mais aspectos de um determinado assunto. Devendo ser sistemático, metódico e crítico. Dessa maneira, o produto da pesquisa deve contribuir para o avanço do conhecimento humano. Existem vários tipos de pesquisa, e todos possuem, além de um núcleo comum de procedimentos, suas peculiaridades próprias. Podendo também variar nas

formas de classificação das pesquisas. A pesquisa sob o ponto de vista da natureza pode ser classificada em: Pesquisa Básica - objetiva gerar conhecimentos novos úteis para o avanço da ciência sem aplicação prática prevista; Pesquisa Aplicada - objetiva gerar conhecimentos para aplicação prática dirigidos à solução de problemas específicos (Prodanov e Freitas, 2013, p.51). Portanto, o presente trabalho, atende a natureza de pesquisa aplicada, visando gerar conhecimento para aplicações práticas, dirigidas à solução de problemas específicos em nossa sociedade, com foco nas empresas que pretendem optar por meios de pagamento alternativos aos que são oferecidos atualmente.

Para Prodanov e Freitas (2013), a pesquisa sob ponto de vista de seus objetivos pode ser classificada em três tipos: pesquisa exploratória, pesquisa descritiva e pesquisa explicativa. Assim, dentre as três classificações, a escolhida foi a pesquisa descritiva, ao qual, neste modelo, o objetivo do pesquisador é descrever os fatos observados sem interferir neles, descrevendo as características de determinada população ou fenômeno ou o estabelecimento de relações entre as variáveis. Portanto, o trabalho apresentado, buscou relatar algumas características da moeda virtual, como proposta inovadora, em comparação com os métodos tradicionais de pagamento conhecidos no mercado. Também analisou algumas informações a respeito dos usuários das criptomoedas, assim como também, o respaldo legal nacionalmente e internacionalmente, estabelecendo relações entre diversas variáveis.

Do ponto de vista dos procedimentos técnicos, ou seja, da maneira pela qual os dados necessários para elaborar a pesquisa são obtidos, faz-se necessário um delineamento da execução pesquisa.

> O delineamento refere-se ao planejamento da pesquisa em sua dimensão mais ampla, envolvendo diagramação, previsão de análise e interpretação de coleta de dados, considerando o ambiente em que são coletados e as formas de controle das variáveis envolvidas. O elemento mais importante para a identificação de um delineamento é o procedimento adotado para a coleta de dados. Assim, podem ser definidos dois grandes grupos de delineamentos: aqueles que se valem das chamadas fontes de papel (pesquisa bibliográfica e pesquisa documental) e aqueles cujos dados são fornecidos por pessoas (pesquisa experimental, pesquisa ex-postfacto, o levantamento, o estudo de caso, a pesquisa-ação e a pesquisa participante). (PRODANOV E FREITAS, 2013, p.54).

Sendo assim, os procedimentos de pesquisa serão feitos de forma bibliográfica, pois as informações serão elaboradas a partir de materiais já publicados, como livros, artigos, periódicos e Internet, com dados escolhidos desde o início da criação das moedas virtuais até o momento presente, ano de 2008 a 2018. Com pesquisas originadas de órgãos públicos e privados, assim como materiais da literatura nacional e internacional, como também, procurando embasamento jurídico e tributário, referente a regulamentação das criptomoedas. Por último, os elementos pesquisados serão quantitativos e qualitativos, no qual os dados quantificáveis serão classificados e analisados de acordo com o contexto do estudo.

4. ANÁLISE

4.1 INSTRUMENTO DE PAGAMENTO E TRANSFERÊNCIA

Analisando um dos benefícios do *Bitcoin* levantados por Ulrich (2014), referente a menores custos de transação, pode-se constatar que o *Bitcoin* como meio de pagamento em transações, representa menores custos do que as transações feitas por rede de pagamentos tradicionais. Tornando-se principalmente um atrativo para pequenas empresas, que possuem margens apertadas e que procurem formas de reduzir seus custos de transação na administração dos seus negócios. Ainda que as formas de cartão de crédito possuam suas vantagens, elas estão acompanhadas de pesados custos aos comerciantes, entre outras exigências como contratar uma conta com as empresas de cartões para aceitar pagamento com cartão de crédito. Dependendo dos termos de cada empresa, os comerciantes precisam pagar várias taxas de autorização, taxas transação, taxas de extrato, etc. Representando muitas vezes boa parte dos custos de uma empresa. Entretanto, caso decida por não aceitar essas formas de pagamento convencionais, como o cartão de crédito, possivelmente perderão boa parte das vendas. Uma vez que esses tipos de pagamento se tornaram muito difundidos entre os compradores.

> Aqueles que querem a proteção e as regalias do uso do cartão de crédito podem continuar a operar assim, mesmo que isso signifique pagar um pouco mais. Aqueles mais sensíveis ao preço ou à privacidade podem usar bitcoins. Não ter de pagar taxas às companhias de cartões de crédito significa que os

> comerciantes podem repassar as economias aos preços finais ao consumidor. (ULRICH, 2014, pg.24)

Outro fator relevante para as empresas, segundo Ulrich (2014), é o fato de que as empresas, ao aceitarem pagamento com cartões de créditos, ficam sujeitas ao risco de fraude de estorno de pagamento *(charge-back-fraud)*. Muitos comerciantes enfrentam esse problema de estornos fraudulentos, ou reversões de pagamento iniciadas por clientes, alegando não terem recebido o que foi solicitado. Dessa forma, os comerciantes podem perder tanto o item vendido, como o pagamento, e ainda terem que pagar a taxa de estorno. Neste ponto, o *Bitcoin* elimina este problema, uma vez que todas as transações confirmadas no *blockchain*, são irreversíveis. Para pequenos negócios, isso pode ser fundamental.

De acordo com dados fornecidos pelo do Banco Central do Brasil (2016), as empresas Credenciadoras, responsáveis pelas maquininhas de cartão e serviços relacionado a pagamentos com cartão de débito e crédito, que mais possuem terminais, ou seja, locais que aceitam esses serviços no Brasil, são a Cielo, Rede e Santander (Getnet).

Portanto, para a atual análise, essas empresas serão comparadas em diversos quesitos em relação ao método tradicional de pagamento e ao método de pagamento através das criptomoedas, mais especificadamente do *Bitcoin*. As informações das empresas citadas, foram retiradas dos próprios sites institucionais com base nas informações levantadas no dia 22/06/2018. No quadro abaixo estão presentes os métodos utilizados para pagamento (Débito, Crédito à vista e Crédito parcelado) que possuem suas respectivas taxas de desconto, que são cobrados dos comerciantes que contratam as empresas credenciadoras; em seguida a tarifa de adesão, que conforme promoção das empresas pode ser cobrada ou não; o aluguel mensal, que em alguns casos é cobrado somente ele, como no caso da Rede, sendo necessário pagar as taxas se o valor ultrapassar o limite contratado de transações no mês, ou o aluguel é cobrado de forma conjunta com as taxas; O tipo de conexão e equipamentos, que costumam variar conforme planos, mas para a atual análise foi utilizada a mais indicada para alto fluxo de clientes; E por último o tempo de recebimento do valor da transação.

