

INSTITUTO FEDERAL FARROUPILHA
CAMPUS SANTO AUGUSTO – RS
CURSO SUPERIOR DE BACHARELADO EM ADMINISTRAÇÃO
TRABALHO DE CONCLUSÃO DE CURSO

BRUNO CASAGRANDE

BITCOIN: SUAS ORIGENS E CARACTERÍSTICAS

Santo Augusto – RS

2021

BRUNO CASAGRANDE

BITCOIN: SUAS ORIGENS E CARACTERÍSTICAS

Trabalho de Conclusão de Curso apresentado ao curso de Administração do Instituto Federal Farroupilha de Educação, Ciência e Tecnologia Farroupilha, como requisito parcial à obtenção do título de Bacharel(a) em Administração.

Professor orientador: Me. Cleber Joel Stevens Kroetz

Santo Augusto – RS

2021

**INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
FARROUPILHA – IFFar
CURSO DE BACHARELADO EM ADMINISTRAÇÃO**

FOLHA DE APROVAÇÃO

BRUNO CASAGRANDE

BITCOIN: SUAS ORIGENS E CARACTERÍSTICAS

Trabalho de Conclusão de Curso apresentado ao curso de Bacharelado em Administração do Instituto Federal de Educação, Ciência e Tecnologia Farroupilha, como requisito parcial à obtenção do título de bacharel em Administração.

Aprovado em: 13/12/2021

Banca Examinadora:

Dr. Cesar Eduardo Stevens Kroetz
Instituto Federal de Educação, Ciência e Tecnologia Farroupilha

Dra. Amanda Caroline Martin
Instituto Federal de Educação, Ciência e Tecnologia Farroupilha

AGRADECIMENTOS

Ao meu Todo-Poderoso Deus, que me privilegiou frequentar uma universidade e me deu força e saúde para a realização deste estudo.

Ao meu orientador, professor Mestre Cleber Joel Stevens Kroetz, pela compreensão e toda ajuda durante o desenvolvimento deste trabalho.

A todos os professores e colegas desta Instituição, pelo carinho, ensinamentos e amizade demonstrados ao longo do curso.

Agradeço, de forma toda especial, aos meus pais, João e Eliane, e meu irmão Andrey, pelo estímulo, compreensão e carinho que sempre demonstraram durante todo o período dos meus estudos.

A todos os meus amigos que sempre me incentivaram nesta caminhada.

Muito obrigado a todos!

RESUMO

Este trabalho apresenta as criptomoedas, tendo como foco principal a moeda Bitcoin, analisando suas principais características, evolução histórica, o diagnóstico do quantitativo de usuários da moeda, seu giro financeiro, a evolução do valor de mercado nos últimos anos e o estágio atual da regulamentação no Brasil. Também foi abordado o sistema blockchain, como é o processo de mineração das criptomoedas, como funciona as carteiras, o armazenamento, as chaves, foram elaboradas e analisadas hipóteses, sendo confirmado que o Bitcoin é finito, é considerado um meio de pagamento, demanda um elevado consumo de energia para a geração e a validação das operações, é uma moeda descentralizada, não é controlado pelo governo e possui riscos de uso ilegal.

Palavras-chave: Criptomoedas; Bitcoin; Blockchain.

ABSTRACT

This work presents cryptocurrencies, focusing on Bitcoin currency, analyzing its main characteristics, historical evolution, the diagnosis of the number of currency users, its financial turnover, the evolution of market value in recent years and the current stage of regulation in Brazil. The blockchain system was also discussed, as is the process of mining cryptocurrencies, how wallets, storage, keys work, hypotheses were developed and analyzed, confirming that Bitcoin is finite, is considered a means of payment, demands a high energy consumption for the generation and validation of operations, it is a decentralized currency, is not controlled by the government and has risks of illegal use.

Keywords: Cryptocurrencies; Bitcoin; Blockchain.

LISTA DE GRÁFICOS

Gráfico 1 – Total de Bitcoins em circulação	40
Gráfico 2 – Taxas de transação totais (United States Dollar – USD)	42
Gráfico 3 – Transações confirmadas por dia	42
Gráfico 4 – Número total de transações	43
Gráfico 5 – Quantidade de usuários do mercado das criptomoedas	44
Gráfico 6 – Preço de mercado (USD)	44
Gráfico 7 – Bitcoins usa mais energia do que a Argentina	46
Gráfico 8 – Tempo médio de confirmação	47
Gráfico 9 – Taxa de hash total (TH/s)	49

SUMÁRIO

INTRODUÇÃO	9
1 CONTEXTUALIZAÇÃO DO ESTUDO	10
1.2 DELIMITAÇÃO DO TEMA	10
1.3 HIPÓTESES	10
1.4 OBJETIVOS	11
1.4.1 Objetivo Geral	11
1.4.2 Objetivos Específicos	11
1.5 JUSTIFICATIVA	11
2 FUNDAMENTAÇÃO TEÓRICA	13
2.1 CRIPTOMOEDAS	13
2.1.1 Ethereum	15
2.1.2 Litecoin	16
2.1.3 Cardano (Ada)	16
2.2 BITCOIN	17
2.2.1 Evolução Histórica do Bitcoin	20
2.2.2 Blockchain	22
2.2.3 Mineração das Criptomoedas	24
2.2.4 Bitcoin Como Reserva de Valor	26
2.2.5 Principais Características	27
2.2.5.1 Moeda somente virtual	27
2.2.5.2 Bitcoin são criados	28
2.2.5.3 Descentralizado	28
2.2.5.4 Transparente	29
2.2.5.5 Sem controle governamental	29
2.2.5.6 Baixas taxas de transação	30
2.2.5.7 Transações irreversíveis	30
2.2.6 Carteira, Armazenamento e Chaves	31
2.2.7 Regulamentação das Criptomoedas	33
2.2.7.1 Regulamentação no Brasil	34
3 PROCEDIMENTOS METODOLÓGICO	37
3.1 QUANTO AOS FINS	37
3.2 QUANTO AOS MEIOS	37

3.3	UNIVERSO E AMOSTRA	38
3.4	COLETA DE DADOS	38
3.5	TRATAMENTO DE DADOS	38
4	ANÁLISE DE DADOS	39
4.1	ANÁLISE DAS HIPÓTESES	39
4.2	ANÁLISE DAS TENDÊNCIAS	53
	CONSIDERAÇÕES FINAIS	54
	REFERÊNCIAS	57
	ANEXO	60

INTRODUÇÃO

Este estudo tem como objetivo apresentar as criptomoedas, a mudança tecnológica que vem ganhando espaço no mercado financeiro mundial, uma nova forma de se utilizar o dinheiro, um novo meio de pagamento, saindo um pouco da forma tradicional pela qual costumamos fazer uso do dinheiro atualmente. Empregamos as criptomoedas para comprar produtos do dia a dia, assim como utilizamos o dólar e o real, posto que o dólar é a moeda de referência para apresentação do valor de mercado das criptomoedas.

O Bitcoin, de acordo com o documento assinado por Satoshi Nakamoto (2008), surgiu para suprir a necessidade de realizar transações monetárias *peer-to-peer*, ou seja, de pessoa para pessoa, de forma segura e transparente, tudo isso sem precisar do intermédio de terceiros, no caso, do governo ou qualquer instituição financeira, como operadoras de cartões de crédito ou bancos virtuais.

O presente estudo tem seu foco na criptomoeda Bitcoin, uma das primeiras moedas a estar presente no mercado e que impulsionou o surgimento das demais. É uma moeda que teve grandes oscilações e aumento em seu valor de mercado nos últimos anos. Muitos locais já aceitam e fazem o uso da moeda, que pode ser convertida em tempo real.

Pretende-se apresentar as características gerais das criptomoedas, as principais moedas presentes no mercado, o Bitcoin e a sua evolução histórica, como é o seu funcionamento e a forma de mineração, o Blockchain, a carteira digital, o armazenamento e as chaves, a regulamentação das criptomoedas no mundo e no Brasil, e também dados numéricos referente ao Bitcoin, com base em algumas hipóteses.

Também foi abordado hipóteses as quais foram criadas para serem analisadas e confirmadas ou descartadas, apresentando um maior embasamento sobre as criptomoedas, apresentando gráficos, possibilitando uma melhor compreensão de fontes confiáveis, trazendo dados para permitir responder as hipóteses e objetivos deste estudo.

1 CONTEXTUALIZAÇÃO DO ESTUDO

1.2 DELIMITAÇÃO DO TEMA

As criptomoedas têm ganhado espaço cada vez maior no mercado financeiro mundial. As pessoas estão cada vez mais conectadas às tecnologias e aos meios digitais, e, com isso, poderá ocorrer uma redução de utilização do dinheiro físico e um aumento da procura pelas moedas virtuais. O mercado das criptomoedas também acompanha a expansão e os avanços tecnológicos, assim ele está sempre buscando aprimorar o seu funcionamento. Podemos verificar que cada vez mais pessoas estão adquirindo criptomoedas, fazendo compras e efetuando pagamentos, entre outras formas de utilização.

O tema estudado é bem atual, e poderá, com o passar do tempo, apresentar ainda mais relevância, por se tratar de uma nova forma de utilização do dinheiro. As criptomoedas são totalmente digitais. No mercado atual é possível encontrar algumas dificuldades, pois muitas pessoas ainda estão sem acesso às plataformas digitais e à internet, porém as criptomoedas estão se mantendo em crescimento, inclusive em seu valor de mercado, o que causou um grande aumento de compra e utilização.

Atualmente, no mercado financeiro, encontram-se disponíveis diversas criptomoedas, e ocorre a criação de novas constantemente. Este trabalho tem ênfase na moeda Bitcoin, uma das mais conhecidas. Pode-se afirmar que é a moeda pioneira, possuindo maior valor de mercado, sendo uma das mais procuradas para aquisição no ambiente financeiro.

Para, no entanto, investir em algo novo, surgido recentemente, comparado às demais formas de dinheiro no mercado, é necessário conhecer melhor sua origem, características, como se deu o surgimento, seu funcionamento e demais informações relevantes, para adquirir, investir e utilizar algo de que se tenha conhecimento.

1.3 HIPÓTESES

De acordo com o documento “Bitcoin: a *Peer-to-Peer Electronic Cash System*”, editado por Satoshi Nakamoto no ano de 2008, o Bitcoin surgiu com as seguintes principais características: a) Dinheiro Virtual; b) Descentralizado; c) Privacidade; d) Transparência.

Com base nas características supracitadas, apresentam-se, na sequência, as hipóteses a serem confirmadas ou refutadas.

1) O quantitativo de Bitcoins a ser criado é finito.

- 2) O Bitcoin é considerado um meio de pagamento ou transferência do dinheiro eletrônico entre partes.
- 3) É necessário um elevado consumo de energia para a geração dos Bitcoins e validação das operações.
- 4) O Bitcoin é uma moeda descentralizada.
- 5) Criptomoedas não são controladas pelo governo.
- 6) Criptomoedas possuem riscos de uso ilegal.

1.4 OBJETIVOS

1.4.1 Objetivo Geral

Analisar as principais características da criptomoeda Bitcoin.

1.4.2 Objetivos Específicos

1. Descrever a evolução histórica da criptomoeda Bitcoin.
2. Diagnosticar o quantitativo de usuários, o giro financeiro e a evolução do valor de mercado do Bitcoin ocorridos nos últimos anos.
3. Analisar o estágio atual da regulamentação do Bitcoin no Brasil.

1.5 JUSTIFICATIVA

A justificativa deste estudo está relacionada a apresentar um conhecimento de como é o funcionamento das criptomoedas presentes no mercado atual, tendo como foco analisar as hipóteses citadas anteriormente, apresentar a origem e as principais características da moeda Bitcoin, a regulamentação, sua criação, as formas de atualização, os tipos de armazenamento, entre outros. A pesquisa demanda informações presentes na internet e livros relacionados ao mercado das criptomoedas.

A principal justificativa do trabalho é em relação ao fato de ser um assunto relevante, novo e com crescente interesse de investidores e pessoas em geral, pois estes descobrem as criptomoedas e desejam saber mais sobre este mercado, porque não vão utilizar e/ou investir em algo desconhecido. O trabalho, então, tem o propósito de apresentar um pouco sobre as criptomoedas e o seu mercado.

Pretende-se com este estudo conhecer melhor as criptomoedas, apresentar as suas propriedades e expor a atuação no mercado atual, com ênfase na moeda Bitcoin, podendo proporcionar um entendimento compreensivo para todos os públicos, não apenas para o autor, mas também aos interessados em saber um pouco mais sobre a criptomoeda, possibilitando que possuam algum conhecimento e se sintam confiantes ou não para utilizar as moedas de uma forma correta e segura.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo foram abordados conceitos sobre as criptomoedas e algumas das moedas mais conhecidas no mercado, com o foco principal no Bitcoin, mostrando sua evolução histórica, o Blockchain, a mineração das moedas e seu funcionamento, a carteira, as formas de armazenamento, as chaves, a regulamentação das criptomoedas no Brasil e no mundo, entre outros temas, com o intuito de responder aos objetivos propostos e à resolução das hipóteses do trabalho.

2.1 CRIPTOMOEDAS

As criptomoedas são uma nova forma de realizar pagamentos e de se utilizar o dinheiro, que possui o intuito de facilitar ainda mais o dia a dia de seus usuários. Assim como o mundo inteiro está sempre em constante evolução, o dinheiro também deve acompanhar as mudanças. Com isso destaca-se o surgimento das criptomoedas, algo que vem ganhando cada vez mais espaço no mercado financeiro e no cotidiano de seus usuários.

Um dos seus principais objetivos é de ser uma modalidade direta de pagamento, não dependente de nenhuma autoridade monetária, por exemplo: caso deseje enviar um valor para um terceiro é necessário que esta operação seja realizada por intermédio de uma instituição financeira e isso ficará registrado, podendo ser informado para o Banco Central, que é o único responsável no Brasil por emitir e controlar a quantidade de moedas no mercado financeiro brasileiro.

Procurando mimetizar as moedas tradicionais, os cultores das criptomoedas passaram a utilizá-las especialmente como meio de pagamento, efetuando sua transferência de um ponto a outro do planeta, sem a necessidade de qualquer intermediação para que tal movimentação ocorresse de forma ágil e segura (GHIRARDI, 2020, p. 34).

As criptomoedas não necessitam de nenhuma instituição financeira para que sejam transferidos valores de uma pessoa para outra, e, caso deseje adquiri-las, precisa ser por meio de uma corretora ou mineração. Todas as movimentações estão vinculadas a um sistema chamado Blockchain, o que garante sua autenticidade e segurança. Outras características das criptomoedas são: tecnologia descentralizada, transparência, privacidade, automaticidade nas transações e baixos custos.

De acordo com Ghirardi (2020, p. 44),

Neste cenário tecnológico de descentralização e transparência, o papel da moeda – e particularmente sua natureza jurídica – tem sido objeto de crescentes indagações ao redor do mundo. Fenômeno social que encontra seus fundamentos na economia, as criptomoedas despertam o interesse de estudiosos dos mais diversos ramos de atividade.

Para algo ser considerado moeda deve-se observar três funções: meio de troca, reserva de valor e unidade de conta. Entende-se, portanto, que as criptomoedas atendem as três funções determinadas, pois são um meio de pagamento, porém totalmente digital, e pode ser uma reserva de valor, pois preserva o poder de compra com o passar do tempo e apresenta uma unidade de conta.

As criptomoedas são consideradas uma forma de dinheiro, como o real ou o dólar que usamos cotidianamente; o que difere uma da outra é que as criptomoedas não são emitidas e nem controladas por nenhum governo, podendo ser utilizadas com a mesma finalidade do dinheiro físico, mas totalmente de forma digital e sem o intermédio de instituições financeiras.

