UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
FACULDADE DE CIÊNCIAS ECONÔMICAS
DEPARTAMENTO DE ECONOMIA E RELAÇÕES INTERNACIONAIS

ALÍCIA PEREIRA MARQUEZIN

EVOLUÇÃO MONETÁRIA:
UM ESTUDO SOBRE A DEMANDA PELO BITCOIN

Porto Alegre
2017

ALÍCIA PEREIRA MARQUEZIN

EVOLUÇÃO MONETÁRIA:
UM ESTUDO SOBRE A DEMANDA PELO BITCOIN

Trabalho de conclusão submetido ao Curso de Graduação em Ciências Econômicas da Faculdade de Ciências Econômicas da UFRGS, como requisito parcial para obtenção do título de Bacharel em Ciências Econômicas.

Orientador: Prof. Dr. Antônio Ernani Martins Lima

Porto Alegre

2017

CIP - Catalogação na Publicação

Marquezin, Alícia Pereira
EVOLUÇÃO MONETÁRIA: UM ESTUDO SOBRE A DEMANDA PELO BITCOIN / Alícia Pereira Marquezin. -- 2017.
66 f.
Orientador: Antônio Ernani Martins Lima.

Trabalho de conclusão de curso (Graduação) -- Universidade Federal do Rio Grande do Sul, Faculdade de Ciências Econômicas, Curso de Ciências Econômicas, Porto Alegre, BR-RS, 2017.

1. Bitcoin. 2. Demanda por Bitcoin. 3. Evolução Monetária. 4. Moeda Digital. 5. Criptomoeda. I. Lima, Antônio Ernani Martins, orient. II. Título.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica da UFRGS com os dados fornecidos pelo(a) autor(a).

ALÍCIA PEREIRA MARQUEZIN

EVOLUÇÃO MONETÁRIA:
UM ESTUDO SOBRE A DEMANDA PELO BITCOIN

Trabalho de conclusão submetido ao Curso de Graduação em Ciências Econômicas da Faculdade de Ciências Econômicas da UFRGS, como requisito parcial para obtenção do título de Bacharel em Ciências Econômicas.

Orientador: Prof. Dr. Antônio Ernani Martins Lima

Aprovada em: Porto Alegre, 20 de dezembro de 2017.

BANCA EXAMINADORA:

_____
Prof. Dr. Antônio Ernani Martins Lima – Orientador
UFRGS

_____
Prof. Dr. Júlio César de Oliveira
UFRGS

_____
Prof. Dr. Ronald Otto Hillbrecht
UFRGS

AGRADECIMENTOS

Agradeço à minha família, meu pai Ivo, minhas queridas irmãs Aline e Ariane e à minha doce mãe Lúcia que hoje me acompanha em pensamentos em memória e no coração.

Agradeço ao meu noivo, Vinícius, que foi quem primeiro me apresentou o Bitcoin e a partir de tal conhecimento que este trabalho teve origem.

Agradeço ao meu orientador Antônio Ernani Martins Lima, pelas preciosas contribuições, pelo aprendizado e pelo tempo dedicado às correções e às revisões do meu TCC.

Agradeço aos professores Júlio César de Oliveira e Ronald Otto Hillbrecht que aceitaram prontamente o convite para a banca.

Agradeço à todos os professores da UFRGS pelo ensino de qualidade e pela contribuição para o meu desenvolvimento e para minha formação como futura economista.

Agradeço aos meus amigos e colegas da UFRGS que com descontração e companheirismo contribuíram para a minha formação ao longo desse período.

Agradeço à todos os meus amigos que, de alguma forma, me presentearam com pequenas ou grandes contribuições e ensinamentos.

Muito obrigada à todos com muito carinho!

RESUMO

A evolução do dinheiro e da moeda modificou o sistema econômico ao longo dos tempos no que tange às trocas entre os agentes econômicos, além de possibilitar a expansão comercial e o crescimento da economia através da sua migração do escambo para a atual moeda de curso forçado. Entretanto, essa evolução não cessou, e atualmente é possível experimentar outras formas desse progresso monetário, como as criptomoedas ou moedas digitais, destacando-se, em meio a estas, o Bitcoin - a mais famosa delas e objeto de estudo dessa monografia. Dentro da perspectiva das moedas virtuais - e voltado ao Sistema Bitcoin – o presente trabalho expõe as características, o funcionamento, a história e a origem da mesma, além de dados evolutivos e suas vantagens e desvantagens; e, especificamente, se propõe a verificar os motivos da demanda pela referida criptomoeda. Concluindo-se que o Bitcoin suscita demanda e atende aos motivos keynesianos de demanda por moeda, a constar: de transação, de precaução e de especulação de forma peculiar a cada motivo analisado.

Palavras-chave: Bitcoin; Moeda Digital; Criptomoeda; Moeda Descentralizada; Demanda por Moeda.