	Cielo	Rede	Getnet	Bitcoin
Débito	2,00%	2,70%	1,95%	-
Crédito à vista	2,50%	4,00%	2,71%	-
Crédito parcelado	3,25%	4,70%	3,44%	-
Tarifa Adesão	R$ 0,00	R$ 0,00	R$ 0,00	-
Aluguel mensal	R$ 119,90	R$ 282,5	R$ 39,00	-
Conexão	Linha Telefônica	Linha Telefônica	Linha Telefônica	Internet
Equipamento	Máquina com fio	Máquina com fio	Máquina com fio	Celular ou Computador
Tempo de recebimento	de 1 até 31 dias	de 1 até 31 dias	de 1 até 31 dias	+- 10 minutos

Quadro 1 – Quadro comparativo formas de pagamento
Fonte: Sites institucionais

Conforme observado no quadro comparativo, a forma de pagamento através do *Bitcoin*, apresenta algumas vantagens em relação as demais, uma vez que a taxa cobrada dos comerciantes por transação no *Bitcoin*, inexiste, pois, os mesmos só precisarão apresentar uma chave pública para a transferência dos valores para suas carteiras, muitas vezes gratuitas, repassando o custo da transferência para o consumidor. Além de possuir simplificação nas formas de pagamento, por só existir o formato a vista, que se aproxima do débito. A inexistência da taxa de adesão, também pode ser encarada como uma vantagem, uma vez que não possui um custo inicial para operacionalização, importante para pequenas empresas. O tipo de conexão, através de linha telefônica, presente nos modelos tradicionais de forma de pagamento, possui vantagens, devido sua estabilidade de conexão, em relação à internet, que pode variar se for utilizada através de conexão 3G, ainda que esta última seja uma alternativa mais barata. Em relação ao tipo de equipamento, como o plano de aluguel está incluso a máquina de cartão, se torna uma vantagem em relação ao *Bitcoin*, que necessita de um computador ou um celular, ainda que esses equipamentos sejam utilizados para outras funções, e não exclusivamente para as transações, sendo assim, não estariam onerando o cálculo. E por último, o tempo de recebimento, que apresenta grande diferença, pois os processos de pagamentos no *blockchain*, são confirmados em cerca de 10 minutos, enquanto nos métodos tradicionais, leva-se de 1 até 31 dias para receber os valores dos pagamentos.

Dessa forma, as principais vantagens observadas no método do *Bitcoin* são: o custo de operacionalização, que inexiste para os comerciantes, pois somente quem irá pagar a taxa de transação será o cliente; e o tempo médio para confirmação por

transação, que podem ser analisados e acompanhados através do site Blockchain.info (2018), conforme demonstrados abaixo:

Os valores relativos aos custos percentuais sobre transações, no qual os consumidores irão ter de pagar, pode ser analisado no gráfico abaixo, que representa a média do custo sobre o valor das transações, dados do dia (20/12/2017 até 15/06/2018). Custo médio do período: 1,57%

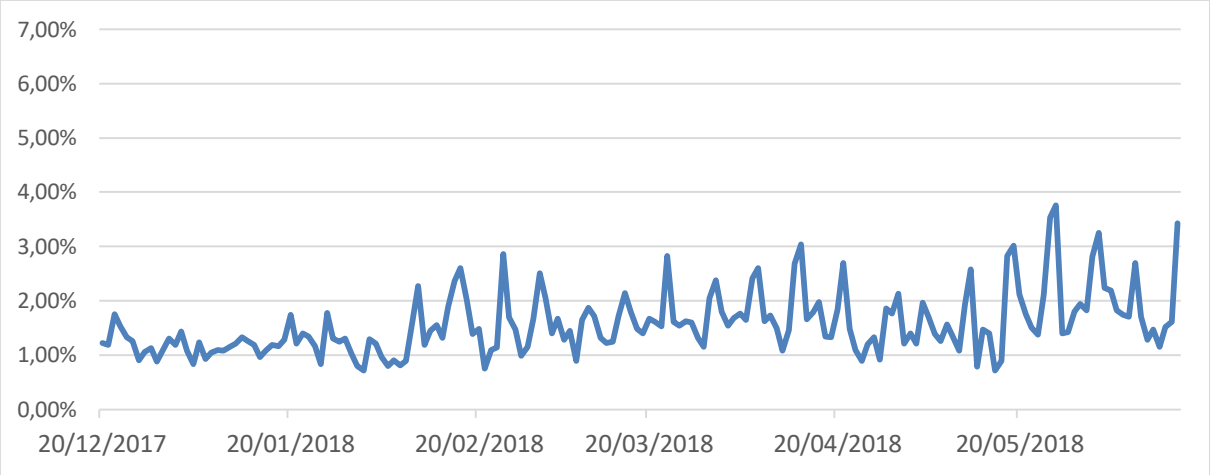

Gráfico 2 – % Custo médio sobre transações Bitcoin

Fonte: Blockchain.info

Também, é possível acompanhar no Blockchain.info (2018) os valores relativos ao tempo médio de confirmação das transações, dados do dia (20/12/2017 até 15/06/2018). Tempo médio do período: 9:43 minutos.

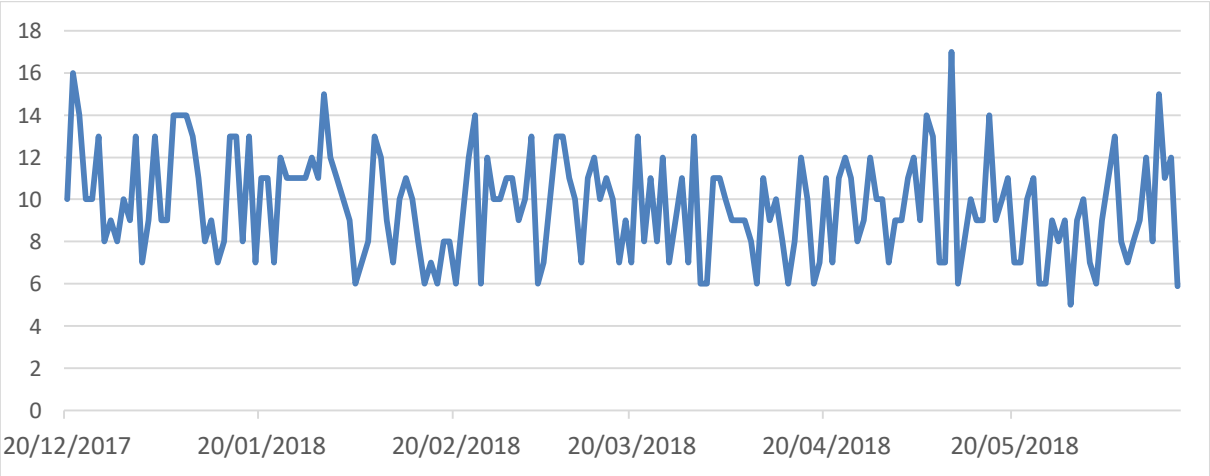

Gráfico 3 – Tempo médio confirmação da transação (minutos)

Fonte: Blockchain.info

Para os dois gráficos apresentados, percebe-se oscilações constantes, tanto no custo por transação, que em alguns momentos chegou a ultrapassar os 3%, quanto no tempo de confirmação das transações que em alguns dias ultrapassou o tempo médio aproximado de 10 minutos. Devendo ser constantemente acompanhados, uma vez que o tempo de confirmação poderá depender da taxa de serviço oferecida aos mineradores

Após os comerciantes receberem seus valores em criptomoedas em suas devidas carteiras, sinalizadas para os consumidores depositarem, o destino dessas moedas será definido conforme o desejo do comerciante, que no momento as possui. Dentre as opções estão: Transferir para uma outra carteira, pessoal ou de terceiros como forma de pagamento por um produto ou serviço; vender para uma casa de câmbio especializada em criptomoedas, ou para alguém que aceite fazer a conversão para alguma outra moeda; ou guardar como forma de investimento. Para muitos que ainda não possuem um conhecimento elevado do funcionamento do *Bitcoin*, mas mesmo assim desejam incorporar essa forma de pagamento em suas operações, uma das alternativas apresentadas no mercado é através das corretoras, que são organizações que oferecem diversos serviços e soluções a respeito do processamento de pagamentos, inclusive de criptomoedas. Dessa maneira, é possível, através de diversas plataformas, acessar sua carteira disponibilizada pela própria corretora e converter todos os recebimentos em criptomoedas. Fazendo com que o valor seja automaticamente transferido para sua conta bancário na sua moeda, caso desejado. Porém, é importante ressaltar que essas operações são cobradas, com o custo variando em torno de 1 a 2 % sobre as transações, conforme limites estabelecidos pelas corretoras.