Cunha *et al.* (2019, p. 59) assim discorrem sobre os primórdios das criptomoedas:

Os primórdios das moedas digitais podem ser traçados até 1976, quando os pesquisadores estadunidenses Whitfield Diffie e Martin Hellman publicaram um artigo seminal sobre os novos rumos da Criptografia, um dos campos de estudo da Matemática, e a ciência-base para a criação de moedas digitais. Em 1982 e 1985, o criptólogo estadunidense David Chaum publicou dois artigos, um sobre assinaturas “cegas” para pagamentos não-rastreáveis e outro sobre a segurança sem identificação. Chaum é, até hoje, considerado uma espécie de “padrinho” do conceito de dinheiro eletrônico. A partir desses artigos, as pesquisas e discussões sobre o tema avançaram, preparando o cenário para a criação do Bitcoin.

As chamadas criptomoedas surgem a partir de 31 de outubro de 2008, tratadas em um artigo denominado “Bitcoin: a *Peer-to-Peer Electronic Cash System*”, de Satoshi Nakamoto. Ao apresentar seu trabalho, no resumo inaugural, Nakamoto deixa claro que sua intenção seria a de possibilitar pagamentos diretamente de um indivíduo ao outro, sem a necessidade de nenhum intermediário financeiro (GHIRARDI, 2020, p. 25).

As criptomoedas estão evoluindo no mercado financeiro mundial, pois as pessoas estão conhecendo as suas características, formas de utilização, os meios de compra e venda, como funciona o seu valor de mercado e demais atributos que possuem. A Tabela 1, a seguir, traz alguns pontos positivos e negativos das criptomoedas.

Tabela 1 – Pontos positivos e negativos das criptomoedas

PONTOS POSITIVOS	PONTOS NEGATIVOS
Clientes possuem privacidade pois não são informados alguns dados pessoais quando efetuadas movimentações.	As moedas podem ser utilizadas para operações ilegais.
A carteira com as moedas não pode ser violada.	Não é possível reverter as transações efetuadas.
Automaticidade nas transações.	Precisa ganhar uma maior aceitação, necessita da adesão da população.
Fácil transporte e possui baixos custos de operação.	Seu preço é bastante volátil.
Pode ser divisível com mais pessoas.	Há dificuldade no cálculo contábil quando ocorre a sua divisão.
Não tem a dependência de uma autoridade monetária.	Não é de fácil aprendizagem e emprego.

Fonte: O autor.

A Tabela 1 apresenta os principais pontos positivos e negativos das criptomoedas, que mostram que, assim como as demais formas de pagamentos, estas também possuem as suas particularidades, as quais, com base em sua evolução, buscam tentativas de minimizar ou eliminar os critérios negativos que são enfrentados.

As criptomoedas têm a sua finalidade descrita em seu projeto de criação, que objetiva solucionar alguns problemas em específico, podendo ser os mais diversos. Um dos pontos principais, e que está presente no plano geral das criptomoedas, é o de utilizar o dinheiro com a tecnologia presente, portanto totalmente de forma digital.

2.1.1 Ethereum

A criptomoeda Ethereum foi criada entre 2013 e 2014, quando surgiram os primeiros esboços da história. Sua estreia é conhecida como o primeiro “ICO” da história. ICO é uma sigla do inglês que significa algo como “oferta inicial de moeda” (Initial Coin Offering), fazendo alusão às operações de IPO (Initial Public Offering), ou ofertas iniciais de ações das empresas. O Ethereum foi o primeiro projeto a captar recursos por meio da própria tecnologia. O desenvolvimento da moeda foi feito a partir de recursos captados em bitcoins (CUNHA *et al.*, 2019, p. 63).

Ethereum é uma plataforma de Blockchain descentralizada, de código aberto, que permite qualquer pessoa a criar e usar aplicações descentralizadas que utilizem a tecnologia Blockchain. Não possui um dono ou controlador e contou com colaboradores de todos os cantos do mundo. Ao contrário do Bitcoin, o Blockchain do Ethereum foi estruturado para ser adaptável e flexível (MIRANDA; SALVATORE, 2018, p. 5).

Esta criptomoeda teve seu surgimento após o Bitcoin, já contando com algumas melhorias e com mais flexibilidade para os públicos. Esse protocolo foi criado para ser mais flexível e dar vazão a outras aplicações que, no protocolo do Bitcoin, seriam inviáveis. Ethereum é o nome da rede, e ether o nome da moeda, que é considerada, por criadores e usuários, um “combustível digital” (CUNHA *et al.*, 2019, p. 64).

2.1.2 Litecoin

A moeda Litecoin é um protocolo que data de antes do Ethereum, com início em 2011. Trata-se de uma cópia (*fork*, no jargão de programação) do Bitcoin, com algumas adaptações. O Bitcoin funciona em um *software* cujo código é aberto. Qualquer programador pode inspecioná-lo e propor melhorias de forma colaborativa (da mesma maneira como funciona o sistema operacional Linux, por exemplo). O Litecoin surgiu, portanto, a partir de modificações no código aberto do Bitcoin (CUNHA *et al.*, 2019, p. 64).

O Litecoin, então, conforme mencionado, teve sua criação mediante repartições do Bitcoin, criando uma nova moeda que compartilha do mesmo código, porém com algumas diferenças. Está aberto a melhorias em seu sistema e funcionamento; tem como objetivo reduzir o tempo necessário para confirmar as transações e também ajustar o seu processo de mineração. A moeda é melhor que o bitcoin para o uso em transações diárias, pois é mais rápida.

Os especialistas consideram que se o Bitcoin é o ouro das criptomoedas, o Litecoin é a prata. Enquanto o Bitcoin tem 21 milhões de unidades, o Litecoin tem 84 milhões. Há diferenças também no tempo de confirmação dos blocos de transações. O Litecoin é considerado uma espécie de rede de teste para o Bitcoin, ou até um *hedge* para quem investe em bitcoins (CUNHA *et al.*, 2019, p. 64).

2.1.3 Cardano (ADA)

A moeda Cardano (ADA) é uma plataforma que foi criada em 2015 por Charles Hoskinson, cofundador da Ethereum, e possui um projeto bastante ambicioso. Sua principal intenção é unir as melhores características e funcionalidades de todas as mais de 2 mil criptomoedas existentes no mundo, resolvendo problemas e oferecendo novas soluções para as moedas digitais, no caso uma moeda mantendo somente os melhores atributos das demais criptomoedas presentes no mercado (INFOMONEY, 2021).

Cardano começou com uma visão de um mundo sem intermediários, em que o poder não é controlado por uns poucos responsáveis, mas sim por muitos com poder. Neste mundo, os indivíduos têm controle sobre os seus dados e sobre a forma como interagem e transacionam. As empresas têm a oportunidade de crescer independentemente das estruturas de poder monopolistas e burocráticas. As sociedades são capazes de perseguir a verdadeira democracia: autogovernada, justa e responsável. Trata-se de um mundo tornado possível por Cardano (AGUIAR; ZAMBUJAL-OLIVEIRA, 2021, p. 61).

O projeto da moeda Cardano promete uma inovação no mercado das criptomoedas. É formado por uma plataforma que tem o objetivo de executar diversos aplicativos financeiros descentralizados para que possa facilitar os processos e ações financeiras para as empresas, governos ou pessoas físicas, ou seja, a plataforma é uma rede que integra várias funcionalidades em um único sistema.

2.2 BITCOIN

Há várias moedas presentes no mercado, mas, de todas as criptomoedas em circulação, sem dúvida o Bitcoin é a mais conhecida e relevante; isso não apenas pelo fato de já estar mais tempo em campo, sendo experimentada e sujeita a mais críticas que as demais, mas também por ser pioneira no desenho da tecnologia Blockchain e pela forma de emissão com que foi criada (GHIRARDI, 2020, p. 47).

Um ponto de grande relevância da moeda Bitcoin é que ela não é controlada por nenhum governo como funcionam hoje as demais formas de pagamento. Nas moedas tradicionais, as autoridades têm o conhecimento e o controle de todo o dinheiro emitido. As transferências efetuadas e demais meios são monitorados diariamente e, caso necessário, são investigados para coibir o uso ilegal do dinheiro.

Neste sentido, Ghirardi (2020, p. 8) descreve que há cerca de uma década surgiu um fenômeno que lentamente passou a atrair a atenção de estudiosos de diferentes ramos da ciência, particularmente da economia, do direito e da sociologia. Trata-se do Bitcoin, alardeado como sendo a primeira “moeda” totalmente desmaterializada, criada por particulares e por eles gerenciada, sem qualquer ingerência do Estado ou de instituições que não o próprio corpo de adeptos dessa nova forma de “moeda”.

Ulrich (2014, p. 15) corrobora, neste aspecto, que: “O Bitcoin é uma forma de dinheiro, assim como o real, o dólar ou o euro, com a diferença de ser puramente digital e não ser emitido por nenhum governo”. Outra característica, segundo o autor, é que “o seu valor é determinado livremente pelos indivíduos no mercado. Para transações on-line, é a forma ideal de pagamento, pois é rápido, barato e seguro”.

Assim, o Bitcoin não possui controle de nenhum órgão e não necessita o intermédio de instituições financeiras, pois permite que qualquer pessoa possa adquirir as moedas, não sendo necessário possuir uma conta bancária, o que é habitual hoje. Para comprar as moedas, todavia, você deve possuir um cadastro com as informações pessoais, que são guardadas sigilosamente; caso necessário, este valor pode entrar no mercado financeiro passando por alguma instituição financeira para saque ou uso, como o cliente desejar.

O sistema que operacionaliza o Bitcoin funciona sem a participação de um terceiro. O que sustenta a transmissão de dados e registra as operações é o Blockchain, que, no caso, não possui intermediário para que ocorra suas transações, como o que acontece atualmente, quando as instituições financeiras são o intermediário financeiro para que suas operações sejam realizadas com sucesso.

A moeda vem ganhando um grande espaço no mercado, conforme ressalta Ghirardi (2020). O Bitcoin popularizou-se rapidamente como uma “moeda digital”, ganhando vários concorrentes, o que acabou por chamar a atenção de instituições financeiras públicas e privadas, bem como dos detentores do poder de emissão de moedas – os Estados.

Há várias críticas sobre o Bitcoin e as demais criptomoedas até mesmo referentes às partes legais do uso perante as leis, devido a ser sem o domínio e controle de nenhum governo, ou seja, sem um intermediário nas transações como são as moedas tradicionais – o real e o dólar. Até o momento, entretanto, todas as moedas digitais seguem seu fluxo normal de uso, inclusive a criação de novas criptomoedas.

O Bitcoin, portanto, é uma criptomoeda que já está fortemente presente no mercado, e pretende expandir-se ainda mais com o intuito de ser utilizada como o real ou o dólar cotidianamente, porém sofre oscilações constantes de preço, o que pode ocasionar ganho ou perda deste valor monetário diariamente.

A dificuldade em realizar a compra e a venda diretamente, sem intermediários como as agências corretoras, certamente desvirtua um dos conceitos centrais do Bitcoin: a ausência de intermediários e controle governamental. É natural que todas e quaisquer transações monetárias e financeiras realizadas por agentes corretores estarão submetidas ao escrutínio do Estado, por meio de agências reguladoras e o fisco (NASCIMENTO; PORTO, 2018)

Conforme já apresentado anteriormente, o Bitcoin não é controlado e não depende de um Estado ou governo para que seja operacionalizado; ele faz a sua própria regulação, como ocorre com as moedas convencionais que temos disponíveis e das quais se faz uso. As criptomoedas são totalmente digitais, intangíveis e descentralizadas, e funcionam com o seu sistema próprio de controle e registro das operações, sendo, em muitas delas, o Blockchain responsável por esta parte.

Pelo alcance, segurança e agilidade, os seus entusiastas e defensores sustentam que o bitcoin é uma forte ameaça aos sistemas de liquidação de pagamentos existentes, capaz de viabilizar a criação de uma nova ordem monetária em substituição à ordem atual, baseada na moeda estatal e na moeda de crédito criada pelos bancos, em razão da oferta de serviços de pagamento e de transferência de recursos com segurança, do custo relativo muito menor e do potencial de se tornar tão rápido quanto os meios de pagamentos eletrônicos atuais (CARVALHO, 2017, p. 4).

O Bitcoin, então, já está consolidado no mercado desde o seu surgimento; continua ganhando novos compradores e usuários com a volatilidade presente em seu valor de mercado, o que ocasiona uma grande atração de clientes, que desejam encontrar na moeda uma tentativa de se obter um ganho financeiro, pois o valor pode sofrer altas e baixas assim como na bolsa de valores, na qual ocorrem oscilações no preço das ações.

O Bitcoin encaixa-se perfeitamente dentro da definição do conceito de criptomoeda por ser uma moeda digital, dado o seu meio de circulação totalmente digital e a sua característica de intangibilidade, por essa ser não regulamentada e independente de uma autoridade emissora central, ainda, contando com o aspecto da segurança criptográfica a qual busca impedir a falsificação ou furto (NASCIMENTO; PORTO, 2018, p. 7).

O Bitcoin é utilizado totalmente de forma digital. Está presente no grupo das criptomoedas no mundo todo. Funciona sem a presença de intermediário bancário a não ser que o cliente planeje receber este valor via instituição financeira. Ele consegue operar com a troca de valores ou parte da moeda, podendo o usuário realizar o que deseja da mesma forma que usa o dinheiro convencional atualmente.

O Bitcoin é classificado como uma criptomoeda considerada uma nova forma de dinheiro eletrônico puramente *peer-to-peer*. Em tradução livre, quer dizer ponto a ponto, que permite o compartilhamento de arquivos de forma anônima sem a intervenção de um terceiro (CAMARA, 2014).

O Bitcoin é uma nova maneira de utilizar o dinheiro do jeito que o usuário deseja, tendo um valor diferente a cada dia conforme seu valor de mercado. Muitas pessoas preferem a estabilidade de valor para não correr riscos de perder dinheiro, mas o mercado financeiro está sempre em constante oscilação, e isto, para muitos, já faz parte de seu cotidiano: assumir riscos na tentativa de conseguir uma maior valorização.

A criação e a disseminação do Bitcoin não podem ser analisadas como um evento historicamente isolado, pois a crise financeira de 2008 teria, pelo menos em partes, revivido a desconfiança nas moedas estatais e nas instituições financeiras convencionais do sistema monetário.

O surgimento do Bitcoin teve um impulsionamento após a crise financeira de 2008, o que, junto a outros fatores, também contribuiu para que a moeda fosse criada. O Bitcoin

transmite uma grande confiança no mercado financeiro, pois o seu funcionamento é por meio do sistema Blockchain, que é seguro, rápido e transparente com todos os seus usuários.

A forma mais fácil de você comprar e vender um Bitcoin é por intermédio das corretoras que possuem a moeda. Há várias no mercado, como Mercado Bitcoin, Binance, Focbit entre outras. Você irá, inicialmente, realizar um cadastro e a abertura de uma conta digital para estar habilitado a operar com as criptomoedas. Há diversas confirmações para validar seu cadastro, mas isso tudo é por questões de segurança de seus usuários e do próprio sistema.

Para realizar operações com o Bitcoin você vai necessitar ter uma carteira digital, a qual possui o mesmo funcionamento que uma conta corrente, porém totalmente *on-line*, podendo enviar e receber valores em Bitcoins ou outras criptomoedas, e, após iniciada uma transação, é enviada a movimentação e feita a validação das informações. Se tudo estiver correto é efetivado, caso contrário esta transação é descartada e o valor retorna para o usuário que enviou.

