INSTITUTO FEDERAL
SANTA CATARINA

CÂMPUS FLORIANÓPOLIS
DEPARTAMENTO ACADÊMICO DE SAÚDE E SERVIÇOS
CURSO SUPERIOR DE TECNOLOGIA EM GESTÃO
DE TECNOLOGIA DA INFORMAÇÃO

Matheus Aragon

CRIPTOMOEDA: UMA ANÁLISE DA UTILIZAÇÃO DO BITCOIN NA SOCIEDADE CONTEMPORÂNEA

Florianópolis – SC
2018

Ficha de Identificação

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SANTA CATARINA
CÂMPUS FLORIANÓPOLIS
DEPARTAMENTO ACADÊMICO DE SAÚDE E SERVIÇOS
CST EM GESTÃO DA TECNOLOGIA DA INFORMAÇÃO

Matheus Aragon

CRIPTOMOEDA: UMA ANÁLISE DA UTILIZAÇÃO DO BITCOIN NA SOCIEDADE CONTEMPORÂNEA

Trabalho de Conclusão de Curso submetido ao Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina como parte dos requisitos para obtenção do título de Tecnólogo em Gestão da Tecnologia da Informação.

Professora Orientadora:
Prof. Mari Néia Valicheski Ferrari, Ma

Professor Coorientador:
Prof. Herval Daminelli, Esp

FLORIANÓPOLIS – SC

2018

Dedico este trabalho à minha mãe, Isabel Teodora dos Anjos, e ao meu pai, Renato Arruda Aragon, por todo apoio que me deram para que eu chegasse até aqui.

AGRADECIMENTOS

Agradeço primeiramente a minha família, em especial meu pai e minha mãe, que fizeram o possível para que eu realizasse meu sonho de estudar e me formar em Florianópolis.

Agradeço aos meus professores orientadores, Herval Daminelli e Mari Ferrari, por dedicarem preciosas horas de seus tempos para me ajudarem a concluir este trabalho.

Agradeço aos professores Antônio Cândido e Egon Junior pela oportunidade de estagiar no Grupo de Modelagem do Conhecimento do IFSC.

E, por fim, agradeço a todos que, direta ou indiretamente, fizeram minha estadia em Florianópolis ser mais agradável.

“Só sei que nada sei.” (Sócrates)

RESUMO

O presente trabalho é resultado de um estudo sobre o *bitcoin*, uma moeda virtual e descentralizada, criada em 2008 por Satoshi Nakamoto para ser uma opção aos meios de pagamentos tradicionais. Este estudo teve como objetivo principal investigar e analisar a utilização do *Bitcoin* na sociedade contemporânea. Para chegar ao objetivo principal, foi abordado a definição de moeda, o funcionamento da rede *Bitcoin,* os fatores que influenciam o seu uso e as vantagens e desvantagens do *Bitcoin* em relação a padrões monetários. O estudo, realizado através de pesquisas em livros, dissertações, artigos, documentos e ferramentas associadas ao *Bitcoin*, teve 2 etapas. A primeira etapa foi a exploratória, onde buscou-se compreender conceitos associados à base que sustenta esta pesquisa, no caso, o *Bitcoin*. A segunda etapa foi de análise, na qual ocorreu a comparação entre a moeda virtual e padrões monetários, mais especificamente, o ouro e o papel moeda; ainda nesta etapa, questionou-se se o *bitcoin* cumpre as funções básicas de uma moeda. Por último, apresentou-se a conclusão do autor sobre o presente estudo.

Palavras-chave: Bitcoin; Moeda; Tecnologia da Informação

ABSTRACT

The present work is the result of a study on bitcoin, a virtual and decentralized currency created in 2008 by Satoshi Nakamoto to be an option to the classroom media. This study aimed to investigate and analyze the use of Bitcoin in contemporary society. To obtain the principal goal, it was necessary to define what is currency, the operation of the Bitcoin network, the factors that influence its use and the advantages and disadvantages of Bitcoin in relation to monetary standards. The study, conducted with researches on books, dissertations, articles, documents and tools associated with Bitcoin, had 2 stages. The first step was a research about the Bitcoin's operation. The second stage was an analysis, with a comparison between bitcoin and monetary standards, in this case gold and paper money; besides that, the bitcoin has been analyzed fulfills the basic functions of a currency. Finally, the author on the present study made a conclusion.

Key words: Bticoin; Currency: Information of Technology

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

- *POW* – *Proof-of-work,* protocolo utilizado para a prevenção de ataques cibernéticos como DDOS e Spam.
- PPC – Plano Pedagógico do Curso, instrumento de concepção de ensino e aprendizagem de um curso e apresenta as características de um projeto.
- TWh - Terawatt-hora, unidade de medida de energia
- DDoS - Um ataque de negação de serviço, é uma tentativa de tornar os recursos de um sistema indisponíveis para os seus utilizadores.
- QR Code - Quick Response Code, é um código de barras bidimensional que pode ser facilmente escaneado usando a maioria dos telefones celulares equipados com câmera
- BTC – abreviação de *bitcoin*
- PL - Projeto de lei, um tipo de proposta normativa submetida à deliberação de um órgão legislativo, com o objetivo de produzir uma lei.
- CVM – Comissão de valores mobiliários, tem a finalidade de disciplinar e fiscalizar o mercado de valores mobiliários.

SUMÁRIO

1. INTRODUÇÃO

Há milhares de ano, as transações comerciais ocorriam por meio de troca de mercadorias – o escambo, um método que até então funcionava. Com o passar dos anos foi desenvolvido um sistema mais eficiente e estável para as negociações, sistema esse que utilizava o conceito de “moeda”, um padrão de valor monetário (LUIZ, 2014). Neste contexto, a moeda tem como função servir como meio de troca.

Atualmente, com a evolução da tecnologia, muitas transações comerciais são realizadas através da internet. De acordo com Nakamoto:

> Estas transações são realizadas quase que exclusivamente com a participação de uma instituição financeira atuando como mediadora, uma terceira parte. Enquanto este sistema funciona bem para a maioria das transações, ele ainda apresenta algumas falhas para a realização de transação de pequenos valores. O custo da mediação aumenta os custos das transações, limitando o valor mínimo de transações e diminuindo o número de pequenas transações via internet. (NAKAMOTO, 2008, p. 1).

Considerando esse contexto, foi criado, em 2008, o *Bitcoin*[1]. Segundo Nakamoto (2008), em seu artigo intitulado “*Bitcoin: A Peer-to-Peer Electronic Cash System*”, o *Bitcoin* é uma moeda virtual e descentralizada, ou seja, não é uma moeda física e nem controlada por nenhum banco central.

O *Bitcoin* é produzido de forma descentralizada por milhares de computadores, mantidos por empresas que fornecem a capacidade de suas máquinas para a criação do *Bitcoin* e validação de transações, em um processo chamado de mineração (ANTONOPOULOS, 2014). A rede *Bitcoin* utiliza a arquitetura de redes de computadores *peer-to-peer,* na qual cada um dos nós da rede funciona tanto como cliente tanto quanto servidor. Para proteger a rede *Bitcoin*, é utilizado o protocolo *PoW*[1] (*Proof-of-work*), que previne a rede de ataques cibernéticos. O *Bitcoin* utiliza

[1] Bitcoin é uma moeda virtual descentralizada, criada por Satoshi Nakamoto. Em português, significa “moeda bit”. Sendo *coin* (moeda) e *bit* (dígito binário). A moeda também é expressada pelo símbolo BTC. (ULRICH, 2014).

ainda a tecnologia *Blockchain*, um sistema de banco de dados distribuído. (NAKAMOTO, 2008).

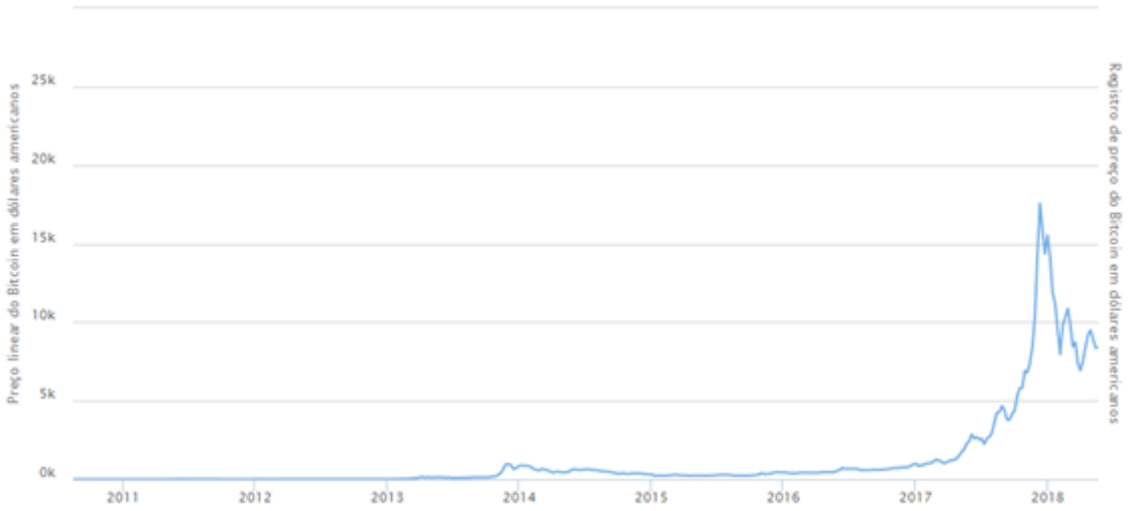
O *Bitcoin* teve uma valorização exorbitante desde que foi criado, em 2008. A título de exemplo, somente nos últimos 5 anos o preço da moeda teve um aumento em 760% (COINMARKETCAP, 2018). Isto inspirou a criação de outras criptomoedas, como o Ethereum, Litecoin, Ripple, Aragon, entre outras. Segundo o site coinmarketcap (coinmarketcap.com, 2018), estas moedas, juntas, possuem atualmente uma capitalização de mercado de mais de 300 bilhões de dólares, após terem atingido um pico de mais de 700 bilhões em janeiro de 2018. Devido à sua alta volatilidade, o *Bitcoin* passou a ser frequentemente classificado como um ativo financeiro, o que se afasta de seu propósito original, que era de atuar como moeda de troca em transações econômicas. Além disso, ainda causa incertezas acerca da sua empregabilidade e se seu uso é vantajoso frente aos meios de pagamentos tradicionais.