Existem atualmente diversas empresas de pagamento através das criptomoedas, diferenciadas pelo tipo de serviços oferecidos ou plataformas específicas, como aplicativos para celular, web etc. A partir de uma pesquisa feita pela Universidade de Cambridge, de acordo com Hileman e Rauchs (2017), com dados coletados através dessas empresas processadoras de pagamentos, utilizando uma amostra de 48 empresas, relativas a 27 países, envolvendo o pagamento de criptomoedas. Foi classificado 4 tipos de serviços principais:

- Serviços de transferência de dinheiro – proporcionam transferências de remessas pessoais, principalmente internacionais
- Pagamentos B2B (Business to Business) – proporciona pagamentos de empresas para empresas.
- Serviços comerciais – processa pagamentos de comércios que aceitam criptomoedas
- Plataforma de criptomoedas de uso geral – plataforma completa que permite que os usuários comprem, armazenem e transfiram criptomoedas, em serviços como contas seguradas e serviços de pagamento de contas.

Os Serviços Comercias são encontrados com maior frequência (52%) entre os demais serviços. Seguidos da Plataforma de criptomoeda de uso geral (46%), Serviços de transferência de dinheiro (29%) e Pagamentos B2B (19%). Assim, pode-se afirmar que os Serviços comerciais, que se destinam a processar os pagamentos para os usos comerciantes é o serviço mais amplamente oferecido pelas empresas do setor, facilitando a contratação dos empresários que optarem por esse tipo de serviço, uma vez que são mais fáceis de se encontrar.

Um dos serviços também disponíveis por essas empresas ou até mesmo para usuários independentes delas, é a transferência de fundos, que de acordo com Ulrich (2014) é uma das vantagens da moeda, sendo uma grande promessa ao futuro das remessas de dinheiro de baixo custo. Nesse cenário, no primeiro trimestre de 2013, a taxa média pelo serviço de transferências girou em torno de 9%. Em contraste as taxas de transações na rede *Bitcoin* que tenderam a ser aproximadamente 1% da transação. Sendo um instrumento em potencial para nações que possuem menos acesso ao serviço financeiro, seja por falta de condições financeiras ou acessibilidade. Também é uma ótima solução para imigrantes que vivem em países desenvolvidos e desejam enviar remessas aos seus parentes em países em desenvolvimento.

> As estimativas são de que as remessas de dinheiro enviado por trabalhadores imigrantes a suas famílias em países mais pobres ajudem 750 milhões de pessoas. [...] Adicionando todos os bilhões de transações financeiras envolvidas, as remessas chegam a quase US$ 500 bilhões. (AGENCIA BRASIL, 2017)

Analisando as informações levantadas, é possível verificar alguns dos diversos benefícios que a moeda digital oferece para os comerciantes, como baixo custo de operacionalização, velocidade no tempo de recebimento do pagamento, ausência de estorno de pagamento por fraude e empresas com soluções de pagamento completas. Como também para consumidores, principalmente devido aos custos de envio de remessas internacionais muito menores dos que as oferecidas no mercado. Entretanto é importante avaliar alguns pontos de atenção, como a preferência dos consumidores por métodos tradicionais de pagamento, como o cartão de crédito e débito, a necessidade de conexão com a internet e de dispositivos, seja ele computador ou celular, para efetuar as transações e também as taxas cobradas pelas empresas que oferecem serviços financeiros, principalmente com foco em converter para as moedas locais.

4.2 COMPORTAMENTO DO CONSUMIDOR

De acordo com Barbosa (2016, p.122), um fator fundamental no modelo de consumo introduzido pelas moedas digitais, é a inserção neste mercado, que enfrenta diversos desafios. O primeiro deles é justamente o de propiciar o acesso ao consumo. Em muitos países, não somente no Brasil, muitas pessoas não fazem parte do sistema bancário pelos custos que representam. A instabilidade financeira e altas inflacionárias dos países também corroboram para diminuição do poder de compra dos trabalhadores, como presenciado na Argentina nos últimos anos, assim como guerras, externas ou civis, como o conflito na Síria, fazem com que indivíduos busquem saídas alternativas para a manutenção no mercado de consumo.

Analisando o comportamento dos consumidores da moeda virtual *Bitcoin*, é interessante primeiramente visualizar o potencial ao qual essa tecnologia está inserida, ou seja, sua disponibilidade de consumo. A internet, como um dos fatores primordiais para o funcionamento do *Bitcoin*, em amplitude nacional, apresenta grande acessibilidade pelos cidadãos brasileiros. Segundos dados do IBGE (2016), o uso da internet tem sido cada vez mais comum, representando cerca de 70% dos domicílios. Presente na maioria das Grandes Regiões: 76,7% das residências na região Sudeste, 74,7% na região Centro-Oeste e 71,3% da Sul, ficando em 62,4%, no Norte, e 56,6%,

no Nordeste. Já nas áreas rurais ainda se percebe dificuldade na acessibilidade da internet, com o resultado abaixo da metade dos domicílios.

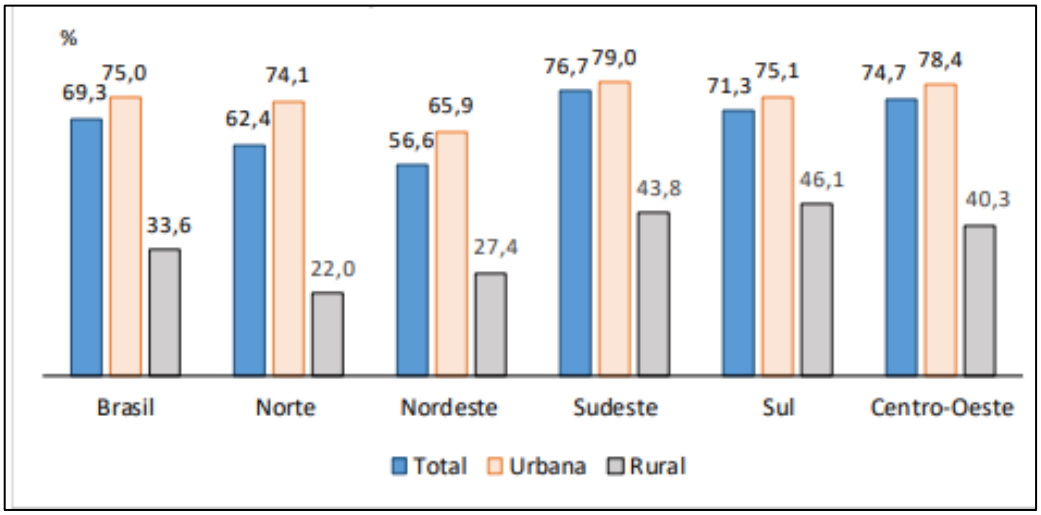

Gráfico 4 – Acesso à internet no Brasil

Fonte: IBGE

Entre 97,2% dos domicílios em que havia internet, o telefone móvel celular era utilizado para este fim, seguido do computador com 57,8%, do tablete com 17,8% e o uso da televisão com 11,7% de representatividade (IBGE, 2016). Assim, percebe-se que além da internet predominar sobre a extensão do país, sendo um ponto positivo na implantação de um sistema voltado as criptomoedas, o acesso por meio de dispositivos móveis, como o celular, é a preferência, levando a entender melhor o comportamento do consumidor em relação as tecnologias e onde poderá ser direcionado o foco das ações voltadas ao público dos usuários/consumidores das criptomoedas.