2.2.1 Evolução Histórica do Bitcoin

A moeda Bitcoin teve seu surgimento após a publicação de um artigo, o “Bitcoin: a *Perr-to-Perr Electronic Cash System*, de Satoshi Nakamoto, no ano de 2008, sendo apresentado por um programador ou grupo de programadores, não se sabe ao certo, na lista de discussão do *The Cryptography Mailing*, um sistema considerado a primeira moeda digital mundial descentralizada.

O surgimento da moeda Bitcoin tem como um dos seus objetivos o de suprir a necessidade de realizar transações monetárias com a forma *peer-to-peer*, ou seja, de pessoa para pessoa, de modo seguro, tudo isso sem o controle do governo e sem necessitar do intermédio de terceiros, no caso, dos bancos ou qualquer instituição financeira, como as operadoras de cartões de crédito, ou bancos virtuais.

É exatamente isso que se observa na comunidade do Bitcoin: diversas fontes de notícias especulando quanto à real identidade de Nakamoto. A teoria mais plausível, utilizando-se da Navalha de Ockham, é a de que o real criador da Bitcoin pode ser um dos ilustres membros da comunidade ou um grupo formado por eles ou teorias mais mirabolantes que variam desde a fusão de grandes corporações, ilustres membros da comunidade de Bitcoins e criptografia ou até mesmo a *National Security Agency* (NSA) estadunidense (NASCIMENTO; PORTO, 2018, p. 4).

Há diversas publicações a respeito da criação e da história da moeda Bitcoin, mas a que possui maior aceitação é a que foi criada por Nakamoto (por ele ou um grupo de pessoas).

A moeda continua presente no mercado financeiro com grande expansão. Pode-se afirmar, então, que é algo que realmente deu certo, pois está há anos no mercado e tem o objetivo de se tornar de uso habitual e diário, assim como os demais meios de pagamento.

Os motivos fundamentais que impulsionaram a criação do Bitcoin são, portanto, evidentes: um sistema financeiro instável e com elevado nível de intervenção estatal e a crescente perda de privacidade financeira. Mas esse estado de coisas não é novidade. A intervenção dos governos no âmbito monetário é milenar, assim como a cumplicidade e conivência do sistema bancário (ULRICH, 2014, p. 43).

A primeira transação do Bitcoin iniciou no ano de 2009, o que marcou o seu começo. Foi entre Nakamoto e Hal Fineey. Após seu surgimento a moeda foi, aos poucos, avançando, mas no ano de 2010 já estava mais bem estabelecida e já permitia fazer compras e vendas. Com o passar dos anos o sistema foi se aprimorando para melhor atender a todos os seus consumidores.

No dia 5 de outubro de 2009, nove meses após o início da rede Bitcoin, o primeiro preço de oferta de Bitcoin registrado foi postado. Atingiu 13 bitcoins por um centavo, ou especificamente, 1.309,03 Bitcoins por dólar, o que o autor da postagem calculou com base em seus custos de mineração variáveis (GRAF, 2016 p. 128).

Após o seu início e o seu primeiro preço definido, as pessoas começaram a adquirir e fazer o uso da criptomoeda, com um valor de mercado bastante inferior comparado com a evolução que a moeda sofreu com o passar dos anos e o seu constante crescimento no mundo inteiro. As pessoas nem imaginavam o que poderia vir para o futuro do Bitcoin.

Alguns meses depois, em maio de 2010, uma pizza foi vendida por 10 mil bitcoins, equivalente a 25 dólares à época. Mas, na realidade, essa não foi uma transação genuína, pois o comprador transferiu 10 mil BTC a um terceiro, que facilitou a compra por cartão de crédito na pizzeria. Ainda assim, a compra foi um registro do preço de um bitcoin então, 4 BTC por centavo de dólar. Para termos uma ideia, em valores de conversão de 2019, essas duas pizzas (10.000 bitcoins) teriam custado USD 52 milhões (CUNHA *et al.*, 2019, p. 65).

Assim como em todo surgimento de novidades, há pontos negativos a serem enfrentados. No ano de 2011 aconteceu o lançamento da Silk Road, um mercado de bitcoins voltado para a negociação de drogas e produtos ilícitos, o qual foi fechado em 2013. Há várias investigações presentes com base na preocupação do uso indevido das criptomoedas, quando são utilizadas para operações fora das leis.

No ano de 2013 ocorreu a não aceitação da moeda pelo Banco Central da China, que proibiu as instituições financeiras do país de realizarem transações com Bitcoins. Na Europa, porém, o Bitcoin foi regularizado e teve uma maior expansão no mundo inteiro, mas alguns

países não aceitam a moeda pelo possível impacto que pode se dar no mercado financeiro tradicional. No Brasil a aceitação para operarmos e utilizarmos a moeda.

Apesar de alguns acontecimentos negativos sobre a moeda, a mesma mantém-se forte no mercado e em constante crescimento e valorização, em busca de ampliar ainda mais o seu espaço de aceitação principalmente nos comércios locais, para que eles possam oferecer mais um meio de pagamento aos seus clientes, de forma segura, rápida e prática.

2.2.2 Blockchain

O Blockchain é uma rede que funciona como blocos encadeados que são bastante seguros, pois sempre carregam o conteúdo junto com uma impressão digital, e, no caso da Bitcoin, este conteúdo é uma transação financeira. O interessante é que o bloco posterior vai conter a impressão digital do anterior e mais o próprio conteúdo, e com estas informações irá gerar a sua própria impressão digital e assim por diante. (PRADO, 2019)

A tecnologia Blockchain surgiu junto com a moeda Bitcoin no ano de 2008. O Blockchain foi pensado como uma forma segura para se transferir bitcoins e trazer confiabilidade à rede Bitcoin, uma vez que o fato de ser uma moeda intangível e desregulamentada gera desconfiança sobre a criptomoeda (PROOF, 2018).

O Blockchain teve seu início juntamente com as criptomoedas e o Bitcoin, e é um sistema entre blocos pensado para fornecer a segurança das operações realizadas com o Bitcoin, pois o controle é feito pelos criadores das moedas e não pelo governo, conforme é o real e o dólar hoje, que possuem um sistema de controle pelos governos.

A transação é, portanto, uma transferência de propriedade das bitcoins, é registrada, carimbada com data e hora e exposta em um “bloco” do *blockchain* (o grande banco de dados, ou livro-razão da rede Bitcoin). A criptografia de chave pública garante que todos os computadores na rede tenham um registro constantemente atualizado e verificado de todas as transações dentro da rede Bitcoin, o que impede o gasto duplo e qualquer tipo de fraude (ULRICH, 2014, p. 19).

Com o uso do Blockchain para realizar as operações financeiras, demonstra-se que as criptomoedas possuem um sistema é bastante seguro, tudo de forma digital, evitando que ocorram fraudes, tudo isso apresentando transparência e a confiança que o mercado das criptomoedas oferece, sendo isto um ponto positivo para a atração de novos investidores e usuários das moedas. Todas as operações realizadas estão disponíveis no *site* do Blockchain (2021) com dados que podem ser públicos.

No caso do Bitcoin, a rede peer-to-peer desempenha uma função fundamental: a de garantir a distribuição do blockchain a todos os usuários, assegurando que todos os nós da rede detenham uma cópia atual e fidedigna do histórico de transações do Bitcoin a todo instante. Dessa forma, novas transações são transmitidas a todos os nós, registradas no log de transações único e compartilhado, tornando redundante a existência de um servidor central. Em um mundo pré-digital, seria simplesmente inconcebível levar a cabo tal logística (ULRICH, 2014, p. 45).

Os especialistas consideram, hoje, que o Blockchain, é a tecnologia por trás do Bitcoins e das outras criptomoedas, sendo tão relevante quanto foi a internet há alguns anos, quando esta surgiu com o potencial de revolucionar as inúmeras áreas de nossa sociedade, indo desde modelos de votação até o sistema financeiro, sempre mantendo o objetivo de possuir segurança, privacidade e transparência.

Uma vez que a transação é validada, o registro dessa transação é adicionado ao Blockchain, que armazena todas as transações já feitas na rede Bitcoin. Nenhuma transação envolvendo bitcoins, porém, é registrada no Blockchain sem antes passar pelo processo de mineração (ANTONOPOULOS, 2014b). O tempo de execução deste processo varia muito, demorando, atualmente, em média cerca de 30 minutos (BLOCKCHAIN, 2021).

Todos os usuários das criptomoedas possuem um cadastro, que, em sua grande maioria, estão nas corretoras, e os movimentos que os clientes fazem com as criptomoedas estão registrados no sistema Blockchain, no qual cada cliente possui seus dados e sua própria identificação. Neste sistema ficarão gravadas as suas transações realizadas com a moeda.

A tecnologia Blockchain tem como principais propriedades a descentralização, uma vez que dispensa a necessidade de uma terceira parte para fazer a transação; a integridade, pois todos os conjuntos de dados são replicados em diferentes pontos da rede de maneira segura; e a transparência, posto que todas as transações registradas na Blockchain são públicas (SAMPAIO *et al.*, 2018, p. 5).

Os responsáveis garantem a segurança dos usuários, e as principais características do Blockchain são: a transparência, quando é possível ter a visualização de qualquer transação; a descentralização, e não há a necessidade de nenhum órgão intermediário aprovar a transação ou determinar sua regulamentação; e a segurança, pois o banco de dados é imutável, ou seja, um registro não pode ser alterado, revisado ou adulterado após registrado.

Segundo Fagundes (2017), a tecnologia Blockchain conta com algoritmos que registram e confirmam todas as transações de forma anônima e compartilhada dentro da rede, independentemente da localização da pessoa, isto é, todos que estão conectados na rede possuem uma cópia idêntica.

Em arquiteturas de servidores tradicionais, todo aplicativo precisa configurar seus próprios servidores que executam seu próprio código em silos isolados, dificultando o compartilhamento de dados. Se um único aplicativo for comprometido ou ficar off-line, muitos usuários e outros aplicativos serão afetados. Em um Blockchain, qualquer pessoa pode configurar um nó que replique os dados necessários para todos os nós para chegar a um acordo e ser compensado pelos usuários e desenvolvedores de aplicativos. Isso permite que os dados do usuário permaneçam privados e os aplicativos sejam descentralizados como a Internet deveria funcionar (ETHEREUM, 2019).

O Blockchain é um sistema que transmite confiança, pois a validação de uma transação requer que outros computadores de outros participantes entrem em um acordo para possibilitar que a transação ocorra. Ele é automatizado, e o software foi desenvolvido para que não haja duplicidade ou informação conflitua, identificando as transações que não respeitem as regras para que não sejam registradas dentro do Blockchain.

Conforme Fagundes (2017), as aplicações iniciais do Blockchain eram restritas às criptomoedas. O autor destaca que, em 2014, surgiu uma nova versão do Blockchain, chamada de Blockchain 2.0, que permitiu que essa ferramenta fosse configurada para responder a certos gatilhos por meio de Contratos Inteligentes. Com isso, o Blockchain abriu-se para outras indústrias.

2.2.3 Mineração das Criptomoedas

A mineração das criptomoedas é baseada na teoria dos jogos, inclusive foi uma das razões pelas quais fizeram com que o Bitcoin prosperasse, apesar de tentativas de destruição da rede. A teoria dos jogos é um método matemático aplicado para estudar o comportamento humano baseado em decisões tomadas, e a mineração de criptomoedas também é a realização de problemas matemáticos.

A combinação entre a criptografia e a teoria dos jogos, então, foi uma das mais importantes características da rede Bitcoin que protege o sistema de atividades maliciosas. É o algoritmo de consenso Proof of Work (PoW) (Prova de trabalho), que foi capaz de tornar o Blockchain um sistema descentralizado, sendo resistente a ataques. Ele aplica técnicas criptográficas que tornam o processo de mineração muito caro e exigente, criando um ambiente muito competitivo (BINANCE ACADEMY, 2021).

Há duas formas de se obter as criptomoedas: comprando-as diretamente em um *site* especializado por intermédio de uma corretora, ou obtendo-se algumas delas por meio do processo de mineração. Surgiram vários investidores neste processo, mas muitos não conseguiram acompanhar o alto valor investido necessário para manter um sistema de mineração em pleno funcionamento, mais no caso da criptomoeda Bitcoin.

Conforme (MILLER, 2021) “O processo de mineração, todavia, envolve certos custos para o minerador, sendo eles para a aquisição de equipamentos, a instalação, a refrigeração, a energia elétrica e a manutenção das máquinas”. Estes itens são indispensáveis para que o processo funcione com alto desempenho, sem pane ou problemas; é pelos altos custos que muitas pessoas não utilizam este processo para obter as moedas.

Na mineração são oferecidos cálculos matemáticos computacionais do *hardware* para criptografar novas transações da criptomoeda em um novo bloco, validá-los, inseri-los no Blockchain e ganhar uma recompensa nessa moeda mediante o desempenho dedicado (BAZAN, 2018).

É possível realizar a mineração de criptomoedas de quatro formas: a mineração com Unidades de Central de Processamento (CPU– Central Processing Unit), quando as versões iniciais do *software* do Bitcoin permitem aos usuários utilizarem suas próprias CPUs para minerar, porém, atualmente, esse tipo de mineração é inviável; a mineração com GPU, drasticamente mais rápida e mais eficiente que a mineração com CPU; a mineração profissional, realizada por *data centers*; e a mineração de Bitcoin em nuvens.(MARQUES, Diego, 2017)

Para ingressar no ramo é necessário ter um investimento em equipamentos, pois o retorno está diretamente relacionado ao processamento da máquina utilizada. No início do Bitcoin, por exemplo, computadores comuns eram usados para extração, mas, com o passar do tempo e com o aumento da concorrência em razão do crescimento do número de mineradores, foram surgindo novos aparelhos mais específicos e mais eficientes voltados para a mineração (ALKUDMANI, 2020).

Assim, há várias pessoas que realizam o investimento neste processo bem complexo de mineração das criptomoedas, que é de alto custo tanto em equipamentos de grande potencial quanto de energia para mantê-los ligados. A mineração das criptomoedas, então, ajuda a manter o sistema Blockchain em funcionamento, realizando as operações das moedas e registrando as mesmas. Ainda, por meio disso, possuem um ganho convertido em parte de criptomoedas.

O protocolo Bitcoin contém algoritmos que regulam a função de mineração através da rede. A dificuldade da tarefa de processamento que os mineradores devem realizar – registrar com sucesso um bloco de transações na rede Bitcoin – ajusta-se dinamicamente de tal forma que, em média, alguém é bem-sucedido a cada 10 minutos, independentemente de quantos mineradores (e CPUs) estejam trabalhando na tarefa a qualquer momento. O protocolo também reduz à metade, a cada 4 anos, a taxa com que novos Bitcoins são criados, limitando, assim, o número total de Bitcoins que serão criados a um máximo de 21 milhões de moedas (ANTONOPOULOS, 2014a, p. 2).

O processo de mineração é, portanto, como se fosse um intermediário e controlador das moedas, que não é centralizado conforme o controle das moedas normais, que possuem um agente intermediário. Para ocorrer a mineração, no entanto, devem ser utilizadas por pessoas habilitadas e com disposição a investir para realizar este trabalho com eficácia, sem falhas, mantendo a segurança de todo o sistema.

2.2.4 Bitcoin Como Reserva de Valor

O Bitcoin pode ter várias funções assim como o dinheiro, mas vem sendo fortemente utilizado para investimentos e reserva de valor, ou seja, os clientes querem obter uma valorização do valor aplicado que não sofra depreciações com o tempo, e a moeda tem este poder, pois seu valor de mercado é conforme a demanda e a oferta, podendo ser transportado ou guardado de maneira mais segura até mesmo em períodos de inflação.