Sendo assim, o presente trabalho tem como objetivo realizar um estudo investigativo acerca da utilização do *Bitcoin* como moeda e os fatores que levam ao seu uso pela sociedade contemporânea.

1.1 Justificativa

O *Bitcoin* ganhou grande visibilidade nos últimos anos, principalmente devido à sua grande valorização. A moda virtual segue a lei da oferta e demanda, ou seja, quanto maior for sua procura, maior será a sua cotação. Segundo o site coinmarketcap (coinmarketcap.com, 2018), quando foi lançado no mercado, o *Bitcoin* valia tecnicamente US$ 0. Em 2010, 1 ano após seu lançamento, chegou a custar US$ 0,39. Em 2013, chegou a ser negociado por US$ 1.200,00. Mais recentemente, em 2018, atingiu o ápice de sua valorização, com sua unidade sendo comercializada por mais de US$ 20.000,00 em algumas corretoras.

Gráfico 1 - Valorização do *Bitcoin* nos últimos 8 anos



Fonte: Buy bitcoin worldwide, https://www.buybitcoinworldwide.com/pt-br/preco/

Essa alta valorização do *Bitcoin* chamou a atenção da mídia e de algumas grandes empresas, como a Dell e a PayPal, que passaram a aceitá-lo como meio de pagamento. De acordo com o site coinmap (coinmap.org, 2018), mais de 13.000 locais já o aceitam como meio de pagamento.

Devido à grande popularização da moeda, alguns países já reconhecem o *Bitcoin* como meio de pagamento legítimo, como por exemplo a Alemanha, onde as pessoas podem utilizar o *bitcoin*[2] para realizar suas transações sem pagar impostos.

Apesar de alguns países já o aceitarem como meio de pagamento, o *Bitcoin*, principalmente devido à sua alta volatilidade e seu modo descentralizado de operar, causa dúvidas e medo em governos de diversos países, que em alguns casos chegam até mesmo a considerá-lo ilegal, como é o caso na Bolívia e no Equador. No Brasil, ainda não foi promulgada nenhuma lei no sentido de regulamentá-lo, embora também não seja proibido.

Em relação aos objetivos do curso de Gestão da Tecnologia da Informação, os itens do PPC[2] (Plano Pedagógico do Curso), que se relacionam com o tema e que justificam a presente pesquisa são:

[2] Para fins explicativos, *bitcoin* com “b” minúsculo se refere à unidade monetária do *Bitcoin*. Já o *Bitcoin* com “b” maiúsculo, se refere à rede Bitcoin.

> - Contribuir para a democratização do acesso à informação de qualidade através da formação de profissionais éticos, críticos, autônomos e atualizados para atuar na área.
>
> - Estimular o espírito crítico, o empreendedorismo e o relacionamento social cooperativo, essenciais a formação de agentes de transformação da sociedade.
>
> - A formação de recursos humanos para o gerenciamento das tecnologias da informação, com vistas a atender as necessidades da sociedade.
>
> - Desenvolver competências para a tomada de decisões estratégicas sobre a adoção de tecnologias da informação de modo alinhado às necessidades do negócio. (IFSC, 2018, p. 5)

Considerando tudo que foi abordado até aqui no presente trabalho, a pesquisa busca contribuir no sentido de entender o funcionamento da rede *Bitcoin* e investigar sua utilização na sociedade contemporânea, sendo, desta maneira, uma pesquisa útil ao curso e à sociedade.

1.2 Problemática

O *Bitcoin* surgiu com o propósito de ser uma moeda virtual e descentralizada, de modo que as pessoas ficassem menos dependentes de instituições financeiras para realizar suas transações econômicas (NAKAMOTO, 2008). Louw (2015), que já foi nomeado ao prêmio Nobel da Paz, diz que “todas as pessoas informadas precisam conhecer o *bitcoin*, pois ele pode ser um dos acontecimentos mais importantes do mundo”.

Por outro lado, por ser uma tecnologia nova, intangível e ter um preço muito volátil, o *Bitcoin* desperta muita desconfiança. Conforme Buffett (2018), um dos empresários de maior sucesso no mundo, “o *Bitcoin* é uma verdadeira bolha”.

A partir da divergência de opiniões sobre o *Bitcoin* e da existência de dúvidas quanto ao seu funcionamento e sua utilização, tem-se a seguinte pergunta norteadora desta pesquisa: de que forma o *Bitcoin* pode ser utilizado na sociedade contemporânea?

1.3 Objetivos

1.3.1 Objetivo Geral

- Investigar e analisar a utilização do *Bitcoin* na sociedade contemporânea, tendo em vista as funções básicas de uma moeda.

1.3.2 Objetivos Específicos

- Compreender o funcionamento da rede *Bitcoin;*
- Identificar os fatores que influenciam o uso da criptomoeda;
- Identificar as vantagens e desvantagens do *Bitcoin* em comparação a padrões monetários.

2. REFERENCIAL TEÓRICO

Visto que o *Bitcoin* é uma *cryptocurrency* (moeda virtual), este capítulo fará um breve histórico dos conceitos relacionados à moeda, assim como suas funções básicas, para uma melhor contextualização do tema.

Além disso, também serão abordados, neste capítulo, temas essenciais para a pesquisa referentes ao *Bitcoin*.

2.1 Moeda

2.1.1 História da Moeda

Em civilizações primitivas, não existia o dinheiro como existe hoje. Tudo era produzido para a própria subsistência do grupo, e não existiam relações comerciais. Conforme foi aumentando a população existente, aumentou também a produção de produtos específicos, como sapatos, roupas e variados tipos de alimentos. O excesso da produção era então trocado com tribos vizinhas, em um processo conhecido por Escambo (ANGLO, 2014).

Estas trocas eram feitas diretamente, sem nenhuma referência externa de valor, de modo que a equivalência em mercadorias era negociada a cada transação. A medida em que as transações comerciais foram se intensificando, este modelo se tornou inviável, uma vez que ocorria muitas trocas injustas. (ANGLO, 2014). Foi então que algumas mercadorias passaram a servir como referência para as negociações, sendo chamadas de moeda-mercadorias. (NASCIMENTO, 2014).

Com o desenvolvimento de companhias de transporte, intensificou-se o número de trocas entre diferentes povos, de modo que se torna necessário que as moedas sejam feitas de material durável e de pequeno tamanho, para facilitar o transporte. Começam então a ser fabricadas moedas de diversos materiais, como madeira, pedra e metal. As moedas de metal se destacaram por algumas de suas características, como a raridade e beleza. No Século XV A.C surgem as primeiras moedas parecidas com as que temos atualmente. (BRASILESCOLA, 2018).

2.1.2 Funções da Moeda

De acordo com Hubbard e O'Brien (2010), "a definição econômica de moeda é qualquer ativo que as pessoas estão dispostas a aceitar em troca de bens e serviços ou pelo pagamento de dívidas".

A moeda possui 3 funções básicas, sendo elas: meio de troca, unidade de conta e reserva de valor. (NUNES, 2016).

A moeda como meio de troca representa a sua capacidade de ser utilizada como meio de pagamento para a compra de bens ou serviços. (NUNES, 2016). Como exemplifica Hubbard e O'Brien (2010), "quando o supermercado local aceita sua nota de US$5 em troca de pão e leite, a nota de US$5 está servindo como um meio de troca comercial".

A função de unidade de conta se refere ao fato da moeda fornecer um padrão para que as mercadorias sejam cotadas no mercado, ou seja, ser o instrumento pelo qual os valores das mercadorias são medidos. (NUNES, 2016). Segundo Hubbard e O'Brien (2010), esta função traz benefício, pois "reduz a necessidade de cotar muitos preços diferentes no comércio".

De acordo com Montoro:

> "[...] as funções da moeda como meio de troca e reserva de valor são inseparáveis, [...] Segundo Laidler (1969), a grande questão é saber se os motivos de transação são suficientes para elaborar isoladamente uma teoria de demanda de moeda. Aparentemente, não. A função de reserva de valor e, portanto, demanda de moeda como um ativo é indissociável da função meio de troca." (MONTORO, 1982, p.5, apud CASTAN, 1985, p.86)

A função de reserva de valor se refere à possibilidade da moeda ser guardada de forma a transferir a capacidade de compra para o futuro, ou seja, permitir que o poder de compra se mantenha com o tempo. (NUNES, 2016). Além disto, a reserva de valor é uma forma de se medir a riqueza. (HUBBARD E O'BRIEN, 2010).

2.2 *Bitcoin*

2.2.1 Definição de *Bitcoin*

O *Bitcoin* é a primeira moeda digital descentralizada do mundo, criada por Satoshi Nakamoto. Ela teve seu *White Paper*[3] publicado em um fórum em 2008, com seu lançamento em código aberto para o público em geral em janeiro de 2009. Ela é produzida por milhares de computadores, mantidos por pessoas que emprestam a capacidade de suas máquinas para criar *bitcoins* e registrar todas as transações feitas, em um processo conhecido por mineração (NAKAMOTO, 2008). Para proteger as transações realizadas na rede *Bitcoin*, é utilizada criptografia assimétrica, que funciona com o esquema de chaves públicas e privadas de Whitfield Diffie e Martin Hellman, que permite a autenticidade, privacidade e integridade da rede. (NAKAMOTO, 2018).

