

**UNIVERSIDADE FEDERAL DO RIO GRANDE - FURG  
INSTITUTO DE CIÊNCIAS ECONÔMICAS, ADMINISTRATIVAS E  
CONTÁBEIS - ICEAC  
CURSO DE CIÊNCIAS ECONÔMICAS**

**LEONARDO DE OLIVEIRA RIBEIRO**

**ESTUDO DO BITCOIN ENQUANTO MOEDA E INVESTIMENTO**

**Rio Grande  
2017**

**Leonardo de Oliveira Ribeiro**

## **ESTUDO DO BITCOIN ENQUANTO MOEDA E INVESTIMENTO**

*Monografia apresentada como requisito parcial para a obtenção do título de Bacharel, pelo Curso de Ciências Econômicas da Universidade Federal do Rio Grande - FURG.*

**Orientadora: Prof<sup>a</sup>. MSc. Carla  
Teresinha do Amaral Rodrigues**

**Rio Grande  
2017**

## **AGRADECIMENTOS**

Agradeço aos meus pais Cláudia de Oliveira e Edison Ribeiro da Cruz, a minha família , a minha namorada Rafaella Martins Corrêa e colegas pelo apoio e incentivo, sem vocês isso não seria possível. Aos meus professores do Instituto de Ciências Econômicas, Administrativas e Contábeis - ICEAC pelos ensinamentos, à Universidade Federal do Rio Grande. E por último mas não menos importante, gostaria de agradecer a minha orientadora Prof<sup>a</sup>. MSc. Carla Teresinha do Amaral Rodrigues e a banca examinadora Prof. Roque Neto e Prof. MSc. Pedro Leivas.

## RESUMO

Com o decorrer da história, a moeda sofreu muitas mudanças, acompanhando sempre as inovações tecnológicas, indo desde mercadorias até o cartão de débito e crédito, como é usado hoje. Porém após o advento da internet nenhuma grande mudança acontecera nesse campo. Assim, o *bitcoin*, objeto de estudo desse trabalho, surgiu em 2008 com uma proposta diferente, de dinheiro digital rastreável, porém anônimo e sem autoridade central reguladora. Basta assim verificar se de acordo com a teoria econômica esse novo meio de pagamento se enquadra como moeda, e mais ainda, como investimento. Nesta monografia será realizada uma análise do *bitcoin* como moeda, investimento e também um panorama do comportamento dos países à moeda digital, em relação a legislação regulatória do próprio bitcoin e outras moedas similares, as criptomoedas. E verificou-se que além de ser considerado um investimento de alto risco, por hora, o *bitcoin* não pode ser considerado uma moeda pelos moldes da teoria econômica, porém pode vir a ser no futuro, pois as funções não exercidas são adquiridas com o uso e difusão de um novo meio de pagamento.

Palavras-chave: Bitcoin, Moeda, Investimento, Teoria Monetária, Regulamentação.

## LISTA DE FIGURAS

Figura 1 –Principais criptomoedas no mercado .....	14
Figura 2 – Criptografia assimétrica .....	15
Figura 3 – Sistemas centralizado e descentralizado. ....	17
Figura 4 – Dificuldade para achar um novo bloco medido pela força computacional.....	19
Figura 5 – Número de carteiras registradas no site <i>blockchain.info</i> .....	20
Figura 6 – Tempo médio de confirmação de uma transação .....	23
Figura 7 – Custo médio de uma transação em porcentagem.....	23
Figura 8 – Exemplificação do blockchain.....	25
Figura 9 – Preço de mercado do bitcoin.....	30
Figura 10 – Preço de mercado do bitcoin em escala logarítmica.....	31
Figura 11 – Número médio de transações por bloco.....	34
Figura 12 – Corretoras de bitcoin no Brasil.....	35
Figura 13 – Matriz de correlação entre o preço do bitcoin e o número de pesquisas no Google trends.....	36
Figura 14 – Distribuição da força computacional (Hashrate).....	38

## SUMÁRIO

1 INTRODUÇÃO.....	1
2 MOEDA.....	4
2.1 Histórico.....	4
2.2 Características da moeda .....	7
2.2.1 Indestrutibilidade e inalterabilidade.....	7
2.2.2 Homogeneidade.....	8
2.2.3 Divisibilidade.....	8
2.2.4 Transferibilidade.....	9
2.2.5 Facilidade de manuseio e transporte.....	9
2.3 Funções da moeda .....	10
2.3.1 Intermediação de trocas.....	10
2.3.2 Medida de valor.....	11
2.3.3 Reserva de valor.....	11
2.3.4 Poder liberatório.....	12
2.3.5 Padrão de pagamentos diferidos.....	12
2.3.6 Instrumento de poder.....	13
3 BITCOIN.....	15
3.1 Criptografia e a Moeda.....	15
3.2 Surgimento.....	17
3.3 Funcionamento.....	18
3.4 Benefícios do uso do bitcoin.....	21
3.4.1 Transação eficiente.....	21
3.4.2 Corruptibilidade.....	24
4 CLASSIFICAÇÃO BITCOIN.....	26
4.1 Enquanto Moeda.....	26
4.2 Enquanto Investimento.....	32
5 PERSPECTIVAS.....	37
5.1 Bitcoin e Blockchain no mundo.....	37
5.2 Regulamentação no mundo.....	40
5.3 Bitcoin no Brasil.....	43
6 CONCLUSÃO.....	46
REFERÊNCIAS.....	49

## 1 INTRODUÇÃO

A moeda é o meio pelo qual são efetuadas as transações monetárias e também uma instituição que evolui em conjunto com a sociedade, adaptando-se principalmente às inovações tecnológicas. No decorrer da história das civilizações, vários bens já foram intitulados moeda: o sal, o açúcar, o ferro e alguns metais preciosos, como o ouro e a prata. Com o desenvolvimento social cada vez maior, esse tipo de moeda-mercadoria se extinguiu: primeiro ela deu lugar à moeda papel, ainda lastreada em ouro e, posteriormente, ao papel-moeda, tal como é hoje conhecida, sendo emitida apenas pelo Banco Central. Entretanto, o advento da tecnologia, principalmente a da Internet, proporcionou ao mercado um novo tipo de moeda descentralizada, de tal forma que nenhum banco central do mundo pode taxá-la ou emití-la: a moeda virtual criptografada.

Neste trabalho, o objetivo será o estudar o sistema Bitcoin, o mais bem-sucedido dentre os existentes nessa área. Inventado supostamente pelo programador japonês Satoshi Nakamoto, em seu *paper* "Bitcoin: a Peer-to-Peer Electronic Cash System", o sistema expõe a ideia de um meio de pagamento eletrônico sem a necessidade de qualquer intermediação para transacionar, nem mesmo a de um banco central, como autoridade central.

Assim como o ouro, o Bitcoin é escasso, tendo oferta limitada desde a sua criação. Como não tem uma autoridade central, não é atrelado a nenhuma moeda convencional; sendo assim, seu valor é determinado pelo mercado, pela oferta e pela própria demanda (HAYES, 2016).

Pode-se observar também que o bitcoin funciona como intermediário de trocas para agentes de todo mundo e de acordo com o site *coinmap.com*, é aceito em mais de 10 mil estabelecimentos comerciais mundialmente.

Encontrado em diversas plataformas de transação, o Bitcoin pode ser adquirido por meio da compra por moedas convencionais, sendo armazenado em uma carteira digital. Além disso, é possível adquirir a moeda criptografada pelo processo de criação - a chamada mineração. Esse processo viabiliza a existência desse meio de pagamento, que nada mais é que o processamento - por computadores - de algoritmos extensos para receber pequenas parcelas de Bitcoin (DWYER, 2014).

Fazendo um paralelo com o ouro, o Bitcoin se faz cada vez mais difícil de se extrair. É necessário cada vez mais esforço para minerar certa quantidade de Bitcoin. Isso se dá porque qualquer pessoa pode incrementar o algoritmo a ser processado pelos computadores, aprimorando a mineração, da mesma forma como são implementadas novas tecnologias para a extração do ouro.

O que mantém o sistema viável é a mineração do Bitcoin, pois ao se autorizarem transações ou ao se acharem novos problemas para aprimorar os algoritmos a serem processados, ganha-se uma pequena parcela de moeda. É fácil de se entenderem as transações: é cobrada uma taxa sobre o valor da transação de uma pessoa a outra e, como acontece em um banco, a taxa fica com quem fiscalizou a transação, no caso o minerador. A tarefa do minerador é fiscalizada por outros que estão na fila para pegar seu lugar. Se ele autorizar uma transação de forma errônea, é trocado por outro, e assim sucessivamente, até que um minerador faça a transação de maneira correta e ela seja aprovada pelos que estão na fila (PREVIDI, 2014 e SCARINCI, 2015).

No caso do aprimoramento do algoritmo, é como se nele algum minerador achasse uma falha. Quando ela é reconhecida por outros mineradores, é adicionado um novo “bloco” para a “corrente” ou algoritmo, aprimorando-se assim o Bitcoin pelo sistema *Blockchain* (SWAN, 2015).

Nesse trabalho será feita revisão uma de literatura sobre o assunto que é novo, mas que possui alto número de publicações por ano. Outra razão para essa revisão é que evolui, a cada dia mais, a ideia de moeda criptografada e, principalmente, a de um sistema de pagamento descentralizado, sendo necessário investigar-se o que já foi pesquisado sobre esse tema.

Serão utilizados os pilares da teoria monetária para se avaliarem as propriedades da moeda, tais quais: Instrumento de Troca; Medida de valor; Reserva de Valor; Poder liberatório; Padrão de pagamentos diferidos e Instrumento de poder.

Além disso, será verificada o bitcoin enquanto investimento, de acordo com a teoria econômica em relação ao risco e rentabilidade da criptomoeda e



também um panorama das criptomoedas no mundo, investigando as legislações e as taxações dos países.

## 2 MOEDA

Neste capítulo será apresentado o histórico da moeda, sua definição e suas funções.

### 2.1 Histórico

A moeda é o meio pelo qual são efetuadas as transações monetárias e desde 2500 anos a.C. o homem já cunhava moedas. No decorrer da história das civilizações, vários bens já foram intitulados moeda: o sal, o açúcar, o ferro e alguns metais preciosos, como o ouro e a prata. Mas antes de existir um meio de intercâmbio para a troca de bens, usavam-se os próprios bens para se transacionar.

Essa troca era fácil de ser resolvida sem um meio de troca unificado, se as duas partes da transação precisassem do bem oferecido pelo outro, ou seja, fazia-se, então, um escambo. Por exemplo, se em razão de uma praga em sua plantação, José estivesse com excesso de arroz e falta de feijão enquanto que Maria estivesse com excesso de feijão e falta de arroz em razão da mesma praga, a troca entre os dois seria fácil, pois as duas partes estariam interessadas no bem oferecido pelo outro. Supondo, porém, outra situação: José com excesso de arroz e falta de feijão; Maria com excesso de feijão mas também de arroz, e agora, falta de trigo. Apesar de José necessitar do excesso de feijão de Maria, ela não tem necessidade de arroz, que é o bem em excesso de José.

Como nesses exemplos foram apresentados somente dois agentes nessa economia, a questão poderia ser resolvida apenas colocando mais um agente que tivesse, para os outros dois agentes, um produto em escassez, outro em excesso e vice-versa. Quando, porém, pensamos em uma economia com diversos agentes, numa transação faz-se necessário um meio de intercâmbio; surge, então, a ideia de moeda, como meio de troca.

No começo das civilizações, além das moedas mercadorias citadas anteriormente, no caso de escambo, como meio de troca já foram utilizados artigos mais exóticos, como gado, conchas, uísque e pedras preciosas e,

embora esses bens sejam muito aproveitados pelos professores de Moeda, nunca foram importantes por muito tempo por pessoas afastadas de uma vida rural primitiva.

E, em razão da falta de praticidade de se utilizar, por exemplo, o gado como meio de troca, precisou-se de um meio de pagamento mais eficiente e unificado. Assim, metais preciosos como o ouro, a prata, o cobre e até uma fusão desses dois metais mais famosos, o electrum, foram utilizados para tal uso.

De acordo com Heródoto (1844), o povo grego foi o primeiro que cunhou moedas de ouro e prata e as negociou generalizadamente. Já Alexander Del Mar (1969) diz que, com base nos autores hindus, moedas já teriam sido utilizadas na Índia centenas de anos antes, inclusive com divisão decimal. Elas, porém, aperfeiçoaram-se na Grécia e em suas colônias, onde a cunhagem de moedas tornou-se uma importante forma de arte (GALBRAITH, 1977).

Na mesma velocidade em que as moedas eram adotadas por civilizações mais avançadas, as fraudes públicas e privadas as acompanhavam. Governantes descobriram, por exemplo, que poderiam cunhar uma moeda de ouro com uma porcentagem maior de outro metal de qualidade inferior, mas que aparentemente continuaria a possuir ouro em sua totalidade. Na teoria, essa moeda falsificada valeria mais do que seu conteúdo e, mesmo valendo menos, compraria a mesma quantidade em bens que a feita totalmente de ouro. E também havia as fraudes privadas, criadas quando empresários descobriram que, após uma transação, era possível raspar as moedas ou até mesmo cortá-las, de forma que não parecessem depreciadas; conseguiam, assim, alguns micromiligramas de "lucro". Surgiu, dessa forma, a inflação decorrente da depreciação das moedas.

Em consequência, tornou-se necessário que uma fiscalização fosse feita, para que reduzissem a falsificação e a duplicação das moedas. Em razão disso, as casas de cunhagem passaram a unificar o sistema, inserindo nas moedas uma espécie de selo, pesando-as e validando-lhes o valor. A falsificação, porém, continuou. "Com numerosas moedas em circulação, adulteradas, cortadas, limadas, refinadas, podadas, sendo as piores oferecidas

em primeiro lugar, elas acabaram por tornar-se um problema”, segundo GALBRAITH (1977, p.10).

Então, as chamadas casas da moeda - que depois virariam os bancos tais como são conhecidos atualmente - eram uma instituição do governo da cidade que fiscalizava o sistema e convertia as moedas estrangeiras e as moedas leves, dando a elas o seu valor intrínseco em termos do padrão monetário local, tomando apenas como taxa o custo da cunhagem e os gastos administrativos (SMITH, 1884).