O aumento de sua liquidez e aceitação, porém, pode definitivamente fazer com que o bitcoin seja não apenas um meio de troca e um ativo para preservação de riqueza, mas também a moeda em função da qual os produtos e serviços são precificados e com a qual é realizado o cálculo econômico. Um sinal de que o bitcoin atingiu um estágio avançado de desenvolvimento será o momento em que a moeda digital for um meio de troca, uma reserva de valor e uma unidade de conta (ULRICH, 2014, p. 95).

Outro ponto é sobre a sua escassez relativa, pois o Bitcoin tem o seu limite máximo de 21 milhões de moedas, por isso é considerado uma ótima alternativa de compra, com possível elevação do poder de compra com o aumento de seu valor de mercado. Então, isso também faz que se encontre uma maior dificuldade de adquirir a moeda, pois está cada vez mais próxima de seu limite.

Para que o Bitcoin seja considerado moeda é necessário que haja, em suas características, a reserva de valor, ou seja, uma proteção contra as variações do mercado, cujo principal ponto é a manutenção do poder de compra com o decorrer do tempo. A moeda pode ser utilizada da forma que o usuário desejar, e pode ser uma possível proteção contra a inflação que o dinheiro normal enfrenta.

Existe, também, quem afirma que o Bitcoin não é uma reserva de valor e, sim, uma aposta similar a um cassino, onde se investe um valor torcendo para que se ganhe um valor maior do que o apostado, assim como pode ocorrer a perda deste valor. Atualmente, a grande maioria dos usuários tem aumentado os seus valores com a moeda.

Há muitas comparações do Bitcoin com o ouro, e assevera-se que a moeda pode ser considerada o “ouro” do futuro. Os investimentos bilionários anunciados pelas empresas

MicroStrategy e Tesla, em fevereiro de 2021, para engordar a participação da criptomoeda em suas carteiras, chamam atenção para a aplicação do Bitcoin como reserva de valor pelas empresas. Algumas empresas, portanto, estão fazendo o uso para a sua segurança. Tem crescido a proporção do varejo, que busca posicionar o Bitcoin como reserva de valor, ainda sem fazer *trade*. “Algumas empresas têm comprado, mas não divulgam, talvez por ainda terem dúvidas sobre questões regulatórias. E temos casos também de companhias que começam a estudar o Bitcoin para operações de câmbio (IBEF, 2021).

A função de reserva de valor é utilizada por diversos ativos e formas além das moedas, por exemplo: carros, imóveis, ações. Os usuários, todavia, veem no Bitcoin uma expectativa de valorização futura, o que, se ocorrer, vai garantir que o montante empregado aumente proporcionalmente, assegurando, então, uma reversão ainda maior que as demais opções.

2.2.5 Principais Características

A seguir serão descritas as principais características da criptomoeda Bitcoin, de acordo com Satoshi Nakamoto (2008), que introduziu a criptomoeda no mercado financeiro.

2.2.5.1 Moeda somente virtual

Todas as criptomoedas são operacionalizadas de forma virtual, inclusive o Bitcoin. Não há nenhuma outra forma de se utilizar as moedas, até o momento, que não seja de modo virtual. Para que ocorram as operacionalizações é necessário estar-se conectado à internet. Pode-se afirmar que, sem a evolução dos meios de comunicação e das tecnologias, as criptomoedas não existiriam. Este é um dos pontos que confirmam que não ocorreu o surgimento anteriormente.

A moeda digital é aquela gerada no próprio ambiente virtual. Tem como característica ser totalmente digital, desvinculada do governo e sem um Banco Central controlador. Segundo Ulrich (2014), é uma forma de dinheiro puramente digital, não sendo emitida por nenhum governo, e seu valor é determinado livremente pelos indivíduos do mercado.

O Bitcoin é virtual e pode ser usado para realizar pagamentos *on-line* ou em lojas físicas, assim como qualquer outra forma de pagamento. Os saldos em bitcoin são armazenados em uma grande rede distribuída e não podem ser fraudados por ninguém. Em outras palavras, os usuários de Bitcoin têm controle exclusivo sobre seus saldos, que não podem desaparecer só porque são virtuais.

2.2.5.2 Bitcoin são criados

Há duas formas de você possuir um Bitcoin. Uma delas é realizando a compra por intermédio de corretoras presentes no mercado, e a outra é o processo de mineração; este exige um grande investimento, e se torna cada vez mais difícil minerar uma moeda ou parte dela. Anos atrás, quando de sua criação, era possível conseguir extrai-lo mais facilmente e com equipamentos mais básicos.

Em outras palavras, o processo de criação do Bitcoin funciona da seguinte forma: os dados de uma transação envolvendo Bitcoins são transmitidos para todos aqueles que participam da rede (*Peer of Peer*), e para que a transação seja viabilizada ela precisa ser processada, ou seja, o problema criptográfico deve ser resolvido (CARVALHO *et al.*, 2017).

Os novos Bitcoins são gerados por meio de um processo competitivo e descentralizado chamado mineração. Esse processo consiste na recompensa dada aos usuários pelos seus serviços. Os mineradores de Bitcoins estão processando transações e fazendo a rede segura, usando *hardware* especializado e coletando novos bitcoins em troca.

O protocolo Bitcoin foi projetado de uma forma que os novos Bitcoins são criados em uma proporção fixa. Isto faz com que a mineração de Bitcoins seja um negócio muito competitivo. Quando mais mineradores se juntam à rede torna-se cada vez mais difícil gerar lucro, e estes precisam buscar eficiência para diminuir os seus custos operacionais.

No caso do Bitcoin, a oferta crescerá de forma paulatina, pré-estabelecida e conhecida por todos os usuários até alcançar o limite máximo de 21 milhões de unidades ao redor do ano de 2140. Mas cerca de 90% de todos os bitcoins já estarão minerados por volta de 2022. Assumindo que a demanda por bitcoins continue crescendo ao longo dos próximos anos, isso significaria que uma unidade bitcoin valeria cada vez mais. E quanto mais se amplie a aceitação da moeda, maior será seu poder de compra. Em face dessa constatação, os economistas leigos em Bitcoin alegam que será quase impossível usar uma unidade de bitcoin em compras do dia a dia, pois ela valerá muito no futuro (ULRICH, 2014, p. 69).

Os Bitcoins são criados em uma taxa decrescente e previsível. O número de novos Bitcoins criados a cada ano é automaticamente reduzido pela metade com o passar do tempo, até que a emissão seja completamente suspensa com um total de 21 milhões de bitcoins existentes. Neste ponto, os mineradores de Bitcoins provavelmente serão remunerados exclusivamente por numerosas pequenas taxas de transação.

2.2.5.3 Descentralizado

O Bitcoin e a grande maioria das criptomoedas utilizam um sistema descentralizado, pois são as criptomoedas presentes no mundo todo não usam o governo e estados para sua

gestão ou controle, e sim os próprios mineradores e os usuários fazem este processo de controle sobre as operações.

Já em sistemas descentralizados, sem autoridade central obrigando as partes a adotar certos tipos de medidas de segurança, como no Bitcoin, a segurança é garantida por um sistema de recompensas. Qualquer usuário do sistema pode manter a rede funcionando, validando transações e confirmando-as na rede. Por essa atividade, o usuário, chamado de minerador, recebe recompensas em Bitcoins. Atualmente, o minerador recebe 12,5 Bitcoins por bloco de transação registrado (CUNHA *et al.*, 2019, p. 75).

2.2.5.4 Transparente

Todas as operações das criptomoedas são transparentes e todas as informações sobre a moeda Bitcoin estão disponíveis no sistema Blockchain para que qualquer pessoa possa verificar o que está ocorrendo, o que acontece em tempo real. O protocolo do Bitcoin é seguro. Nenhuma pessoa ou governo consegue controlar ou manipular, portanto isso faz com que o Bitcoin seja transparente e previsível.

Esse sistema de combinação de chave pública e chave privada é usado nas transações em bitcoins. Todas as transações são públicas e transparentes, para que qualquer usuário possa fiscalizar. Para isso, é preciso que seja possível ver a transação e identificar as partes envolvidas. Isso é feito justamente pelas assinaturas digitais e pela criptografia de chave pública. O sistema permite a checagem dos dados básicos da transação, necessários à fiscalização, e disponíveis pelo acesso via chave pública, sem revelar nenhuma informação sigilosa sobre as partes (protegida pela chave privada (CUNHA *et al.*, 2019, p. 75).

2.2.5.5 Sem controle governamental

O Bitcoin não tem o controle de nenhum governo e não necessita o intermédio de instituições financeiras, o que permite que qualquer um pode adquirir as moedas, não sendo necessário possuir uma conta bancária, o que é habitual hoje para que você consiga realizar operações financeiras. Muitas pessoas pensam que o governo irá intervir e proibir o uso das criptomoedas.

A perspectiva de se efetuar pagamentos diretamente entre credor e devedor, sem a participação de intermediários, parecia oferecer uma real oportunidade de se reconfigurar custos transacionais, o que só foi possível graças à tecnologia no seio da qual nasce o Bitcoin (GHIRARDI, 2020).

O fato de o governo ou país bloquear o uso das criptomoedas pode ocorrer, mas isso pode ser uma questão de estar com receio que o mercado das criptomoedas impacte na economia com o dinheiro tradicional. Muitos países, entretanto, já estão regulamentados para aceitação e dispostos a acompanhar esta nova forma de economia.

2.2.5.6 Baixas taxas de transação

A questão de custos e taxas para as movimentações que os clientes desejarem, como depósitos ou saques das criptomoedas, é bastante relativa de uma corretora para outra. Algumas delas estavam oferecendo serviços totalmente gratuitos e outras com valores bem baixos.

Na corretora Mercado Bitcoin existem duas possíveis comissões que podem ser cobradas no momento da compra ou venda de criptomoedas: as ordens executadas têm a comissão de 0,3%, mas tudo dependerá de que ordem chegar primeiro. Conforme o site do Mercado Bitcoin: se sua ordem de compra chegar em nosso livro antes de uma ordem de venda com os mesmos valores, ela será executada (0,3%) pela próxima ordem de venda compatível e as ordens executoras têm a comissão de 0,7%, mas, se sua ordem de venda chegar depois de uma ordem de compra com os mesmos valores de sua ordem, ela será executora (0,7%) dessa ordem de compra (BITCOIN, 2021).

A corretora Binance faz a cobrança com base em uma tabela que varia de acordo com a quantidade de moeda que você possui ou deseja comprar, sendo a taxa mais alta de 0,1000% sobre o valor transacionado. Para a realização de depósitos de valores acredita-se que nenhuma corretora faz cobrança sobre esta operação (BINANCE ACADEMY, 2021).

No *site* do Bitcoin encontramos a seguinte informação quanto às taxas de transações: “A maior parte das transações pode ser processadas sem taxas, mas usuários são encorajados a pagar uma pequena taxa voluntária para uma confirmação de suas transações mais rapidamente e para remunerar ‘mineiros’. Quando as taxas são necessárias, elas normalmente não excedem alguns centavos. Seu programa de Bitcoin normalmente tentará estimar uma taxa apropriada, quando for necessário” (BITCOIN, 2021).

2.2.5.7 Transações irreversíveis

Na forma tradicional hoje, ao se fazer uma transferência bancária de qualquer valor com todas as informações certas, a operação é irreversível, e no mercado das criptomoedas não é diferente. Após realizada uma transação não é possível fazer o seu cancelamento ou estorno.

Uma das características das criptomoedas é o fato de que as transações em papel moeda são irreversíveis: uma vez realizadas, não é possível voltar atrás para reaver o dinheiro. Finalmente, as transações são feitas sem a necessidade de se conhecer as identidades das partes que estão transacionando (CUNHA *et al.*, 2019, p. 61).

É muito importante, portanto, muita atenção e tome cuidado ao realizar uma transferência de Bitcoin, pois no mercado de criptomoedas, depois de uma transação ser anexada ao bloco e inserida no Blockchain, ela se torna imutável. Não há como voltar atrás em uma transação, e você não pode chamar nenhuma autoridade para cancelar uma transação já confirmada.

2.2.6 Carteira, Armazenamento e Chaves

A carteira digital tem o funcionamento semelhante a uma conta corrente em qualquer instituição financeira, quando somente o detentor da senha, que no caso é a chave criptográfica, consegue realizar as transferências. As carteiras digitais são, então, formas de armazenar estas chaves, promovendo, assim, a segurança necessária para os usuários.

Quem investe em moedas digitais como o Bitcoin tem a possibilidade de custodiar seus ativos por conta própria em carteiras. É possível armazenar a moeda tanto em carteiras próprias, quanto em empresas como as Exchanges. Para que isso seja feito, contudo, é preciso aprender como essas carteiras funcionam, e ter em mente boas práticas para evitar fraudes e perdas (CUNHA *et al.*, 2019, p. 76).

A custódia de criptoativos é realizada em uma infraestrutura tecnológica para que o investidor consiga armazenar e ter acesso às suas criptomoedas e seus ativos digitais em um ambiente totalmente digital e privado. Nas criptomoedas que são criadas pela tecnologia Blockchain a custódia destes ativos também deve ocorrer em um ambiente digital de Blockchain.

Ulrich (2014, p. 26) afirma, acerca da violação do sigilo do Blockchain, que “As carteiras de Bitcoin agora podem ser protegidas por criptografia, mas os usuários devem selecionar a ativação da criptografia. Se um usuário não cifra a sua carteira, os Bitcoins podem ser roubados por malware”.

A carteira de *hardware* é conhecida como armazenamento frio; ela não está conectada à internet e garante a segurança de seus Bitcoins e outras criptomoedas de forma *off-line*. A carteira é um pequeno dispositivo digital, similar ao tamanho de um chaveiro ou um *pen drive*, utilizado para armazenar as suas chaves privadas.

Estas chaves privadas permitem que somente o proprietário acesse o controle de suas moedas, pois possui um endereço de carteira, que é o que possibilita receber qualquer criptomoeda que seja enviada para você, assim como pode fazer o envio para outra pessoa, tendo o endereço da carteira pública desta pessoa para quem desejar enviar.

As carteiras não guardam as moedas digitais propriamente. Elas são, na verdade, um software que contém um conjunto de chaves públicas (as “contas correntes” do investidor) e privadas (as senhas de tais contas). Por meio do software, o dono das moedas faz as transações, assina digitalmente, envia e transmite para a rede, para que possa ser validada e confirmada por um minerador. Após a validação, a operação é incluída em um bloco de transação, sendo finalmente registrada na rede (CUNHA *et al.*, 2019, p. 77).

É preciso, todavia, ter um certo cuidado, pois, caso alguém tenha acesso à sua chave privada, esta pessoa poderá imediatamente esvaziar os seus fundos, mesmo sem o seu conhecimento e autorização; por isto, é muito importante fazer o uso correto da sua carteira digital e guardar as informações com o máximo de segurança.

O fato de possuir uma carteira vai do consumidor, mas quando ele adquire alguma moeda é automaticamente criada pelo próprio *site* ou corretora, mas quanto a guardar e à segurança de seus ativos, são da vontade do usuário. Vale lembrar que a prerrogativa de armazenar criptomoedas por conta própria é opção, não obrigação. As empresas chamadas *exchanges* também fazem o trabalho de custódia, guardando as moedas do investidor. Esse, para acessar seus recursos e fazer transações, precisa solicitar a movimentação à empresa custodiante (CUNHA *et al.*, 2019, p. 77).