De acordo com Nakamoto (2008, p.1), a ideia da rede *Bitcoin* é ser “um sistema eletrônico de pagamento baseado em criptografia *PoW,* permitindo que duas partes façam transações diretamente entre elas sem a necessidade de uma terceira parte confiável”.

Todas as transações que ocorrem no *Bitcoin* são registradas em uma espécie de livro caixa público e distribuído chamado de *Blockchain* (corrente de blocos), o que nada mais é do que um grande banco de dados público, contendo o histórico de todas as transações relacionadas. (ULRICH, 2014).

Além do processo de mineração, é possível adquirir *bitcoins* comprando-os de corretoras. Os *bitcoins* ficam armazenados em uma espécie de carteira, que pode ser física ou virtual, onde é possível gerenciar *bitcoins.*

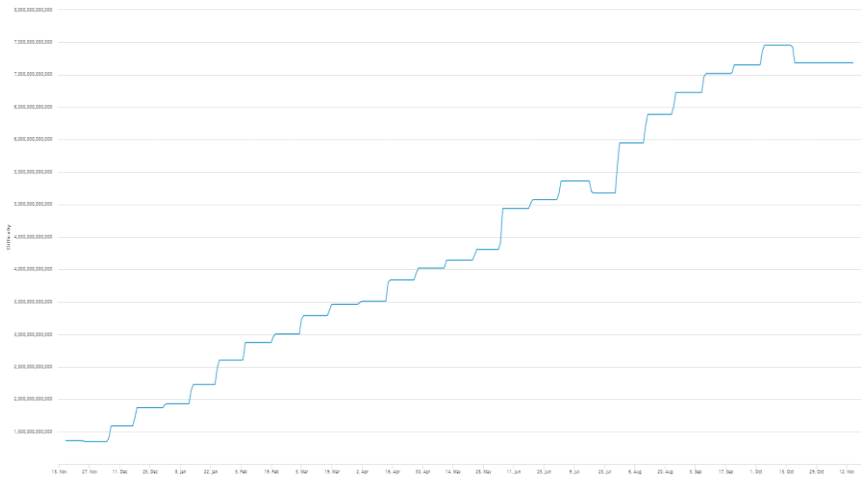
[3] Documento oficial que aprofunda determinado assunto, trazendo seus problemas, causas e, principalmente, sua solução (HUBSPOT, 2018).

2.2.2 Mineração

O processo de “nascimento” do *bitcoin* é chamado de mineração. Este é um processo em que os computadores mineradores[4] conectados à rede *Bitcoin* competem entre si para resolver cálculos matemáticos. Quem ganha, valida um bloco de transações na rede e recebe uma fração da moeda que foi criada no processo. O nível é ajustado pela rede, para que a moeda consiga cumprir o plano de expansão que lhe foi atribuída, que é de ter 21 milhões de unidades até 2140 (ULRICH, 2014). Atualmente já existem mais de 17 milhões de *bitcoins* em circulação. (COINRANKING, 2018).

Quanto mais *bitcoin*s são criados pelo processo de mineração, mais difícil fica sua criação, ou seja, mais cálculos os computadores da rede precisam realizar antes de processar um bloco de *bitcoins.* Ulrich (2014), faz um paralelo entre a mineração e os números primos, uma vez que é relativamente fácil achar os menores, porém a medida em que são encontrados, fica mais difícil de encontrar os maiores. Segue abaixo um gráfico ilustrando o aumento na dificuldade de mineração do *bitcoin* durante o último ano, levando-se em conta que a dificuldade diz respeito a quantidade de cálculos que serão necessários para validar um bloco.

Gráfico 2 - Incremento na dificuldade do processo de mineração do *bitcoin*



Fonte: Blockchain, disponível em <https://www.blockchain.com/pt/charts/difficulty>

[4] Para fins explicativos, quando associado ao bitcoin, mineradores geralmente são as pessoas que possuem as máquinas que fornecem poder de processamento para a rede. Porém em alguns casos, o termo “mineradores” se refere aos próprios computadores que fazem parte da rede

Uma vez que o último *bitcoin* for minerado, os mineradores serão recompensados com taxas de serviço, em vez de novos *bitcoins*. Isso garante que os mineradores ainda tenham um incentivo de manter a rede operando após a extração do último *bitcoin*. (ULRICH, 2014).

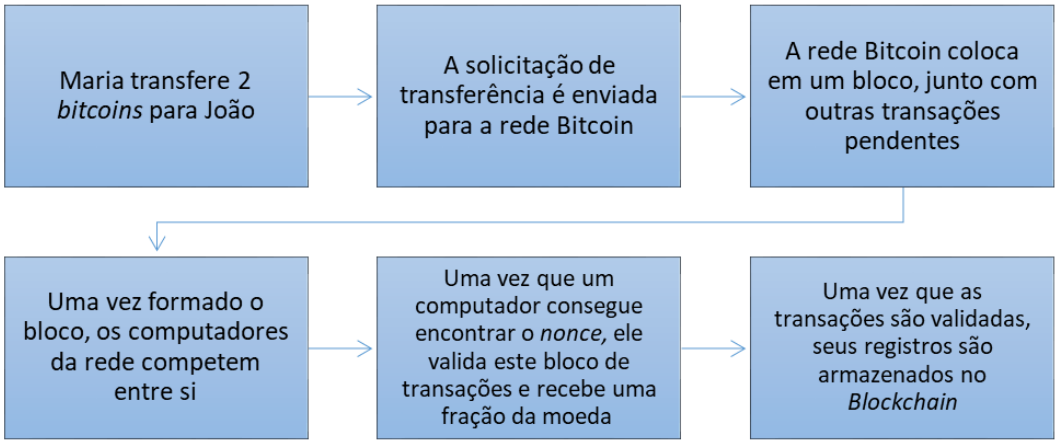
Conforme explica a revista Exame, o processo de mineração do *bitcoin* consiste em:

> [...] decifrar códigos com valores criptografados emitidos pelo software que implementa o algoritmo da criptomoeda e envolve equações matemáticas altamente complexas para encontrar um código, chamado *nonce*. Quem conseguir computar o *nonce* primeiro ganha uma determinada quantidade de *bitcoins*. O “vencedor” e os seus novos *bitcoins* são informados pelo seu nó aos demais para que todos validem e saibam que esses *bitcoins* pertencem a esse minerador. (EXAME, 2017)

O tempo de execução deste processo varia muito, atualmente demorando em média cerca de 30 minutos (BLOCKCHAIN, 2018). Uma vez que a transação é validada, o registro dessa transação é adicionado ao *blockchain,* que armazena o registro de todas as transações já feitas na rede *Bitcoin.* Nenhuma transação envolvendo *bitcoins* é registrada no *blockchain* sem antes passar pelo processo de mineração. (ANTONOPOULOS, 2014).

Para uma melhor compreensão do processo de mineração, apresenta-se, a seguir, um fluxograma exemplificando o processo:

Figura 1 - Fluxograma do processo de mineração



Fonte: Elaborado pelo autor

A atividade de mineração atingiu a marca total de 29,05 TWh[3] (Terawatt-hora) gastos em novembro de 2017, o que representa 0,13% de toda a energia consumida no mundo. No último ano, essa atividade gastou cerca de US$ 1,5 bilhão em eletricidade. (DIGICONOMIST, 2017).

2.2.3 Blockchain

A tecnologia *Blockchain* surgiu junto com o *Bitcoin*, em 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* é uma plataforma de banco de dados distribuído, ou seja, uma maneira de armazenar de forma imutável dados digitais para que possam ser compartilhados de forma segura entre redes e usuários. Como uma rede *peer-to-peer*, combinada com um servidor de *data-stamping* distribuído, os bancos de dados *Blockchain* podem ser gerenciados de forma autônoma. Não há necessidade de um administrador – os usuários são os administradores. (CIO, 2017).

A tecnologia *Blockchain* têm 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, visto que todas as transações registradas na blockchain são públicas. (SAMPAIO, et al., 2018).

Segundo Sampaio et al. (2018), o *Blockchain* é uma tecnologia disruptiva, pois "[...] cria digitalmente uma entidade de confiança descentralizada, eliminando a necessidade de uma terceira parte de confiança."

Desta forma, podemos comparar o *Blockchain* à um livro caixa, onde estão inseridas todas as transações feitas em *bitcoin*, desde a primeira, que foi realizada em 2009, até hoje.

2.2.4 Segurança

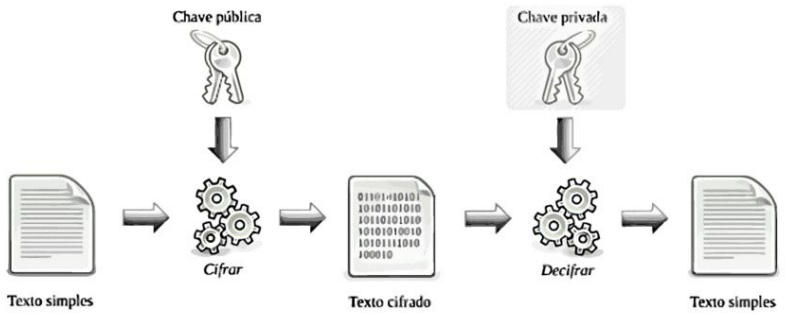
2.2.4.1 Criptografia

Segundo Pereira (2016), a criptografia é um conjunto de técnicas empregadas para cifrar mensagens, as quais são decifradas por meio de uma chave. Desta forma, somente emissor e emissário conseguem ter acesso ao conteúdo enviado, enquanto que terceiros apenas conseguem visualizar códigos aleatórios sem conseguir extrair nada daquilo.