Os bancos, ainda com problemas de fraude, começaram a emitir certificados de valor monetário. Assim, qualquer indivíduo que possuísse certo valor em moedas de ouro, por exemplo, poderia trocá-las por um certificado, no qual o banco garantia que aquele pedaço de papel em qualquer data teria o mesmo valor que o apresentado na hora de sua emissão. Surgiu, assim, a moeda-papel (GALBRAITH, 1977).

Essa garantia que os bancos asseguravam a quem obtivesse a moeda-papel recebeu o nome de lastro, que nada mais é do que a certeza de que esse valor estaria guardado no banco, de tal forma que se a qualquer momento o indivíduo decidisse converter o certificado em moedas, ele o conseguiria.

Com muitas pessoas convertendo suas moedas em papéis-moeda, existia cada vez mais depósitos ociosos no banco. E como não havia motivo para aquele dinheiro ficar parado, o banco decidiu emprestá-lo, cobrando taxas pelo empréstimo, assim aumentando seus ganhos. Além disso, os bancos depositários passaram a emitir certificados que já não apresentavam 100% de lastro. Criou-se, assim, a moeda fiduciária.

A moeda fiduciária tem como essência a confiança (*fiducia*, em latim), de forma que a moeda funciona de acordo com a confiabilidade dos agentes em relação aos depositários (LOPES e ROSSETTI, 1998).

Para regulamentar todo esse sistema de depósitos e empréstimos e organizar/ordenar a circulação do dinheiro, tornou-se necessária a criação de um novo tipo de banco, o Banco Central, que tem como principais funções controlar a emissão de moeda e fiscalizá-la. Serve também como o banco dos bancos e como banco do governo (LOPES e ROSSETTI, 1998).

Com isso, o papel-moeda ganhou um complemento, tornando-se papel-moeda de curso forçado, com o atributo da inconvertibilidade, com emissão exclusivamente estatal e sem lastro metálico (LOPES e ROSSETTI, 1998).

Entretanto, o advento da tecnologia computacional, principalmente a Internet, proporcionou ao mercado um novo tipo de moeda, a moeda virtual, cujos registros eletrônicos, como transações, são efetuados sem o agente ao menos tocar em uma nota física de dinheiro. Com a moeda eletrônica, os agentes têm a praticidade de armazenar unidades da moeda nacional em dispositivos eletrônicos, além de poderem transacionar no mundo digital sem muitos impasses (LEI Nº 12.865, 2013).

## **2.2 Características da moeda**

Como visto na seção anterior, a moeda passou por várias mudanças, indo desde a moeda-mercadoria até o dinheiro como é conhecido hoje. Tais mudanças se deram com o objetivo de melhorar a qualidade das transações monetárias. E, assim, a moeda foi se caracterizando, acompanhando as mudanças ocorridas. Essas características se definiram após a análise empírica de particularidades de cada tipo de moeda utilizada ao longo da história, pois elas se adaptavam às necessidades de cada época.

As mais relevantes características das moedas analisadas e estudadas desde Adam Smith são: indestrutibilidade e inalterabilidade; homogeneidade; divisibilidade; transferibilidade; facilidade de manuseio e transporte (LOPES e ROSSETTI, 1998).

### **2.2.1 Indestrutibilidade e inalterabilidade**

A moeda deve conter uma certa durabilidade, de modo que não se deteriore quando são feitas transações (LOPES e ROSSETTI, 1998). Ou seja, se fossem utilizadas como moedas mercadorias, por exemplo, algum alimento perecível como a carne, a cada uso para a intermediação das trocas desse bem, a qualidade se perderia muito rapidamente, a ponto de dar prejuízo a seu

destinatário, como uma espécie de inflação, em que o dinheiro perde valor. Só que, nesse caso, de forma muito mais acelerada.

### **2.2.2 Homogeneidade**

Moedas de mesmo valor, porém de diferentes unidades monetárias devem ser idênticas (LOPES e ROSSETTI, 1998). Continuando com os exemplos de moedas mercadorias, mas usando agora grãos de trigo, para que uma transação ocorresse de forma justa, os dois agentes deveriam saber as condições desses grãos. Se estão quebrados e miúdos ou se estão inteiros e graúdos. Ou seja, para se evitar uma assimetria de informação na transação, é necessário que já haja uma pré-determinação na qualidade do meio de troca em questão.

### **2.2.3 Divisibilidade**

Essa característica da moeda se deve à sua capacidade de se dividir e subdividir em quantidades menores, ou seja, é necessário haver notas de alto e de baixo valor circulando no mercado. Se existisse uma economia na qual só houvesse notas de alto valor, por exemplo para acompanhar o preço de imóveis e carros, as transações menores, do dia a dia, ficariam prejudicadas e impossíveis de serem feitas. Assim como a existência de notas pequenas dificultaria muito a compra de um bem com maior valor de mercado (LOPES e ROSSETTI, 1998).

Outro aspecto da divisibilidade é que a moeda não deve perder valor se repartida. Se fossem usados bens manufaturados como moeda e se fosse preciso dividi-los para transacionar um menor valor, suas partes separadas não teriam o mesmo valor do produto original (LOPES e ROSSETTI, 1998). Da mesma forma, por exemplo, um vaso só terá valor se estiver inteiro; se repartido em vários pedaços, perderá valor em relação ao produto original.

#### **2.2.4 Transferibilidade**

A moeda deve apresentar certa facilidade, para que sua transferência entre os agentes possa ser processada. Dessa forma, a nota não deve conter dificuldades burocráticas ou depreciabilidade em razão de seu antigo portador. Ou seja, diferentemente do mercado de ações, em que existem ações nominativas, a moeda deve ser exclusivamente do portador e sem nenhuma identificação ou marca de seu antigo ou atual dono (LOPES e ROSSETTI, 1998).

Se, por hipótese, em uma economia, o gado fosse utilizado como meio de troca, a mercadoria se depreciaria com o tempo, em razão de seus sucessivos donos terem gravado a fogo sua marca no couro do animal. Ou seja, haveria uma hora em que o gado não possuiria mais lugar para uma nova marca, impossibilitando uma nova transação em que ele fosse utilizado como moeda de troca.

Essa característica dá menos segurança ao portador da moeda; como, porém, a prioridade é facilitar o processo da transação e não dar garantias ao portador, esse é um aspecto importante.

#### **2.2.5 Facilidade de manuseio e transporte**

A utilização da moeda não pode ser dificultada em razão de seu manuseio e transporte. Características, como o peso da moeda, não devem dificultar as transações. Se fosse utilizado um material muito pesado como meio de troca, não seria prático portá-lo. Assim, logo ele entraria em desuso e seria substituído. Os primeiros metais abundantes utilizados como moeda foram sendo substituídos com o passar do tempo, pois tinha-se dificuldade para transacionar bens de alto valor; e, quanto mais abundante o metal, menor ficava o seu valor. Começou-se, portanto, a utilizar metais preciosos, menos abundantes, para transacionar bens, já que uma menor quantidade de um metal raro apresentava o mesmo valor agregado que uma maior quantidade de um metal abundante.

## 2.3 Funções da moeda

Se uma moeda apresentar as características mostradas na seção anterior, ela estará apta a exercer as funções para as quais a moeda fora inventada. Segundo LOPES e ROSSETTI (1998), são elas: intermediação de trocas; medida de valor; reserva de valor; poder liberatório; padrão de pagamentos diferidos; instrumento de poder.

### 2.3.1 Intermediação de trocas

No item 2.1, ao se apresentar o histórico da moeda, citou-se a utilização do escambo para o intercâmbio de mercadorias, mencionando-se que um bem deveria ser escolhido para melhorar as relações de troca entre os agentes. Essa função da moeda é, portanto, a razão principal de seu aparecimento. A unificação e a aceitação generalizada de um instrumento de troca levam não somente a uma melhoria na qualidade no sistema de trocas mas também a uma especialização e a uma divisão social do trabalho (LOPES e ROSSETTI, 1998).

Na hipótese de uma inexistência de moedas, as transações tenderiam a ser mais demoradas quando as trocas diretas prevalecessem. Ou seja, com a utilização da moeda, essas transações tendem a ser mais rápidas, deslocando para outras atividades - por exemplo para o trabalho produtivo - o tempo gasto para intermediar essas trocas. Um exemplo clássico do que ora se afirma é o da produção de alfinetes, na obra de Adam Smith, *Riqueza das Nações*, em que fica explícita a ideia de que a divisão do trabalho pode aumentar a produtividade (LOPES e ROSSETTI, 1998).

Com a separação entre compra e venda e com o abandono das trocas de mútuos interesses, o homem ganhou maior racionalidade, havendo também maior poder de escolha para os agentes. Essa inovação contribuiu para uma melhoria nos meios de satisfação da sociedade, os quais passaram a ter o poder de escolher não só o que queriam, mas também quando queriam (ROBERTSON, 1978).



### **2.3.2 Medida de valor**

A utilização da moeda como medida de valor remete à ideia de existência de um denominador comum de valores. Ou seja, remete à ideia de que, em sua ausência, os bens são valorados em quantidades da unidade monetária e poderão ser trocados baseados nesses valores.

Além dessa racionalização no sistema de valoração - o sistema de preços -, a existência dessa função na moeda leva ao aumento do número de informações econômicas que, conseqüentemente, amplia as margens de eficiência tanto dos produtores quanto dos consumidores, fazendo com que os agentes atuem de forma mais racional (LOPES e ROSSETTI, 1998).

Isso também torna a contabilização de atividades econômicas de uma unidade de produção muito mais viável - tanto para a questão macroeconômica, como o balanço de pagamentos de um país, quanto para a microeconômica, como a economia doméstica de uma família - já que ela passa a ser expressa em uma única unidade monetária, o que leva ao melhor entendimento dos ganhos e gastos e, conseqüentemente, ao desenvolvimento da economia e à melhoria do bem-estar coletivo (LOPES e ROSSETTI, 1998).

### **2.3.3 Reserva de valor**

Diferente das funções anteriores, essa não é exclusiva da moeda, podendo ser exercida por outros ativos financeiros e não financeiros. O que difere a moeda dos outros instrumentos de reserva de valor é sua liquidez e seus graus de incerteza, uma vez que investimentos de, por exemplo, renda fixa têm um risco maior, já que se trata de um investimento a longo prazo entre uma instituição financeira e o investidor. Mas esses ativos possuem uma rentabilidade maior que a moeda em si (LOPES e ROSSETTI, 1998).

Apesar de a moeda não ser o único ativo financeiro que exerce essa função, ela é preferível aos outros ativos por duas principais razões. Primeiramente, em razão da sua liquidez, que dá a ela uma aceitação pronta e imediata. Além disso, ela é conversível em meios de pagamento convencionais em ampla área geográfica. E, em segundo lugar, pela incerteza sobre se os

outros ativos perderão reversibilidade após certo tempo. Por exemplo, alguns bens de uso durável, como um carro, chegam a perder boa parte de sua reversibilidade logo após a compra. Ou seja, o valor desses ativos não é garantido no futuro; eles podem não alcançar o nível esperado pelo investidor, quando vierem a ser utilizados (LOPES e ROSSETTI, 1998).

#### **2.3.4 Poder liberatório**

Essa função ocorre pela opção, que é dada ao agente de sanar dívidas, de liquidar débitos e de livrar-se de uma situação passiva. Essa opção é garantida pelo Estado, o qual tem o poder de forçar o curso da moeda, aceitando-a com exclusividade como forma de pagamento. Sua aceitação, porém, não é garantida apenas pelo Estado. Para circular, uma moeda deve ser aceita pela sociedade como um todo. Esse fato confere ao agente o poder de escolha em relação ao recebimento da moeda que pode não ser confiável, como, por exemplo, foi o caso do marco, na época da hiperinflação alemã (LOPES e ROSSETTI, 1998).

O poder liberatório da moeda tem, portanto, uma forte relação com a credibilidade da mesma e, assim, depende não só da imposição por parte do Estado mas também da aceitação do meio de pagamento por parte dos agentes.

#### **2.3.5 Padrão de pagamentos diferidos**

Refletindo-se sobre as características da função de poder liberatório, principalmente a de saldar dívidas e a de medida de valor, automaticamente destaca-se a moeda como padrão de pagamentos diferidos. Ou seja, destaca-se a capacidade da moeda de facilitar os pagamentos de médio e longo prazo, seja sob a forma de concessão de crédito seja sob outras formas de adiantamento. A moeda tem, assim, uma importante função nos fluxos de produção e renda, viabilizando-os (LOPES e ROSSETTI, 1998).

Embora os fluxos de produção e renda sejam interdependentes, acontecem em etapas nas quais são necessários pagamentos antecipados de

tipos variados. Exemplificando: se o processo produtivo não tiver sido concluído antes da data de pagamento dos funcionários, uma empresa pode não ter dinheiro em caixa para pagar os salários; então, o empresário poderá conseguir com os bancos o valor correspondente ao pagamento, para pagá-lo ao final do desenvolvimento de sua produção. Esse adiantamento bancário para ser pago ao final do processo produtivo é o que se chama de pagamento diferido, pois ele contribui para a formação do resultado. Esse procedimento, assim como o do mercado de crédito por exemplo, seria impraticável sem a existência da moeda, uma vez que os pagamentos diferidos, distribuídos no tempo, entre outros, são os principais pilares das atividades econômicas de investimento (LOPES e ROSSETTI, 1998).

### **2.3.6 Instrumento de poder**

Por último, tem-se a moeda exercendo a função de instrumento de poder econômico, político e social. A partir do momento em que a moeda é admitida como um título de crédito, essa função se torna efetiva, pois os portadores desse crédito têm o direito de possuir os bens e serviços disponíveis no mercado, de acordo com o montante de moeda disponível. Isso se traduz numa forma de poder econômico, oriundo dos direitos concedidos. Além disso, os portadores da moeda adquirem um poder de decisão. E esses dois tipos de poder – o econômico e o de decisão – se superpõem, gerando, por consequência, um terceiro poder, o poder político.

De acordo com LOPES e ROSSETTI, 1998, p.25, referindo-se a KEYNES, em sua *Teoria Geral*, "[...] *certas inclinações da natureza humana, que, amparadas pelo dinheiro e pela fortuna, tanto podem tornar-se relativamente inofensivas, como cruéis, à medida que sejam conduzidas à desenfreada ambição do poder, de autoridade e de outras formas de engrandecimento pessoal*".