As carteiras estão divididas em dois tipos: as carteiras quentes, que são conectadas à internet, tornando bem mais fáceis de acessar os fundos armazenados nela, porém são menos seguras devido aos ataques de *hackers* e demais riscos da internet; e as carteiras frias, que são *off-line*, utilizadas, na grande maioria, para o armazenamento de enormes quantias de Bitcoins ou outras criptomoedas, em razão da dificuldade de um *hacker* atacá-las.

Quanto à criação das chaves de criptografias, sabemos que as transações usando criptomoedas envolvem uma conta corrente – a chave pública –, que podemos definir como um “endereço” onde estão os ativos, e a senha da conta – a chave privada. Quem cria o endereço ou a conta corrente, não é um banco ou qualquer instituição, e, sim, o *software* que faz a função de carteira. Esses *softwares* possibilitam a criação aleatória de endereços únicos, cuja variedade de possibilidades passa da casa dos bilhões. Portanto, a probabilidade de um mesmo endereço (mesma conta corrente) ser criado duas vezes, portanto, é desprezível (CUNHA *et al.*, 2019, p. 64).

2.2.7 Regulamentação das Criptomoedas

A regulamentação das criptomoedas é algo que vem sendo elaborado e estudado pelos países, mas tem-se dois lados: alguns querendo permitir que as moedas sejam utilizadas, e outros, conforme alguns acontecimentos, inclusive do uso incorreto da moeda, por exemplo para a lavagem de dinheiro, estão querendo restringir o seu uso. Na China, no ano de 2017, o governo proibiu todas as instituições financeiras e as empresas, que a utilizavam como forma de pagamento, de realizarem o uso ou aceitarem as criptomoedas (REIS; COELI, 2019)

Apesar de ser uma tecnologia inovadora com potencial de trazer inúmeros benefícios à sociedade, ainda há importantes barreiras a serem ultrapassadas. Especialmente no âmbito legal e regulatório, ainda há enormes incertezas quanto à ação dos governos diante do crescimento do Bitcoin. Muitos adeptos da moeda digital clamam pela legitimidade legal, sob a justificativa de que ela é necessária para o seu desenvolvimento (ULRICH, 2014, p. 108).

Na Coreia do Sul, por sua vez, em 2017, os reguladores propuseram uma alteração na lei de transações financeiras eletrônicas vigente, que passaria a regulamentar negócios envolvendo criptomoedas, como a atividade das corretoras, dos negociantes, emissores e gestores. Já em dezembro de 2017, a comissão de serviços financeiros do país proibiu a negociação de futuros Bitcoins. As Exchanges, por outro lado, não sofreram limitações (REIS; COELI, 2019, p. 10).

O Japão foi um dos países que mais evoluiu para regulamentar as criptomoedas. No ano de 2016 foi aprovada uma lei que regulamenta as moedas. No ano de 2017 foram determinadas as criptomoedas como meio de pagamento, colocando na mesma configuração jurídica do dinheiro tradicional. Isso resultou fortemente no crescimento que as criptomoedas tiveram no país, e também concedeu as primeiras licenças, com exigências severas de transparência e aprimoramento do sistema computacional, a 11 corretoras de criptomoedas (REIS; COELI, 2019, p. 10).

O tema das criptomoedas tem surgido em diversas reuniões do G20 (grupo das 20 maiores economias do mundo). Na reunião realizada em dezembro de 2018, um dos pontos abordados foi sobre aumentar os esforços para garantir os benefícios potenciais da tecnologia no setor financeiro e a regulamentação dos criptoativos, visando à prevenção da lavagem de dinheiro e do financiamento do terrorismo em linha com os padrões do Grupo de Ação Financeira Internacional (Gafi). (ULRICH, Fernando, 2018)

2.2.7.1 Regulamentação no Brasil

No Brasil não há nenhuma regulamentação específica sobre a moeda Bitcoin, mas não é ilegal. Os brasileiros podem possuir e negociar as criptomoedas no mercado, mas, dependendo do valor mensal movimentado, devem declarar seus ganhos com o investimento. Para a Receita, o Bitcoin e outras criptomoedas são equiparadas a ativos financeiros, por isso a exigência em informar a posse a partir de R\$ 5.000,00 pelo preço de aquisição, além de declarar ganho de capital do que exceder R\$ 35 mil mensais em vendas ou alienações, segundo disposto na Instrução Normativa 1.888, que entrou em vigor em agosto de 2019 (ALVES, 2021).

Assim que as criptomoedas tomaram maior expansão no Brasil, o primeiro pronunciamento de um órgão do mercado brasileiro sobre criptomoedas foi feito pela Receita Federal em 2013. O entendimento da Receita é semelhante ao do fisco nos Estados Unidos: as criptomoedas são vistas como mercadoria, ou propriedade (bem incorpóreo, digital), havendo incidência de Imposto de Renda sobre ganho de capital. A alíquota é de 15% sobre vendas que excedam R\$ 35 mil por mês (CUNHA *et al.*, 2019, p. 71).

Outra tentativa de regulação surgiu em 2015, que propunha incluir programas de milhagens aéreas e criptomoedas sob as disposições da Lei 12.865, de 2013, que trata de moedas digitais no Brasil. O projeto foi desenvolvendo-se até que se criou uma comissão especial que conduziu várias audiências públicas em 2017 e 2018 para tratar do tema. O Projeto de Lei foi arquivado no fim de 2018, mas reaberto no começo de 2019. Neste ano de 2019 foi criado novo Projeto de Lei para tratar exclusivamente da regulação de criptoativos (CUNHA *et al.*, 2019, p. 71).

O Brasil não possuía nenhuma regulamentação específica, até que, então, ocorreram importantes alterações realizadas na Instrução Normativa 1.899 de 10 de julho de 2019, quando foi definida para fins jurídicos a configuração como criptoativos e *Exchanges* de criptoativos, conforme segue:

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

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

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

Parágrafo único. Incluem-se no conceito de intermediação de operações realizadas com criptoativos, a disponibilização de ambientes para a realização das operações de compra e venda de criptoativos realizadas entre os próprios usuários de seus serviços (INSTRUÇÃO NORMATIVA, 2019).

A alteração também criou a obrigação da prestação de informações para as pessoas físicas, investidoras, de forma independente, sem recorrerem às Exchanges ou utilizarem as domiciliadas em estrangeiros, que, no caso, movimentam valores acima de 30 mil reais em criptomoedas, sendo transacionadas mensalmente, conforme expõe o artigo a seguir:

DA OBRIGATORIEDADE DE PRESTAÇÃO DE INFORMAÇÕES

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

I – A Exchange de criptoativos domiciliada para fins tributários no Brasil;

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

a) as operações forem realizadas em Exchange domiciliada no exterior; ou

b) as operações não forem realizadas em Exchange.

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

§ 2º A obrigatoriedade de prestar informações aplica-se à pessoa física ou jurídica que realizar quaisquer das operações com criptoativos relacionadas a seguir:

I – Compra e venda;

II – Permuta;

III – Doação;

IV – Transferência de criptoativo para a exchange;

V – Retirada de criptoativo da exchange;

VI – Cessão temporária (aluguel);

VII – Dação em pagamento;

VIII – Emissão; e

IX – Outras operações que impliquem em transferência de criptoativos (INSTRUÇÃO NORMATIVA, 2019).

A norma teve um avanço ainda maior, pois passou a obrigar todas as Exchanges a fornecerem as informações à Receita Federal de todas as transações de seus usuários, como nome dos negociantes, valores movimentados, datas, taxas das operações, dentre outras. Isso está no artigo 7º exibido a seguir:

DAS INFORMAÇÕES SOBRE OPERAÇÕES COM CRIPTOATIVOS

Art. 7º Deverão ser informados para cada operação:

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

a) a data da operação;

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

c) os titulares da operação;

d) os criptoativos usados na operação;

e) a quantidade de criptoativos negociados, em unidades, até a décima casa decimal;

f) o valor da operação, em reais, excluídas as taxas de serviço cobradas para a execução da operação, quando houver;

g) o valor das taxas de serviços cobradas para a execução da operação, em reais, quando houver; e

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

a) a identificação da Exchange;

b) a data da operação;

c) o tipo de operação, conforme o § 2º do art. 6º;

d) os criptoativos usados na operação;

e) a quantidade de criptoativos negociados, em unidades, até a décima casa decimal;

f) o valor da operação, em reais, excluídas as taxas de serviço cobradas para a execução da operação, quando houver;

g) o valor das taxas de serviços cobradas para a execução da operação, em reais, quando houver (INSTRUÇÃO NORMATIVA, 2019)

De acordo com as leis presentes no Brasil, o dinheiro é o instrumento base que constitui o sistema financeiro de praticamente todas as economias mundiais, e esse meio é regulado pela conveniência da política monetária de cada Estado. No Brasil, a competência para emitir moeda é da União, por intermédio do Banco Central, conforme o artigo 164 da Constituição Federal de 1988 (REIS; COELI, 2019, p. 9).

Já a posição do Banco Central do Brasil, em pronunciamento que fez junto com a Comissão de Valores Mobiliários (CVM), em 2017, deixou claro que os investidores que desejassem adquirir criptoativos deveriam certificar-se dos riscos e da volatilidade desse tipo de ativo, e que não há entidade que regule o preço das criptomoedas. Mais um avanço, entretanto, ocorreu em setembro de 2018. A CVM pronunciou-se autorizando expressamente o investimento indireto em criptoativos, ou seja, tornou-se possível que um fundo de investimentos aplique seus recursos que possui, em carteira, criptoativos, em cotas de outros fundos no exterior (CUNHA *et al.*, 2019, p. 71).

3 PROCEDIMENTOS METODOLÓGICO

3.1 QUANTO AOS FINS

Quanto aos fins, a presente pesquisa classifica-se como descritiva, pois busca apresentar e descrever a origem e as características da moeda Bitcoin, com a finalidade de suprir os objetivos propostos, apresentando um conhecimento sobre determinada moeda desde o seu surgimento até suas propriedades atuais.

As pesquisas descritivas têm como objetivo a descrição das características de determinada população ou fenômeno. Podem ser elaboradas também com a finalidade de identificar possíveis relações entre variáveis. São em grande número as pesquisas que podem ser classificadas como descritivas e a maioria das que são realizadas com objetivos profissionais provavelmente se enquadram nesta categoria (GIL, 2017, p. 26).

3.2 QUANTO AOS MEIOS

O trabalho utilizou a pesquisa bibliográfica em livros, artigos e demais obras científicas, pois, apesar de ser um tema da atualidade, é possível encontrar referências sobre o estudo abordado.

A pesquisa bibliográfica é elaborada com base em material já publicado. Tradicionalmente, esta modalidade de pesquisa inclui material impresso, como livros, revistas, jornais, teses, dissertações e anais de eventos científicos. Todavia, em virtude da disseminação de novos formatos de informação, estas pesquisas passaram a incluir outros tipos de fontes, como discos, fitas magnéticas, CDs, bem como o material disponibilizado pela Internet (GIL, 2017, p. 28).

Conforme mencionado, a pesquisa bibliográfica é bem ampla, pois abrange uma grande gama de materiais que podem ser utilizados como referência para o desenvolvimento do estudo. Por serem temas atuais, pode ser encontrado um grupo de autores ou livros tratando do assunto, e é sempre possível garimpar pesquisas e pessoas escrevendo e discorrendo sobre o tema.

Praticamente toda pesquisa acadêmica requer em algum momento a realização de trabalho que pode ser caracterizado como pesquisa bibliográfica. Tanto é que, na maioria das teses e dissertações desenvolvidas atualmente, um capítulo ou seção é dedicado à revisão bibliográfica, que é elaborada com o propósito de fornecer fundamentação teórica ao trabalho, bem como a identificação do estágio atual do conhecimento referente ao tema (GIL, 2017, p. 28).

Há sempre um grande campo para utilizar como pesquisa, indiferente do tema abordado. De acordo com Gil (2017, p. 28), “a principal vantagem da pesquisa bibliográfica é o fato de permitir ao investigador a cobertura de uma gama de fenômenos muito mais ampla do que aquela que poderia pesquisar diretamente”.

3.3 UNIVERSO E AMOSTRA

Por se tratar de uma pesquisa bibliográfica, o presente estudo não terá Universo e Amostra.

3.4 COLETA DE DADOS

A coleta de dados foi realizada em *sites* oficiais de criptomoedas, com o objetivo de apresentar e analisar a evolução monetária histórica da moeda digital Bitcoin, possibilitando, ainda, compará-la com a evolução monetária de outras criptomoedas, ou, até mesmo, outros ativos financeiros.

De acordo com Constant (2016, p. 12), “na coleta de dados, o leitor deve ser informado como você pretende obter os dados de que precisa para responder ao problema”. Como mencionado anteriormente, há vários meios para a coleta de dados para a realização deste estudo.

3.5 TRATAMENTO DE DADOS

Os dados coletados foram de natureza qualitativa, pois buscou-se abordar as características e a origem da moeda bitcoin, possibilitando uma compreensão sobre como se dá o funcionamento da moeda. Também apresentar-se-ão dados quantitativos quanto à valorização e os valores de mercado da moeda digital.

Tratamento dos dados refere-se àquela seção na qual se explicita para o leitor como se pretende tratar os dados a coletar, justificando por que tal tratamento é adequado aos propósitos do projeto. Objetivos são alcançados com a coleta, o tratamento e, posteriormente, com a interpretação dos dados; portanto, não se deve esquecer de fazer a correlação entre objetivos e formas de atingi-los (CONSTANT, 2016. p. 12).

Os dados foram expostos por meio de gráficos e imagens extraídos da internet de fontes confiáveis, para que possam ser analisados e, com isto, responder-se aos objetivos e hipóteses propostas por este trabalho.

4 ANÁLISE DE DADOS

Neste capítulo serão analisadas as hipóteses criadas pelo autor com base em algumas características da criptomoeda Bitcoin, podendo então as hipóteses ser confirmada ou descartada, também será utilizado a representação de gráficos e de imagens apresentando dados de como está a criptomoeda em determinados períodos, sendo possível visualizar os estágios que a moeda enfrentou desde o seu surgimento.

Também possibilitou uma melhor compreensão sobre a criptomoeda, vendo quais são alguns pontos da moeda, tendo uma análise mais abrangente sobre o Bitcoin, podendo compreender se: o Bitcoin tem um quantitativo finito de moedas, e qual é este numero máximo, a evolução de seu quantitativo, se é a resolução dos problemas que geram moedas, é considerado um meio de pagamento ou transferências entre partes, a quantidade de transações confirmadas por dia desde o seu início.

Do mesmo modo abordou-se também o número total de usuários até certa data, a sua evolução histórica do valor de mercado. Se é necessário um elevado consumo de energia para operacionalizar, tempo médio de confirmação das transações, os equipamentos necessários para mineração, se o Bitcoin é uma moeda descentralizada, não controlada pelo governo, e os possíveis riscos que pode apresentar.

4.1 ANÁLISE DAS HIPÓTESES

Hipótese 1) O quantitativo de Bitcoins a ser criado é finito

A. Evolução do quantitativo de Bitcoin em circulação

O Bitcoin está em constante crescimento e expansão de usuários. O número de moedas em circulação aumenta a cada momento e estes dados são atualizados em tempo real. Isso demonstra, portanto, que realmente as pessoas estão utilizando o Bitcoin em suas formas de pagamento.

Gráfico 1 – Total de Bitcoins em circulação



Fonte: BLOCKCHAIN (2021).

Analisando o Gráfico supra constata-se a evolução que o Bitcoin sofreu nos últimos anos, chegando a alcançar 18 milhões de bitcoins que já foram extraídos e estão em circulação no mundo todo, um número bastante expressivo que, convertido para o seu valor de mercado, apresenta um valor muito grande já presente no mercado financeiro mundial.