Classificação JEL: E41 – Demanda por Moeda; E42 – Sistemas Monetários; Padrões; Regimes; Governo e o Sistema Monetário; Sistemas de Pagamento.

ABSTRACT

The evolution of both money and currency has modified the economic system over time on what relates to the exchanges between economic agents, as well as making possible commercial expansion and economical growth through the migration of direct exchanges to the current forced course currency. However, this evolution has not ceased, and nowadays it is possible to experiment other forms of this monetary progress, such as cryptocurrencies or digital currencies, among which Bitcoin stands out as the most famous one and this monography's subject of choice. Within the perspective of virtual currencies, and focused on the Bitcoin System, this paper exposes the characteristics, the operation, the history and the origin of Bitcoin, as well as evolutionary data and both its advantages and disadvantages; specifically, it reaches out to verify the reasons for this cryptocurrency's demand. As a conclusion, Bitcoin leverages demand and gives support to the Keynesian motives for currency demand – transaction, precaution, and speculation – in peculiar form for each analyzed motive.

Keywords: Bitcoin; Digital Currency; Cryptocurrency; Decentralized Currency; Demand for Currency.

JEL Classification: E41 – Demand for Money. E42 – Monetary Systems; Standards; Regimes; Government and the Monetary System; Payment Systems.

LISTA DE FIGURAS

Figura 1 – Carteira de bitcoins *on line*. 36
Figura 2 – Esquema do modelo *peer-to-peer* (P2P). 37
Figura 3 – Últimas transações registradas no *Blockchain*. 38
Figura 4 – Carteira *Blockchain* com últimos blocos minerados. 39
Figura 5 – Relação das quinze *altcoins* com maior *market cap*. 60

LISTA DE GRÁFICOS

Gráfico 1 – Total de bitcoins minerados. 42
Gráfico 2 – Evolução do preço do Bitcoin em dólares. 45
Gráfico 3 – Preço atualizado de uma unidade de bitcoin 46
Gráfico 4 – Número total de transações em bitcoins. 47
Gráfico 5 – Volume diário de transações em bitcoins, medido em bitcoins. 47
Gráfico 6 – Volume estimado de transações diárias medido em dólares. 48
Gráfico 7 – Quantidade de usuários da carteira de bitcoins do *Blockchain*. 49
Gráfico 8 – Evolução da quantidade de usuários da carteira de bitcoins do *Blockchain*. 50

SUMÁRIO

1 INTRODUÇÃO 9

2 A EVOLUÇÃO HISTÓRICA DA MOEDA 13
2.1 CONCEITUAÇÃO, CARACTERÍSTICAS E FUNÇÕES DA MOEDA 13
2.2 HISTÓRIA DA MOEDA 17

3 A DEMANDA POR MOEDA 22
3.1 ABORDANDO A DEMANDA POR MOEDA 22
3.2 OS MOTIVOS PARA DEMANDAR MOEDA PROPOSTOS POR KEYNES 25

4 ENTENDENDO O BITCOIN 27
4.1 CRIPTOGRAFIA E CRIPTOMOEDA 27
4.2 BITCOIN: DEFINIÇÃO E SURGIMENTO 31
4.2.1 Definição: o que é o Bitcoin? 31
4.2.2 Surgimento 33
4.3 COMO FUNCIONA - FUNCIONAMENTO TÉCNICO 35
4.4 ENTRANDO NO MERCADO BITCOIN 42

5 ENQUADRAMENTO GERAL DA DEMANDA POR BITCOIN 44
5.1 ANÁLISE EVOLUTIVA DO BITCOIN 44
5.1.1 Preço 44
5.1.2 Volume de transações 46
5.1.3 *Downloads* de carteiras do *Blockchain* 49
5.2 VANTAGENS E DESVANTAGENS DO BITCOIN 50
5.2.1 Vantagens 50
5.2.2 Desvantagens 52
5.3 O BITCOIN COMO UMA ALTERNATIVA MONETÁRIA 54
5.4 A DEMANDA POR BITCOIN 56

6 CONCLUSÃO 62

REFERÊNCIAS 64

1 INTRODUÇÃO

Assim como a tecnologia, as ciências e os processos evoluíram e continuam a mudar, com a moeda não é diferente, pois ela também se desenvolveu com o passar do tempo. O que começou como uma troca direta de mercadorias, onde os agentes trocavam seus produtos entre si, evoluiu para a troca indireta, onde produtos de vasto interesse em comum assumiram o papel de moeda - favorecendo as trocas entre os indivíduos - a chamada moeda mercadoria, que podia ser representada por produtos como sal, gado, cereais e açúcar, terminando por se fixar nos metais preciosos.