A partir de uma pesquisa feita pela University of Cambridge, pelos autores Hileman e Rauchs (2017), chegou-se a uma estimativa, através de grande esforço, do total de detentores de criptomoedas, dificuldade devido ao fato de que usuários podem ter mais de uma carteira de vários fornecedores. Além disso, podem ter diferentes tipos de criptomoedas, podendo ser contato múltiplas vezes. Ou seja, é impossível saber precisamente quantas pessoas utilizam as criptomoedas. Entretanto, usando dados obtidos dos participantes do estudo de diversos países, assumiu-se que um indivíduo detém em média duas carteiras, estimou-se na pesquisa que existam, mundialmente, entre 2,9 milhões e 5,8 milhões de usuários únicos ativos no ano de 2017. Importante ressaltar que os valores certamente são muito maiores pois não

incluem usuários que utilizam carteiras de corretoras, ou empresas de serviço de pagamento como plataforma de transações.

Conforme observado, o cenário de usuários aumentou significativamente desde 2013. Utilizando os dados oferecidos pela pesquisa dos autores Hileman e Rauchs (2017) foi possível criar uma previsão pela ferramenta de estatística do Excel, a partir do histórico do ponto médio de usuários, utilizando um intervalo de confiança de 95%, sendo assim, no ano de 2022 estima-se que deva existir entre 7,8 milhões e 10,3 milhões de usuários únicos ativos. Uma quantidade ainda muito baixa quando comparada com os 7,6 bilhões de habitantes no planeta, representando atualmente cerca de 0,08% da população.

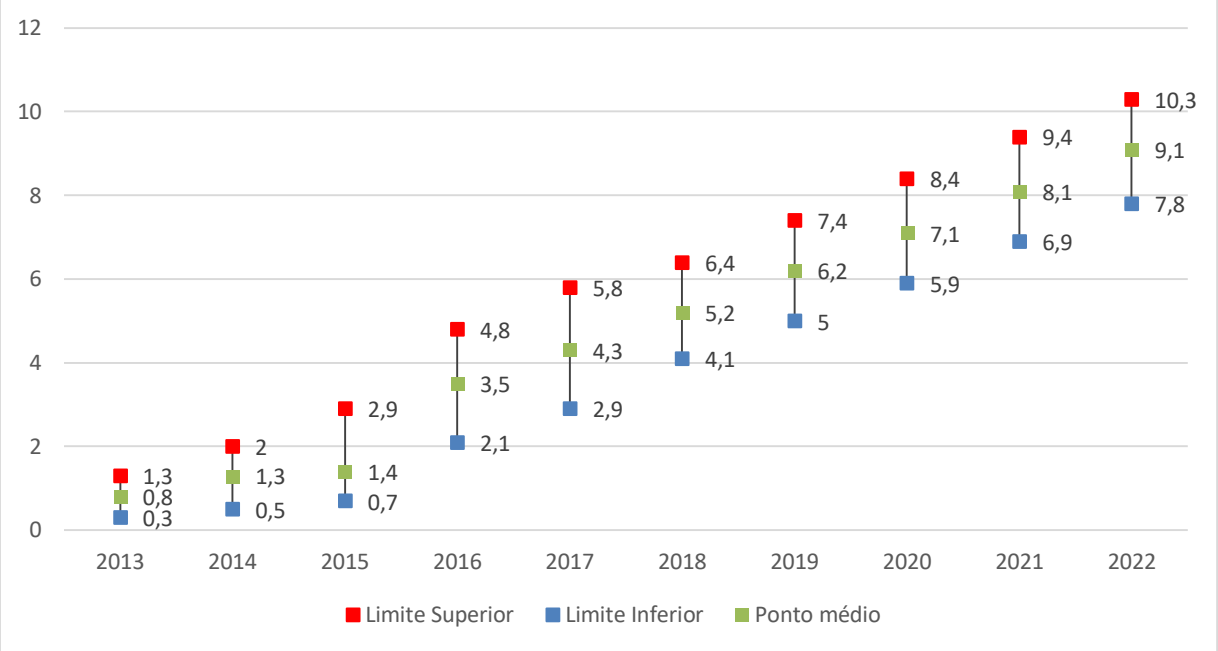

Gráfico 5 – Usuários únicos ativos de Bitcoin no mundo (em milhões)

Fonte: Previsão realizada pelo autor

Aplicando o percentual de 0,08% (2018) ao número de habitantes no Brasil (cerca de 207 milhões), estima-se que o público das criptomoedas no país é de aproximadamente 174 mil usuários únicos ativos. Lembrando que esses dados podem sofrer grandes variações, pois é de grande complexidade estimar volumes em uma tecnologia que preza pelo anonimato, e também devido a grandes oscilações na demanda por criptomoedas os valores e previsões podem ser alterados constantemente.

Ainda que a quantidade de usuários não seja tão significativa, percebe-se uma grande quantidade, representadas em dólares, de transações realizadas no *Blockchain*. Segundo dados do site Blockchain.info (2018) o valor estimado de transações em USD (dólares) ocorridas nos dias avaliados (20/12/2017 até 15/06/2018) foi em média de $1.570.392.398,00 (um bilhão e quinhentos e setenta milhões e trezentos e noventa e dois mil e trezentos e noventa e oito dólares). Chegando a bater o recorde de transações em um dia na data 11/12/2017 com o total de $5.760.245.260,00 (cinco bilhões e setecentos e sessenta milhões e duzentos e quarenta e cinco mil e duzentos e sessenta dólares). Porém, percebe-se que a média tenha sofrido uma drástica redução nos últimos 15 dias avaliados, chegando a $726.369.536,00 (setecentos e vinte e seis milhões e trezentos e sessenta e nove mil e quinhentos e trinta e seis dólares).

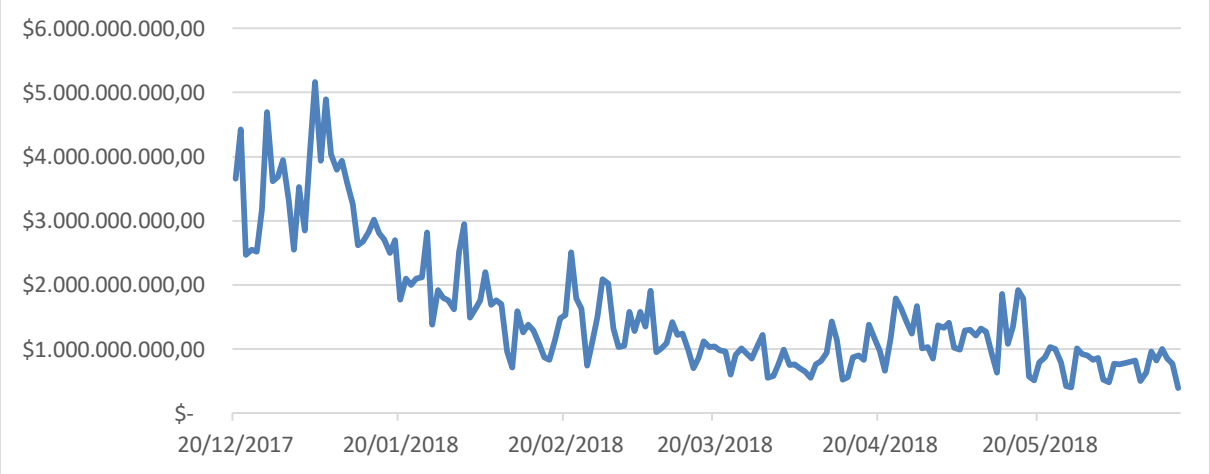

Gráfico 6 – Quantidades de Transações diárias (em dólar)

Fonte: Blockchain.info

Segundo dados do site Blockchain.info (2018) a média da quantidade confirmada de transações *Bitcoin* ocorridos no período avaliado (20/12/2017 até 15/06/2018) foi de aproximadamente 215.420 (duzentos e quinze mil e quatrocentos e vinte). Chegando a bater o recorde da quantidade confirmada de transações na data 13/12/2017 com 490.644 (quatrocentos e noventa mil e seiscentos e quarenta e quatro). Entretendo, assim como o valor das transações sofreu queda, nos últimos 15 dias avaliados, a quantidade de transações confirmadas também caiu, chegando a média de 196.059 (cento e noventa e seis mil e cinquenta e nove).