Cabe, porém, ressaltar que a posse de moeda não é sempre nociva ao agente, pois o mesmo é capaz de contribuir para a sociedade com atitudes edificantes. Portanto, sendo nociva, edificante ou apenas neutra, a posse de

moeda cria uma relação direta do poder econômico com poder político (LOPES e ROSSETTI, 1998).

### 3 BITCOIN

Nesse capítulo será feito o panorama geral de uma criptomoeda, em especial o *bitcoin*, que não é a única criptomoeda existente no mercado, mas é a mais famosa e a mais usada em seu segmento.

Figura 1 - Principais criptomoedas no mercado

#	Nome	Cap. de Mercado	Preço	Volume (24h)	Fornecimento Circulante	Câmbio (24h)	Gráfico de Preço (7d)
1	 Bitcoin	R\$919.484.947.533	R\$54.944.98	R\$38.580.969.760	16.734.650 BTC	7.90%	
2	 Ethereum	R\$151.779.907.224	R\$1.576.50	R\$4.657.435.364	96.276.527 ETH	5.49%	
3	 Bitcoin Cash	R\$80.549.515.769	R\$4.780.41	R\$2.994.555.640	16.849.925 BCH	9.39%	
4	 IOTA	R\$39.647.494.595	R\$14.26	R\$1.491.412.036	2.779.530.283 MIOTA *	-0.57%	
5	 Litecoin	R\$35.020.442.938	R\$645.45	R\$6.260.716.623	54.257.133 LTC	28.78%	

Fonte: <coinmarketcap.com>. Acesso em: 12 de dezembro de 2017.

#### 3.1 Criptografia e a moeda

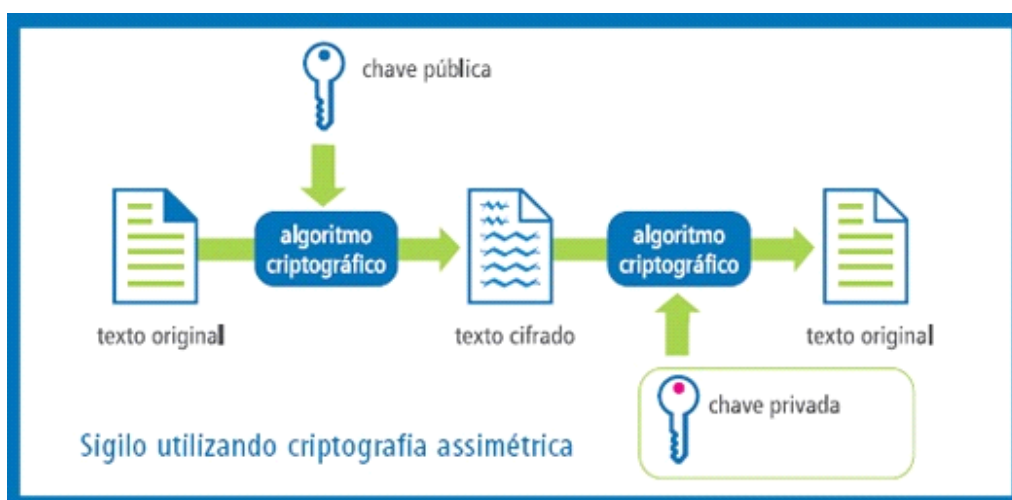
Antes de explicar como funciona a criptomoeda em questão, o bitcoin, é preciso entender o conceito de criptografia. Criptografar uma mensagem nada mais é que codificá-la para que apenas seu destinatário consiga decifrá-la. Um bom exemplo é a Enigma, uma máquina de escrever modificada, inventada pelos nazistas, com o fim de enviar mensagens para todo o Eixo na Segunda Guerra Mundial, pois mesmo após os Aliados terem conseguido um de seus exemplares, não foi possível decifrar suas mensagens, em razão de que o método de criptografia nela usado era modificado diariamente; ou seja, o que num dia era um "a", no seguinte poderia ser um "b". Isso dificultou o trabalho dos Aliados, até quando o britânico Alan Turing inventou outra máquina para decifrar a Enigma (HODGES, 2012).

Existem alguns tipos de criptografia. O utilizado pelas criptomoedas é o assimétrico. Também conhecido como chave pública, esse sistema de protocolos criptográficos requer o uso de duas chaves: uma pública, com o fim

de codificar uma mensagem; e outra privada, com o fim de descodificá-la. Com esse método, qualquer pessoa tem a capacidade de enviar uma mensagem criptografada usando a chave pública, mas apenas os receptores com a chave privada conseguem descodificá-la (OLIVEIRA, 2012).

Para simplificar esse conceito, faz-se a analogia com um cadeado, um baú e uma chave. Suponha-se que dentro do baú existe um bem, no caso a mensagem a ser transmitida; o cadeado, a chave pública que protege esse bem, já que outras pessoas senão o destinatário podem vê-lo e tocá-lo; e, por fim, a chave que seria capaz de abrir o cadeado, seria uma chave privada, em posse apenas do destinatário (OLIVEIRA, 2012).

Figura 2 – Criptografia assimétrica



Fonte: <<https://www.oficioeletronico.com.br/downloads/CartilhaCertificacaodigital.pdf>>. Acesso em: 14 mai.2017.

A junção desses dois conceitos - de um lado, o das chaves pública e privada; de outro, o de baú, cadeado e chave – dá-se quando se pergunta por que motivo um pedaço de papel com um número de série autorizado pelo governo deve ser aceito como um meio de pagamento, mas não o número de série sozinho. Esse questionamento leva à ideia de se trocar a mensagem contida no baú - nesse caso, a carteira digital - pelo número de série da moeda.

### 3.2 Surgimento

O bitcoin surgiu em um fórum de criptografia *on line*, em um artigo publicado anonimamente com um pseudônimo, Satoshi Nakamoto. Em seu artigo, o autor apresenta a ideia de um sistema monetário *peer-to-peer* (P2P) - traduzindo, de ponta a ponta -, descentralizado e sem a necessidade de um terceiro fiduciário. Apesar de ser uma ideia inovadora, Nakamoto não foi o primeiro a sugerir esse tipo de sistema. Em 1998, o membro da lista de discussão *cipherpunk*, Wei Dai, já havia proposto os protocolos de funcionamento de uma criptomoeda (ULRICH, 2014).

Após a publicação do artigo de Nakamoto, essa ideia nova gerou muitas perguntas e dúvidas, que foram direcionadas ao seu criador. Ele, então, dispôs-se a ajudar os outros usuários do fórum a entenderem o sistema. Além de esclarecer as dúvidas, no mesmo fórum de criptografia que publicou seu artigo, Nakamoto também expôs sua motivação à criação do método, que se resume em questões de assimetria de informação de bancos centrais, bancos comerciais e governos (ULRICH, 2014).

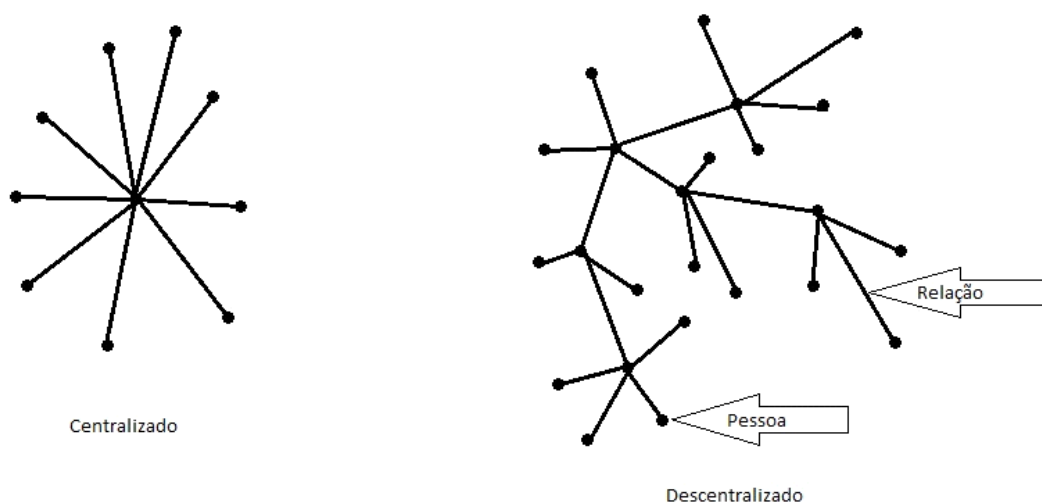
Em suas postagens, ficou claro o pensamento político e econômico do autor, que foi questionado sobre o problema político que um sistema monetário com a tecnologia *peer-to-peer* poderia trazer a um país. Nakamoto concordou com que uma solução para os problemas políticos da criptografia não poderia ser encontrada, mas afirmou que redes P2P parciais, como o Napster, eram facilmente controláveis pelo governo, enquanto redes P2P puras, como o TOR, ou até mesmo o Torrent trazendo para exemplos mais atuais, seguiam inabaladas (ULRICH, 2014).

Conforme Angel e McCabe (2014), existe um poder assimétrico entre o banco e o cliente no quesito opções de pagamento, com amplo domínio do primeiro. E, nas situações em que o poder de barganha de uma das partes é limitado, deve-se questionar a justiça do resultado.

Apesar de ter sido concebido em 31 de agosto de 2008, seu nascimento se deu às 18h15 do dia 3 de janeiro de 2009, no momento de sua primeira transação. Nesse momento, por conseguinte, aconteceu a adição do

primeiro bloco do *blockchain*, rede de funcionamento do bitcoin, acompanhado pela mensagem: “*The times 03/Jan/2009 Chancellor on brink of second bailout for banks*”. A mensagem expressa a “[...] *visão crítica de Satoshi sobre o sistema bancário e a desordem financeira reinante*” (ULRICH, 2014, p.43).

Figura 3 – Sistemas centralizado e descentralizado



### 3.3 Funcionamento

Primeiramente, deve-se entender que, como Satoshi Nakamoto descreveu em seu artigo, o *bitcoin* é um *eletronic cash system*. A chave para seu entendimento está na palavra *cash*, que não tem tradução literal para o português, mas que simplificada é o papel-moeda utilizado em transações mais informais, como a que acontece no ato de se comprar um pão na padaria: o padeiro não precisa fornecer o CNPJ da padaria, nem o cliente precisa fornecer o seu CPF, caracterizando-se assim o *cash* como um meio de pagamento ao portador, em que não há necessidade da presença de uma autoridade central no momento da transação. O *bitcoin*, portanto, é um meio de pagamento ao portador, eletrônico, criptografado e P2P, ou seja, de ponta a ponta, sem uma autoridade central. É o dinheiro vivo, digital e anônimo, do qual



não se sabe quem são os donos, apenas se sabe quais carteiras estão presentes na transação (ULRICH, 2014).

Posteriormente, é preciso compreender esse sistema de pagamentos, novo e diferente. Para isso, deve-se entender como funciona um sistema com entidades financeiras convencionais, como bancos comerciais e bancos centrais. Em termos de segurança, o único responsável pela proteção das próprias informações é o banco, que, então, contrata funcionários ou auditorias externas para controlar desde balanços e falhas no sistema até *hackers* e pessoas que agem de má-fé.

O *bitcoin*, diferentemente de uma moeda convencional, não tem autoridade central para garantir a segurança de informações de transações. Esse fato acarreta alguns questionamentos: quem protege esse sistema para que não haja gasto duplo ou para que pessoas mal intencionadas o utilizem? Quem valida as transações e as registra na rede? Quem faz o balanço das transações? A resposta intrigante é que qualquer pessoa pode dar conta dessas tarefas. Melhor dizendo, qualquer usuário da rede que esteja disposto a fazer o *download* do *software* disponibilizado pelo criador dessa moeda pode programá-lo para validar e registrar transações (NAKAMOTO, 2008).

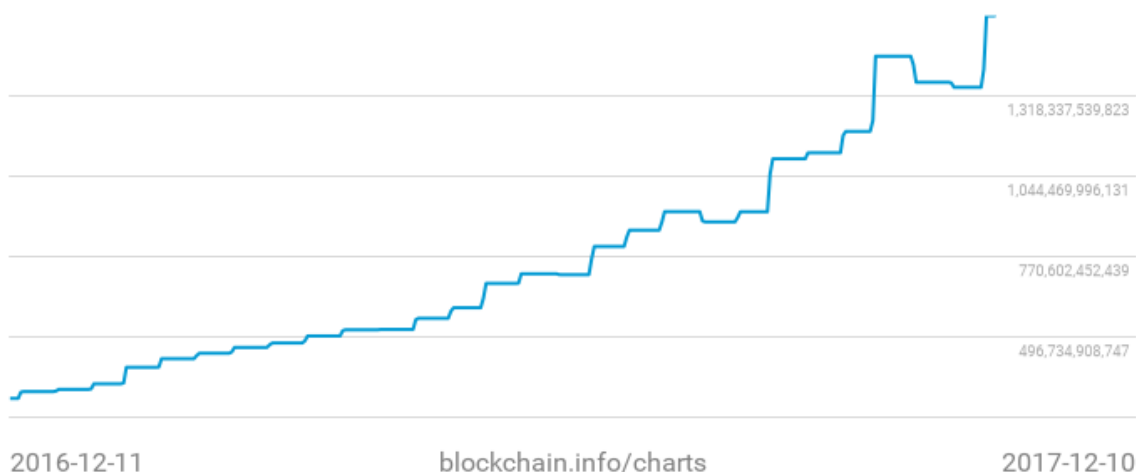
Por que, porém, uma pessoa iria querer os recursos escassos provenientes do gerenciamento do uso dessa moeda virtual, tendo despesas com um processamento computacional pesado e com a energia elétrica para manter o sistema funcionando? A recompensa para se tornar um validador de transações, os chamados mineradores, é a remuneração com novos *bitcoins*, além da taxa de validação da transação.

Nesse software de código aberto (*open source*), disponibilizado por Satoshi, existem duas tarefas para serem desempenhadas pelo minerador. A primeira é a validação de alguma transação feita em *bitcoins*; a segunda é a chamada prova de trabalho (*proof-of-work*).