B. Número máximo de Bitcoins

Logo quando foi criada a criptomoeda Bitcoin, foi informado que se teria um número máximo de moedas para ser comprado ou minerado, e este número é de 21 milhões de bitcoins, ou seja, somente este número estará em circulação no mundo todo, sendo bastante diferente do dinheiro normal, quando o governo pode dar o comando para emitir mais moedas.

A oferta de Bitcoin que pode existir durante o tempo em que a moeda for usada já está dada: 21 milhões de unidades, a uma taxa de criação também definida (começou com 50 bitcoins a cada 10 minutos, em média, caindo pela metade a cada 4 anos) até chegar aos 21 milhões de unidades. Isso vale para outras criptomoedas, que têm sua própria dinâmica de criação, que pode ser auditada e inspecionada (CUNHA *et al.*, 2019, p. 68).

C. A resolução dos problemas que geram os Bitcoins

A criação das criptomoedas tem, como objetivo, a intenção de desenvolver uma nova economia e resolver alguns problemas no mercado financeiro tradicional. A mineração de Bitcoins ocorre mediante a resolução dos problemas matemáticos, que é feita por computadores potentes. Após a resolução do problema, o minerador precisa desenvolver um bloco válido para provar que o trabalho está correto (*Proof of Work*).

Conforme Ulrich (2014, p. 19), a real mineração de Bitcoins é puramente um processo matemático. Hoje em dia, pesquisadores usam computadores avançados de alto desempenho para encontrá-los, e suas façanhas são observadas pela comunidade da matemática. À medida que mais capacidade computacional é dedicada à mineração, o protocolo incrementa a dificuldade do problema matemático, assegurando que Bitcoins sejam sempre minerados a uma taxa previsível e limitada.

Hipótese 2) O Bitcoin é considerado uma criptomoeda, ou seja, um meio de pagamento ou transferência do dinheiro eletrônico entre partes

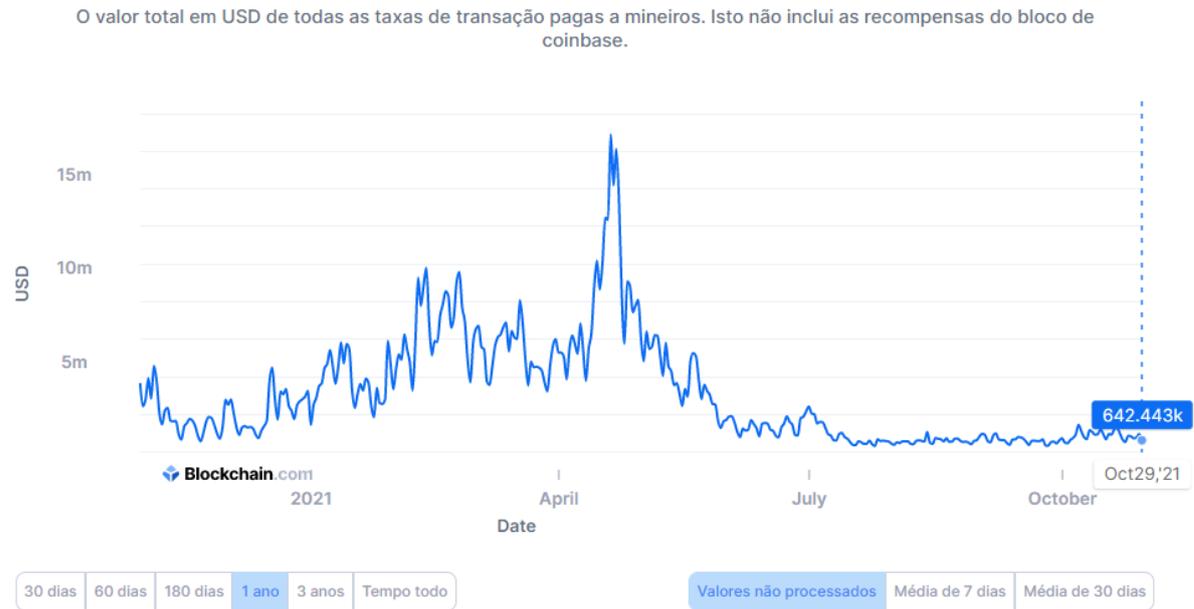
Para que a criptomoeda seja considerada moeda precisa-se cumprir três funções: meio de pagamento, unidade de conta e reserva de valor. As criptomoedas têm a sua maior ênfase em ser um meio de pagamento, ou seja, uma forma totalmente virtual com criptomoedas, e, dependendo da análise que for realizada, é possível constatar que elas cumprem estas funções e podem ser consideradas moeda.

As funções comumente atribuídas ao dinheiro são as de servir como i) meio de troca, ii) reserva de valor e iii) unidade de conta. Porém, as três funções não emergem instantaneamente no momento em que um bem passa a ser utilizado como meio de troca. Na verdade, facilitar as trocas, desempenhar a função de meio de troca é a função da moeda e, como elaborado acima, é como a moeda deve ser, inclusive, definida (ULRICH, 2014 p. 93).

A. Dados dos quantitativos de transações efetuadas (em dólar) no último ano

Fazendo-se uma análise sobre o Gráfico 2, nota-se as oscilações que o Bitcoin sofreu em cada mês referente ao último ano, mas, se olharmos o dado somente de um dia, percebe-se o grande valor transacionado em dólares; por exemplo, conforme no gráfico acima cita-se que na data de 29/10/2021 foram transacionados mais de 642 mil dólares em apenas um único dia, um alto valor, e, por isso, frisamos que o Bitcoin e outras criptomoedas já estão presente na parte financeira e pessoal de muitas pessoas.

Gráfico 2 – Taxas de transação totais (United States Dollar – USD)



Fonte: BLOCKCHAIN (2021).

Analisando-se o Gráfico 3 é possível visualizar a quantidade de transações realizadas durante um dia somente com a moeda Bitcoin. No dia 29 de outubro de 2021 foram feitas mais de 252 mil transações, um número bastante interessante. Observando-se em meses, porém, a criptomoeda teve oscilações.

Gráfico 3 – Transações confirmadas por dia



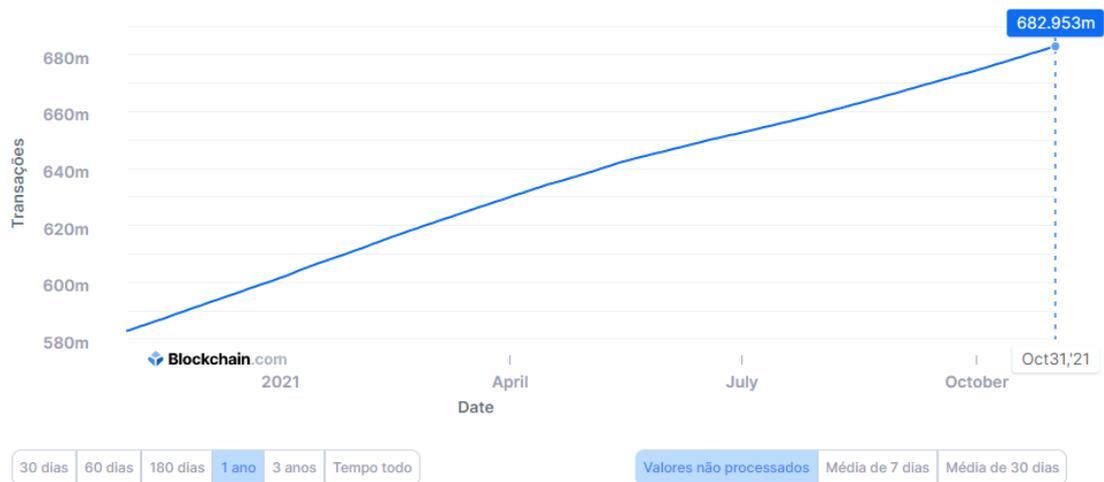
Fonte: BLOCKCHAIN (2021).

B. Número total de transações com Bitcoins

O Gráfico a seguir apresenta os números de transações realizadas com a moeda Bitcoin. São mais de 682 milhões de operações feitas desde a sua criação até o final do mês de outubro de 2021, um número expressivo, que demonstra que a moeda está em constante movimentação financeira e em diversos locais do mundo.

Gráfico 4 – Número total de transações

O número total de transações no blockchain.

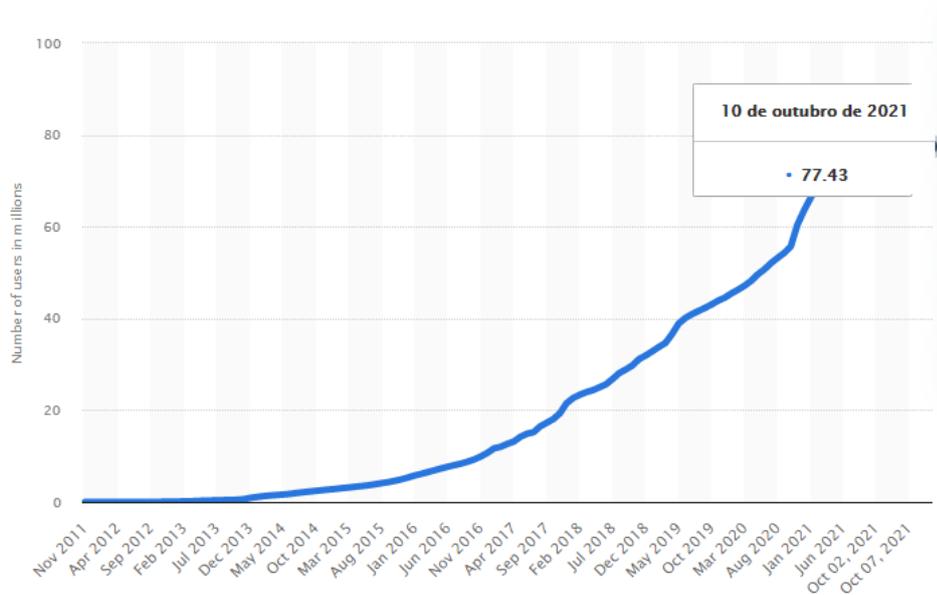


Fonte: BLOCKCHAIN (2021).

C. Quantitativo de usuários – investidores – (mundo)

Até dia 10 de outubro de 2021 foi registrado o total de 77,43 milhões de pessoas cadastradas no sistema Blockchain, ou seja, um número bastante alto, que, assim como os demais indicadores das criptomoedas, sofrem o aumento diário destes números. Com o passar dos meses mais pessoas vão conhecendo este mercado e são inseridas e convidadas a fazer parte desta economia.

Gráfico 5 – Quantidade de usuários do mercado das criptomoedas



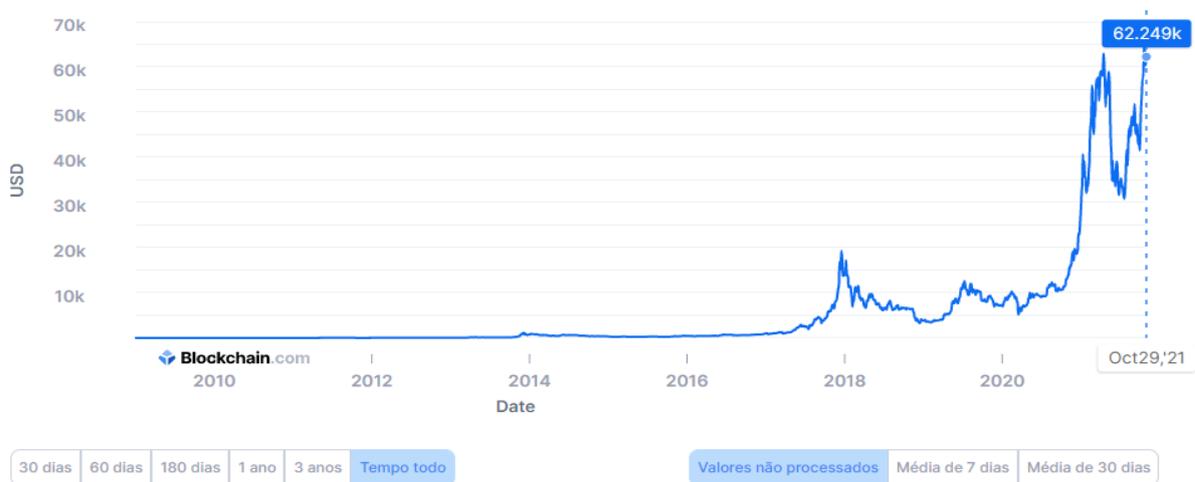
Fonte: STATISTA (2021).

D. Evolução histórica do valor de mercado

Observa-se no Gráfico 6 que, no dia 29 de outubro de 2021, a moeda fechou com o valor total de 62.249 mil dólares, ou seja, mais de 350 mil reais. Os usuários que utilizam a criptomoeda Bitcoin acabam ganhando com o seu aumento de valor de mercado. Muitos adquiriram a moeda com valores bem inferiores do que se encontra atualmente, e possuem, então, seus valores com uma alta taxa de valorização. O Gráfico a seguir apresenta a variação de preço que a moeda Bitcoin sofreu desde o seu início.

Gráfico 6 – Preço de mercado (USD)

O preço médio do mercado em USD nas principais plataformas de troca de bitcoin.



Fonte: BLOCKCHAIN (2021).

Conforme Graf (2016, p. 128), logo no início de seu surgimento o Bitcoin ainda não possuía um valor definido, mas, no dia 5 de outubro de 2009, nove meses após o início da rede Bitcoin, o primeiro preço de oferta desta criptomoeda registrado foi postado. O valor atingiu 13 Bitcoins por um centavo, ou, especificamente, 1.309,03 Bitcoins por dólar, calculado pelo autor da postagem com base em seus custos de mineração variáveis.

Quanto à demanda há uma grande imprevisibilidade e, portanto, a principal causa está no preço. Para entendermos a demanda é preciso compreender os principais fatores que levam os usuários à adoção desse novo ativo. Dentre eles podemos destacar:

Oferta inelástica – o máximo que pode haver de Bitcoin são as 21 milhões de unidades previstas desde a criação da moeda.

Redução dos custos de transação – o Bitcoin barateia os custos de transferências internacionais de recursos, sem depender de intermediário, e com transparência e segurança.

Dinheiro apolítico à prova de censura – ativo que não está submetido a pressões políticas de nenhum governo ou banco central, e que não pode ser confiscado.

Potencial novo ativo de proteção – por suas características de ser “não inflacionável” (tem um limite de criação de bitcoins) e “não confiscável”.

Ouro Digital

Efeito rede – trata-se da maior rede de circulação de moeda digital.