Para que os *bitcoins* sejam transferidos de forma segura, a rede *Bitcoin* utiliza a criptografia assimétrica. (NAKAMOTO, 2008). A diferença entre criptografia simétrica e assimétrica é que na simétrica os algoritmos simétricos de uma chave (um pedaço de informação que controla a operação de um algoritmo) são usados tanto para criptografar quanto para descriptografar, enquanto que na criptografia assimétrica há duas chaves, sendo uma a chave pública, para encriptar as mensagens, e a privada, para desencriptar. As chaves são completamente independentes uma das outras. (ANTONOPOULOS, 2014).

Para uma melhor exemplificação do esquema de chave dupla, segue abaixo uma ilustração do processo:

Figura 2 - Esquema de chave dupla



Fonte: Research Gate, disponível em <https://www.researchgate.net/figure/Figura-33-Processo-da-criptografia-assimetrica-Adaptado-de-Pires-2010_fig3_298421681>

2.2.4.2 Proof-of-work

O princípio central do *Bitcoin* é a descentralização, e isto tem suas implicações na segurança. Em um modelo centralizado, como um banco tradicional, a responsabilidade do sistema é do próprio banco, diferentemente de um sistema descentralizado como o *Bitcoin*, onde esta responsabilidade é de todos os usuários finais. (ANTONOPOULOS, 2014).

Para implementar o modelo descentralizado na rede *Bitcoin* foi utilizado o protocolo *Proof-of-Work* (*PoW),* utilizado na prevenção de ataques cibernéticos, como DDOS e Spam (NAKAMOTO, 2008). Ainda segundo Nakamoto:

> [...] O protocolo *PoW* envolve escanear um valor utilizando a função *hash*[5], como a função SHA-256, onde o *hash* começa com *n* bits 0. O trabalho médio requerido é exponencial ao número de bits 0 e podem ser verificados utilizando um único *hash*. (NAKAMOTO, 2008, p.3).

Na rede *Bitcoin*, o protocolo PoW também é utilizado para garantir que os computadores da rede estejam realmente gastando seu processamento em prol da rede. (ANTONOPOULOS, 2017).

2.2.4.3 Carteiras

Para receber, armazenar, proteger e gastar *bitcoins* é necessário possuir uma espécie de carteira. Esta carteira é meramente um aplicativo, site ou dispositivo que contém uma chave privada que permite acessar o endereço onde os *bitcoins* do usuário estão guardados (TUWINER, 2018). As principais carteiras de *bitcoins* são a carteira de hardware e a carteira online.

Uma carteira de hardware é um dispositivo físico eletrônico, desenvolvido com o propósito de proteger *bitcoins*. Para que os *bitcoin*s destas carteiras possam ser gastos, eles precisam estar conectados ao computador, telefone ou tablete. Carteiras de hardware mantém as chaves privadas em um ambiente off-line, sendo desta maneira protegidas de *malwares* e cibercriminosos. Para ter acesso a carteira de hardware, seria necessário roubar a carteira em si. (TUWINER, 2018). Segue abaixo uma ilustração de uma carteira de hardware.

Figura 3 - Carteira de Hardware

Fonte: Carteira Digital, disponível em <http://carteiradigital.eu>

Já as carteiras web armazenam as chaves privadas online, onde a carteira é criptografada por uma senha escolhida pelo usuário. Pelo fato de ser online, ela possui um menor nível de segurança quando comparado com as carteiras de hardware. (TUWINER, 2018)

2.2.4.4 Privacidade

O modelo bancário tradicional atinge um nível de privacidade ao limitar o acesso à informação ao partes envolvidas e o terceiro de confiança. A necessidade de anunciar publicamente todas as transações da rede *Bitcoin* exclui esse método, mas a privacidade ainda pode ser mantida quebrando-se o fluxo de informações de outro modo: mantendo as chaves públicas anônimas. O público pode ver que alguém está enviando uma quantia para outra pessoa, mas sem informações que vinculem a transação a qualquer pessoa. Isto é semelhante ao nível de informação divulgado pelas bolsas de valores, em que o tempo e o tamanho dos negócios individuais, a operação, é tornada pública, mas sem dizer quem eram as partes (NAKAMOTO, 2018).

Como dito no capítulo 2.2.2.1, a rede *Bitcoin* utiliza o esquema de criptografia assimétrica, onde uma chave envia e a outra recebe. De acordo com Nakamoto (2008), o problema do modelo de privacidade do *Bitcoin* é que, caso o dono de uma chave seja descoberto de alguma forma, é possível verificar todas as transações que este usuário realizou na rede.

2.2.4.5 Violação de segurança

O *Bitcoin* apresenta alguns desafios de segurança específicos, uma vez que não é uma referência abstrata de valor, como o saldo de uma conta no banco (ANTONOPOULOS, 2014). Para acessar os *bitcoins* guardados em uma carteira digital, é necessário possuir uma chave, uma sequência de caracteres aleatórios (KELLY, 2015). Se esta chave for perdida ou roubada, não é possível de forma alguma recuperar os *bitcoins.*

Como uma moeda digital, o *Bitcoin* está sujeito a ataques hackers. Enquanto que as carteiras de hardwares não sofrem deste problema, por guardar os *bitcoin*s de modo off-line, as carteiras digitais de *Bitcoin* podem ser protegidas por criptografia, no momento em que o usuário ativá-la. Se o usuário não cifra sua carteira, os *bitcoins* podem ser roubados por *malwares*. (ULRICH, 2014).

Os usuários que optam por deixar seus *bitcoins* em carteiras online de casas de câmbio também estão sujeitos a perdê-los. Em 2012, hackers furtaram 24 mil BTC[5] (então avaliados em 250 mil dólares) de uma casa de câmbio chamada *Bitfloor.* (COLDEWEY, 2013). Em 2013, houve uma série de ataques DDoS[4] contra a popular casa de câmbio Mt.Gox (KELLY, 2013). Nestes casos, as casas de câmbio chegam a ressarcir seus clientes pelos *bitcoins* roubados (ULRICH, 2014), porém, em outros, como o ataque a Youbit em 2017, os usuários têm que arcar com o prejuízo. (TECMUNDO, 2017).

Evidentemente, muitos dos riscos de segurança enfrentados pelo *Bitcoin* são parecidos aos que as moedas tradicionais também enfrentam. Cédulas de dinheiro podem ser perdidas, contas podem ser *hackeadas* e bancos podem ser assaltados. Desta forma, os usuários da rede *Bitcoin* devem aprender e preparar-se contra estes riscos, da mesma forma que fazem com outras atividades financeiras. (ULRICH, 2014).

3. PROCEDIMENTOS METODOLÓGICOS

Neste capítulo serão mostrados os procedimentos metodológicos que foram utilizados para a elaboração desta pesquisa. Serão apresentados neste capítulo a caracterização e as etapas da presente pesquisa.

3.1 Caracterização da Pesquisa

Referente à sua aplicação, este trabalho de conclusão de curso está caracterizado como pesquisa documental e bibliográfica. Segundo Gil (2002), a pesquisa bibliográfica é desenvolvida com base em materiais já elaborados, principalmente artigos, livros e dissertações. Já a pesquisa documental, segundo Guba & Lincoln (1981), consiste em um intenso e amplo exame de diversos materiais que não foram utilizados para nenhum trabalho de análise, ou que podem ser reexaminados, buscando-se outras interpretações ou informações complementares, chamados de documentos.

Referente à abordagem, esta é uma pesquisa qualitativa, pois para Lüdke e André (1986), na abordagem qualitativa são analisados os dados obtidos com os materiais durante a pesquisa.

Referente ao objetivo, esta pesquisa caracteriza-se como exploratória e descritiva. Exploratória pois tem como objetivo aprofundar os conhecimentos acerca do funcionamento da rede *Bitcoin.* Descritiva, pois investiga a utilização do *Bitcoin* na sociedade contemporânea.

3.2 Fontes de Dados

Segundo Gil (2002), as fontes devem fornecer respostas adequadas ao entendimento e/ou resolução do problema.

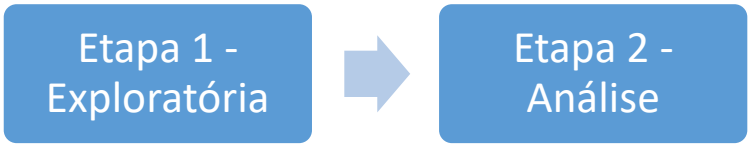
As principais fontes utilizadas nesta pesquisa foram livros, artigos, documentos e ferramentas associadas à rede *Bitcoin*.

3.3 Etapas da Pesquisa

Apresentam-se nesta seção os passos utilizados no desenvolvimento da pesquisa. Esta pesquisa será composta por duas etapas, sendo elas: exploratória e análise.

Abaixo, se especifica estes passos em ordem cronológica.

Figura 3 - Etapas da pesquisa



Fonte: Elaborada pelo autor

Etapa 1 - Exploratória: Nesta etapa, procedeu-se o estudo exploratório sobre a base que sustenta esta pesquisa, que no caso é o *Bitcoin,* com o objetivo de obter um profundo conhecimento acerca do seu funcionamento e da sua utilização na sociedade.

Etapa 2 - Análise: Nesta etapa foi realizado um comparativo entre os atributos do *Bitcoin* e de padrões monetários, como o ouro e o papel-moeda. Além disto, nesta etapa foi analisado se o *bitcoin* cumpre as três funções básicas de uma moeda.