Mas o avanço continuou, e para dispensar o esforço e o custo em carregar metais preciosos, a moeda-mercadoria progrediu e os metais passaram a ser substituídos por notas (moeda-papel), que possuíam a garantia de resgate em quantidade estipulada de metal precioso (ouro, e até o final do século XIX, a prata) e plena conversibilidade, novamente facilitando as transações. Posteriormente, a moeda-papel passou a não estar mais totalmente garantida para troca, por ser parcialmente lastreada, assim o sistema assumiu o uso do papel-moeda, ou moeda fiduciária, não lastreada integralmente e baseada na confiança dos agentes em suas transações. Entretanto, esse sistema ruiu, seja em decorrência de emissões de papel-moeda desproporcionais e audazes em períodos de crises, seja pela relativa escassez de ouro, o que levou o Estado a controlar os mecanismos de emissão de moeda, surgindo assim as moedas de curso forçado, com inexistência de lastro metálico, inconversibilidade absoluta e com monopólio estatal.

O avanço tecnológico e o desenvolvimento da internet propiciaram novas alternativas ao uso da moeda. Os agentes econômicos passam a perder o contato físico com o dinheiro e a fazer as transações via canais eletrônicos, via cartão de débito e crédito, transferências bancárias eletrônicas e modalidades como o *Paypal*[1], *PagSeguro*[2] ou *Samsung Pay*[3]. Esses tipos de uso da moeda para transações possibilitam compras em qualquer lugar do mundo e demonstram que a moeda passa a se desmaterializar, pois o contato com a moeda física passa a ser cada vez menor.

---

[1] *Paypal* é um sistema que permite a transferência de dinheiro entre indivíduos ou negociantes usando um endereço de e-mail, assim, evitando métodos tradicionais como cheques e boleto bancário.

[2] *PagSeguro* é outra forma de pagamento eletrônico para compra de mercadorias para pessoas físicas ou jurídicas efetuarem compras de forma segura via internet.

[3] *Sansung Pay* é um meio de pagamento por celular Samsung onde o usuário cadastra cartões de débito ou crédito e necessita somente aproximar seu celular para autenticar a transação de compra com uso de sua digital.

Mais recentemente surgem novas alternativas monetárias como as moedas virtuais e as moedas sociais, paralelas às moedas oficiais, estas instituídas pelos governos e bancos centrais, enquanto aquelas são criadas e geridas por seus próprios usuários.

Dentre diversas outras, nesse meio destaca-se a criptomoeda Bitcoin, com maior popularidade, aceitação e número de transações, que será objeto de estudo dessa monografia.

O Bitcoin é exposto ao mundo no ano de 2008, quando Satoshi Nakamoto[4] publica um *paper* e o lança na internet explicando a criação e o funcionamento da referida criptomoeda. A moeda Bitcoin tem a particularidade de ser descentralizada e não depender de instituições financeiras para suas transações ou de Bancos Centrais para sua manutenção, pois ela é gerida e criada pelos próprios usuários e transacionada no mundo digital.

O Bitcoin vem ganhando força desde a sua criação, apesar de ser uma moeda recente. E nesse contexto, este trabalho busca analisar a demanda por esse tipo de moeda, se de fato ela existe e se o Bitcoin atende todos os motivos de demanda que uma moeda tradicional possui, usando para tal fim, em especial, os motivos keynesianos de demanda por moeda: transação, precaução e especulação.

O objetivo geral do trabalho consiste em, à luz da evolução das moedas e das teorias da demanda de moeda, avaliar se a criptomoeda Bitcoin atende aos motivos da demanda por moeda, em especial os de transação, de precaução e de especulação.

Já os objetivos específicos deste trabalho são expor a evolução histórica da moeda e suas funções e características; expor as teorias da demanda por moeda, com foco na teoria keynesiana; verificar a origem, a história, a conceituação, as características e o funcionamento do Bitcoin; e avaliar a evolução da moeda Bitcoin e se a mesma atende aos motivos de demanda por moeda (desvendados por Keynes e hoje já estabelecidos e ainda ensinados na academia econômica), com base na literatura, em dados evolutivos do Bitcoin e em estudos empíricos.

A hipótese levantada no estudo visa responder se a criptomoeda Bitcoin atende aos motivos keynesianos de demanda existentes para uma moeda: de transação, de precaução e de especulação.

---

[4] Pseudônimo utilizado pelo (s) criador (es) do sistema Bitcoin, cujo nome e nacionalidade reais ainda são desconhecidos.

Para tanto, este trabalho será subdividido para atender aos objetivos. Sendo a primeira parte responsável pelo esclarecimento quanto à conceituação, às características e às funções da moeda. Além de relatar a história e a evolução da moeda ao longo do tempo até as atuais alternativas, como as moedas digitais ou virtuais.

Na segunda parte do trabalho serão abordados a demanda por moeda e os motivos de demanda por moeda propostos por Keynes.

A terceira parte adentra o Bitcoin, na qual o mesmo será conceituado, ademais o surgimento da criptomoeda e do Bitcoin serão esclarecidos, e o seu funcionamento técnico e do seu mercado também serão analisados.