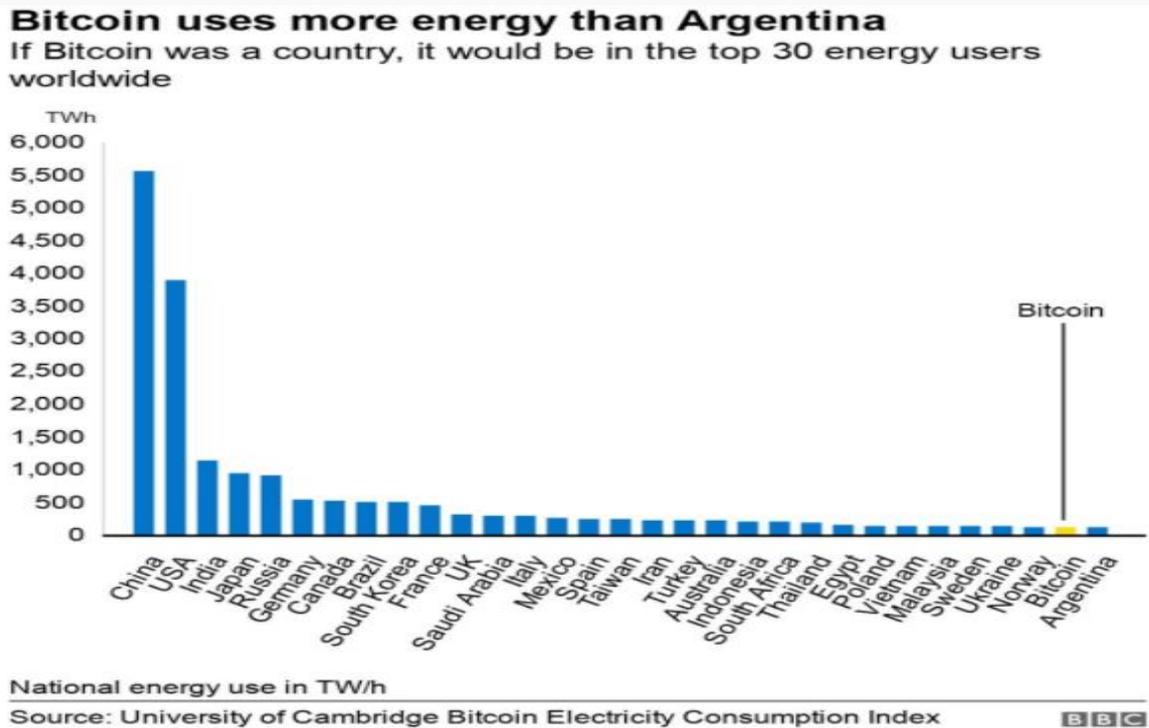
Diversas aplicações do blockchain (CUNHA *et al.*, 2019, p. 69).

Hipótese 3) É necessário um elevado consumo de energia para a geração dos Bitcoins e validação das operações

A. Gráfico do consumo de energia total

Um dos pontos de grande influência na mineração são os gastos e o consumo de energia, pois é necessário que os computadores fiquem ligados 24 horas por dia. Segundo um levantamento feito pela Universidade de Cambridge, no Reino Unido, o Bitcoin consome mais energia que todo o país da Argentina. Segundo os pesquisadores, a mineração da criptomoeda consome cerca de 130,9 terawatt-horas por ano, enquanto a Argentina tem o consumo de 125 terawatt-horas por ano, posto que um terawatt equivale a 1 bilhão de kilowatts. (CRIDDLE, 2021)

Gráfico 7 – Bitcoins usa mais energia do que a Argentina



Fonte: CRIDDLE (2021).

Na reportagem publicada pelo *site* BBC, na data de 10/2/2021 (CRIDDLE, 2021), constata-se, conforme mostra o Gráfico 7, que se o Bitcoin fosse um país estaria entre os 30 principais usuários de energia no mundo todo, estando à frente de países como a Argentina, que consome 125,03 TWh por ano de energia, a Holanda (110,68 TWh), os Emirados Árabes (119,46 TWh) e a Noruega (124,13 TWh).

B. Tempo médio de confirmação das operações

O Gráfico a seguir apresenta quanto tempo em média demora para que seja confirmada a transação de Bitcoins. Este tempo oscila conforme o número de transações a serem realizadas ou quando ocorre alguma falha no sistema. Pode-se notar que no mês de maio de 2021 o sistema, em alguns dias, pode ter enfrentado uma pane ou uma grande oscilação de preço, que resultou bruscamente no aumento do tempo.

Gráfico 8 – Tempo médio de confirmação



Fonte: BLOCKCHAIN (2021).

C. Equipamentos necessários

Para começar a minerar criptomoedas, primeiramente é preciso estar disposto a investir e adquirir os equipamentos corretos. No início apenas um computador comum, equipado com algumas placas de vídeos, era o suficiente, porém, agora, com o aumento do número de mineradores, são necessários equipamentos mais potentes, como o produto conhecido como Asic Miners, que é especializado na tarefa, e tem custo médio de US\$ 10 mil a US\$ 15 mil (R\$ 50 mil a R\$ 75 mil), que trazem retornos maiores do que um computador convencional; somente computadores com superprocessamento conseguem resolver os problemas matemáticos impostos na mineração.

Outro ponto importante é possuir acesso à internet, de preferência de boa potência. Além de ter um computador potente e moderno, deve-se levar em consideração o uso de energia elétrica, que é alto, pois os equipamentos necessitam ficar ligados 24 horas por dia. Também é preciso ter ciência que a mineração é um processo intenso e capaz de desgastar os componentes rapidamente. Em outras palavras, seus equipamentos provavelmente vão ter de ser substituídos em pouco tempo, e você vai ter de tirar os gastos de renovação de seus lucros.

Ainda, é necessário que o minerador tenha uma carteira de criptomoedas, participe da cooperação entre os mineradores e possua um programa de mineração em seu computador. Há vários *softwares* presentes no mercado, ficando a seu critério qual deseja escolher. Há pessoas que possuem equipamentos de refrigeração para contribuir para o melhor funcionamento das máquinas, mas isto vai de cada minerador.

Hipótese 4) O Bitcoin é uma moeda descentralizada

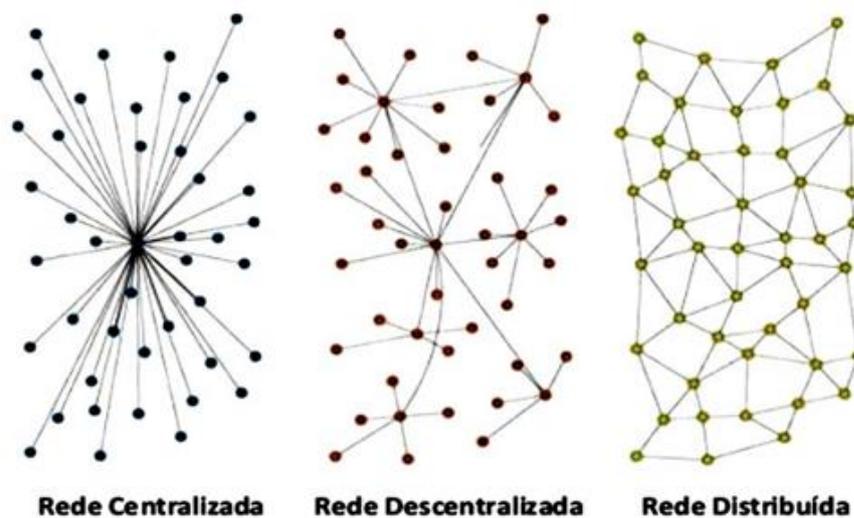
A. Explicação da rede centralizada, descentralizada e distribuída

Na rede centralizada os dados são armazenados em um único computador, chamado de servidor, ao qual você precisa se conectar para acessar as informações. Como exemplo pode-se citar o mercado financeiro brasileiro, onde o ponto no centro é o Banco Central e os pontos que surgem a partir dele são as instituições financeiras.

Já na rede descentralizada não há um ponto central e os dados são armazenados em vários servidores conectados entre si, que podem estar em um mesmo local físico ou dispersos. Para ter acesso aos dados é preciso conectar-se a um desses servidores. Este tipo, portanto, é o utilizado pelas criptomoedas, quando cada minerador gera a distribuição e a conexão para os demais usuários, e os mineradores são conectados a um ponto central.

O sistema Blockchain é uma base de dados distribuída, pois cada computador tem uma cópia de todos os dados, tendo acesso a todas as informações, podendo interagir com elas diretamente. A manutenção e a sincronização são feitas por um algoritmo de consenso, que requer um acordo entre todos os participantes da rede para as tomadas de decisão, algo que consome mais recursos e esforços.

Figura 1 – Rede centralizada, rede descentralizada e rede distribuída



Fonte: Paulo Baran (2016)

B. Blocos

A tecnologia do Blockchain é a base tecnológica do Ethereum. Um Blockchain é uma arquitetura de computação distribuída na qual cada nó (usuários que cooperam com a estrutura, cedendo poder computacional) da rede executa e registra as mesmas transações, que são agrupadas em blocos. Apenas um bloco pode ser adicionado ao Blockchain por vez. Cada bloco contém uma prova matemática (hash) responsável por certificar que determinado bloco segue na sequência do bloco anterior (FOXBIT, 2021).

Os blocos formam, então, uma cadeia de blocos, cada um contendo informações, e isso tudo fica registrado no sistema Blockchain. Trata-se de um banco de dados distribuído numa rede *peer-to-peer*, no qual não há unidade centralizadora e nenhum componente da rede possui prioridade quando comparado a outro. A cada movimentação do Bitcoin, portanto, são criados novos blocos.

C. Quantidade de Hash

O Gráfico a seguir apresenta a quantidade de *hash*, que é um algoritmo utilizado pelo protocolo do Bitcoin e de outras criptomoedas para transformar um grande número de informações em uma sequência numérica. No caso das criptomoedas, cada *hash* é criado com o auxílio de um algoritmo duplo SHA-256.

Gráfico 9 – Taxa de *hash* total (TH/s)



Fonte: BLOCKCHAIN (2021).

Segundo Ulrich (2014, p. 19), o Bitcoin busca encontrar a sequência de dados (chamada de “bloco”) que produz certo padrão quando o algoritmo é o “*hash*” do Bitcoin e é aplicado aos dados. Quando uma combinação ocorre, o minerador obtém um prêmio de Bitcoins e também uma taxa de serviço, em Bitcoins, no caso de o mesmo bloco ter sido usado para verificar uma transação.

Hipótese 5) Criptomoedas não são controladas pelo governo

A. Funcionamento sem o controle governamental

As criptomoedas não são controladas pelo governo como ocorre com as moedas físicas tradicionais, que são reguladas pelos governantes, que conseguem fazer a gestão do número de moedas disponíveis e outros índices. Com as criptomoedas é diferente: o controle é feito pelos próprios usuários e as operações ficam registradas em sistema que, no caso do Bitcoin, é o Blockchain, de livre acesso para todos os públicos, totalmente de forma transparente.

Conforme Ulrich (2014, p. 13), o Bitcoin propicia a perspectiva de restaurar a solidez e o universalismo do padrão-ouro do mundo antigo, além de aprimorá-lo por existir fora do controle direto do governo. Isso é, mais uma vez, digno de admiração. Um dos objetivos que o Bitcoin tem é não ser controlado por nenhum governo.

B. Quanto à operações em países

As criptomoedas não são controladas pelos países, mas, para que elas sejam utilizadas, é necessário que o país não proíba este tipo de moeda em seu território. Isso é bastante relativo em cada local, pois há países que já estão regulamentados e as criptomoedas já fazem parte de seu mercado financeiro, mas, de outro lado, há locais que não permitem que sejam utilizadas as moedas em seu território.

Antes de começar a comprar e utilizar as criptomoedas, portanto, é importante ver o que seu país de residência tem como regulamentação nesta área. No Brasil ocorreu a alteração de algumas leis, e vem sendo realizado um trabalho sobre as criptomoedas para que os brasileiros continuem a poder fazer uso em conformidade com tais leis.

Observando a Figura 2 é possível ter uma noção de em quais países é regulado o Bitcoin e onde pode ser operacionalizado e também minerado. Nota-se que há uma grande extensão no mapa de abrangência da moeda. Em alguns locais devido a alguns acontecimentos ocorreu a proibição

B. Utilização para Lavagem de Dinheiro

A moeda Bitcoin e as criptomoedas podem estar sendo utilizadas de forma errada por alguns usuários, como para o crime de lavagem de dinheiro para coisas ilícitas, com finalidade de dificultar a identificação e origem dos valores e até mesmo para fazer a tentativa de colocar este valor no mercado financeiro de forma “legal”, pois as criptomoedas permitem a transferência de valores de forma segura, sem o controle de nenhum órgão e sem intermediação bancária, sendo de difícil rastreamento do usuário.

No Brasil, Andrade (2017) pesquisou se a falta de regulamentação específica para as criptomoedas possui relação com a expansão das modalidades criminosas relacionadas ao tema. Por meio de uma ampla análise bibliográfica, conclui-se que não é possível associar diretamente este fenômeno, entretanto, há relação entre a falta de regulamentação e a especialização de práticas criminosas que usam o ciberespaço como ambiente.

Conforme já mencionado neste estudo, os países já estão alterando suas leis para que as criptomoedas possam ser utilizadas legalmente. Sobre a lavagem de dinheiro, no Brasil foram alteradas algumas leis, que mudou para que o crime de lavagem de dinheiro seja também aplicado no contexto virtual e não somente em ambientes reais, abrangendo, então, as transações realizadas virtualmente. Tudo isso se deu com o avançar da internet, mas devemos enfrentar mais mudanças.

Já existem, na indústria brasileira, associações de classe como a ABCRIPTO (Associação Brasileira de Criptoconomia), que reúne as principais plataformas de negociação do Brasil e a ABCB (Associação Brasileira de Criptoativos e Blockchain), que está em contato com o ENCRA (Estratégia Nacional de Combate à Corrupção e Lavagem de Dinheiro). Do ENCRA fazem parte órgãos como a Receita Federal, o Ministério da Fazenda, o BCB, a CVM, a Advocacia Geral da União, o Ministério Público Federal, dentre outros (CUNHA *et al.*, 2019. p. 72).

C. Risco de mercado e sistêmico

As criptomoedas também possuem riscos de mercado, e a volatilidade é um risco que precisa ser considerado pelos usuários. Outro ponto é os estabelecimentos permitirem o uso das moedas como meio de troca. Ainda, a regulamentação das moedas no mundo pode sofrer grandes impactos referentes a não aceitação e até à proibição do uso em alguns países.

Outros riscos que podem ser encontrados são os sistêmicos, pois podem ocorrer falhas no sistema utilizado. Para o uso do Bitcoin é necessário que sejam atualizados e corrigidos alguns erros constantemente, o que pode resultar no funcionamento de todo o sistema, gerando influência sobre o preço. Todos os usuários precisam estar sincronizados atualizando suas cópias de Blockchain.

Há pessoas e empresas que prometem grandes valorizações com o investimento em criptomoedas, mas isso não pode ser uma confirmação, pois é como no mercado de ações, podendo ocorrer o aumento e a baixa do valor de mercado. Atualmente as criptomoedas encontram-se em alta comparado a anos anteriores.

4.2 ANÁLISE DAS TENDÊNCIAS

Nesta área as inovações acontecem a todo instante, pois há muitos estudos com o propósito de facilitar a vida das pessoas, visando à otimização do tempo e à economia de dinheiro, tudo isso conectado de forma digital. Alguns produtos/serviços já estão consolidados no mercado, porém necessitam acompanhar a evolução tecnológica para que se mantenham no segmento em que estão atuando e não sejam ultrapassados pela concorrência.

Uma destas inovações é a rede social BitClout, que está conectada à Blockchain “Decentralized Social” (DeSo), e isso permite que a rede social seja descentralizada. Quando o usuário cria uma conta, ele recebe um número de *tokens* que cresce conforme a pessoa ganha mais seguidores e podem se valorizar. Esta rede já está bem evoluída e conhecida em alguns países, porém tem pouca exposição no Brasil.

Outra tendência disponível na internet é um *site* chamado EOS.IO, uma plataforma de Blockchain de código aberto para inovação e desempenho, a qual funciona como um contrato inteligente para a instituição de aplicativos e corporações autônomas descentralizadas. Ela foi introduzida para resolver os problemas de escalas, elevadas taxas de transação e outras questões relacionadas às criptomoedas. Ainda, disponibiliza cursos sobre criptomoedas, principalmente focado na tecnologia Blockchain. Algumas empresas e desenvolvedores usam o EOS.IO para criar infraestruturas digitais seguras, transparentes e determinísticas.