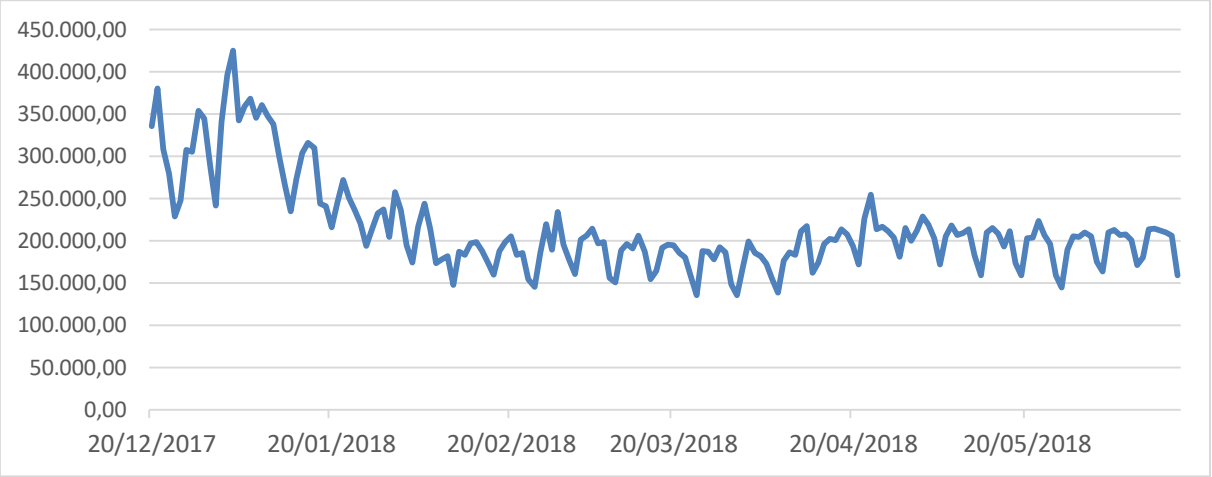

Gráfico 7 – Quantidades de Transações diárias confirmadas

Fonte: Blockchain.info

Analisando essas duas informações, é possível dizer que no período avaliado, a média de Transações (USD) pela Quantidade Transações é de U$ 6.830 (seis mil e oitocentos e trinta dólares). Por se tratar de um valor alto por transação, presume-se que possivelmente a maioria das operações que estão sendo realidades são fruto de compra e venda de moeda em corretoras, para especulação e ganhos com a variação, utilizadas como forma de investimento de alto risco e grande rentabilidade.

4.3 REGULAMENTAÇÃO DAS MOEDAS VIRTUAIS

Segundo Silva (2018, p.13), atualmente o Brasil não possui qualquer tipo de regulamentação específica no direito pátrio a respeito do uso das criptomoedas por qualquer ente público ou privado em qualquer tipo de atividade. Gerando várias dúvidas de como será o futuro nos campos das exigências tributárias e jurídicas. Uma regulamentação específica desta natureza deverá ser analisada com cautela, pois pode sufocar o mercado interessado pelo o uso das criptomoedas, fazendo com que a tecnologia *Blockchain* perca força. Entretanto, para o Estado e o Mercado se posicionarem, será necessário um grande esforço no que se refere ao conhecimento da tecnologia.

O cartão de débito é o meio de pagamento que mais se aproxima do entendimento das Criptomoedas, uma vez que a transação é feita de maneira direta de recursos de uma parte para outra, onde os bancos, como verificadores, exercem a

mesma função que os mineradores do *Blockchain*, analisando os valores em conta e a documentação. O conceito presente na resolução do CMN 4.282 de 2013, elenca o entendimento a respeito dos arranjos de pagamento (SILVA, 2018, p.16):

I. pagador: pessoa natural ou jurídica, que autoriza a transação do pagamento
II. recebedor: pessoa natural ou jurídica, destinatário final dos recursos de uma transação de pagamento
III. transação de pagamento: ato de pagar, de aportar, de transferir ou de sacar recursos independentemente de quaisquer obrigações subjacentes entre o pagador e o recebedor; e
IV. usuário final de serviços de pagamento: pessoa natural ou jurídica que utiliza um serviço de pagamento, como pagador ou recebedor.

Até o momento, essa relação de usuário final de serviços de pagamento, pagador, recebedor, se assemelha ao conceito utilizado na plataforma *Blockchain*. Onde o usuário final de serviços de pagamento (consumidor) emite à rede *Blockchain*, no caso o pagador, uma solicitação de transferência de uma carteira, registrada em um endereço eletrônico especifico para outra carteira determinada, dessa forma, a transação de pagamento chega ao recebedor, conforme os termos indicados pelo usuário final. As duas formas de transação, por cartão de débito e por criptomoedas, passam por uma verificação das informações referentes a transação dos usuários envolvidos, a primeira forma é feita pelos Bancos, exigindo o cumprimento de vários requisitos, descritos na Resolução 2.025 do BACEN, como qualificação do depositante, endereços residencial e comercial, telefones, assinaturas e outras informações sobre a conta. Esse é um dos motivos que faz com que as operações realizadas através dos cartões de débito e débito sejam mais custosas, em relação ao criptomoedas, pois estão expostas a diversos processos, que envolvem diversas tarifas, aumentando o custo das transações.

Já a segunda forma de transação, através do *Blockchain* requer, em alguns casos, apenas um endereço de e-mail de cadastro e a inserção de uma senha, para a criação de uma carteira, em seguida já é possível iniciar uma operação. Que passará pela validação de outros usuários, conhecidos como mineradores, cobrando apenas uma pequena taxa por transação pela prestação de serviço.

SILVA (2018, p.31) faz um comparativo entre os arranjos de pagamento convencionais e as criptomoedas:

	PAGAMENTO VIA CRIPTOMOEDA	**ESQUEMAS DE PAGAMENTO**
ORIGEM	Realizado via sistema da Criptomoeda	Realizado via instituição financeira
MEIO DE PAGAMENTO	Utiliza Criptomoedas	Utiliza moeda tradicional
INTERMEDIÁRIO	Usuários do sistema da Criptomoeda	Instituição financeira
REGULAÇÃO	Não possui regulamentação própria, mas é abarcado por legislação geral	Altamente regulado pelo Estado, via agências reguladoras e legislação

Quadro 2 – Comparação Sistemas de Pagamento (adaptado)
Fonte: SILVA (2018)

Conforme Silva (2018, p.19), o mercado de meios de pagamento convencional, é altamente regulado, contendo várias normas emitidas por autoridades, guiadas de forma a penalizar infratores em termos da legislação. Como o meio de pagamento passa por uma instituição financeira, a mesma é obrigada a realizar uma análise, conhecida como análise de risco de *Compliance,* investigando a probabilidade do uso do sistema financeira para realização de crimes, como lavagem de dinheiro e financiamento ao terrorismo. Envolvendo não somente instituições financeiras, mas vários órgãos estatais como: COAF, o BACEN, a Receita Federal e o Ministério da Fazenda. Logo, percebe-se a complexidade envolvida para a realização das operações de pagamento via cartão de débito e crédito.