Para que não se alcance o número máximo de *bitcoins* em um curto período de tempo, com os mineradores apenas validando transações, o *software* vem acompanhado da prova de trabalho, que consiste em resolver um problema matemático complexo, um algoritmo. O sistema exige, portanto, que o usuário desempenhe uma atividade complexa e custosa, e prove para a rede

que essa resolução foi bem executada. Uma vez verificado pelos outros mineradores que a resolução está correta, o usuário é recompensado por sua parcela de novos *bitcoins* criados, de tal forma que, a cada resolução matemática, aumenta-se a dificuldade do problema matemático. E, em razão desse aumento da dificuldade, os mineradores tendem a juntar-se para executar um trabalho mais rentável, obtendo, então, melhores resultados e maiores ganhos. Surgem, assim, as chamadas *Mining Pools*. Para melhor entendimento desse sistema, é possível fazer-se uma analogia com os jogos sudoku ou palavras cruzadas, dos quais, à primeira vista, não é possível saber-se a resolução, mas que, depois de feitos, facilmente pode-se verificar se estão certos (ULRICH, 2014).

Figura 4 – Dificuldade para se achar um novo bloco medido pela força computacional.

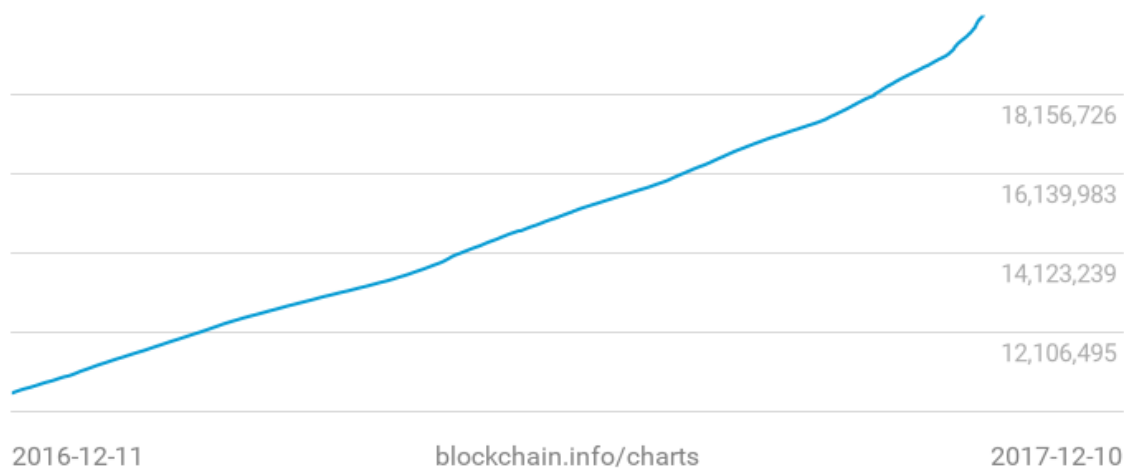


Acesso em: 11 dez. 2017.

Outra característica dessa criptomoeda é o anonimato com transparência. Essas duas palavras se complementam quando se pensa que, como não existe uma autoridade central, não seria necessário ao usuário fornecer um número de identificação, como o do Registro Geral (RG), no Brasil, ou o do Seguro Social, nos Estados Unidos. O endereço para onde devem ser enviados os *bitcoins* chama-se carteira digital, cujo conceito, na criptografia, é explicado pela chamada chave pública, uma espécie de conta corrente na qual ficam armazenados os *bitcoins*. Qualquer pessoa tem acesso a esse endereço.

Sendo assim, qualquer pessoa pode enviar *bitcoins* a essa carteira, mas apenas o dono da mesma pode movimentá-los (NAKAMOTO, 2008).

Figura 5 – Número de carteiras registradas no *site blockchain.info*



Acesso em: 14 mai. 2017.

### 3.4 Benefícios do uso do bitcoin

Por qual motivo se usaria o *bitcoin* como meio de pagamento, em vez dos meios convencionais? Quais são os seus benefícios? O que essa moeda traz de tão novo e inovador? Para se procurar responder a essas questões, algumas das vantagens de um meio de pagamento ao portador, digital, criptografado e descentralizado, serão aqui consideradas.

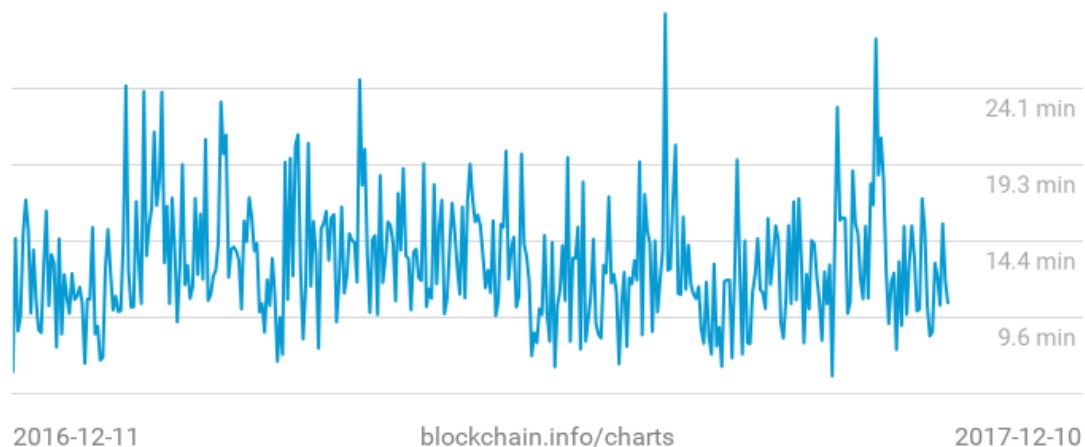
#### 3.4.1 Transação eficiente

O *bitcoin* não oferece apenas um novo meio de pagar, em substituição às moedas convencionais, mas propõe um novo meio de pagamento. Como funciona em sistema próprio e descentralizado, portanto sem uma autoridade central para processar todas as informações, o processo se torna mais eficiente e menos burocrático. Funcionando num sistema de ponta-a-ponta (P2P), o *bitcoin* oferece operações financeiras mais rápidas e com menos falhas, ou seja, mais eficientes (ULRICH, 2014).

Duas características de uma transação em um sistema descentralizado podem ser facilmente detectadas. Uma é a rapidez: em comparação com as transações efetuadas em bancos comerciais convencionais, as realizadas em sistemas descentralizados são infinitamente mais rápidas. Naqueles, no caso em que um indivíduo A queira fazer uma transferência a um indivíduo B, estando envolvidas nessa transação duas nações diferentes, o dinheiro fará um caminho extenso: sairá do banco comercial do indivíduo A e irá para o banco central do seu país; dali, irá para o banco central estrangeiro, depois para o banco comercial do indivíduo B, chegando finalmente à conta corrente do indivíduo B. No Brasil, uma transferência nacional demora entre 1 e 3 dias úteis para ser finalizada e uma internacional pode demorar até 6 dias úteis. Além disso, as taxas para se fazer uma transação desse tipo são infinitamente maiores que as do *bitcoin*.

A velocidade de uma transação feita com *bitcoins* demora em média quinze minutos, não importando se se trata de uma transferência nacional ou internacional. A razão dessa rapidez repousa no sistema de pagamentos do *bitcoin*, o *blockchain*. Como se afirmou em 3.3, para que ganhe a sua recompensa em *bitcoins* por validar e registrar uma transação na rede, um minerador deve executar uma prova de trabalho, completando assim a sua função. Como a prova de trabalho não é feita de forma separada da validação da transação, o tempo de espera da sua aprovação é o próprio tempo de resolução do algoritmo. Portanto, como em média os algoritmos são resolvidos em quinze minutos, esse será o tempo médio de finalização da transação (ULRICH, 2014).

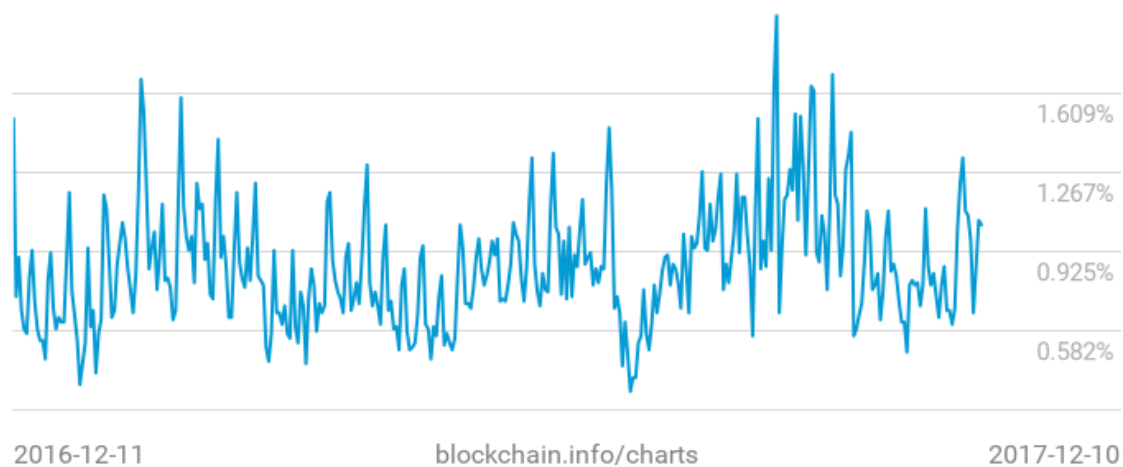
Figura 6 – Tempo médio de confirmação de uma transação



Acesso em: 11 dez. 2017.

Além disso, como o sistema de pagamentos do *bitcoin*, o *blockchain*, não tem vínculo empregatício com os mineradores, os usuários desse meio de pagamento são agraciados com as baixas taxas operacionais. Ou seja, os mineradores trabalham como uma espécie de *freelancer*, sendo pagos por trabalho feito. Assim, como a remuneração do minerador não passa por um terceiro para depois ser redistribuída, o mesmo recebe sua recompensa diretamente, diminuindo-se assim a burocracia e, conseqüentemente, a taxas (ULRICH, 2014).

Figura 7 – Custo médio de uma transação, em níveis percentuais.



Acesso em: 14 mai. 2017.

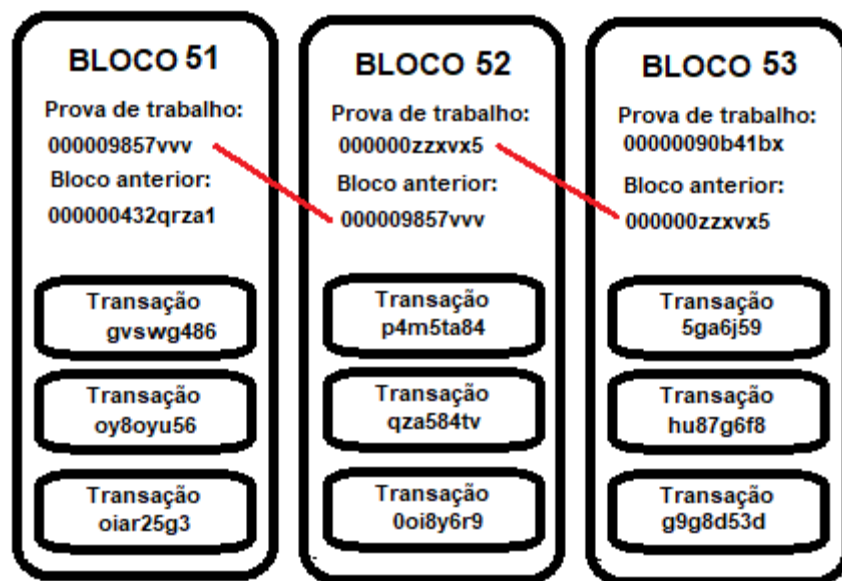
### 3.4.2 Corruptibilidade

Pode-se pensar que, por ser utilizada em um meio digital, essa moeda seja facilmente fraudada. Ser digital, porém, não é sua única particularidade. A descentralização da moeda faz com que todas as pessoas que estão nesse sistema sejam aptas a verificar qualquer falha no mesmo, aprimorando o algoritmo *open-source* disponibilizado pelo seu criador, ou verificando pessoas mal intencionadas e *hackers*.

O sistema se mantém incorruptível até hoje em razão de nele valer mais a pena ser honesto, de tal forma que, se houvesse a opção de fraudá-lo, tal coisa provavelmente não seria feita. Nos sistemas convencionais, a fraude se dá pelo custo e pela oportunidade do crime. No caso do uso de *bitcoins*, o trabalho é dado aos mineradores em um processo concorrencial. Quem fizer mal seu trabalho, será substituído por outro e assim sucessivamente, até que um o faça de forma correta e honesta.

Como, então, esse sistema trabalha para evitar o gasto duplo? Se um usuário tentar enviar, ao mesmo tempo, a mesma moeda para dois destinatários, havendo apenas um minerador, apenas uma transação será autorizada. Agora, se dois mineradores autorizarem uma transação cada um, apresentando as provas de trabalho, ocorrerá uma bifurcação na corrente de blocos. Nesse caso, estará ocorrendo um gasto duplo, até que um terceiro minerador envie um novo bloco à rede. Por sua vez, esse novo minerador deverá escolher um bloco anterior para se ligar. Com isso, o bloco duplicado será rejeitado e o sistema continuará funcionando (ULRICH, 2014).

Figura 8 – Exemplificação do *blockchain*.



Fonte: <<http://dataconomy.com>>. Acesso em: 14 mai.2017.

Para corromper a rede, alterando uma transação já feita, o usuário deverá reverter tal transação passada, criando uma bifurcação na corrente, como dito anteriormente. Supondo que a transação a ser corrompida esteja a dez blocos antes do atual, o usuário deverá refazer todas as provas de trabalho anteriores para fraudar o sistema, em razão dos blocos estarem interligados pela prova de trabalho. Além disso, esse usuário deverá refazê-las antes que um novo bloco seja adicionado à *blockchain* (SWAIN, 2015).

Para fazer isso, o usuário deverá estar provido de uma força computacional impraticável nos dias atuais. Essa é, portanto, a razão de o *blockchain* ser considerado um sistema de pagamento computacionalmente incorruptível.

## 4 CLASSIFICAÇÃO DO BITCOIN, SOB A PERSPECTIVA DA TEORIA ECONÔMICA

Nesse capítulo faz-se uma análise do *bitcoin* dentro da teoria econômica, tanto como moeda, quanto como investimento ou ativo financeiro, utilizando-se de teorias apresentadas em capítulos anteriores.