CONSIDERAÇÕES FINAIS

Com esta pesquisa foi possível realizar algumas reflexões. O objetivo foi descrever um pouco sobre as criptomoedas, com foco principal na moeda Bitcoin, discorrendo sobre a sua origem, as principais características, a evolução histórica que a moeda teve desde o seu surgimento, as formas de possuir uma criptomoeda e como ocorre o seu funcionamento. Também foi abordado o sistema Blockchain, que sustenta a moeda Bitcoin no mercado em constante operação.

As principais características do Bitcoin são ser totalmente virtual, descentralizado e transparente, pois todas as transações efetuadas são registradas em tempo real e apresentadas no sistema Blockchain, e ficam disponíveis para todos as pessoas no *site* do sistema. É uma criptomoeda sem o controle governamental e de instituições financeiras, com baixas taxas de transações e irreversíveis.

Quanto à forma de criação é mediante o processo de mineração. Neste estudo apresentou-se como ocorre este meio, quais equipamentos são necessários para que o sistema funcione, minimizando possíveis falhas e interrupções, e alguns custos de investimento para instalação e manutenção do sistema de mineração em pleno funcionamento, lembrando que é necessário estar conectado à internet. Atualmente a forma mais fácil de comprar ou vender as criptomoedas é por intermédio das corretoras.

A criptomoeda Bitcoin surgiu após a publicação de um artigo escrito por Satoshi Nakamoto no ano de 2008, para ser uma opção de intermédio de pagamento diferente das formas tradicionais, permitindo a realização de transações monetárias de pessoa para pessoa de maneira segura.

Diante disto, foi diagnosticado, por meio de representações gráficas, o quantitativo de usuários da criptomoeda que está em constante crescimento, aproximando-se do limite máximo de bitcoins disponíveis. O giro financeiro que a moeda tem realizado no mercado financeiro mundial tem fortes impactos, pois ocorrem transações de altos valores monetários diariamente.

Em relação à evolução do valor de mercado do Bitcoin, manifestada nos últimos anos, ele pode ser considerado uma criptomoeda de alta valorização. Salienta-se o grande número de transações realizadas desde o surgimento da criptomoeda, pois a sua criação aconteceu para a resolução de problemas presentes no mercado financeiro tradicional. Demonstra-se, então, mediante os gráficos, a quantidade de transações efetuadas em dólares em apenas um dia, está sendo bastante expressiva. Também se expõe o quantitativo de usuários presentes nas criptomoedas até a data estabelecida, e que este número está em constante crescimento.

Assim, quanto à questão da regulamentação das criptomoedas, apresentou-se uma imagem que demonstra quais países já possuem aceitação da moeda Bitcoin, trazendo alguns acontecimentos relevantes e como está o processo no Brasil, e se o país já possui leis que permitem o uso e a mineração das criptomoedas. Destacam-se, ainda, as principais regras que devemos seguir para não descumpriremos a Constituição e as leis brasileiras.

Na primeira hipótese, portanto, foi confirmado que o Bitcoin possui um quantitativo finito de criação, que são de 21 milhões de moedas, e este número está próximo do limite máximo, pois, conforme a análise gráfica apresentada neste trabalho, a quantidade total está em constante crescimento.

Na hipótese 2 foi verificado que o Bitcoin é considerado um meio de pagamento e pode ser utilizado para transferência do dinheiro eletrônico entre partes ou pessoas. Para ser respeitado como moeda é necessário que o Bitcoin cumpra três funções: meio de pagamento, unidade de conta e reserva de valor, mas a criptomoeda não é reconhecida como unidade de conta, ou seja, não é um padrão para que as mercadorias sejam cotadas no mercado.

Na hipótese 3 afirma-se que para o processo de mineração é necessário energia elétrica para manter o sistema em pleno funcionamento, e este consumo é elevado para a geração dos Bitcoins e a validação das operações. Constata-se, na Figura 2 apresentada, comparando-se a energia gasta pelos países e se o Bitcoin fosse considerado um país, que este estaria na posição 30º dos países do mundo que mais consomem energia elétrica. O tempo médio para confirmar as transações entre Bitcoins com base nos últimos meses é de, em média, oito minutos.

Nas hipóteses 4 e 5 é confirmado que o Bitcoin é uma moeda descentralizada, ou seja, funciona sem a ajuda de um terceiro, pois não há nenhuma instituição financeira ou governo que responda e possua o controle, como acontece com as moedas tradicionais, porque são os próprios usuários e os mineradores que efetuam o registro e o controle da rede Blockchain.

Já na hipótese 6, um dos riscos que as criptomoedas e o Bitcoin podem apresentar é em relação ao uso inadequado, apresentando alguma possibilidade de se fazer o uso ilegal da moeda, como a lavagem de dinheiro. Já existem leis, todavia, na tentativa de dificultar que isto aconteça, e, caso identificado, devem ser punidos os infratores. Também há o risco de volatilidade devido à oscilação de preços que a criptomoeda possui.

Quanto à análise das tendências, já temos disponíveis, de forma gratuita, até o momento, uma rede social em que, conforme você vai ganhando amigos, pode conseguir obter pontos e estes serem transformados em porcentagens de criptomoedas, e também existe um *site* de livre acesso com plataformas de ensino para o público que desejar conhecer mais sobre este mercado das criptomoedas e o seu funcionamento.

Foi observado, com a investigação, que o Bitcoin é uma criptomoeda consolidada no mercado financeiro que já proporciona aos seus usuários uma forma diferente de utilização do dinheiro, apresentando características e algumas vantagens em relação às moedas tradicionais. Constatou-se que é possível, então, que as criptomoedas aumentem gradativamente a sua participação na economia, mas isso depende da credibilidade junto ao público, afirmando-se que as criptomoedas podem, futuramente, vir a fazer parte do cotidiano de um grande número de pessoas no mundo inteiro.

Durante o desenvolvimento desta pesquisa, surgiu a dificuldade de encontrar mais bibliografias a respeito do tema. Este estudo, porém, pode ser continuado e utilizado como fonte de próximas pesquisas e de novas leituras, uma vez que sempre há algo a acrescentar, e existem muitos aspectos a serem estudados em relação ao assunto.

Ao finalizar este trabalho, acrescenta-se que o mesmo é considerado uma conquista, pois concluí-lo é de grande satisfação para este graduando.

REFERÊNCIAS

AGUIAR, Antonio; ZAMBUJAL-OLIVEIRA, João. **Tecnologias de Informação de Suporte a criptomoedas**. Oeiras, Portugal: Atlântica – Instituto Universitário Fábrica da Pólvora, 2021.

ALKUDMANI, Fares. **Como funciona a mineração de criptomoedas**. 2020. Disponível em: <https://portaldobitcoin.uol.com.br/como-funciona-a-mineracao-de-criptomoedas/>. Acesso em: 6 jul. 2021

ALVES, Paulo. **Bitcoin é legal?** Saiba mais sobre a regulamentação das criptomoedas. Disponível em: <https://www.cnnbrasil.com.br/business/bitcoin-e-legal-saiba-mais-sobre-a-regulamentacao-das-criptomoedas/>. Acesso em: 2 out. 2021.

ANDRADE, Mariana Dionísio de. Tratamento jurídico das criptomoedas: a dinâmica dos bitcoins e o crime de lavagem de dinheiro. **Revista Brasileira de Políticas Públicas**, v. 7, n. 3, 2017.

ANTONOPOULOS, Andreas, M. Mastering Bitcoin. **Unlock digital crypto-currencies**. Sebastopol: O'Reilly, 2014a. (Versão traduzida em 2016).

ANTONOPOULOS, Andreas M. Mastering Bitcoin. **Unlock digital crypto-currencies**. 1. ed. Sebastopol: O'Reilly Media, 2014b.

BAZAN, Vinícius. **O que é mineração e como minerar Bitcoin?** 2018. Disponível em: <https://www.empiricus.com.br/artigos/investimentos/o-que-e-mineracao-e-como-minerar-bitcoin/>. Acesso em: 6 jul. 2021.

BARAN, Paulo. **Centralização, descentralização e distribuição 2016** Disponível em: <https://entrenostodos.wordpress.com/2016/09/21/centralizacao-descentralizacao-e-distribuicao/>. Acesso em: 17 out. 2021.

BINANCE ACADEMY. **Teoria dos Jogos e Criptomoedas** (artigo). Disponível em: <https://academy.binance.com/pt/articles/game-theory-and-cryptocurrencies>. Acesso em: 2 nov. 2021.

BLOCKCHAIN. Disponível em: <https://www.blockchain.com/explorer>. Acesso em: 30 out. 2021.

BITCOIN. Disponível em: <https://www.bitcoinregulation.world/>. Acesso em: 30 out. 2021.

CAMARA, Michele Pacheco. **O Bitcoin é alternativa aos meios de pagamento tradicionais?** 2014. 76 f. Monografia (Graduação) – Universidade Federal do Rio Grande do Sul, Escola de Administração, Porto Alegre, 2014.

CARVALHO, Carlos Eduardo *et al.* **Bitcoin, criptomoedas, blockchain: desafios analíticos reação dos bancos, implicações regulatórias**. 2017. Disponível em: liberdadeeconomica.mackenzie.br. Acesso em: 13 out. 2021.

CONSTANT, V. S. **Projetos e relatórios de pesquisa em administração**. 16. ed. Grupo GEN. 2016. Disponível em: <https://app.minhabiblioteca.com.br/#/books/9788597007480/>. Acesso em: 22 jul. 2021

CUNHA, Gustavo *et al.* **Investimentos no exterior coe e criptomoedas**. [S.l.]: [s.n.] 2019. 97 p.

CRIDDLE, Cristina. BBC News. **Bitcoin consumes 'more electricity than Argentina**. Disponível em: <https://www.bbc.com/news/technology-56012952>. Acesso em: 10 out. 2021

ETHEREUM PROJECT. Build unstoppable applications. Disponível em: <http://www.ethereum.org>. Acesso em: 9 out. 2021.

EOS.IO. Disponível em: <https://eos.io/>. Acesso em: 7 nov. 2021.

FAGUNDES, Paulo. Blockchain: O que é? De onde vem? Do que vive? O que come? 2017. E-book Kindle. Disponível em: [Blockchain-que-onde-vive-come-ebook/dp/B075WMP2HW](https://www.amazon.com.br/dp/B075WMP2HW)

FOXBIT. Disponível em: <https://foxbit.com.br/blog/ethereum-em-minutos-uma-nova-geracao-de-blockchain/>. Acesso em: 30 out. 2021.

GHIRARDI, M. D. C. G. **Criptomoedas**. Coimbra, Portugal: Grupo Almedina, 2020. Disponível em: <https://app.minhabiblioteca.com.br/#/books/9786556270364/>. Acesso em: 28 jun. 2021.

Gil, Antonio Carlos, 1946 – Como elaborar projetos de pesquisa / Antonio Carlos Gil. – [2.Reimpr.]. – 6. ed. – São Paulo: Atlas, 2018.

GRAF, Konrad S. Sobre as origens do bitcoin: estágios da evolução monetária – parte II. **Mises: Revista Interdisciplinar de Filosofia, Direito e Economia**, v. IV, n. 1, Edição 7, p. 121-139, jan./jun. 2016. ISSN 2318-0811

INSTRUÇÃO NORMATIVA. RFB Nº 1.888, de 3 de maio de 2019. Publicado(a) no DOU de 7/5/2019, seção 1, página 14. Disponível em: <http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=100592>. Acesso em: 10 out. 2021

IBEF. Instituto Brasileiro de Executivos de Finanças. São Paulo. Disponível em: <https://ibefsp.com.br/tesouraria-bitcoin-como-reserva-de-valor-e-ativos-tokenizados-podem-ser-futuro-do-mercado-financeiro/>. Acesso em: 23 out. 2021.

INFOMONEY. Disponível em: <https://www.infomoney.com.br/cotacoes/cardano-ada/>. Acesso em: 10 out. 2021.

MARQUES, Diego. Disponível em: <https://guiadobitcoin.com.br/noticias/bitcoin-mineracao-entenda-como-funciona-ao-final-do-post-responda-nossa-pesquisa-e-concorra-a-0-02-bitcoins/>. Acesso em: 10 out. 2021.

MILLER. Ruan Mendes Lima Fonseca. Bitcoin: Um estudo sobre as formas de aquisição e de utilização no Brasil. 2021

MIRANDA, Marcelo; SALVATORE, Eduardo. **Tudo que você pode saber sobre Ethereum**. 1. ed. São Paulo: FlowBtc. 2018. Vol. I.

NAKAMOTO, Satoshi. **Bitcoin: a Peer-to-Peer Electronic Cash System**. 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 7 jun. 2021.

NASCIMENTO, Gregory Zechmann; PORTO, Pedro Augusto Cruz. O surgimento do bitcoin e sua análise à luz da legislação brasileira enquanto ativo financeiro. **Revista Tuiuti: Ciência e Cultura**, Dossiê Facjur, Curitiba, n. 57, c. 5, 2018.

PRADO, Magaly Parreira. Rede descentralizada blockchain: cultura do “faça você mesmo” com estrutura matemática de algoritmos de consenso. **Revista Eptic**. VOL. 22, Nº 2, MAI.-AGO. 2020

PROOF. **Blockchain**. 2018. Disponível em: <https://www.proof.com.br/blog/blockchain/>. Acesso em: 4 jul. 2021.

REIS, Lucas Fernandes Alves dos; COELI, Andrea Medina. **A regulamentação das criptomoedas como meio garantidor de segurança jurídica**. 2019. Disponível em: <http://dspace.uniube.br:8080/jspui/handle/123456789/1294>

SAMPAIO, Leobino *et al.* **Blockchain e a revolução do consenso sob demanda**. 2018. Disponível em: <https://portaldeconteudo.sbc.org.br/>. Acesso em: 4 jul. 2021.

STATISTA. Disponível em: <https://www.statista.com/statistics/647374/worldwide-blockchain-wallet-users/>. Acesso em: 30 out. 2021.

ULRICH, Fernando. **Bitcoin: a moeda na era digital**. São Paulo: Instituto Ludwig von Mises Brasil, 2014. 110 p.

ANEXO

FICHA DE REGISTRO DE ATIVIDADES DE ORIENTAÇÃO DE TCC

Nome: **BRUNO CASASGRANDE** Curso: **ADMINISTRAÇÃO (BACHARELADO)**Semestre: **8º** Ano: **2021**Professor(a) orientador(a) de TCC: **CLEBER JOEL STEVENS KROETZ**

REGISTRO DE ATIVIDADE DE ORIENTAÇÃO DE TCC			
DATA	ATIVIDADE DESENVOLVIDA	CARGA HORÁRIA	ASSINATURA
14/09/2021	Conversa Online com o Orientador	0:30 minutos	
06/10/2021	Conversa pelo WhatsApp		
17/10/2021	Conversa pelo WhatsApp		
22/10/2021	Conversa pelo WhatsApp		
26/10/2021	Conversa Online sobre o trabalho com o Orientador e convidado	0:45 minutos	
28/10/2021	Conversa com o orientador	1:00 horas	
06/11/2021	Conversa pelo WhatsApp		
11/11/2021	Conversa com Orientador	0:30 minutos	
13/11/2021	Conversa pelo WhatsApp		
16/11/2021	Conversa pelo WhatsApp		
18/11/2021	Conversa online com o Orientador	0:45 minutos	
23/11/2021	Conversa pelo WhatsApp		
29/11/2021	Conversa pelo WhatsApp		
01/12/2021	Conversa pelo WhatsApp		

(ASSINATURA VIA SIPAC)

_____/_____/_____

Assinatura do estudante_____
Assinatura do professor(a) orientador(a) de TCC