A quarta parte, nomeada como o capítulo 5, trará informações evolutivas do Bitcoin, no qual dados gráficos apresentarão informações relevantes para esse estudo, além de suas vantagens e desvantagens, desaguando na avaliação se o Bitcoin atende aos motivos de demanda por moeda, objeto precípuo dessa monografia. E por fim será apresentada a conclusão do trabalho.

Para atender aos objetivos do trabalho será feita uma revisão da literatura econômica teórica, mas também de estudos e dados empíricos que contribuam para a finalidade de entender a demanda pela criptomoeda Bitcoin.

Justifica-se a importância desse estudo uma vez que o Sistema Bitcoin de moedas virtuais vem ganhando gradativamente destaque na mídia, nos meios digitais, e até mesmo por parte dos Bancos Centrais mundiais, seja de forma positiva ou negativa, mas cada vez mais pessoas conhecem algo sobre essa moeda.

Segue como exemplo, uma citação publicada no site do Banco Central do Brasil:

> A utilização das chamadas moedas virtuais e a incidência, sobre elas, de normas aplicáveis aos sistemas financeiro e de pagamentos têm sido temas de debate internacional e de manifestações de autoridades monetárias e de outras autoridades públicas, com poucas conclusões até o momento. (BANCO CENTRAL DO BRASIL, 2014, p.1)

Conforme a citação do BCB[5], o debate sobre o Bitcoin, apesar de possuir poucas conclusões até o momento, é de proporções internacionais e prevê declarações das autoridades monetárias, demonstrando a importância sobre o tema.

[5] Sigla para Banco Central do Brasil (pode ser escrita também como BACEN).

Outro indicativo sobre a relevância do assunto são os dados que apontam um aumento considerável no número de transações com a moeda bitcoin, o que pode ser classificado como um evento bem sucedido, já que os números de aceitação para transações estão em constante evolução e isso demonstra uma maior confiança por parte dos usuários para transacionar essa moeda. Outros dados relevantes sobre a força que o Bitcoin vem ganhando, serão apontados graficamente no decorrer dessa monografia.

Outra situação interessante nas transações com bitcoins, é que diversos países e empresas já estão aceitando a moeda como forma de pagamento, o que também eleva sua confiança. A exemplo disso segue um trecho do artigo de Fernando Ulrich:

> Atualmente, a moeda digital inspira soluções criativas para a débâcle econômica da Grécia. Embora o Bitcoin não seja uma solução aos apuros fiscais do governo do país, ele está servindo como refúgio genuíno para o povo grego, impossibilitado de transferir dinheiro ao exterior e refém de um possível confisco ou retorno ao antigo dracma.
> Hoje, empresas do calibre de Dell e Microsoft aceitam bitcoins como forma de pagamento. Consultorias como a Deloitte testam a utilização do blockchain — o grande "livro-contábil" do Bitcoin — para processos de auditoria. O governo de Honduras estuda um projeto-piloto para registrar a titularidade de terras no blockchain. (ULRICH, 2015, p.4).

Conforme citação do autor empresas globais, de grande porte, estão aceitando transações com bitcoins além de países com alguma dificuldade, como na citação feita sobre a Grécia, o que demonstra que a unidade monetária bitcoin passa a ser uma segunda alternativa à moeda oficial em determinadas situações e lugares, além de revelar a procura por essa moeda.

2 A EVOLUÇÃO HISTÓRICA DA MOEDA

A moeda tem papel fundamental na sociedade, pois além de ser condição essencial para a existência do Sistema Financeiro, através dela é possível transacionar de forma mais rápida, eficiente e em maiores proporções do que em sistemas anteriores, como o escambo.

A moeda pode ser descrita de forma abrangente como alguma coisa que é aceita pela coletividade e desempenha as funções de meio ou instrumento de troca, unidade de conta e reserva de valor. (GREMAUD *et al*., 2003).

Ademais a moeda é um objeto que responde a uma necessidade social decorrente da divisão do trabalho, característica da economia capitalista moderna, que especializou indivíduos e unidades de produção. Reduzindo, assim, o tempo para se concretizar uma operação comercial, já que a moeda cumpre o papel de intermediária (CARVALHO *et al*., 2007).

Visando entender a moeda Bitcoin, e situar o seu lugar na evolução monetária, este capítulo pretende resgatar a origem e a história da moeda. Ainda, como o objeto deste trabalho é um tipo de moeda, faz-se necessário entender as características e as funções da mesma.

Portanto, este capítulo abrangerá em um primeiro momento o conceito, as funções e as características relevantes da moeda, e em segundo a história da moeda e sua evolução do escambo até as moedas atuais de curso forçado.

2.1 CONCEITUAÇÃO, CARACTERÍSTICAS E FUNÇÕES DA MOEDA

A fim de demonstrar a evolução da moeda, do seu formato mais primitivo até os moldes atuais - como a criptomoeda Bitcoin - primeiramente é importante saber como se classifica e conceitua a moeda.