4. BITCOIN NA SOCIEDADE CONTEMPORÂNEA

4.1 Compra e venda de *Bitcoins*

Devido à forma como o algoritmo da rede *Bitcoin* funciona, onde, quanto mais *bitcoin*s são minerados, mais difícil fica minerá-los, esta atividade está praticamente restrita a grandes empresas de mineração (KELLY, 2017). Atualmente, o modo mais fácil de comprar/vender *bitcoins* são através de corretoras de *bitcoin*.

Corretoras de *bitcoins* são plataformas onde é possível comprar e vender *bitcoin*s, além de trocá-lo por outras moedas virtuais, como Ethereum, Ripple, Litecoin, Aragon, entre outras. Estas plataformas não realizam a venda direta de *bitcoins*, elas apenas facilitam o contato entre as pessoas que querem comprar ou vender. (FOXBIT, 2018).

Para se cadastrar na plataforma e poder realizar as operações de compra e venda, é necessário enviar, em ambiente virtual, documentos que comprovem a identidade da pessoa. Este processo foi adotado para evitar que pessoas utilizem a plataforma para realizar atividades ilícitas, como lavagem de dinheiro. Este é um procedimento adotado por corretoras no mundo todo.

Uma vez cadastrado, o usuário pode movimentar seus *bitcoin*s para sua carteira online pessoal dentro da plataforma. Caso queria comprar *bitcoin*s dentro da plataforma, o usuário deposita o valor desejado na conta da corretora e, após a dedução de taxas de serviço da corretora, o saldo é depositado na conta daquele usuário. (FOXBIT, 2018).

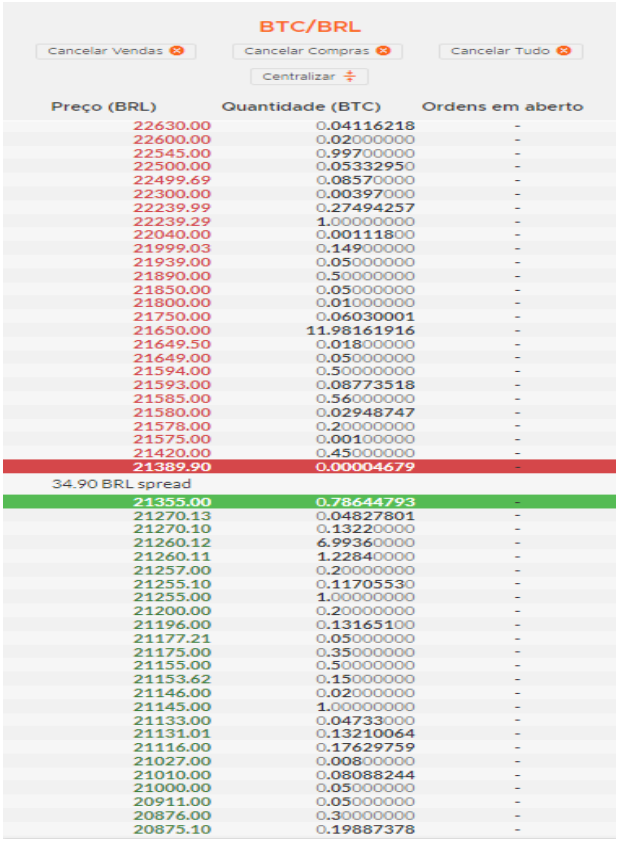
Após o saldo depositado na conta, o usuário pode começar a realizar *trades*. O *trade,* em tradução direta, significa troca, neste caso a troca de *bitcoin*s pela moeda local, e *é* realizado de forma similar ao do mercado de ações, onde os usuários colocam ordens de compra ou venda. Para ilustrar o processo, segue, abaixo, uma a imagem da simulação da ordem de compra de 100 *bitcoin*s.

Figura 4 - Simulação de compra de *bitcoin*s

Fonte: FoxBit, disponível em <https://app.foxbit.com.br/trade.html>

Após efetuada, a ordem de compra fica em um “livro de vendas” da plataforma, esperando que alguém aceite esta oferta. Uma vez aceita, a operação de compra/venda é realizada. (FOXBIT, 2018). Desta forma, o preço do *bitcoin* é definido pela lei da oferta e demanda (ULRICH, 2014). A seguir, apresenta-se uma ilustração do livro de ofertas da corretora de *bitcoins* FoxBit:

Figura 5 - Livro de ofertas FoxBit



Fonte**:** Foxbit, disponível em <https://app.foxbit.com.br/trade.html>

São comuns notícias de problemas técnicos nestas plataformas, ocasionando perdas financeiras para os usuários. A FoxBit, por exemplo, chegou a ficar 14 dias fora do ar durante o ano de 2018, em um período em que o valor do *Bitcoin* estava caindo. (INFOMONEY, 2018).

Atualmente, o Brasil ocupa o 8° lugar entre os países com maior volume de negociações envolvendo *bitcoins* no mundo. (*BITCOIN* AVARAGE, 2018). As corretoras mais populares no país são a FoxBit e a Mercado *Bitcoin* que, juntas, movimentaram cerca de 108.000 *bitcoins* durante 2018. (PORTAL DO *BITCOIN*, 2018).

4.2 Transferência de *bitcoin*s

Uma vez que se possui saldo na carteira de *bitcoins*, é possível transferi-lo diretamente para qualquer outra.

A rede *Bitcoin* trabalha com o esquema de chaves duplas, uma pública e outra privada. A chave pública é utilizada para receber *bitcoins*, enquanto que a chave privada é utilizada para enviar. (NAKAMOTO, 2008).

Toda carteira *Bitcoin* possui um endereço, que, normalmente, é formado por 26 caracteres, incluindo letras e números. Este endereço também pode ser obtido através de um QR code[5]. Para receber, é necessário apenas comunicar o número da carteira. Para enviar *bitcoin*s, basta digitar a quantidade e o endereço de destino. Abaixo, uma ilustração da tela de envio de *bitcoins.*

Figura 6 - Tela de envio de *bitcoin*s

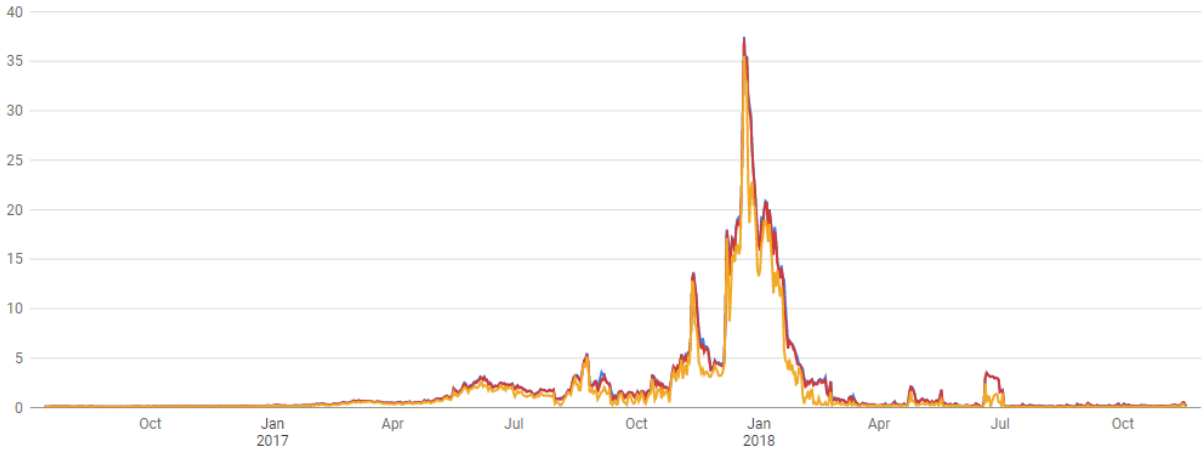
Fonte: ilemone1, disponível em <https://ilemone1.wordpress.com/category/bitcoin-portugal/>

4.3 Influenciadores no uso do *Bitcoin*

O *Bitcoin* foi criado como objetivo de eliminar terceiras partes de transações financeiras, diminuindo, assim, seus custos de transação. (NAKAMOTO, 2008). Porém, devido à alta valorização da moeda, não é mais vantajoso seu uso em pequenas transações.

Em toda transação envolvendo *bitcoin* é cobrada uma taxa, chamada de “taxa do minerador”, que pode variar dependendo da prioridade. Porém, em geral, é de 0.0005 BTC[6] a 0.001 BTC (BLOCKCHAIN, 2018). Quando o *bitcoin* foi criado, esse valor era insignificante. Mas, com a valorização do *bitcoin* em relação ao dólar e outras moedas nacionais, isto mudou. Considerando que a cotação atual do *bitcoin* é de $5600.00, o custo de transação média atual é de $3 (BITCOIN FEES, 2018), o que torna insatisfatória sua utilização em pequenas transações. Abaixo, segue um gráfico com a variação da taxa de transação na rede *Bitcoin* nos últimos dois anos.

Gráfico 3 - Variação da taxa de transação na rede *Bitcoin* nos últimos 2 anos



Fonte: Bitcoin Fees, disponível em <https://bitcoinfees.info>

Considerando o fato de que seu principal atrativo era a redução dos custos de transação, uma das grandes dúvidas que se tem quanto ao *bitcoin* é o porquê de utilizá-lo, ao invés da moeda corrente local. Segundo Ulrich (2014), “ajuda se pensarmos que o *Bitcoin* não é necessariamente um substituto às moedas tradicionais, mas sim um novo sistema de pagamentos”.

O *Bitcoin* pode ajudar, por exemplo, pessoas vivendo em países onde o controle de capital é bem estrito, uma vez que o número total de *bitcoins* é limitado e não pode ser manipulado. Além disso, transações envolvendo *bitcoins* são muitos mais difíceis de se rastrear (ULRICH, 2014).