> [...] outra preocupação é que o Bitcoin seja usado para a lavagem de dinheiro para o financiamento do terrorismo e tráfico de produtos ilegais. Apesar de essas inquietações serem, neste momento, mais teóricas do que empíricas, o Bitcoin poderia de fato ser uma opção àqueles que desejam mover dinheiro sujo discretamente (ULRICH, 2014, p.32).

De fato, a utilização das moedas virtuais como meio de atividades ilegais é possível, uma vez que permite a criação de pseudônimos, facilitando as ações de

criminosas, através de lavagem de dinheiro, financiamento de atividades terroristas e do tráfico. Sendo um dos pontos de atenção entre os envolvidos, que precisa ser analisado com cautela, para evitar generalização e depreciação da proposta ao qual a tecnologia se oferece. Uma vez que, mesmo com o sistema convencional, e todas as normas de *Compliance* exercidas pelas instituições financeiras, esses problemas não foram extintos.

No comunicado nº 31.379 realizado pelo Banco Central do Brasil (2017), decorrente ao crescente interesse dos agentes econômicos nas moedas virtuais, o Banco Central realizou algumas advertências a respeito das transações da moeda virtual:

> 3. Destaca-se que as moedas virtuais, se utilizadas em atividades ilícitas, podem expor seus detentores a investigações conduzidas pelas autoridades públicas visando a apurar as responsabilidades penais e administrativas.
>
> 4. As empresas que negociam ou guardam as chamadas moedas virtuais em nome dos usuários, pessoas naturais ou jurídicas, não são reguladas, autorizadas ou supervisionadas pelo Banco Central do Brasil. Não há, no arcabouço legal e regulatório relacionado com o Sistema Financeiro Nacional, dispositivo específico sobre moedas virtuais. O Banco Central do Brasil, particularmente, não regula nem supervisiona operações com moedas virtuais.

Portanto, conclui-se que mesmo o ambiente permitindo uma liberdade maior para atividades ilícitas, não está impune de investigações e consequentemente punições em casos de transgressões a lei. Uma vez que, em muitos casos, é possível através de cruzamento de informações e rastros deixados na internet, saber de onde são feitas as operações e quem são os responsáveis. O Comunicado também isenta a responsabilidade do Estado a respeito da supervisão das empresas que negociam ou guardam as moedas virtuais, tornando-se de total responsabilidade dos usuários zelar pelos seus ativos.

Após o entendimento do funcionamento das criptomoedas, é preciso, conforme Silva (2018) identificar a natureza jurídica deste instrumento, para então, indicar como será considerado conforme o arcabouço jurídico brasileiro. Enquanto o Estado não definir, terá grande dificuldade de lidar com esta nova tecnologia, seja para tributar qualquer transação, ou julgar causas envolvendo seu uso. Por exemplo, caso a criptomoeda seja considerada como valor mobiliário, a CVM possuirá

competência regulamentar sobre seu uso, excluindo BACEN ou a Receita Federal. Já se for considerada uma moeda, estará sujeita a regulamentação por parte do BACEN. Caso seja considerada como um bem em geral, possuirá tutela jurídica própria. A complexidade classificação advém de uma série de características próprias que diferem de vários outros instrumentos existentes.

Analisando as criptomoedas a fundo é possível identificar que elas possuem diferentes interpretações de como pode ser considerada, variando de moeda, para bem móvel, *commodity,* e até mesmo valor mobiliário, dependendo da situação e contexto que é utilizada. Possuindo assim, uma natureza jurídica mutante, variando de acordo com o seu uso. Esse conceito abre margem para interpretações, que podem ser avaliadas conforme descrita no art. 4º da lei de Introdução às normas do Direito brasileiro: " Art. 4º Quando a lei for omissa, o juiz decidirá o caso de acordo com a analogia, os costumes e os princípios gerais de direito". Assim, o poder judiciário, representado pelos juízes, terão livre interpretação dos casos apresentados, com base no seu conhecimento, e/ ou subsídios históricos. Porém esse tipo de liberdade, acaba resultando em uma insegurança quanto ao assunto, uma vez que por ser algo tão novo, não possui tantos fundamentos para apoio. Mesmo alguns países já terem emito algumas decisões jurídicas e pareceres a respeito das criptomoedas, percebe-se ainda uma ausência de consenso entre tais decisões, demonstrando a inexistência de qualquer tipo de linha de pensamento dominante a respeito da natureza jurídicas. (SILVA, 2018, p.41).

Desde sua criação, as moedas virtuais, geraram grande discussão em diversos cenários, envolvendo muitos setores e especialistas, principalmente economistas, advogados, juízes, administradores, comerciantes, desenvolvedores de tecnologia etc. Com isso, surgiu a necessidade de regulamentação a respeito do uso das moedas virtuais, uma vez que cada país, conforme seu entendimento da nova proposta da moeda, interpretou de maneira diferente e estabeleceu decisões que melhor se adequavam a suas estratégias como nação. Algumas tiveram o entendimento de ameaça, principalmente aos bancos centrais e instituições financeiras, outras entenderam como uma tecnologia crescente e incremental ao sistema financeiro existe.

Conforme o passar dos anos, o conhecimento das criptomoedas vem aumentando, fazendo com que as decisões a respeito estejam sempre sujeitas a

alterações. Conforme Silva (2018), através das respostas emitidas pelos bancos centrais e demais instituições financeiras, elencou-se três decisões tomadas pela grande maioria dos países a respeito das criptomoedas: Abolição, regulação e ausência de resposta regulatória. Abaixo uma tabela, sintetiza as decisões de alguns países:

Jurisdição	**Lavagem de dinheiro e financiamento ao terrorismo**	**Tributação**	**Advertências e aviso ao consumidor**	**Licença/registro de intermediadoras de moedas virtuais**	**Setor financeiro, advertências ou banimento**	**Proibição de emissão e/ou uso**
ARGENTINA	Aviso de riscos	---	Advertência ao consumidor	---	Advertência da necessidade de reporte	---
BOLÍVIA	---	---	---	---	---	Sim
CANADÁ	Alterou a regulação existente	Tratamento fiscal esclarecido	Parecer consultivo	Incorporou em Lei existente	---	---
CHINA	---	---	---	---	Baniu	---
FRANÇA	Aplicação de regulação existente	Tratamento fiscal esclarecido	Advertência ao consumidor	---	---	---
ALEMANHA	Aplicação de regulação existente	---	---	---	---	---
ITÁLIA	---	---	Advertência ao consumidor	---	Advertiu	---
JAPÃO	Pretensão de introdução de nova regulação	---	Advertência ao consumidor	Pretensão de introdução a uma nova regulação	---	---
RÚSSIA	Aplicação de regulação existente	---	Advertência ao consumidor	---	---	Sim, via projeto de lei
CINGAPURA	Aplicação de regulação existente	Tratamento fiscal esclarecido	Advertência ao consumidor	---	---	---
ÁFRICA DO SUL	---	---	Advertência ao consumidor	---	---	---
REINO UNIDO	Aplicação de regulação existente	Tratamento fiscal esclarecido	---	---	---	---
ESTADOS UNIDOS	Tratamento fiscal esclarecido (federal)	Tratamento fiscal esclarecido (federal)	---	Estado licenciou	---	---
AUSTRÁLIA	---	Equivalente moeda tradicional	---	Equivalente a moeda tradicional	Equivalente a moeda tradicional	---

Quadro 3 – Decisões criptomoedas no mundo

Fonte: SILVA (2018)

Assim, Silva (2018), afirma que o Brasil, é um dos países que se encontra na classificação de Ausência de Regulação Efetiva. Ainda que, o projeto de Lei 2.303/2015, do Deputado Federal Áureo Lídio Moreira Ribeiro, vise incluir as moedas virtuais e programas de milhagem aéreas na definição de “arranjos de pagamento” sob a supervisão do Banco central. Assim, caso o projeto de lei obtenha sucesso, as moedas virtuais passarão a ser consideradas como ativos financeiros, e a regulamentação será de responsabilidade do BACEN.