De acordo com Galbraith (1983) o conceito de moeda é aquilo que é comumente oferecido ou recebido pela compra ou venda de bens, serviços ou quaisquer outras coisas. Para o autor o significado é descomplicado mesmo, simples e sem delongas, e

qualquer tentativa de complexidade para o tema é uma forma de disfarçar a simplicidade sobre o mesmo.

Hillbrecht (1999) complementa que a concepção de moeda para os economistas é aquilo que geralmente é aceito como meio de pagamento por bens e serviços e como pagamento ou liquidação de dívidas, além de também ser conhecida como meio de troca. Moeda também é considerada um ativo, ou seja, algo de valor que se possa possuir. Sendo a riqueza dos indivíduos composta por suas moedas e seus ativos.

Outra análise verificada é que a moeda, mesmo em seu estágio mais primordial e antigo é utilizada para intermediar processos rudimentares de troca, pode ser conceituada como um bem econômico qualquer que desempenha as funções básicas de intermediário de trocas, que serve como medida de valor e que possui aceitação geral. Além disso, como a moeda representa um poder de aquisição, desde o momento em que é recebida até o momento em que é dada em pagamento de outra transação, ela também se caracteriza como uma reserva de valor. (LOPES; ROSSETTI, 2005).

Desse modo, as três principais funções da moeda são entendidas como:

1) Intermediária de trocas (ou meio de trocas);

2) Medida de valor (ou unidade de medida);

3) Reserva de valor. (FROYEN, 2013; HILLBRECHT, 1999; LOPES E ROSSETTI, 2005).

Os autores Lopes e Rossetti (2005) complementam e listam outras três funções da moeda conforme a seguir:

4) Liberatória;

5) De padrão de pagamentos diferidos;

6) De instrumento de poder.

A primeira função, de intermediária de trocas, é definida por Lopes e Rossetti (2005) como a função essencial da moeda e, geralmente, caracterizada como a razão principal do seu aparecimento. Essa função permite a superação da economia de escambo e a passagem à economia monetária.

De acordo com Hillbrecht (1999), a função meio de troca da moeda é um meio de pagamento normalmente aceito para liquidar transações de bens e serviços e por ser

amplamente aceito elimina a necessidade de dupla coincidência de desejos. Assim como Froyen (2013), que acrescenta que a moeda serve como meio de transação através da qual compram-se bens e serviços com a mesma.

A segunda função da moeda apresentada, de medida de valor (ou unidade de medida) permite que se possa medir valor em uma economia em termos de moeda, ou seja, ao invés de ter preços para cada mercadoria em termos de outra mercadoria a unidade de medida vai medir em unidades monetárias, simplificando o processo (como dólares ou reais). De acordo com os autores "a utilização generalizada da moeda implica a criação de uma unidade-padrão de medida, à qual são convertidos os valores de todos os bens e serviços disponíveis." (LOPES; ROSSETTI, 2005, p. 20). E a sua função torna-se clara quando imaginamos uma economia de escambo, ou seja sem moeda, e portanto, sem uma unidade de conta, na qual cada produto tem seu valor expresso em relação a todos os demais produtos disponíveis.

A terceira função, de reserva de valor, permite que se possa poupar poder de compra da renda recebida no presente para efetuar gastos no futuro, ou seja, permite que se possa transferir consumo e gastos para o futuro. (HILLBRECHT, 1999). Sendo assim, a moeda pode funcionar como um estoque de riqueza, um modo de economizar e poupar para gastos futuros, funcionando como um ativo financeiro (FROYEN, 2013).

Lopes e Rossetti (2005) acrescentam que a função de reserva de valor da moeda, além da capacidade de guardar riqueza, assim como outros ativos financeiros, é também um reservatório por excelência de poder de compra, pois a moeda possui liquidez por excelência. Os autores explicam que Keynes, em seu livro clássico *A Teoria Geral* (1936) trouxe a função de reserva de valor para o primeiro plano ao enfatizar a incerteza inerente a uma economia monetária. A proporção da moeda conservada em relação aos outros ativos é exercida pelo grau de preferência pela liquidez.

A quarta, a quinta e a sexta funções da moeda, são funções que não constam de forma generalizada nas bibliografias, mas são apresentadas por Lopes e Rossetti (2005). A quarta função da moeda, a função liberatória, apresenta o poder da moeda, como nenhum outro ativo, de saldar dívidas, liquidar débitos, e de livrar seu detentor de uma situação passiva. Esse poder é garantido pelo Estado, que é a única instituição que pode forçar o curso da moeda, impondo sua aceitação como forma de pagamento. A função de pagamentos diferidos, tida como a quinta função "resulta de sua capacidade de facilitar a distribuição de pagamentos ao longo do tempo, quer para a concessão de

crédito ou de diferentes formas de adiantamentos", e é relevante para viabilizar fluxos de produção e renda (LOPES; ROSSETTI, 2005, p. 23). E a sexta e última função desempenhada pela moeda é a de instrumento de poder - de poder econômico, político e social. Essa função existe efetivamente a medida em que se admite a moeda como um título de crédito, e os que o detêm possuem direitos de haver sobre os bens e serviços disponíveis no mercado. Em essência, esses direitos levam a uma espécie de poder de decisão que conduzem a uma forma de poder econômico.