Em países em que a moeda nacional está sofrendo forte inflação ou deflação, a demanda por *bitcoins* é maior. (ULRICH, 2014). Na Argentina, por exemplo, muitos argentinos adotaram o *Bitcoin* como resposta às altas taxas de inflação e ao rigoroso controle de capitais (MATONIS, 2013). Já na Venezuela, a população está utilizando *bitcoins* para poder comprar no exterior aquilo que não encontram no mercado nacional, além de os utilizarem para o envio de remessas para familiares que deixaram o país, e vice-versa. (G1, 2018).

Pessoas em situação de opressão e emergência também podem beneficiar-se da privacidade financeira que o *Bitcoin* proporciona. Segundo Ulrich:

> Há muitas razões legítimas pelas quais pessoas buscam privacidade em suas transações financeiras. Esposas fugindo de parceiros abusivos precisam de alguma forma de discretamente gastar seu dinheiro sem ser rastreadas. Pessoas procurando serviços de saúde controversos desejam privacidade (ULRICH, 2014, p.27).

Apesar de ser apontado como um dos pontos positivos do *Bitcoin*, o anonimato também faz com que governos tenham resistência à moeda, uma vez que é mais fácil praticar atividades ilícitas utilizando o *bitcoin*, como lavagem de dinheiro e compra/venda de produtos no mercado negro.

4.4 Legislação e regulação

Pode parecer contraditório o tópico de regular o *Bitcoin*, já que a moeda foi lançada justamente com um dos objetivos sendo o de eliminar o controle do governo sobre as transações financeiras. Porém, de acordo com Ulrich (2014), uma vez que a regulação do *Bitcoin* tem influência direta na adesão do uso da moeda, é de suma

importância para a consolidação do *Bitcoin* a questão sobre a sua regulação ao redor do mundo.

Com o aumento da popularidade do *Bitcoin,* causado, principalmente, pela sua valorização, muitos países começaram a se posicionar em relação ao tratamento jurídico que deve ser dado à moeda (ULRICH, 2014). Embora nota-se que, em nível global, ainda há carência de legislação específica sobre a moeda, muitos países já se posicionaram mediante seus respectivos órgãos fiscais quanto ao tratamento jurídico do *Bitcoin* (PEREIRA, 2016). A seguir, é apresentado o tratamento recebido pelo *Bitcoin* em alguns países:

4.4.1 Brasil

No Brasil, não há nenhuma lei especifica sobre moedas virtuais. Porém, há um projeto de lei de 2015 (PL[7] 2303/2015) do deputado Aureo, que defende a regulamentação das criptomoedas. O projeto está, atualmente, sendo avaliado por uma comissão especial. (R7, 2017)

Apesar do *Bitcoin* não possuir nenhum amparo jurídico específico até o presente momento, o posicionamento oficial do governo é de que é preciso declará-lo no imposto de renda, uma vez que, por regra, pessoas físicas precisam declarar todos os bens e direitos acima de R$ 1 mil. (EPOCA, 2018).

Além disso, a CVM[8] proibiu a compra de criptomoedas por fundos de investimentos, afirmando que tais criptomoedas não podem ser qualificadas como ativos financeiros. (ESTADAO, 2018).

4.4.2 Canadá

O *Canada Revenue Agency (CRA)*, órgão máximo tributário do Canadá, declarou que a aquisição de bens com *bitcoin*s não exime o estabelecimento comercial de pagar o *Good and Services Tax* (GST) e o *Harmonized Sales Tax* (HST), principais impostos indiretos no Canadá. (PEREIRA, 2016).

Na mesma declaração, o CRA afirmou que o ganho de capitais na venda de *bitcoins* deve ser tributado pelo *Income Tax*, o que seria equivalente ao imposto de renda brasileiro. (CANADA REVENUE AGENCY, 2013).

4.4.3 Estados Unidos

Nos Estados Unidos, o *Internal Revenue Service (IRS)* classificou o *bitcoin* como propriedade para fins tributários, descartando qualquer equiparação entre a moeda virtual e a moeda nacional ou estrangeira (INTERNAL REVENUE SERVICE, 2014). Desta forma, todo ganho de capital no patrimônio do contribuinte através de transações envolvendo *bitcoins* deve ser tributado a título de *Income Tax* – imposto direto que incide sobre o acréscimo patrimonial. (PEREIRA, 2016).

Além disto, a atividade de mineração também é taxada nos Estados Unidos. Sempre que um minerador tem sucesso ao minerar uma fração do *bitcoin*, ele deve realizar a conversão dos *bitcoins* em dólares daquele momento e declarar este valor, de acordo com a legislação local. (INTERNAL REVENUE SERVICE, 2014).

4.4.4 Bolívia

Em 2014, o banco central da Bolívia baniu oficialmente moedas não reguladas pelo governo, incluindo moedas virtuais como o *Bitcoin*. A justificativa dada pelo governo para a proibição é de que estavam tentando proteger os consumidores de potencial perda financeira, haja vista a alta volatilidade do *bitcoin*. (BITCOINREGULATION, 2018).

4.4.5 Alemanha

Na Alemanha, o *Bitcoin* é legalizado e reconhecido como meio de pagamento. (EPOCA, 2018).

Segundo o Ministério das Finanças do País, o *Bitcoin* é um meio de pagamento legitimo e que não deve ser taxado. Desta forma, o *bitcoin* e outras moedas virtuais podem ser usadas para comprar itens do cotidiano. (INFOMONEY, 2017).

A decisão foi tomada apoiando-se em uma resolução do Tribunal de Justiça Europeu de 2015, acerca dos impostos sobre o valor acrescentado (IVA), que abriu um precedente para as nações da União Europeia tributarem o *bitcoin*, oferecendo isenções para alguns tipos de transações. (INFOMONEY, 2017).

4.4.6 Arábia Saudita

Em 2018, a Arábia Saudita anunciou que o *Bitcoin* e outras moedas virtuais são ilegais no país. O regulador citou as consequências negativas e os altos riscos aos quais os usuários de criptomoedas estão expostos como a principal razão para a proibição. O movimento seguiu uma série de comentários negativos feitos pelo príncipe saudita Al-Waheed bin Talal em relação às criptomoedas. Ele havia especulado que o *Bitcoin* vai apenas implodir um dia.

5. ANÁLISE DAS PROPRIEDADES E FUNÇÕES DO BITCOIN

Levando-se em conta todo o estudo exploratório realizado até aqui, este capítulo tem como objetivo comparar as propriedades do *Bitcoin* com propriedades de padrões monetários, no caso o ouro e o papel-moeda, e também analisar se o *bitcoin* cumpre as três funções básicas de uma moeda.

5.1 Propriedades

Em relação às suas propriedades, o *bitcoin* apresenta algumas vantagens em relação a padrões monetários, como o ouro e o papel-moeda.

No quesito durabilidade, o *bitcoin* supera tanto o ouro quanto o papel-moeda. Por ser uma moeda digital, o *bitcoin* não sofre alteração espacial ou temporal. (ULRICH, 2014).

Sobre a divisibilidade, o *bitcoin* possui, atualmente, 8 casas decimais (NAKAMOTO, 2008), possuindo uma divisibilidade muito maior do que o papel-moeda e o ouro.

Em relação a maleabilidade, pelo fato do *bitcoin* ser algo intangível, esta propriedade não se aplica a ele, enquanto que o ouro é o elemento conhecido mais maleável. (ULRICH, 2014).

O *bitcoin* apresenta homogeneidade matemática (por definição), sendo praticamente impossível de falsificá-lo, enquanto que o ouro depende de averiguações para comprovar sua pureza. O papel-moeda, apesar de homogêneo, pode ser mais facilmente falsificado. (ULRICH, 2014).

Em relação a oferta, o *bitcoin* é limitado ao número de 21 milhões de unidades (BLOCKCHAIN, 2018), enquanto que o ouro tem uma limitação pela natureza. Já o papel-moeda é ilimitado, embora tenha sua fabricação controlada pelo governo.

Criado justamente para eliminar a necessidade de uma terceira parte, o *bitcoin* não tem dependência de terceiros fiduciários (NAKAMOTO, 2008), como é o caso do papel-moeda e do ouro, que jamais poderiam eliminar terceiros fiduciários. (ULRICH, 2014).

Segue, no quadro abaixo, a exemplificação da comparação de propriedades entre *bitcoin*, ouro e papel-moeda.

Quadro 1 – Comparação de propriedades entre ouro, papel moeda e *bitcoin*.

Propriedade	Ouro	Papel-moeda	*Bitcoin*
Durabilidade	Alta	Baixa	Perfeita
Divisibilidade	Média	Alta	Perfeita
Maleabilidade	Alta	Alta	Incorpóreo
Homogeneidade	Média	Alta	Perfeita
Oferta	Limitada pela natureza	Ilimitada e controlada politicamente	Limitada matematicamente
Dependência de terceiros fiduciários	Alta	Alta	Baixa ou quase nula

Fonte: ULRICH (2014, p.67)

Levando-se em conta a comparação de propriedades entre o *bitcoin,* ouro e o papel-moeda, pode-se dizer que o *bitcoin* é superior aos outros dois.

5.2 Funções de moeda do *Bitcoin*

De acordo como Nunes (2016), as três funções básicas de uma moeda são: servir como meio de troca, servir como unidade de conta e servir como reserva de valor. A seguir, avalia-se se o *bitcoin*, atualmente, cumpre estas funções.