### 4.1 *Bitcoin* enquanto moeda

Uma observação faz-se necessária antes de se analisarem as características da moeda. Como o relatado em capítulos anteriores (3.4.1), todas as características se focam em um fato: em qualquer que seja a finalidade, a moeda não pode ser depreciada quando manuseada; sempre existe, porém, em qualquer transação, a taxa cobrada pelos mineradores, para verificar e autorizar a negociação. Na hora de se negociar uma transação de uma carteira digital para outra, essa taxa já é expressa, por isso ela é considerada como uma taxa sobre o serviço realizado e não, como uma depreciação da moeda.

Como visto no Capítulo 2, para que algo possa ser considerado *moeda* é necessário que tenha certas características e exerça funções essenciais. Assim, a primeira característica a ser analisada será a da indestrutibilidade e inalterabilidade da moeda, ou seja, a moeda deve conter certa durabilidade, de modo que não se deteriore quando utilizadas em transações (PINHEIRO, 2009). O *bitcoin* respeita essa característica, de forma que o montante transacionado não perde valor quando negociado. Por exemplo, se for feita uma compra utilizando-se 10 *bitcoins*, o vendedor receberá os mesmos 10 *bitcoins*, sem deterioração. O que acontece na criptomoeda é que ela pode perder ou ganhar valor de mercado ao longo do tempo, mas o motivo disso não se dá pela negociação em si, mas pela oferta e demanda da mesma.

A segunda característica é a homogeneidade dessa moeda, ou seja, o fato de ela não ser diferente entre si. Melhor dizendo: montantes traduzindo o mesmo valor, ainda que expressos por meio de diferentes unidades monetárias, devem resultar em valores idênticos, de forma que, por exemplo,



uma nota de 1 real valha a mesma coisa que duas moedas de 50 centavos de real ou quatro moedas de 25 centavos de real e assim por diante (PINHEIRO, 2009). O *bitcoin* respeita essa característica. Como não existe uma forma física desse dinheiro, uma vez que ele é cem por cento digital, é possível facilmente verificar que, quando duas quantidades de moeda se somam, viram uma terceira, sem que cada uma delas se diferencie de seu valor original. Além disso, não existe assimetria de informação entre os agentes que transacionam a moeda, já que a condição da moeda é sempre a mesma, de acordo com o *blockchain*.

A terceira característica dessa moeda é sua divisibilidade: ela deve ser capaz de se dividir em menores parcelas, de modo a possibilitar tanto a negociação de bens mais caros utilizando-se moedas de menor valor, como a de bens mais baratos, com moedas de menor valor; em ambos os casos, essa divisão não pode fazer com que a moeda perca valor (PINHEIRO, 2009). Como dito anteriormente (3.3), o *bitcoin* é 100% digital e seu valor hoje passa dos R\$ 25.000,00 (vinte e cinco mil reais) nas corretoras no Brasil. Ou seja, são pouquíssimos os bens que podem ser adquiridos pela moeda de valor cheio. Assim, grande parte das transações feitas nessa moeda é realizada usando-se parcelas da moeda, cujas subdivisões são casualmente chamadas de “satoshis”, em homenagem ao seu criador, Satoshi Nakamoto. Assim, 1 satoshi vale 0.00000001 *bitcoin* e, portanto, 1 bitcoin vale 100 milhões de satoshis.

A quarta característica apresentada no Capítulo 2 foi a transferibilidade, segundo a qual a moeda deve proporcionar facilidade, para que sua transferência entre os agentes possa ser realizada. Assim, no trâmite com a moeda não deve haver burocracias depreciativas que dificultem sua negociação. Ou seja, a moeda não pode ter sido ligada burocraticamente ao seu antigo portador. Com essa característica, o *bitcoin* expressa a principal vantagem de sua utilização: o fato de ser tratado como um dinheiro digital e não apenas como uma moeda. Como já dito (3.2), seu inventor Satoshi Nakamoto, descreve-o como um sistema de pagamentos eletrônico de ponta a ponta em *cash*, palavra sem tradução literal para o português e que se refere ao papel moeda utilizado sem o monitoramento do banco. Assim, apesar do monitoramento do *blockchain* sobre as carteiras digitais, o *bitcoin* não revela os

donos das carteiras. Isso não dificulta a sua negociação; muito pelo contrário, só a facilita ainda mais, pois é essa tecnologia que permite aos mineradores verificarem e autorizarem transações, viabilizando o sistema.

E, finalmente, a última característica a ser analisada antes de se verificar se o *bitcoin* exerce as funções da moeda, é a facilidade de manuseio e de transporte que ele oferece. A utilização da moeda não pode ser dificultada por características físicas como, por exemplo, tamanho e peso, de sorte que objetos muito grandes ou muito pesados seriam inviáveis de ser utilizados como moedas (PINHEIRO, 2009). O *bitcoin* respeita essa característica pelo fato simples de ser 100% digital. As únicas coisas que talvez pudessem complicar o seu uso seriam a necessidade de se utilizar um aplicativo de uma carteira digital em um aparelho eletrônico, como um celular ou um computador, e a necessidade de conexão com a internet. O que se pode argumentar é que a tecnologia computacional e a própria internet vêm progressivamente atingindo mais lares e espaços acadêmicos no mundo todo e que empresas como o *Facebook* têm programas de difusão da internet, como a chamada inclusão social, em lugares onde o acesso a essa ferramenta/mídia é escasso.

Como dito anteriormente no capítulo 2, se uma moeda tem as características mencionadas ela tem a capacidade de exercer as funções a ela designadas. Isso posto, é possível analisar-se se o *bitcoin* respeita essas características, para ser considerado uma moeda segundo os moldes da teoria econômica.

A primeira função e também a principal razão da moeda ter sido inventada é a intermediação de trocas, essencial para haver uma organização nesse tipo de mercado, pois, se não houvesse um intermediário, seria preciso usar o escambo, muito menos eficiente (MISHKIN, 1998). No caso do *bitcoin*, essa função é exercida em parte, já que, atualmente, ele só é aceito sem restrições em 96 das 246 regiões ou países do mundo (COIN DANCE, 2017). Ou seja, em termos mundiais, como não há um consenso sobre ele por não ser emitido por nenhum banco central, o *bitcoin* não pode servir como intermediário para qualquer cidadão do mundo.

Nesse sentido, nenhuma moeda convencional é 100% usada e aceita em todo o mundo. Até a moeda mais difundida mundialmente, o dólar

americano, pode não ser aceita por alguns comércios ou por pessoas em outros países, já que cada país ou bloco econômico tem sua própria moeda centralizada. Com isso, verifica-se que o *bitcoin* chega a ser até mais democrático quando se trata de uso internacional de moeda, já que a taxa para a transação feita entre pessoas da mesma cidade é igual à de transações entre pessoas que estão em pontos do planeta muito distantes entre si.

A segunda função a ser analisada no *bitcoin* é a medida de valor, segundo a qual, mesmo na ausência da moeda, é possível valorar os bens em quantidades da unidade monetária e também trocá-los baseados nesses valores (MISHKIN, 1998). No caso da criptomoeda, o *bitcoin* não exerce essa função, principalmente por dois fatores: em muitos países, não ser tratada como moeda, mas como *commodity*; e por ter alta volatilidade. Assim, quando se compra algo em *bitcoin*, é necessário fazer-se uma conversão do preço daquele produto em alguma moeda convencional para que não seja cobrado um preço errado, de acordo com a cotação da criptomoeda no momento.

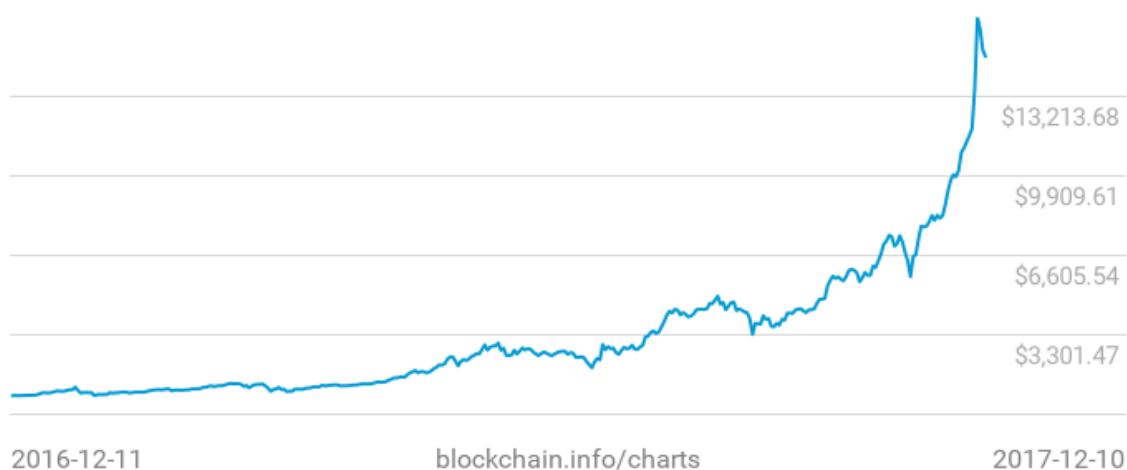
É interessante ressaltar que essa é uma função que demora a ser adquirida por uma moeda, principalmente quando ela está sendo usada há pouco tempo. É possível encontrar a falta dessa função em moedas recém inseridas no mercado, como o papel-moeda que, historicamente, passou a ser utilizado após o uso do ouro como moeda. Durante um período, embora se usasse o papel-moeda, os produtos ainda eram valorados de acordo com o meio de troca antigo. Isso ocorreu até o momento em que os agentes se acostumaram com a utilização da nova moeda e começaram a usá-la integralmente. Outro exemplo disso aconteceu no Brasil, quando o país passou por um período de hiperinflação e foi necessária a utilização de uma moeda, a URV (criada em 01/03/1994), que depois se transformou no Real, usado até hoje. Naquela ocasião, foi elaborado um plano econômico segundo o qual duas moedas – o Cruzeiro Real (que funcionou de 01/08/1993 até 30/06/1994) e a URV - passaram a funcionar ao mesmo tempo, mas cada uma com a sua função: a URV era a unidade de conta dos produtos ou medida de valor, e o Cruzeiro Real era a moeda utilizada para, após a conversão em URV, adquirir bens e serviços. As duas moedas foram utilizadas concomitantemente, até que, por ocasião do ajuste econômico do governo federal, instituindo o Plano Real, o

Cruzeiro Real passou a ser utilizado com o nome Real, mas com cotação igual à da URV.

A reserva de valor, função que difere das anteriores, pois não é exclusiva da moeda, pode ser atribuída a diversos ativos financeiros. Essa função nada mais é que a garantia de que, se guardada, não se deteriorará ou depreciará com o tempo. Diversos ativos financeiros fazem isso, acrescentando até certa rentabilidade. Dentre todos os ativos, entretanto, a moeda é escolhida principalmente por ter alta liquidez e fácil conversibilidade, tanto em outras moedas quanto em outros ativos financeiros ou bens, os quais podem ser desvalorizados ou não alcançarem a rentabilidade prevista pelo investidor (MISHKIN, 1998).

Essa é a principal função na qual os críticos do *bitcoin* mais se apoiam para rejeitá-lo em razão de sua alta volatilidade. Entretanto, por exemplo, foi verificado que, desde o começo deste trabalho até hoje, o *bitcoin* valorizou cerca de 500% no Brasil, saindo de 5mil para 25mil reais. Assim, quanto a esse quesito, o *bitcoin* aproxima-se mais de um ativo financeiro que pode vir a não ter a rentabilidade prevista do que de uma reserva de valor constante, que tem poucas variações de acordo com a inflação e a desvalorização do câmbio.

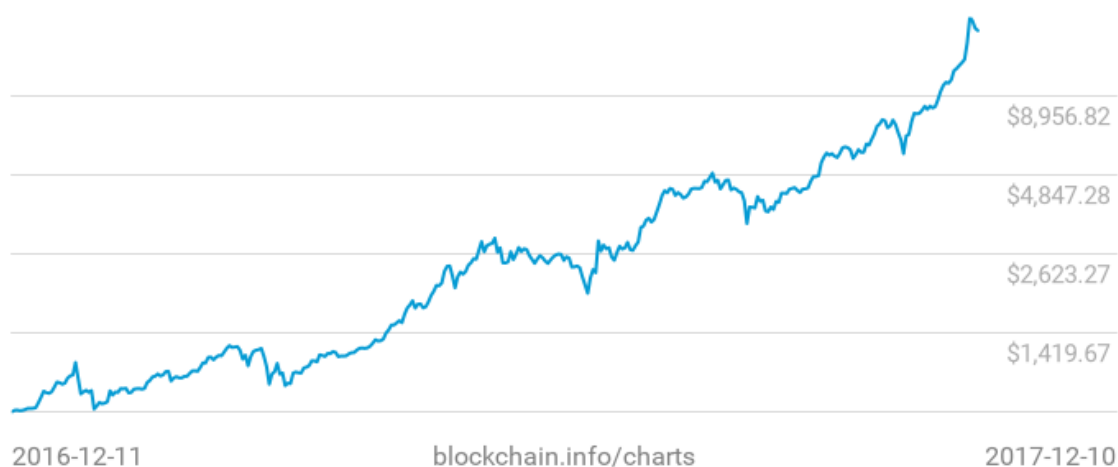
Figura 9 – Preço de mercado do *bitcoin*



A moeda também deve/pode exercer a função de poder liberatório, segundo a qual ao agente é dada a opção de sanar dívidas, de liquidar débitos e de livrar-se de uma situação passiva, com a garantia do Estado, para servir como meio de pagamento. Além disso, ela deve também ser aceita pela sociedade como um todo (LOPES; ROSSETI, 1998). O *bitcoin* não respeita essa função, garantida pelo Estado ou instituição financeira responsável; ele é descentralizado e não é controlado por nenhum órgão central.