A fim de desempenhar suas funções recém examinadas, a moeda deve seguir algumas características que são essenciais.

As características de maior relevância que a moeda deve cumprir são (LOPES; ROSSETTI, 2005):

1) Indestrutibilidade e inalterabilidade;

2) Homogeneidade;

3) Divisibilidade;

4) Transferibilidade;

5) Facilidade de manuseio e transporte.

A moeda então, de acordo com a primeira característica, deve ser suficientemente durável, a fim de que não se destrua ou se deteriore, à medida que os agentes econômicos a manuseiam para intermediar trocas. A característica da homogeneidade diz respeito à padronização, em que duas unidades monetárias distintas, de igual valor devem ser iguais rigorosamente. A terceira característica, da divisibilidade, é necessária pois a moeda deve poder ser fracionada em múltiplos e submúltiplos, para que qualquer tipo de transação, de pequeno ou grande porte possam ser realizadas sem dificuldades (LOPES; ROSSETTI, 2005).

A penúltima característica, a transferibilidade, diz respeito à facilidade com que se deve processar uma transferência monetária de um possuidor para outro. Os autores Lopes e Rossetti (2005) exemplificam essa característica com o gado, pois na sua utilização como moeda-mercadoria, caso fosse necessário gravar a fogo sua marca na pele do animal, chegaria um momento em que, após diversas transações, não restariam espaços para novas marcas. E por fim, a sexta característica da moeda, a facilidade de manuseio e transporte, informa que o manuseio e transporte da moeda não pode ser

prejudicado na sua utilização, pois, no caso de ser dificultado, sua utilização será gradativamente descartada (LOPES; ROSSETTI, 2005).

Quando uma moeda possui as características físicas essenciais, pode-se dizer que ela está habilitada as desempenhar suas três funções monetárias de meio de troca, unidade de conta e reserva de valor (CARVALHO *et al*., 2007).

2.2 HISTÓRIA DA MOEDA

Esclarecido o conceito de moeda, suas funções e suas características é mais fácil entender porque ela surgiu. Além de sua necessidade frente a uma economia que foi se desenvolvendo e necessitava superar obstáculos para evoluir seu sistema. Além do mais, a divisão do trabalho e a especialização individual intensificaram a necessidade de um regime social de interdependência (LOPES; ROSSETTI, 2005).

No decorrer deste tópico, será apresentado a história da moeda contemplando o período desde sua origem até o atual modo de utilização.

No livro de Hillbrecht (1999), o autor esclarece que, nas sociedades mais primitivas e em seus estágios iniciais de desenvolvimento, os indivíduos eram relativamente autossuficientes, ou seja, se auto supriam daquilo que necessitavam para o seu consumo individual. Esse processo impedia a geração de riqueza pois não havia especialização naquilo que cada um sabia fazer melhor, alocando esforços de maneira não eficiente.

Já as sociedades mais complexas, geravam ganhos proporcionados pela especialização. Nessas sociedades os indivíduos são mais eficientes pois são especializados na produção de bens que possuem melhor aptidão, e então trocam parte de seu produto por outros que desejam consumir (HILLBRECHT, 1999).

Senna (2010) relata que Adam Smith em seu livro *The wealth of nations* observou que, até mesmo nas sociedades primitivas, já se fazia presente uma tendência à especialização do trabalho. Pois nas tribos de caçadores, alguns se mostravam mais capazes e rápidos de produzir arcos e flechas do que outros, sendo assim, conseguiam produzir uma quantidade maior do que a necessária para seu consumo individual, podendo trocar esses produtos por outros que necessitassem. Ao mesmo tempo, outros

se descobriam melhor dotados para construir cabanas, ou ferramentas, ou roupas, podendo trocar seu excedente produtivo pelo excedente de outras pessoas.

Uma maneira inicial de estabelecer trocas entre indivíduos, provenientes dos seus ganhos com a especialização acima do seu consumo individual, é o escambo, situação na qual as pessoas trocam seus produtos diretamente com as outras. (HILLBRECHT, 1999).

Uma troca através do escambo se dá, por exemplo, quando um produtor de batatas que necessite vestimentas, troca com um fabricante de roupas um saco de batatas por duas peças de roupas. Cada um deles é especializado em fazer melhor aquele produto, mas também necessita de outros bens ou serviços (HILLBRECHT, 1999).

A maior dificuldade do escambo é, em primeiro lugar, combinar a dupla coincidência de desejos e em segundo é precificar cada item em relação a todos os outros produtos do mercado, por exemplo um saco de batatas deve ser precificado em relação ao pão, a ovos, a cadeiras, etc. o que dificulta e aumenta os custos de transação (HILLBRECHT, 1999)

Para Rothbard (2013) o processo de escambo, também chamado de trocas diretas, similarmente ao autor anterior, também apresenta duas dificuldades a “indivisibilidade”, é difícil trocar todos os bens, e a “coincidência de desejos”, que é necessária para que ocorra a troca. Devido a esses problemas o escambo dificilmente seria capaz de manter uma economia acima de seu nível mais primitivo.