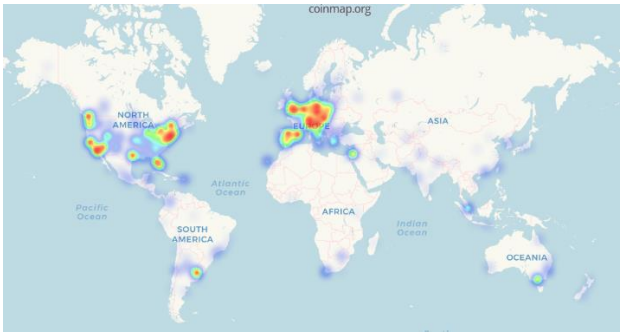
5.2.1 Meio de Troca

Como já abordado neste estudo, meio de troca representa a capacidade da moeda de ser utilizada como meio de pagamento para a compra de bens ou serviços. (NUNES, 2016).

Pode-se afirmar que o *bitcoin* realiza esta função, embora com muito menor liquidez quando comparado com moedas correntes locais. Neste último ano, foram realizadas, em média, 275 mil operações envolvendo *bitcoin*s por dia (BLOCKCHAIN, 2018). Segundo Ulrich (2014), a primeira transação onde o *bitcoin* foi aceito como meio de troca que se tem notícia aconteceu em maio de 2010, quando o programador Lazlo Hanyecz gastou cerca de dez mil *bitcoin*s em duas pizzas.

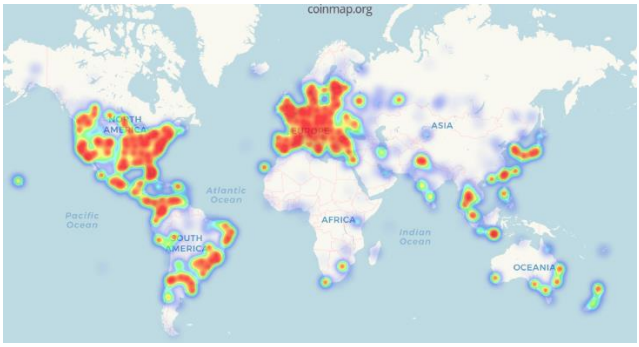
De acordo com o site coinmap.org, há mais de 13 mil estabelecimentos em todo o mundo que aceitam o *bitcoin* como meio de pagamento. O número bruto pode ser pequeno quando comparado ao total de estabelecimentos existentes. Porém, é importante destacar o crescimento no número de lojas que aceitam o *bitcoin* nos últimos anos. A seguir, são mostrados dois mapas de calor ilustrando o aumento significativo no número de lojas que aceitam o *bitcoin*.

Figura 7 - Mapa de calor de lojas que aceitavam o *bitcoin* em 2013



Fonte: Coinmap, disponível em https://coinmap.org

Figura 8 - Mapa de calor de lojas que aceitam o *bitcoin* atualmente



Fonte: Coinmap, disponível em https://coinmap.org

5.2.2 Unidade de conta

De acordo com Nunes (2016), a função de unidade de conta se refere ao fato da moeda fornecer um padrão para que as mercadorias sejam cotadas no mercado, ou seja, ser o instrumento pelo qual os valores das mercadorias são medidos. Segundo Ulrich:

> A terceira função comumente atribuída à moeda – unidade de conta –também é derivada de seu uso como meio de troca. À medida que a liquidez de um bem monetário aumenta e este passa a circular como a principal moeda em uma economia, os indivíduos tenderão a precificar os produtos e serviços e a realizar o cálculo econômico em função dessa moeda. Talvez resida aqui o marco de uma moeda amplamente aceita e desenvolvida, quando ela passa a ser usada não somente como meio de troca, mas também como a unidade de conta geral. (ULRICH, 2014, p.93)

Considerando o fato de que os produtos que compramos e consumimos no dia-a-dia não são cotados em *bitcoins*, é incorreto afirmar que o *bitcoin* realiza a função de unidade de conta. O principal obstáculo para que o *bitcoin* possa realizar esta função é sua alta volatilidade. A título de exemplo, somente no último ano o valor do *bitcoin* caiu cerca de 50% comparado ao dólar (COINMARKETCAP, 2018). Abaixo, temos um gráfico que mostra a variação do preço do Bitcoin comparado ao dólar durante o último ano.

Gráfico 4 - Variação do preço do *bitcoin* durante o último ano

Fonte: Coinmarketcap, disponível em https://coinmarketcap.com/currencies/bitcoin/

Segundo Pereira (2016), o principal responsável por estabelecer uma moeda que servirá como unidade de conta dentro de um país é do governo, uma vez que ele regula e define a moeda corrente local. Somente em países que sofrem de forte crise econômica e sua moeda tem uma alta inflação, como é o caso atual da Venezuela, a moeda corrente do país deixa de ser referência e perde sua função como unidade de conta.

Embora o *bitcoin* não sirva atualmente como unidade de conta, não é impossível que no futuro ele possa vir a realizar esta função. Isto dependerá de alguns fatores, como a sua regulamentação ao redor do mundo, a atenuação de sua volatilidade e a ampliação de seu uso. (ULRICH, 2014).

5.2.3 Reserva de Valor

De acordo com Nunes (2016), a função de reserva de valor se refere à possibilidade da moeda ser guardada de forma a transferir a capacidade de compra para o futuro, ou seja, permitir que o poder de compra se mantenha com o tempo.

Ainda que desperte inseguranças, o *bitcoin* cumpre a função de reserva de valor, a longo prazo. Apesar do gráfico 3 apresentar uma queda considerável no valor do *bitcoin* no último ano, a moeda, desde que foi criada, nunca apresentou prejuízos

financeiros para quem a manteve guardada por mais de 4 anos. A seguir, um gráfico ilustrando a variação do preço do *Bitcoin* desde que foi comercializado.

Gráfico 5 - Variação do preço do *bitcoin* desde seu início

Fonte: buybitcoinworldwide, disponível em https://www.buybitcoinworldwide.com/pt-br/preco

Hubbard e O'Brian (2008) destacam que a reserva de valor também é uma forma de se medir a riqueza. Considerando que uma unidade de *bitcoin* vale, atualmente, cerca de cinco mil e quinhentos dólares e pode ser facilmente convertido em outra moeda, como o dólar ou real, é possível afirmar que o *bitcoin* é um instrumento para mensuração de riqueza.

6. CONCLUSÃO

Neste último capítulo do trabalho buscou-se trazer os resultados obtidos em relação aos objetivos gerais e específicos. Os resultados obtidos foram satisfatórios, uma vez que todos os objetivos do trabalho foram cumpridos. Vejamos, abaixo, as considerações sobre cada um deles, e também a conclusão final do autor do estudo.

6.1 Em relação ao objetivo geral

O estudo da utilização do *Bitcoin* na sociedade contemporânea trouxe resultados surpreendentes. Conforme o capítulo 4.3, apesar do *bitcoin* ter sido criado por Satoshi Nakamoto com a ideia de facilitar as pequenas transações, atualmente ele não é adequado para este fim, visto que a taxa de transação está por volta de US$3, ocasionando sua pouca utilização em transferências de pequeno porte quando comparado a outros meios de pagamentos.

Durante a pesquisa, também foi constatado que o *Bitcoin* atua como meio de troca e reserva de valor, porém não é reconhecido como unidade de conta.

Apesar de não ser utilizado no seu objetivo primário – pequenas transações, o *Bitcoin* se mostrou útil em países que sofrem forte controle estatal, como foi abordado no capítulo 4.3. Devido a sua difícil rastreabilidade, ele pode ser usado pela população para escapar do controle do governo. Em países onde há crise econômica, ele pode ser utilizado para “fugir” da inflação.

6.2 Em relação aos objetivos específicos

No que diz respeito ao objetivo de compreender o funcionamento da rede *bitcoin*, pode-se afirmar que foi completamente alcançado. Durante o estudo, foram abordados todos os conceitos relevantes a respeito do *Bitcoin*, incluindo o processo de mineração, sua criptografia e o *Blockchain*.

No que diz respeito ao objetivo específico de identificar os fatores que influenciam o uso da criptomoeda, pode-se dizer que o objetivo foi concluído. Como

visto no capítulo 4.3, governos autoritários, crises econômicas e o desejo de privacidade são os principais fatores que influenciam no uso do *bitcoin.*

Para o objetivo especifico relativo a identificar vantagens e desvantagens do *Bitcoin* em relação a padrões monetários, pode-se afirmar que o objetivo foi parcialmente atingido. Conforme observado no capítulo 5.1, foram encontradas diversas vantagens nas propriedades do *Bitcoin* sobre o papel-moeda e o ouro. Porém, não foi encontrada nenhuma desvantagem na comparação realizada.

6.3 Considerações finais

Tendo como referência os resultados obtidos, espera-se que este estudo possa servir como base de conhecimento para pessoas que possuam dúvidas quanto ao funcionamento do *Bitcoin*, inclusive pessoas totalmente leigas no assunto. É muito fácil encontrar pessoas que já ouviram falar no *Bitcoin*, porém é raro encontrar pessoas que entendam o seu funcionamento, mesmo que superficialmente. Tendo isto em mente, espera-se este trabalho possa ser utilizado como referência para uma leitura rápida e esclarecedora sobre o *Bitcoin.*

Sobre o futuro do *Bitcoin*, é muito difícil fazer qualquer previsão, pois é uma tecnologia nova e sua consolidação como moeda depende de inúmeros fatores. O que se pode afirmar após o estudo realizado, é que os principais problemas atuais do *Bitcoin* são a sua alta volatilidade e a falta de regulação ao redor do mundo.

Para que o *Bitcoin* venha a ser comumente utilizado como moeda, é necessário haver uma estabilização de seu valor e um entendimento dos governos sobre sua natureza jurídica, pois apenas desta forma ele poderá servir como unidade de conta.

7. REFERÊNCIAS

ANGLO. **Apostila Anglo História**. São Paulo: Editora Anglo, 2014

ANTONOPOULOS, M. Andreas. **Mastering Bitcoin**. 1° Edição. Sebastopol: O'Reilly Media, Inc. 2014

BLOCKCHAIN. Disponível em <https://blockchain.info/markets>. Acesso em 30 de maio de 2018.