Em relação ao Brasil, o Comunicado nº 31.379 realizado pelo Banco Central do Brasil (2017), também apresenta um posicionamento a respeito das moedas virtuais:

> Considerando o crescente interesse dos agentes econômicos (sociedade e instituições) nas denominadas moedas virtuais, o Banco Central do Brasil alerta que estas não são emitidas nem garantidas por qualquer autoridade monetária, por isso não têm garantia de conversão para moedas soberanas, e tampouco são lastreadas em ativo real de qualquer espécie, ficando todo o risco com os detentores. Seu valor decorre exclusivamente da confiança conferida pelos indivíduos ao seu emissor.
>
> 2. A compra e a guarda das denominadas moedas virtuais com finalidade especulativa estão sujeitas a riscos imponderáveis, incluindo, nesse caso, a possibilidade de perda de todo o capital investido, além da típica variação de seu preço. O armazenamento das moedas virtuais também apresenta o risco de o detentor desses ativos sofrer perdas patrimoniais.
>
> 7. Embora as moedas virtuais tenham sido tema de debate internacional e de manifestações de autoridades monetárias e de outras autoridades públicas, não foi identificada, até a presente data, pelos organismos internacionais, a necessidade de regulamentação desses ativos. No Brasil, por enquanto, não se observam riscos relevantes para o Sistema Financeiro Nacional. Contudo, o Banco Central do Brasil permanece atento à evolução do uso das moedas virtuais, bem como acompanha as discussões nos foros internacionais sobre a matéria para fins de adoção de eventuais medidas, se for o caso, observadas as atribuições dos órgãos e das entidades competentes.

Ainda que não possua uma efetiva regulamentação, para fins tributários é necessária sua declaração no Imposto de Renda, conforme esclarecimento da pergunta feita à Receita Federal: as moedas virtuais devem ser declaradas?

> Sim. As moedas virtuais (bitcoins, por exemplo), muito embora não sejam consideradas como moeda nos termos do marco regulatório atual, devem ser declaradas na Ficha Bens e Direitos como “outros bens”, uma vez que podem

> ser equiparadas a um ativo financeiro. Elas devem ser declaradas pelo valor de aquisição (RECEITA FEDERAL, 2018, p.182).

A própria Receita Federal ainda faz uma ressalva quanto a declaração de qualquer valor:

> Como esse tipo de “moeda” não possui cotação oficial, uma vez que não há um órgão responsável pelo controle de sua emissão, não há uma regra legal de conversão dos valores para fins tributários. Entretanto, essas operações deverão estar comprovadas com documentação hábil e idônea para fins de tributação (RECEITA FEDERAL, 2018, p. 182).

Outra pergunta também respondida pela instituição, diz a respeito da alienação de moedas virtuais:

> Os ganhos obtidos com a alienação de moedas virtuais (bitcoins, por exemplo) cujo total alienado no mês seja superior a R$ 35.000,00 são tributados, a título de ganho de capital, segundo alíquotas progressivas estabelecidas em função do lucro, e o recolhimento do imposto sobre a renda deve ser feito até o último dia útil do mês seguinte ao da transação. As operações deverão estar comprovadas com documentação hábil e idônea. RECEITA FEDERAL, 2018, p. 245).

Entretanto, existe uma realidade diferente para outros países, classificados como aderentes a regulação do uso de criptomoedas, como é os Estados Unidos da América, sendo o primeiro país a emitir efetiva regulação a respeito do tema, estabelecendo as maneiras de integração desse novo instrumento à econômica local. O comunicado 2014.21 foi o responsável por responder diversas perguntas a todos os contribuintes, esclarecendo como lidar com as criptomoedas em 25 de março de 2014. A IRS, equivalente a Receita Federal no Brasil, determinou que as criptomoedas devem ser classificadas como bens, aplicando-se a legislação a respeito de bens em todos os tipos de transações que envolvessem criptomoedas. No entanto, o Departamento de Serviços Financeiros de Nova Iorque, emitiu uma regulação específica no uso das criptomoedas, impondo que todas as operações financeiras que estejam envolvidas com moedas virtuais, sejam elas de câmbio, pagamento, transferências, devem ser intermediadas por empresas que possuam uma licença para tais ações, licenças expedidas por instituições financeiras (Silva, 2018, p.106).

Existem também países que proibiram o uso de criptomoedas, como é o caso do Equador, e não somente ele, como a China e Bolívia, que optaram por banir o uso das criptomoedas de maneira parcial ou completa. O posicionamento ocorre pelas dificuldades e riscos gerados pelo uso das criptomoedas, em especial as questões de *Compliance*, prevenção à lavagem de dinheiro e proteção da economia nacional. No caso do Equador, o país proibiu somente a circulação das criptomoedas que não são emitidas pelo Banco Central do país, já que as criptomoedas são geradas pelo Estado, fazendo com que as demais não sejam reconhecidas em território nacional. Já no caso da China, apenas os bancos estão proibidos de lidar com criptomoedas nas suas atividades, assim, somente o povo e as demais empresas estão livres para qualquer tipo de transação desta tecnologia. Já na Bolívia, houve proibições totais do uso de criptomoedas, alegando afetar o poder aquisitivo interno da moeda emitido pelo Estado, e não atenderem aos sistemas de segurança imposto pela legislação boliviana. Ainda que efetivamente, não seja possível uma proibição total, uma vez que apenas possuindo acesso à internet, já seja possível realizar qualquer ação no sistema *Blockchain* (SILVA, 2018, p.112).

5. CONCLUSÃO

O presente estudo, tinha como principal objetivo, analisar os principais benefícios, riscos e desafios que possivelmente empresários teriam caso adotassem uma política de pagamento através da criptomoeda *Bitcoin*. Levando em consideração o fato do tema ser ainda pouco difundido no mundo e principalmente no Brasil, muitas dúvidas, devido à sua natureza inovadora e tecnológica, acabam por suprimir ações de desenvolvimento na área, mesmo para aqueles que demonstram um desejo inicial de se aprofundarem no assunto. Assim, este projeto visou contribuir, não somente para a literatura nacional a respeito das criptomoedas, mas também para as empresas que estejam buscando conhecimento sobre maneiras alternativas aos modelos financeiros impostos pelo Estado e pelos grandes monopólios que são os bancos.

Conforme pode ser observado, ao longo da história da criação das primeiras moedas, a humanidade sempre esteve preocupada em buscar moedas que viabilizassem suas negociações e melhor representassem suas necessidades. Assim, as evoluções de vários tipos de meios de troca ocorreram em diversos locais do mundo, até finalmente chegar ao que conhecemos hoje. Este fato demonstra a necessidade de busca constante de melhoria em nossa moeda, uma vez que as suas caraterísticas de divisibilidade, durabilidade, dificuldade em falsificação e facilidade em transportar devem ser atendidas da melhor forma. Assim, o *Bitcoin* se propõe, como moeda virtual, atingir todas essas características de forma satisfatória.

Como qualquer tecnologia, alguns recursos se tornam indispensáveis para o funcionamento perfeito, não seria diferente com o *Bitcoin*, que requer não só um recurso, mas diversos como a Internet, a criptografia, a Prova de Trabalho, a rede peer-to-peer, entre outros, como a energia elétrica, que pode ser considerada, mas que está tão presente em nossa realidade, que não é possível ainda imaginar um mundo sem ela.