Devido a tais problemas o homem conseguiu evoluir para o sistema de trocas indiretas, que permitiu que a economia crescesse de forma contínua. Nas trocas indiretas, o indivíduo vende seu produto em troca de um outro mais comercializável no qual poderá trocar pelo bem que realmente deseja no futuro (ROTHBARD, 2013). Assim, se o produto A (exemplo a manteiga) é altamente demandado no mercado, os indivíduos vão trocar suas produções por manteiga, para posteriormente ter maior facilidade em trocar por aquilo que realmente desejam. A manteiga passa a ser uma espécie de moeda, sendo usada como meio de troca.

Lopes e Rossetti (2005) expõem que as primeiras moedas foram mercadorias que deveriam ser suficientemente raras (para que tivessem valor de troca) e deveriam atender uma necessidade comum e geral (para que tivessem valor de uso). As moedas-mercadorias variaram de acordo com cada comunidade e alguns exemplos são: o cobre,

a cevada e os escravos na Antiguidade; as moedas de couro, o gado e alguns cereais na Idade Média; o fumo, as carnes-secas, a madeira e os metais preciosos na Idade Moderna. Para Rothbard (2013) também diversos bens, ao longo da história foram usados como meio de troca, como: tabaco, açúcar, sal, gado, grãos, conchas, etc. Posteriormente, metais preciosos, como ouro e prata.

De acordo com Hillbrecht (1999), o primeiro modelo de um sistema de pagamentos utilizava metais preciosos e essa forma de moeda era chamada de moeda-mercadoria. A moeda mercadoria tinha o seu valor na dependência de seu peso e na pureza do metal, isso acabou tornando-se um problema, pois os mercadores tinham elevados custos de transação para transportar grandes quantidades de metal, além de correr o risco de serem roubados.

A solução para tal problema foi a estocagem da moeda-mercadoria (metais preciosos) e a emissão de certificados que representassem os valores em metais preciosos que eram emitidos por governos ou instituições privadas e que poderiam ser convertidos a qualquer momento, assim os certificados eram totalmente lastreados nos metais de valor e esses certificados eram denominados de moeda-papel (HILLBRECHT, 1999).

Entretanto, conforme declaram Lopes e Rossetti (2005), os então “guardiões dos metais preciosos” começaram a emitir certificados não integralmente lastreados da moeda-papel, dando origem ao papel-moeda, com lastro inferior a 100%. Esse processo evoluiu para o que hoje chamamos de moeda-fiduciária.

A denominação, portanto, de moeda fiduciária advém do fator de confiança da sociedade nos agentes responsáveis pela guarda de suas reservas monetárias metálicas o que implica confiança na solidez da função de intermediação exercida pelos mesmos. São características do papel-moeda fiduciário o lastro inferior a 100%, menor garantia de conversibilidade (em contrapartida a moeda papel) e a emissão feita por particulares (LOPES; ROSSETTI, 2005).

Após tentativas mal sucedidas de reestabelecer a conversibilidade monetária qualquer tipo de lastro foi sendo desvinculado por completo. Atualmente os sistemas monetários estabelecidos e aceitos por lei são denominados de curso forçado, no qual prevalecem as características de: inexistência de lastro metálico, inconversibilidade absoluta e monopólio estatal nas emissões da moeda (LOPES; ROSSETTI, 2005).

Outra evolução do sistema foram os cheques, que são promessas de pagamento em dinheiro. O cheque evita que se transacione um valor muito elevado de notas e pode ser sacado ou depositado em instituições bancárias (pode ser chamado de moeda bancária). Entretanto, o processo de transações com cheques é um pouco mais burocrático, e, na opção de depósito pode ser necessário esperar dias para compensação. Porém, as evoluções tecnológicas em informática e telecomunicação vem possibilitando transações ainda mais eficientes. Operações podem ser feitas com cartões de débito e/ou crédito, além dos sistemas de transferências *online* feitas por computador e com uso da internet (HILLBRECHT, 1999).

Atualmente as moedas emitidas pelos governos não possuem mais nenhum lastro e são baseadas na confiança dos agentes econômicos. Mas, em uma economia moderna, a oferta de moeda não é composta apenas por cédulas e moedas de metal; os depósitos bancários também fazem parte da oferta monetária, uma vez que desempenham a mesma função que a moeda física. Ainda que não "existam" materialmente, os depósitos constituem parte da oferta monetária total (ULRICH, 2014).

De acordo com Ulrich (2014) a expansão do crédito pelo sistema bancário aumenta a quantidade de moeda no mercado, e consequentemente, gera inflação. Além disso contribui com a formação de ciclos econômicos, o que gera crises financeiras. Para o autor, nesse contexto, começa a ganhar vida a discussão de uma nova forma de dinheiro, as criptomoedas.