BRASIL ESCOLA. **História da Moeda.** Disponível em <https://brasilescola.uol.com.br/historia/historia-da-moeda.htm>. Acesso em 06 de junho de 2018.

BUYBITCOINWORLDWIDE. Disponível em <https://www.buybitcoinworldwide.com>. Acesso em 20 de maio de 2018.

BITCOIN AVARAGE .Disponível em <https://bitcoinaverage.com/en/bitcoin-price/btc-to-usd>. Acesso em 08 de Novembro de 2018.

BITCOIN REGULATION. Disponível em <https://www.bitcoinregulation.world>. Acesso em 16 de novembro de 2018.

CANADA REVENUE AGENCY. **CRA Document nº 2013-0514701I7**. Disponível em: <http://www.canadiantaxlitigation.com/wp-content/uploads/2014/01/2013-0514701I7.txt>. Acesso em:12 de Novembro de 2018.

CASTAN, Nelson B. **O conceito de moeda e processo inflacionário: a necessidade de uma revisão contextual abrangente**. Porto Alegre: Ensaios FEE, 1985.

CIO. **5 princípios básicos do blockchain.** Acesso em 28 de maio de 2018. Disponível em <http://cio.com.br/tecnologia/2017/03/06/cinco-principios-basicos-do-blockchain/>. Acesso em 28 de maio de 2018.

COINDESK. **What is Blockchain Technology?** Disponível em <https://www.coindesk.com/information/what-is-blockchain-technology/>. Acesso em 30 de maio de 2018.

COINMAP. Disponível em <http://coinmap.org/>. Acesso em 27 de maio de 2018.

COINMARKETCAP. Disponível em <https://coinmarketcap.com>. Acesso em 27 de maio de 2018.

COINRANKING. Disponível em <https://coinranking.com>. Acesso em 27 de maio de 2018.

COLDEWEY, Devin. **$250,000 Worth of Bitcoins Stolen in Net Heist**, NBC News, 2012. Disponível em: <http://www.nbcnews.com/technology/250-000-worth-bitcoins-stolen-net--heist-980871>. Acesso em: 11 de outubro de 2018.

DIGICONOMIST. **Bitcoin mining consumes more electricity a year than Ireland.** Disponível em <https://www.theguardian.com/technology/2017/nov/27/bitcoin-mining-consumes-electricity-ireland/ >. Acesso em 28 de maio de 2018.

EPOCA. **Imposto de renda 2018: É preciso declarar bitcoin?** Disponível em <https://epocanegocios.globo.com/Dinheiro/noticia/2018/03/imposto-de-renda-2018-e-preciso-declarar-bitcoin.html>. Acesso em 12 de novembro de 2018.

EPOCA. **Alemanha decide não taxar pagamentos com criptomoedas**. Disponível em <https://www.infomoney.com.br/mercados/bitcoin/noticia/7313971/alemanha-legaliza-criptomoedas-reconhece-bitcoin-como-meio-pagamento>. Acesso em 12 de novembro de 2018.

ESTADAO. **Bitcoins e os desafios para sua regulamentação**. Disponível em <https://politica.estadao.com.br/blogs/fausto-macedo/bitcoins-e-os-desafios-para-sua-regulamentacao/>. Acesso em 12 de novembro de 2018.

EXAME. **Entenda o que é Bitcoin.** Disponível em <https://exame.abril.com.br/mercados/entenda-o-que-e-bitcoin/>. Acesso em 28 de maio de 2018.

G1. **Venezuela inicia a pré-venda da Petro, moeda virtual similar ao bitcoin.** Disponível em <https://g1.globo.com/economia/noticia/venezuela-inicia-a-pre-venda-da-petro-moeda-virtual-similar-ao-bitcoin.ghtml>. Acesso em 12 de novembro de 2018.

GUBA, E; Lincoln, Y. **Effective Evaluation**. São Francisco: Jossey-Bass. 1981

HUBBARD, R. Glenn; Anthony O'Brien. **Introdução a Economia.** 2° Edição. Porto Alegre: Bookman, 2010.

IBGE. **Portal do IBGE**. Disponível em <https://www.ibge.gov.br/>. Acesso em 02 de junho de 2018.

IFSC. **Plano Pedagógico do Curso de Gestão da Tecnologia da Informação.** Disponível em <https://moodle.ifsc.edu.br/pluginfile.php/58896/mod_resource/content/1/PPC_GTI_2016_19_09_2017.pdf>. Acesso em: 20 de maio de 2018.

INFOMONEY. **Alemanha legaliza criptomoedas e reconhece Bitcoin como meio de pagamento**. Disponível em <https://www.infomoney.com.br/mercados/bitcoin/noticia/7313971/alemanha-legaliza-criptomoedas-reconhece-bitcoin-como-meio-pagamento>. Acesso em 12 de novembro de 2018.

INTERNAL REVENUE SERVICE. Notice 2014-21. 2014. Disponível em: https://www.irs.gov/pub/irs-drop/n-14-21.pdf. Acesso em 12 de novembro de 2018.

KELLY, Meghan. **Fool Me Once: Bitcoin Exchange Mt.Gox Falls after Third DDoS Attack This Month**, Disponível em: <http://venturebeat.com/2013/04/21/mt-gox-ddos/>. Acesso em 15 de outubro de 2018.

LATORRE, Leonardo M. Munhoz. **A contribuição da tecnologia de informação no apoio às atividades do esquadrão de infraestrutura da aérea de Florianópolis: um estudo de caso.** 2017. 71f. Trabalho de Conclusão de Curso - IFSC, Florianópolis, 2017.

LUIZ, Edson. **Do Escambo à inclusão financeira**. Rio de Janeiro: Linotipo Digital, 2014.

MARQUES, Adriana A. Shinoda**. A Gestão do conhecimento nas empresas de tecnologia da informação: Uma análise a partir de um estudo bibliométrico.** 2014. Florianópolis. 205f. Trabalho de Conclusão de Curso - IFSC, Florianópolis, 2014.

MATONIS, Jon**. Bitcoin's Promise in Argentina**. Forbes, 27 abr. 2013. Disponível em: <http://www.forbes.com/sites/jonmatonis/2013/04/27/bitcoins-promise-in-argentina/>. Acesso em: 13 de novembro de 2018

NAKAMOTO. Satoshi. 2008. **Bitcoin: A Peer-to-Peer Electronic Cash System**. 2008. Disponível em <https://bitcoin.org/bitcoin.pdf>. Acesso em 30 de maio de 2018.

NASCIMENTO, Anderson. **História da moeda**. 2010. (3m16s). Disponível em: <https://youtu.be/3XvnaonC0U8>. Acesso em: 20 de maio de 2018.

NORMAS E REGRAS. **Referências Bibliográficas nas Normas ABNT**. Disponível em <https://www.normaseregras.com/normas-abnt/referencias/>. Acesso em 03 de junho de 2018.

NUNES, Paulo. **Conceito de moeda.** Disponível em < http://knoow.net/cienceconempr/economia/moeda/>. Acesso em 27 de maio de 2018.

WEGNER, F. Henrique. **Democracia digital: Revolucionando a prática democrática por meio da tecnologia da Informação**. 2014. 95f. Trabalho de Conclusão de Curso - IFSC, Florianópolis, 2014.

PEREIRA, Kevin. **Bitcoin: uma análise jurídico-tributária da moeda virtual**. 2016. 71f. Trabalho de Conclusão de Curso – UFAM, Manaus. 2016

PROOF. **Blockchain.** Acesso em 28 de maio de 2018. Disponível em <https://www.proof.com.br/blog/blockchain/>. Acesso em 28 de maio de 2018.

PORTAL DO BITCOIN. Disponível em <https://portaldobitcoin.com/cotacao-bitcoin/>. Acesso em 13 de novembro de 2018.

ROCHA, José Cláudio. **A Reinvenção Solidária e Participativa da Universidade: Um Estudo sobre Redes de Extensão Universitária**. EDUNEB: Salvador, 2008.

R7. **Câmara avança na regulamentação do 'Bitcoin' no Brasil.** Disponível em <https://noticias.r7.com/prisma/coluna-do-fraga/camara-avanca-na-regulamentacao-do-bitcoin-no-brasil-02012018>. Acesso em 12 de novembro de 2018

SAMPAIO et al. (2018). **Blockchain e a revolução do consenso sob demanda**. Disponível em <https://portaldeconteudo.sbc.org.br>. Acesso em 28 de maio de 2018.

TECMUNDO. **Corretora de bitcoins na Coreia do Sul é hackeada e decreta falência**. Disponível em <https://www.tecmundo.com.br/seguranca/125395-corretora-bitcoins-coreia-sul-hackeada-decreta-falencia.htm>. Acesso em 15 de outubro de 2018.

THOMSON REUTERS. **Como o mundo está lidando com as moedas digitais?** Disponível em <https://www.thomsonreuters.com.br/pt/financeiras/blog/como-o-mundo-esta-lidando-com-as-moedas-digitais.html>. Acesso em 30 de maio de 2018.

TUWINER, Jordan. **Tipos de Carteira.** Disponível em <https://www.buybitcoinworldwide.com/pt-br/carteiras-bitcoin/>. Acesso em 02 de Novembro de 2018.

ULRICH, Fernando. **Bitcoin - A moeda na era digital**. 1° Edição. São Paulo: Instituto LudWig Von Mises Brasil, 2014.

WEGNER, F. Henrique. **Democracia digital: Revolucionando a prática democrática por meio da tecnologia da Informação**. 2014. 95f. Trabalho de Conclusão de Curso - IFSC, Florianópolis, 2014.