Juntamente com essa função, destaca-se a da moeda como padrão de pagamentos diferidos, ou seja, a capacidade da moeda de facilitar os pagamentos de médio e longo prazo, sob a forma de crédito ou outras formas de adiantamento. Dessa forma, a moeda assume um grande papel na viabilização de fluxos de produção e renda. Em razão disso, os salários podem ser pagos aos trabalhadores antes do final do processo produtivo sob a forma de empréstimo. Assim, a moeda deve dar a garantia de que, ao final do processo, ocorrerá um retorno do investimento para cobrir esse empréstimo, sem risco da desvalorização da moeda (LOPES; ROSSETI, 1998). O *bitcoin* também não respeita essa regra, pois sua volatilidade é muito alta. Entretanto, se se pensar na forma de retorno do investimento (cf. seção 4.2), o *bitcoin* respeita essa função, pois desde a sua criação não se teve uma desvalorização da moeda relativa ao período anterior, como pode ser visto no gráfico a seguir, sobre o preço do *bitcoin* em escala logarítmica.

Figura 10 – Preço de mercado do *bitcoin* em escala logarítmica



Por último, tem-se a moeda exercendo a função de instrumento de poder econômico, político e social. A partir do momento em que ela é admitida como título de crédito, seus portadores têm a capacidade de adquirir bens e serviços disponíveis no mercado, traduzindo-se assim em uma forma de poder econômico. Como o poder econômico é atrelado ao poder de decisão, que por sua vez leva ao poder político, é possível dizer que um agente com maior poder aquisitivo tem também um maior poder político. De forma alguma, porém, isso é sempre nocivo ao seu portador, de modo que esse poder político adquirido pode ser usado de maneira que melhore o bem-estar da sociedade com atitudes edificantes (LOPES; ROSSETI, 1998). Assim, o *bitcoin* respeita essa função, as vezes até melhor que algumas moedas convencionais, já que o mercado para adquirir bens, serviços e moedas acaba não sendo apenas o país em que o agente está localizado, e sim todas as nações que aceitem *bitcoin*. O poder político, entretanto, é mais difícil de adquirir, em razão do anonimato em que são feitas transações financeiras com a criptomoeda. Assim, uma carteira “x” pode possuir um alto poder econômico com a criptomoeda, mas ninguém saberá quem é o dono dela, a não ser que o agente dono da carteira se manifeste. Desse modo, o poder político pode ser adquirido, mas apenas se o agente tiver esse interesse de expor sua privacidade financeira.

**“A abordagem empírica encontra dificuldades porque as evidências de qual seria a medida de moeda preferida são pouco claras, e mesmo que não estivessem, não poderíamos estar seguros de que uma medida que tenha funcionado bem no passado funcionaria bem no futuro” (MISHKIN, 1998, p36).**

#### **4.2 *Bitcoin* enquanto investimento**

Para que se possa classificar o *bitcoin* como investimento, primeiro é necessário definir que um investimento é qualquer aplicação de capital com expectativa de um benefício no futuro. Dessa forma, nessa seção é apresentada uma classificação de investimentos em ativos financeiros e sua relação entre liquidez, risco e rentabilidade.

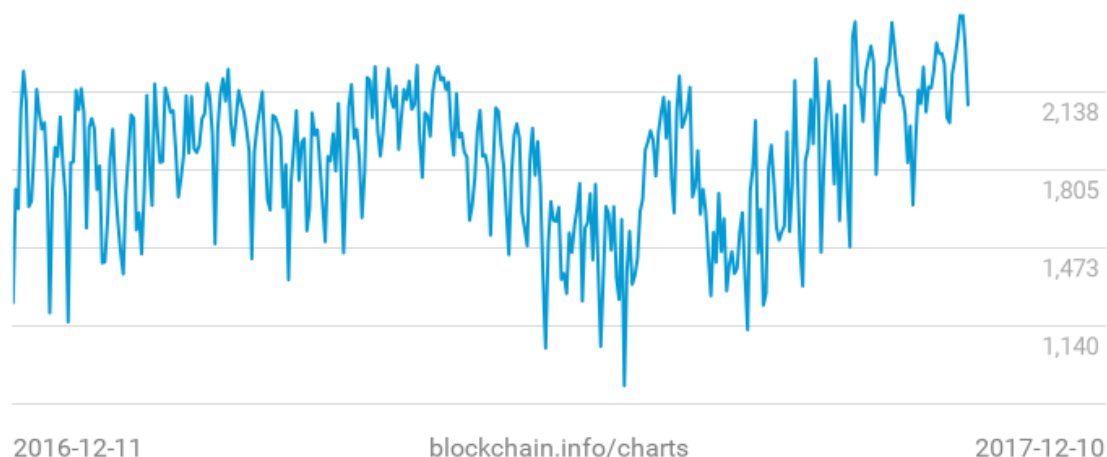
Os ativos financeiros são divididos em primários e indiretos. Os primários são emitidos pelos tomadores últimos e demandantes últimos de fundos, existindo assim um contato direto entre os mediadores financeiros. São exemplos de ativos primários as ações da Bolsa de Valores. Já os ativos indiretos são investimentos mais ajustados às necessidades do investidor, em razão de as necessidades dos agentes econômicos serem cada vez mais sofisticadas. Assim, os chamados poupadores últimos não negociam com os tomadores últimos e, sim, com os intermediários financeiros (PINHEIRO, 2009).

Dentro dos ativos primários têm-se os títulos de renda fixa, patrimoniais e derivativos. O primeiro promete um rendimento fixo, como o próprio nome diz; o segundo representa uma participação na propriedade de uma empresa, e os derivativos rendimentos determinados ou derivados de outros ativos financeiros, como o mercado de opções ou o mercado futuro. Além deles, têm-se os ativos de renda variável, que são aqueles em que não há um conhecimento prévio de sua rentabilidade nem do valor de resgate; o mesmo pode ser superior, igual ou inferior ao investimento inicial (PINHEIRO, 2009).

A diferença entre esses ativos se dá pelos níveis de rentabilidade esperada, que são resultados da liquidez e do risco que o agente está disposto de arcar. Assim, têm-se que quanto maior o risco e menor a liquidez do ativo, maior será o seu ganho esperado. Por exemplo, um título de renda variável, - como uma ação -, ou um ativo de renda fixa -, como um título do tesouro direto com resgate de longo prazo-, terá uma rentabilidade maior que a poupança que tem alta liquidez e um risco quase inexistente. Isso se dá porque o tomador do empréstimo (investimento feito) terá mais tempo para ganhar em cima do montante e/ou maior margem de erro para aplicar o mesmo (PINHEIRO, 2009).

Assim, pelas características citadas, pode-se verificar que o *bitcoin* pode ser considerado um ativo de renda variável com altíssimo risco em razão da sua alta volatilidade (Figura 9), porém de alta liquidez (Figura 11) e de fácil uso pelo fato de o agente poder investir qualquer quantia nesse ativo, sem determinação de valor mínimo. Como pode ser visto no gráfico a seguir, seu volume de transações vem aumentando nos últimos anos.

Figura 11 - Número médio de transações por bloco



Acesso em: 10 nov.2017

Bernardo Faria, sócio e vice-presidente da FoxBit, a maior corretora de *bitcoin* em volume no Brasil, afirma em uma entrevista ao InfoMoney que a *bitcoin* é um investimento fácil de ser aplicado e de se aprender sobre ela, pelo fato de não haver valor mínimo para investimento, como citado anteriormente. Assim, o investidor pode investir um valor baixo com o fim de aprender e, posteriormente, quando estiver mais seguro, pode vir a investir mais. Na mesma entrevista, é explicado também que o perfil do investidor de *bitcoin* é o de jovens adultos ou de pessoas que já trabalharam em algum setor bancário, onde se tem o pensamento de que a *bitcoin* é o “ouro digital”, e principalmente, de um investidor engajado na *bitcoin* e *blockchain*. Portanto, o acesso à informação e o conhecimento na moeda são os principais fatos de um agente ter a possibilidade de investir na *bitcoin* (INFOMONEY, 2017).

Como as ações em bolsas de valores, existem algumas maneiras de se investir na *bitcoin*, além da forma intuitiva, que é apenas deixando-a render a médio (*positive trade*) e longo prazo (*buy-and-hold trade*). A Figura 9 e 10 mostram a cotação dessa moeda, com um alto rendimento em curto prazo. Em razão da sua alta volatilidade, porém, outros investidores, além dos convencionais, apostam nessa variação do preço, como é o caso, por exemplo, dos chamados *Scalper-traders* que negociam um alto volume de moeda em um período curto de tempo, ganhando em cima das pequenas variações diárias do ativo.



Finalmente existem aqueles que se utilizam da chamada arbitragem. Em razão desses tipos de ativos não terem apenas um lugar para serem negociados, é normal que os preços do mesmo ativo em diferentes corretoras sejam distintos. Dessa forma, quando a taxa de transação da moeda, de uma corretora para a outra, for menor que o seu ganho total, é viável comprar a moeda na corretora que oferece preço mais baixo e vendê-la onde o preço é superior.

Figura 12 – Corretoras de *bitcoin* no Brasil

EXCHANGE	ÚLTIMO (R\$)	Variação	VOLUME BTC	VOLUME R\$
 FoxBit	55.766,00	7,68%	951	50.574.667,61
 Mercado Bitcoin	56.000,00	5,07%	869	47.375.438,85
 Negocie Coins	57.150,52	5,44%	308	17.428.032,18
 BitcoinToYou	56.220,01	4,11%	126	6.961.666,35
 BitcoinTrade	57.007,07	5,82%	80	4.398.570,62
 LocalBitcoins	57.799,00	11,54%	4	251.794,42
 flowBTC	57.350,00	2,59%	3	191.424,68
 Arena Bitcoin	56.000,00	1,82%	0	9.799,88

Fonte: <bitvalor.com>. Acesso em: 12 nov.2017

O *bitcoin* se mostra um bom investimento, tanto para os investidores de curtíssimo/curto prazo por causa de sua alta volatilidade, quanto para os de médio e longo prazo, pois sua oferta é limitada a 21 milhões de unidades monetárias. Como hoje ainda se tem apenas 16 milhões de moedas mineradas, a *bitcoin* está em expansão. É, porém, uma questão de tempo até que se chegue ao limite de moedas mineradas. Assim, sua oferta é limitada, mas sua demanda não. Ou seja, quanto mais acesso à informação e mais pessoas engajadas no assunto, tende a ser maior o crescimento do uso da moeda, o que leva ao aumento da sua capitalização de mercado e consequentemente ao aumento de seu preço.

Analisando o preço de mercado da *bitcoin* desde 2012 até hoje e correlacionando-o com o engajamento das pessoas no assunto, expresso no volume de pesquisas relacionadas a essa moeda no Google, tem-se um alto grau de correlação, expresso na matriz de correlação a seguir.

Figura 13 – Matriz de correlação entre o preço da *bitcoin* e o número de pesquisas no Google trends.

	Preço <i>bitcoin</i>	Número Pesquisas
Preço <i>bitcoin</i>	1	0,908223
Número Pesquisas	0,908223	1

Fonte: Resultados do autor de acordo com dados obtidos em [blockchain.info](http://blockchain.info) e [trends.google.com](http://trends.google.com)

A matriz revela um coeficiente de correlação de 0,908223, ou seja, o interesse e o engajamento da população mundial tem uma correlação positiva no preço do *bitcoin* em 90,82%.

## 5 PERSPECTIVAS

Nesse capítulo é apresentado um panorama geral da *bitcoin* e do *blockchain* no mundo, verificando-se como os países estão lidando com a tecnologia das criptomoedas em geral.

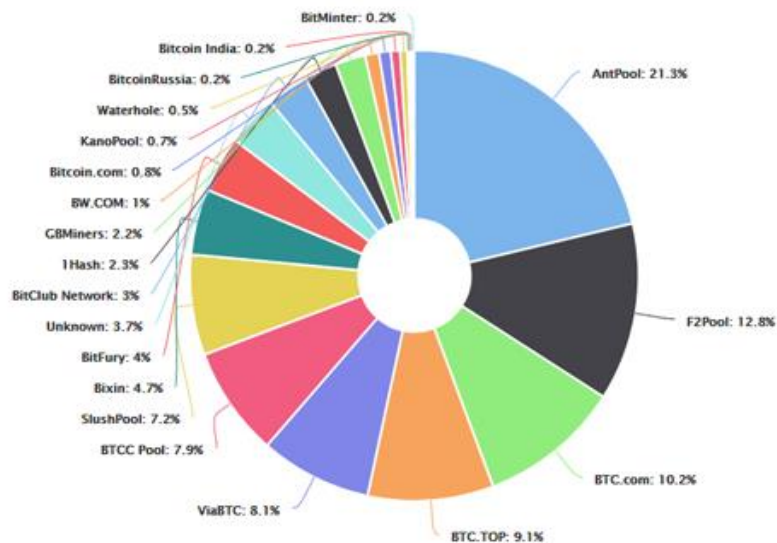
### 5.1 *Bitcoin e blockchain* no mundo

Hoje no mundo não é viável um computador pessoal simples exercer a tarefa de minerar *bitcoin*, porque a mineração requer tanta força computacional, que a conta de energia elétrica chegaria a ser mais alta do que o retorno monetário para aprovar transações e aplicar a prova de trabalho. Por isso, foram desenvolvidas máquinas especializadas para a mineração, como por exemplo, a AntMiner S9, fabricada pela empresa chinesa Bitmain. A AntMiner S9 atualmente é a máquina mais rentável para se minerar *bitcoins*.

Para se defender de problemas e obter mais ganhos, alguns investidores da criptomoeda chegam a encher containers com máquinas especializadas para a mineração e emergi-los em óleo de resfriamento, que não afetam os circuitos, para diminuir o consumo de energia. Grandes empresas se empenham para desenvolver um óleo de resfriamento cada vez melhor. É o caso da 3M, empresa multinacional mundialmente conhecida pelos seus produtos de tecnologia variada, com sede em Maplewood, Minnesota, nos Estados Unidos (3M, 2014).

Outra alternativa para o melhor rendimento da força computacional vem das chamadas *mining pools*. Como explicado no capítulo anterior, os mineradores juntam suas máquinas para gastar menos energia elétrica e, assim, conseguirem maior rentabilidade. Atualmente 61,5% da mineração de *bitcoin* ou das *mining pools* estão localizadas na China, que detém o monopólio de mineração de *bitcoin*. A razão disso é o baixo custo dos insumos na China, como energia elétrica e mão de obra, por exemplo. Além disso, os circuitos de computadores mineradores (máquinas especializadas em mineração) e os próprios computadores são fabricados naquele país, o que contribui para também baratear o custo.