Desde a criação do *Bitcoin*, pelo denominado Satoshi Nakamoto, percebe-se muita discussão a respeito dos papéis e responsabilidades dos bancos. Uma vez que devido suas manobras podem ocasionar grandes impactos, como períodos de inflação, resultando em consequências catastróficas para a população. Logo, o Bitcoin, por não possuir autoridades centrais que manipulem a criação de moeda desregradamente, surge como uma solução para diversos problemas. Como pode ser

analisado, o *Blockchain*, sendo uma plataforma de registros de todas as movimentações das transações do *Bitcoin*, é interpretado como uma plataforma extremamente transparente, por permitir que todos vejam as transações que ocorrem nela, permitindo inclusive anonimato dos seus usuários. Além de ser um sistema, de fácil acesso para a maioria da população, pois necessita incialmente apenas de uma conexão com a internet, e um conhecimento prévio do funcionamento do sistema.

Devido a rede do *Blockchain* não possuir um órgão centralizado que viabilize as transações que ocorrem a todo instante, os chamados mineradores, através de seu poder computacional, exercem o papel de aprovadores de todas as movimentações. Como qualquer outro serviço, há um custo envolvido no processo, dessa forma, os mineradores utilizam de uma pequena porcentagem para manter seus computadores trabalhando e adquirirem lucros devido a seu trabalho.

Atualmente, um dos problemas mais presentes referente a utilização do *Bitcoin*, é a volatilidade, indicando a intensidade e frequência da oscilação do seu preço, uma vez que, a moeda *bitcoin*, possui seu preço definido pelo mercado. Conforme observado, em alguns meses teve uma variação de 450% sobre seu preço em apenas dois meses. Apresentando como uma das justificativas as "bolhas" especulativas, ocasionadas pela cobertura de imprensa em excesso. Impulsionando novos investidores, fazendo com que o preço oscile.

Dentre os principais benefícios encontrados na literatura, estão os menores custos de transação, potencial arma contra pobreza e a opressão, e o estimulo à inovação financeira. Como pode ser visto na análise, conclui-se que esses benefícios de fato são observados. Uma vez que, principalmente para empresas, que aceitarem o *Bitcoin* como meio de pagamento, terão seus custos próximos a zero, se tratando de pagamentos. Pois não precisam dispender grandes investimentos, ou pagar diversas taxas de serviços para credenciadores, que nem sempre atendem suas necessidades. Também foi observado a diferença do tempo de recebimento que em comparação aos 10 minutos do *Bitcoin* com um sistema de pagamento convencional, podendo levar até 31 dias. Assim como também o benefício de pessoas que estejam em situação de pobreza e opressão, e não se encontrem em seus países, podem ter grandes benefícios, principalmente fazendo transferências internacionais para suas respectivas famílias.

Se tratando do comportamento do consumidor, percebe-se grande dificuldade na obtenção de informações concisas, que possam ser utilizadas, principalmente para definir potenciais consumidores e perfis. Uma vez que o sistema do *Blockchain* preza justamente pela ausência de informações referente a pessoa, e as empresas que trabalham como intermediadoras, por questões de privacidade também se mostram resistentes na divulgação de informações sobre seus clientes. Mesmo assim, pode-se estimar uma quantidade de utilizadores ativos do *bitcoin*, e mesmo representando uma quantidade pequena em comparação com o mundo, para melhores análises deve ser analisado localmente, e de preferência por setor, pois podem existir ramos que sejam mais propícios a sua utilização, como os envolvidos com tecnologia. Também foi suposto que a maioria das transações feitas atualmente sejam com o foco em ganhos imediatos em função da valorização da moeda. O que pode representar um grande empecilho para evolução como meio de pagamento, pois torna o preço da moeda mais volátil.

Por último, a análise visou responder algumas possíveis dúvidas referente a legislação das criptomoedas. Trazendo alguns comparativos entre a regulação no Brasil e nos principais países. Sendo possível verificar que o Brasil ainda se encontra no status de ausência de uma regulação efetiva. Ainda que exista um projeto de lei para regularizar essa situação. Sendo um grande desafio para todas as ordens, por se tratar de um assunto novo. Mesmo já existindo advertências do Banco Central sobre a ausência de responsabilidade das entidades financeiras sobre as criptomoedas e suas consequências. Podendo ser um impeditivo para grandes investimentos, decorrentes da falta de visibilidade que podem seguir os caminhos da regulamentação das moedas digitais.

Portanto, conclui-se que o trabalho tenha atingido seu propósito esclarecedor e contributivo para futuras tomadas de decisões, agregando valor na evolução e conhecimento das criptomoedas e sua caraterísticas.

REFERÊNCIAS

AGENCIA BRASIL. **Remessas de imigrantes somam cerca de US$ 500 bilhões ao ano no mundo**, 2017**.** Disponível em < http://agenciabrasil.ebc.com.br/ > Acesso em 03 de julho de 2018.BANCO CENTRAL DO BRASIL. Estatísticas de Pagamentos de Varejo e de Cartões no Brasil,2016. Disponível em <https://www.bcb.gov.br/?SPBADENDOS> Acesso em: 20/06/2018.

BANCO CENTRAL DO BRASIL. Comunicado nº 31.379, 2017. Disponível em <http://www.bcb.gov.br/pre/normativos/busca/normativo.asp?numero=31379&tipo=Comunicado&data=16/11/2017> Acesso em: 22/06/2018.

BARBOSA, Tatiana Casseb B.M. **A Revolução das Moedas Digitais**: Bitcoins e Altcoins. São Paulo: Revoar, 2016.

BLOCKCHAIN.INFO. Disponível em: <https://blockchain.info/charts> Acesso em: 20 de junho de 2018.

BLOCKGEEKS. **Cryptocurrency Wallet Guide: A Step-By-Step Tutorial**, 2017**.** Disponível em <https://blockgeeks.com/guides/cryptocurrency-wallet-guide/> Acesso em 26 de fevereiro de 2018.

CARVALHO, Fernando J. Cardim de et al. **Economia monetária e financeira**: teoria e política. 2. ed. rev. e atual. Rio de Janeiro: Campus, Elsevier, 2007.

COINMAP. Disponível em: <https://coinmap.org/> Acesso em: 30 de março de 2018.

COMER, Douglas E. **Redes de computadores e internet**. 6. ed. Porto Alegre: Bookman, 2016.

HILEMAN, Garrick; RAUCHS, Michel. **Global Cryptocurrency Benchmarking Study**, 2017. Disponível em: <https://www.jbs.cam.ac.uk/home/> Acesso em 23 de junho de 2018.

INFOMONEY. Disponível em: <http://www.infomoney.com.br/cryptos/bitcoin/> Acesso em 1 de abril de 2018.

JUELS, Ari; JAKOBSSON, Markus. **Proofs of Work and Bread Pudding Protocols** (Tese). Disponível em: < http://www.hashcash.org/papers/bread-pudding.pdf> Acesso em 10 de Junho de 2018.

MOUGAYAR, William. **Blockchain para negócios:** promessa, prática e aplicação da nova tecnologia da internet. Rio de Janeiro: Alta Books, 2017.

NAKAMOTO, Satoshi. **Bitcoin**: A peer-to-peer Electronic Cash System, 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em 26 de fevereiro de 2018.

PRODANOV, Cleber Cristiano; FREITAS, Ernani Cesar de**. Metodologia do trabalho científico**: métodos e técnicas de pesquisa e do trabalho acadêmico. 2. ed. Novo Hamburgo/RS: Feevale, 2013. Disponível em:

RECEITA FEDERAL. Perguntas e Respostas. 2018. Disponível em: <http://idg.receita.fazenda.gov.br/interface/cidadao/irpf/2018/perguntao/perguntas-e-respostas-irpf-2018-v-1-0.pdf > Acesso em: 23/06/2018.

SILVA, Luis Gustavo Doles. **Bitcoins & outras criptomoedas:** teoria e prática à luz da legislação brasileira. Curitiba: Juruá, 2018.

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