Figura 14 – Distribuição da força computacional (Hashrate).



Fonte: <blockchain.info>. Acesso em: 5 out. 2017.

Como mostrado na Figura 14, a fabricante da AntMiner S9 é também a “dona” da AntPool que hoje representa 21,3% de toda a mineração existente no mundo. Justificando o monopólio chinês, destaca-se que, além da AntPool, são *pools* chinesas a F2Pool(12,8%), a BTC.com(10,2%), a BTC.TOP(9,1%) e a ViaBTC(8,1%).

Apesar de o *bitcoin* não ter sido considerado uma moeda alternativa oficial para nenhum país no mundo, principalmente pela falta de controle sobre sua política monetária e fiscal, alguns países vêm investindo na tecnologia por trás do bitcoin, o blockchain. O Japão, já conhecido por seu pioneirismo tecnológico, planeja lançar uma moeda digital nacional com a tecnologia. De acordo com a Reuters, autoridades japonesas planejam disponibilizar para a população japonesa a moeda digital *J-Coin*, até as Olimpíadas de 2020, que acontecerão em Tóquio. E assim, da mesma forma que as moedas digitais estatais já existentes, a *J-Coin* será interligada à própria moeda nacional, o iene. O porta-voz do banco Mizuho Financial Group disse ao CNBC (*Consumer News and Business Channel*) que "O projeto ainda está nos estágios iniciais e (...) ainda serão realizadas reuniões com outras instituições. Isso será atrelado ao iene e ainda esperamos o desenvolvimento de um *app mobile* para realizar pagamentos e transferências". (SHINO, 2017)

O projeto tem o apoio do banco central e reguladores. O objetivo do governo é perder a dependência do dinheiro, que representa cerca de 70% das transações financeiras no país. A J-Coin será cotada a uma taxa de um-para-um com o iene e possibilitará aos japoneses realizar transações financeiras sem a necessidade de dinheiro, usando apenas um celular (KHARPAL, 2017).

Mais recentemente, Dubai também assinou um acordo para criar a sua moeda digital, a *emCash*. De acordo com a WAM (*Emirates News Agency*), uma parceria foi formada pela Emcredit, uma subsidiária da economia de Dubai, com a Object Tech Group Ltd com o apoio do Dubai Economy Accelerators, uma iniciativa financeira para alavancar o desenvolvimento econômico e tecnológico de Dubai, parecido com o BNDES brasileiro. A moeda será usada para pagar uma variedade de serviços - por exemplo, impostos estatais e compras no mercado -, usando a carteira digital *emPay wallet*, lançada pela Emcredit para dar o suporte às transações com a nova moeda. Ale Ibrahim, vice-diretor geral da economia de Dubai, disse que o emCash dará uma identidade financeira às transações sem uma terceira parte, reafirmará Dubai como um destino de negócios competitivos e aumentará a felicidade do consumidor, levando assim, a evolução de Dubai para uma *smart economy* ou economia inteligente. De acordo com Tom Morgan, diretor e co-fundador da Object Tech Group, a moeda se aproveitará da tecnologia do *blockchain*, garantindo transações mais baratas, mais rápidas e mais seguras, sendo esse o caminho para criar uma cidade verdadeiramente conectada (ARABIAN BUSINESS, 2017).

Outro país a demonstrar interesse em aprimorar seu sistema de pagamentos nacional foi a Ucrânia, onde em um comunicado oficial do Diretor de Sistemas de Pagamento e Departamento de Desenvolvimento Inovador do National *Bank Of Ukraine* (NBU), Serhii Shatskyi afirma que o banco está interessado em um maior desenvolvimento do mercado financeiro de alta tecnologia no país, o que influenciará positivamente na implementação do projeto *Cashless Economy*, ou economia sem dinheiro em espécie (NATIONAL BANK OF UKRAINE, 2017).

Por último, existem países que já demonstraram interesse na moeda virtual, mas nada foi anunciado oficialmente. Foi esse o caso da Rússia:

Vladimir Putin, presidente desse país, recentemente se reuniu com Vitalik Buterin, o criador da criptomoeda digital Ethereum, uma das criptomoedas com maior capitalização de mercado, estimada em US\$8,5 bilhões. Diz-se que Putin se interessou em firmar um acordo para a criação de uma moeda digital estatal russa em parceria com Buterin, mas nada foi confirmado até o momento (MAVADIYA, 2017).

## 5.2 Regulamentação no mundo

Com o alto crescimento do uso do *bitcoin*, os governos começaram a dar atenção aos seus termos regulatórios, por conta de uma questão: como regular uma moeda que não tem uma agência controladora? Nesse quesito, o Japão foi uma das primeiras nações a regulamentar criptomoedas como um método legal de pagamento. O país passou a aplicar a lei, a partir de 1º de abril de 2017, categorizando a moeda digital como uma espécie de instrumento de pagamento pré-pago. De acordo com a agência de serviços financeiros do Japão, essa lei estabelece condições de capital para corretoras, em relação à cibersegurança e aos contratos operacionais. Além dessas condições estabelecidas na lei, as corretoras deverão fornecer programas de treinamento para seus funcionários e submeterem-se a auditorias anuais. O pioneirismo japonês se deu pela vontade *startup* de empreender usando a tecnologia *bitcoin* e *blockchain*. De acordo com a *Nikkei Asian Review*, agência de notícias asiática, o Conselho de Normas Contábeis do Japão além de regulamentar o *bitcoin* quer também regulamentar outras criptomoedas, com o intuito de padronizá-las (NIKKEI ASIAN REVIEW, 2017).

Seguindo os passos do Japão, a Austrália planeja aprimorar suas leis contra a lavagem de dinheiro (transformação dos proventos resultantes de atividades ilícitas em capitais reutilizáveis nos termos da lei, dando-lhes uma aparência legal). E, para isso, o país pretende regulamentar as moedas digitais, o que ajudará a fiscalizar melhor o movimento de dinheiro para criminosos e terroristas, sendo essa uma parte vital para o sistema de defesas nacional australiano, segundo afirma Michael Keenan, Ministro de Justiça da Austrália (SMYTH, 2017). No Brasil, a prática conhecida como lavagem de

dinheiro também constitui crime, nos termos do artigo 368º- A do Código Penal (CP).

Já nos Estados Unidos foi implementada a *bitlicence*, uma licença de negócio referente às moedas digitais emitida pelo Departamento de Serviços Financeiros do Estado de Nova Iorque (NYDFS). Por enquanto, as cláusulas estão restringidas a empresas localizadas em Nova Iorque e aos nova-iorquinos. Para usufruir da *Bitlicence*, a empresa deverá realizar as seguintes atividades: transmitir moeda virtual ou recebê-la para transmissão; armazenar, ter participação, ou manter custódia ou controle de moedas virtuais em nome de terceiros; comprar e vender moeda virtual como um cliente empresarial; executar os serviços de câmbio; e controlar, administrar ou emitir moeda virtual. A lei entrou em vigor em 8 de agosto de 2015 e, em setembro, a primeira empresa já havia recebido sua *bitlicence*, a Circle, baseada em Boston; em julho de 2016 a segunda empresa a ter a licença concedida foi a Ripple, cuja criptomoeda, chamada pelo mesmo nome, tem uma das maiores capitalizações de mercado dentre as moedas digitais existentes. Por fim, uma empresa com base em São Francisco, a Coinbase, uma das startups com mais financiamentos na indústria do *bitcoin*, foi licenciada em janeiro de 2017. Assim totalizando, três *bitlicenses* já foram emitidas até a data em que foi escrito esse trabalho; há, entretanto, por parte de outras empresas, muita procura para conquistar a licença (NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES, 2015).

Na União Europeia, aplicava-se o IVA (Imposto sobre o Valor Acrescentado) em compras de mercadorias feitas com *bitcoins*. Entretanto, por meio de um comunicado de imprensa, a Corte de Justiça da União Europeia determinou aos países-membros que o *bitcoin* não é mercadoria, mas meio de pagamento. Dessa forma, o imposto deixou de ser aplicável, já que aquisições com a moeda não significavam mais uma troca de mercadorias, mas uma compra normal com uma moeda e uma mercadoria. Essa medida teve como objetivo aliviar as dificuldades que surgem no contexto da tributação das transações financeiras, relacionadas com a determinação do montante taxável e o montante do IVA dedutível (COURT OF JUSTICE OF THE EUROPEAN UNION, 2015).

Atualmente, o *bitcoin* tem em sua lista de países que o aceitam como uma prática legal de transação, 90 nações - e cada dia mais esse número cresce. Cada um desses países considera-o de uma maneira: como meio de pagamento, bem de troca, ou como *commodity*.

Na China, recentemente foi anunciado pelo *People's Bank of China* (PBoC) a proibição da ICO (Initial Coin Offering) ou Oferta Inicial de Moeda, que nada mais é que uma arrecadação de fundos para criar uma nova moeda digital. Ao comprar uma ICO de qualquer moeda digital, o indivíduo está contribuindo para que aquela criptomoeda saia do papel e seja comercializada, numa espécie de *crowdfunding*, que pode ser comparado a um IPO (*Initial Public Offering*) de uma empresa para abrir seu capital em uma bolsa de valores. Segundo o comunicado do PBoC, o dinheiro investido em ICOs deve retornar aos seus apoiadores em certo prazo e as corretoras ou *exchanges* não podem mais negociar os ICOs. Ou seja, as criptomoedas, como o *bitcoin*, não foram banidas da China e nem sua negociação. Esse fato põe em evidência o ponto fraco do *bitcoin*, criado com o intuito de ser descentralizado. Se, entretanto, as corretoras não tiverem permissão do país, fica inviabilizada a comercialização da moeda. "Isso é um pequeno avanço, talvez não na mesma extensão, do que estamos começando a ver em outras jurisdições - o inevitável é que todos sabemos que as regulamentações estão chegando", disse Jehan Chu, sócio-gerente da *Kenetic Capital Ltd.* em Hong Kong, que investe e aconselha vendas de ICOs. "A China, devido ao seu tamanho e sendo um dos mercados de IPO mais especulativos, precisou tomar uma ação mais firme". De acordo com a Bloomberg, essa ação da China deu-se pela falta de controle sobre essas novas moedas, e ressaltam que o país tem a intenção de criar a sua própria moeda digital no futuro, mas nada pôde ser confirmado até o momento (CHEN; LEE, 2017).



### 5.3 Bitcoin no Brasil

As criptomoedas, em especial o Bitcoin, vêm tomando espaço no mercado mundial. Desde 2014, porém, ou seja, apenas de pouco tempo para cá os governos no mundo têm se mobilizado para regulamentar ou rechaçar esse novo tipo de meio de pagamento. No Brasil, por exemplo, o deputado Aureo Lidio Moreira Ribeiro apresentou na Câmara dos Deputados, em julho de 2015, um projeto de lei (PL 2303/2015) cuja ementa dispõe “sobre a inclusão das moedas virtuais e programas de milhagem aéreas na definição de ‘arranjos de pagamento’, sob a supervisão do Banco Central”. Em 30 de agosto de 2017, o deputado Aureo Ribeiro fez uma audiência de apresentação do projeto. Nela estavam presentes os seguintes convidados: Bernardo Faria, sócio da Foxbit, empresa de compra e venda de *bitcoins* no Brasil; Helena Margarido, advogada, investidora e mentora de *startups* e especialista em novas tecnologias, em especial *bitcoin*, *blockchain* e criptomoedas; deputado Alexandre Valle e Mardilson Fernandes Queiroz, consultor do Departamento de Regulação do Sistema Financeiro do Bacen, entre outros. Na audiência, Queiroz afirmou que a instituição era contra a proposta de incluir as moedas digitais dentro dos padrões de meios de pagamentos definidos pela Lei 12.865/2013, e ressaltou que o banco não havia encontrado elos nas dimensões jurídica e econômica que pudessem caracterizá-las como moedas.

**“Na dimensão jurídica, não tem o condão de ser moeda de curso forçado, nem lastro na moeda soberana, que é o real. Na dimensão econômica, ela pode até ter reserva de valor, mas podemos citar vários ativos que também podem ter, como uma casa ou apartamento. Como meio de pagamento, já restringe bastante os ativos possíveis de serem aceitos dentro de uma sociedade para ser utilizadas como meio de troca. Elas também não preenchem a função de unidade de conta, explicou o representante.”** (QUEIROZ, em audiência do projeto de lei PL 2303/2015, 30 ago. 2017)

De acordo com Mardilson Fernandes Queiroz, é preciso separar a moeda virtual da tecnologia subjacente a essas inovações tecnológicas e analisá-las separadamente. Dessa forma, ficaria claro que, como explicado anteriormente, as moedas virtuais não se enquadram como arranjo de

pagamento à luz da Lei 12.865/2013 e, assim, não seria do interesse do Bacen a regulação desse tipo de moeda. Pelo *site* da Câmara dos Deputados, porém, sabe-se que serão realizados mais encontros como aquele.

Até então, o que se tinha em termos regulatórios dessas moedas era o comunicado nº 25.306, do Banco Central, datado de 19 de fevereiro de 2014. Esse comunicado “esclarece sobre os riscos decorrentes da aquisição das chamadas ‘moedas virtuais’ ou ‘moedas criptografadas’ e da realização de transação com elas”. De acordo com esse texto, as moedas virtuais não são classificadas como “moedas eletrônicas” de que tratam a Lei 12.865 em razão de não terem lastro em moeda nacional ou estrangeira, como prevê a lei. E também, pela falta de lastro, não são garantidos por ativo real de qualquer espécie. Além disso, ele alerta a população de que, em função do baixo volume de transações e da baixa aceitação (em 2014), “a variação dos preços das moedas virtuais pode ser muito grande e rápida, podendo até mesmo levar a perda total de seu valor”. Finaliza afirmando: que as moedas virtuais ainda não são capazes de oferecer risco para o Sistema Financeiro Nacional; que o mesmo está acompanhando as discussões nos foros internacionais sobre o assunto; e que o uso da moeda, tanto por pessoas físicas quanto jurídicas, é legal, de forma que o ato em si de transacionar moeda não é contra as leis, mas que não pode ser descartado que o motivo para sua troca pode ser ilícito.

Apesar de pouco tempo, muitos trabalhos acadêmicos sobre as moedas digitais vêm sendo publicados e a explicam cada vez, tornando-a mais tangível para todos. Esse é o caso da monografia de Andrade, 2017, graduado em Direito pelo Instituto de Educação Superior de Brasília, que tem como tema a “Regulamentação Jurídica de Moedas Virtuais”, que muito acrescentou nesse trabalho. De acordo com Andrade, 2017, a moeda virtual hoje é classificada, por exclusão, simplesmente como bens jurídicos intangíveis de caráter patrimonial, conceito adotado pela Receita Federal do Brasil e por autores como Balduccini. As atuais leis do Brasil se aplicam às moedas virtuais. Sendo elas bens intangíveis, uma aquisição hoje feita com *bitcoins* não pode ser considerada um contrato de compra e venda, mas um contrato de permuta, pois, pelo Código Civil, uma das partes do contrato de compra e venda se obriga a transferir o domínio de certo bem, e a outra se responsabiliza em

pagar-lhe certo preço em dinheiro. Como as criptomoedas não são consideradas dinheiro, o melhor contrato a ser utilizado é o de permuta, no qual se trocam dois bens sem a presença de um meio de troca, como uma espécie de escambo.

Em relação à tributação, Andrade afirma que a Receita Federal já se posicionou nesse sentido e que tais moedas devem ser declaradas no imposto de renda na ficha de bens e direitos, como outros bens. Elas são taxadas de forma similar às ações em bolsas de valores, ou seja, os ganhos cujo valor ultrapasse R\$35.000 são tributados no mês à alíquota de 15%. E conclui que há possibilidade de tributação do ICMS sobre a aquisição de mercadorias com *bitcoins*, já que, como dito anteriormente, essa transação comercial é feita sobre um contrato de permuta. Já na compra e venda de *bitcoins*, em operações realizadas com reais ou moedas estrangeiras, não é aplicado o imposto.

## 6 CONCLUSÃO

Ao longo deste trabalho, o *bitcoin* foi avaliado de forma que pudesse ser considerado uma moeda e um investimento de acordo com a teoria econômica. Verificou-se que o *bitcoin* respeita todas as qualidades físicas para exercer suas funções. Conferiu-se, porém, que essa criptomoeda as exerce apenas em partes, pois, por ser descentralizada, não respeita as funções de moeda relacionadas a uma entidade financeira central, ou seja, a característica de poder liberatório e a de padrão de pagamentos.

Atualmente, em todo o mundo, várias empresas aceitam o *bitcoin* como pagamento de seus produtos ou serviços. Exemplo disso são empresas gigantes da tecnologia, como a Dell (ALBUQUERQUE e CALLADO, 2015).

Portanto, a criptomoeda exerce suas funções apenas em partes já que tem abrangência mundial, mas não é acessível a todos. Já como medida de valor, nem parcialmente o *bitcoin* as exerce, pois os preços ainda são tabelados em moedas convencionais e apenas convertidas em *bitcoin*, em razão de sua alta volatilidade. Essa característica também impede que a função de reserva de valor seja exercida pela criptomoeda. Entretanto, como visto ao longo do trabalho, essa função só pode ser vista após um longo prazo de seu uso. Assim, atualmente, a função que é exercida em sua totalidade pelo *bitcoin* é a de instrumento de poder, ou seja, um agente que tenha um alto número da moeda pode vir a ter poder econômico e, por conseguinte, poder político. Portanto, de acordo com a teoria econômica, hoje não se pode dizer que o *bitcoin* seja considerado uma moeda em sua totalidade, mas com o tempo e com o aumento de sua utilização, ele pode vir a ser, em um futuro próximo.

Já como investimento, o *bitcoin* se mostrou muito forte principalmente em função de sua alta volatilidade, fazendo com que investidores tanto de curtíssimo e curto prazo, quanto de médio e longo prazo pudessem obter ganhos. Verificou-se também que existe uma relação direta entre o nível de interesse no assunto – demonstrado pelo aumento da procura pelo tema no principal veículo de pesquisa do mundo, o Google - e o preço de mercado do

*bitcoin*: o preço do *bitcoin* é afetado pelo aumento da procura e vice-versa, como observado na matriz de correlação apresentada neste estudo.

Frederich Mishkin, em seu livro *The Economics of Money, Banking and Financial Markets*, 1998, faz um questionamento sobre a sociedade sem dinheiro e se estamos caminhando para ela. Em sua reflexão, esse autor diz que um sistema sem dinheiro em espécie não seria possível por quatro motivos: o alto valor de se montar uma rede de computadores para utilizar-se apenas pagamentos digitais, os cheques convencionais permitem o fornecimento de recibos; o uso de cheques possibilita dias de “circulação” e, uma vez que o cheque pode demorar alguns dias para ser descontado, pode render sobre a taxa de juros, antes de ser utilizado; os meios de pagamentos eletrônicos aumentam a preocupação com a segurança digital, principalmente em relação aos *hackers*, que aparecem como usuários de computador, com o acesso não autorizado. Mishkin conclui que o mundo está se movendo rapidamente para uma sociedade com menos dinheiro em espécie em circulação, mas que esse é um processo gradual, que pode demorar de 10 a 20 anos para se realizar.

O *bitcoin* já demonstrou, porém, que pode liquidar esses problemas que o autor defende, já que existe um intervalo de 19 anos entre o livro citado e este trabalho. Como o *bitcoin* já tem uma rede de computadores pública, o *blockchain* eliminaria o problema do alto custo para a criação de uma nova rede. Todas as transações são registradas no *blockchain*, possibilitando obter recibos digitais visíveis a todos, mas anonimamente. O *bitcoin* também não pode ser corrompido, em razão da grande força computacional exercida, tanto para a mineração como para manter o sistema funcionando. Resta ainda avaliar um ponto defendido pelo autor: o rendimento do dinheiro em uma poupança até que seja descontado o cheque. É preciso considerar que, com raras exceções, o cheque está cada vez mais em desuso em todo o mundo, principalmente em razão da necessidade de rapidez em tudo, incluindo aí as transações e a informação no mundo.

Dessa forma, caminha-se para uma sociedade sem moeda em espécie e não para uma sociedade sem dinheiro. Da mesma forma como Satoshi Nakamoto, autor do artigo *Bitcoin: A Peer-to-Peer Electronic Cash System*, utiliza

esse termo, os homens continuariam utilizando o *cash*, ou apenas, dinheiro, porém de forma digital.

## REFERÊNCIAS

ALBUQUERQUE, Bruno; CALLADO, Marcelo. *Understanding Bitcoins: Facts and Questions*, 2015. Disponível em: <<http://bibliotecadigital.fgv.br/ojs/index.php/rbe/article/view/33090>>. Acesso em: Outubro, 2016.

ANDRADE, Walmar. *Regulamentação jurídica de moedas virtuais*, 2017. Trabalho de Conclusão de Curso (Bacharel em Direito) – Curso de Direito, Instituto De Educação Superior De Brasília (IESB), Brasília, 2017.

ANGEL, James; McCABE, Douglas. *The Ethics of Payments: Paper, Plastic, or Bitcoin*, 2014. Disponível em: <<http://connection.ebscohost.com/c/articles/112000081/ethics-payments-paper-plastic-bitcoin>>. Acesso em: Outubro, 2016.

ANGELL, Norman. *The history of money*. 1 ed. NOVA YORK: FREDERICK A STOKES Co, 1929. 116-117 p.

ARABIAN BUSINESS. *Dubai signs deal to create digital currency emCash*, set. 2017. Disponível em: <<http://www.arabianbusiness.com/industries/banking-finance/379617-dubai-signs-deal-to-establish-digital-currency-emcash>>. Acesso em: 28 de out. de 2017.

CHEN, Lulu; LEE, Justina. *Bitcoin Tumbles as PBOC Declares Initial Coin Offerings Illegal*, set. 2017. Disponível em: <<https://www.bloomberg.com/news/articles/2017-09-04/china-central-bank-says-initial-coin-offerings-are-illegal>>. Acesso em: 28 de out. de 2017.

COURT OF JUSTICE OF THE EUROPEAN UNION *Press Release No 128/15. The exchange of traditional currencies for units of the 'bitcoin' virtual currency is exempt from VAT*, out. 2015. Disponível em: <<https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150128en.pdf>> Acesso em: 28 de out. de 2017.

DWYER, Gerald. *The Economics of Bitcoin and Similar Private Digital Currencies*, 2014. Disponível em: <<https://brianmlucey.files.wordpress.com/2014/01/gerald-dwyer-economicsdigitalcurrency.pdf>>. Acesso em: Setembro, 2016.

GALBRAITH, John. *A moeda: De onde veio, para onde foi*. 2ed. [S.L.]: PIONEIRA, 1977.

GRINBERG, Reuben. *Bitcoin: An Innovative Alternative Digital Currency*, 2011. Disponível em: <<http://www.bitcointrading.com/pdf/bitcoinbyreubengrinberg.pdf>>. Acesso em: Outubro, 2016.

HAYES, Adam S. *Cryptocurrency value formation: An empirical study leading to a cost of production model for valuing bitcoin*, 2016. Disponível em: <<http://www.sciencedirect.com/science/article/pii/S0736585315301118>>. Acesso em: Outubro, 2016.

HERODOTO, Clío: *LIVRO I. FILADÉLFIA: M'CARTY AND DAVIS*, 1844. 31 p.

HODGES, Andrew. *Alan turing: the enigma*. [S.L.]: RANDOM HOUSE, 2012.

INFOMONEY. *A era das moedas digitais*. Disponível em: <<http://educacao.infomoney.com.br/era-moedas-digitais/video-20170818.html>> Acesso em: 11 de nov. de 2017.

KHARPAL, Arjun. *Japanese banks are thinking of making their own cryptocurrency called the J-Coin*, set. 2017. Disponível em: <<https://www.cnbc.com/2017/09/27/japanese-banks-cryptocurrency-j-coin.html>>. Acesso em 28 de out. de 2017.

LOPES, João; ROSSETI, José. *Economia monetária*. 9 ed. [S.L.]: ATLAS, 1998.

MADHVI. *Putin And Ethereum: A Match Made In Fintech*, ago. 2017. Disponível em: <<https://www.forbes.com/sites/madhvimavadiya/2017/08/29/putin-ethereum-fintech/#787263526b5c>> Acesso em: 28 de out. de 2017.

MAR, Alexander Del. *History of monetary systems*. LONDRES: EFFINGHAM WILSON, 1895. 1-2 p.

MISHKIN, Frederic S. *The economics of Money, Banking and Financial Markets*, 1998. Columbia University: Addison Wesley Longman Inc.

NAKAMOTO. Satoshi. *Bitcoin: A Peer-to-Peer Eletronic Cash System*, 2008. Disponível em: <[www.bitcoin.org](http://www.bitcoin.org)>. Acesso em: Outubro, 2016.

NATIONAL BANK OF UKRAINE. *NBU Supports Development of Financial Technology in Ukraine*, set. 2016 Disponível em: <[https://bank.gov.ua/control/en/publish/printable\\_article.jsessionid=C0FCD9EAFBEBE9628685B20102FF09B?art\\_id=36788628&showTitle=true](https://bank.gov.ua/control/en/publish/printable_article.jsessionid=C0FCD9EAFBEBE9628685B20102FF09B?art_id=36788628&showTitle=true)>. Acesso em 28 de out. de 2017.

NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES. *Regulations Of The Superintendent Of Financial Services Part 200. Virtual Currencies*, jun. 2015. Disponível em: <<http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf>> Acesso em: 28 de out. de 2017.

NIKKEI ASIAN REVIEW. *Japan eyes treating bitcoins the same as real money*, fev. 2016. Disponível em: <



*Politics/Japan-eyes-treating-bitcoins-the-same-as-real-money*> Acesso em: 28 de out. de 2017.

OLIVEIRA, Ronielton Rezende. *Criptografia simétrica e assimétrica - os principais algoritmos de cifragem. Segurança Digital, BRASÍLIA, p. 21-24, mar. 2013.*

PINHEIRO, Juliano L. *Mercados de capitais, fundamentos e técnicas.* 2009. São Paulo: Editora Atlas.

PREVIDI, Gustavo de Souza. *Descentralização monetária: Um estudo sobre o bitcoin, 2014. Trabalho de Conclusão de Curso Bacharel em Ciências Econômicas) – Curso de Ciências Econômicas, Universidade Federal do Rio Grande do Sul (UFRGS), Porto Alegre, 2014.*

ROBERTSON, Denis. *A moeda.* 3 ed. [S.L.]: ZAHAR, 1978.

SCARINCI, Filipe. *A factibilidade do bitcoin enquanto moeda: um estudo acerca das criptomoedas, 2015. Trabalho de Conclusão de Curso (Bacharel em Ciências Econômicas) – Curso de Ciências Econômicas, Universidade Federal do Rio Grande do Sul (UFRGS), Porto Alegre, 2015.*

SHINO, Yuya. *Japan considers killing cash by launching own cryptocurrency,* set. 2017. Disponível em: <<https://www.rt.com/business/404771-japan-digital-currency-cash>> Acesso em: 29 de out. de 2017.

SMITH, Adam. *Wealth of nations.* 1 ed. LONDRES: T. NELSON AND SONS, 1884. p.196.

SMYTH, Jamie. *Australia follows Japan in move to regulate bitcoin,* ago. 2017. Disponível em: <<https://www.ft.com/content/4cd5cc3c-8309-11e7-a4ce-15b2513cb3ff?mhq5j=e5>> Acesso em: 28 de out. de 2017.

SWAN, Melanie. *Blockchain: Blueprint for a new economy,* O'Reilly Media Inc. 2015.

ULRICH, Fernando. *Bitcoin – A moeda na Era Digital. Instituto Ludwig Von Mises.Brasil,* 2014. Disponível em: <[http://www.mises.org.br/files/literature/MisesBrasil\\_BITCOIN\\_BROCHURA.pdf](http://www.mises.org.br/files/literature/MisesBrasil_BITCOIN_BROCHURA.pdf)>. Acesso em: Setembro, 2016.

3M. *Immersion cooling for data centers,* 2014. Disponível em: <[https://www.3m.com/3M/en\\_US/novec-us/applications/immersion-cooling/](https://www.3m.com/3M/en_US/novec-us/applications/immersion-cooling/)>. Acesso em 29 de out. de 2017.