Em 2008 é publicado um *paper* baseado na ideia de um “dinheiro eletrônico” descentralizado e sem a necessidade de um terceiro fiduciário e, a partir dessa ideia, surge o Bitcoin, a mais nova forma de dinheiro com novas propostas para o método atual, sem a dependência do Estado ou Bancos Centrais para operar e de acesso global.

Desse modo, é possível verificar de acordo com o que foi visto até o momento, que a moeda deve exercer três funções principais a fim de desempenhar seu papel na sociedade: a de meio de troca, a de reserva de valor e a de unidade de conta. Além de possuir seis características para o bom desempenho de suas funções: indestrutibilidade, homogeneidade, divisibilidade, transferibilidade e facilidade de manuseios e transporte.

A moeda, entretanto, evoluiu desde a sua origem deixando, inclusive, de ser material. A desmaterialização da moeda abriu espaço para seus novos formatos e até

mesmo para moedas externas ao regime regulamentado pelo Sistema Financeiro, como a criptomoeda Bitcoin, objeto de estudo desta monografia. Sendo assim, faz-se necessário, além de conhecer as características, as funções e a história da moeda, entender também o que gera sua demanda, análise que será feita no próximo capítulo.

3 A DEMANDA POR MOEDA

Este trabalho se propõe a tentar verificar a demanda pela criptomoeda Bitcoin. Se de fato ela existe e em quais situações ela se dá - visto que o Bitcoin opera como um complemento a moeda corrente e não isoladamente. Para tanto, será verificado se o Bitcoin atende aos motivos de demanda por moeda propostos por Keynes e aceitos pelas demais escolas econômicas.

O cerne deste capítulo é, portanto, a teoria keynesiana de demanda por moeda, porém aponta outros autores importantes que tratam do tema, mas de forma apenas superficial, o que será visto na primeira parte do item terceiro. Na segunda parte do capítulo serão analisados os motivos de demanda por moeda keynesianos.

3.1 ABORDANDO A DEMANDA POR MOEDA

Anteriormente à abordagem keynesiana, o autor Irving Fischer, inspirado em outros autores como Simon Newcomb e dando continuidade à Teoria Quantitativa da Moeda (TQM), pressupôs em seu livro *"The Purchasing Power of Money, its Determination and Relation to Credit, Interest and Crises"*, a existência de uma relação estável entre a demanda por moeda e o rendimento nominal, admitindo que a velocidade de circulação da moeda é constante no curto prazo, pois depende essencialmente de aspetos institucionais e tecnológicos (REGALADO, 2015).

Essa teoria não considera a taxa de juros para análise, partindo do pressuposto que a mesma não tem efeito sobre a demanda por moeda. "Na teoria clássica, a quantidade de moeda determina a demanda agregada, que, por sua vez, determina os níveis de preços." (FROYEN, 2013, p. 56). Além do mais, de acordo com essa teoria, a demanda por moeda (M^d) é função do rendimento nominal (PY), sem o efeito da taxa de juros sobre a demanda por moeda conforme a expressão: $M^d = \frac{PY}{V}$, sendo (V) a velocidade constante de circulação da moeda (REGALADO, 2015). Tal expressão foi posteriormente dada em equivalência na abordagem de Cambridge da TQM, por Alfred Marshall, pela fórmula $M^d = \frac{1}{K}.PY$, onde V e 1/k são equivalentes. (FROYEN, 2013).

Posteriormente à Teoria Quantitativa da Moeda, Keynes apresenta outra abordagem para explicar a demanda por moeda, abandona o pressuposto clássico e atribui à taxa de juros papel importante para explicar tal demanda.

A moeda, na concepção keynesiana, não é neutra, ou seja, não é apenas um meio de troca que estabelece uma conveniente ponte entre os fluxos de entrada e saída de recursos, como determinava a teoria clássica. Ela é também reserva de valor, pois possui o atributo de transportar riqueza no tempo, assim ela desempenha duplo papel de meio de pagamento e forma de riqueza (CARVALHO *et al.*, 2007).

A moeda na visão keynesiana é tida como um ativo, que possui a maior liquidez dentre todos os demais ativos. E o retorno pela retenção de moeda é dado na forma de prêmio pela liquidez.

Uma característica da economia monetária é possuir incertezas. Quanto maior as incertezas do futuro percebidas pelos agentes econômicos, maior será a tendência à retenção de moeda. Dessa forma, quando, *coeteris paribus*[6], mais incerto for o futuro, maior será a preferência pela liquidez (CARVALHO *et al*., 2007).

De acordo com Keynes (1985), a preferência pela liquidez dos indivíduos é representada por uma escala do volume dos seus recursos, medidos em termos monetários ou em unidades de salário, na qual deseja conservar em forma de moeda em diferentes circunstâncias.

Ademais, conforme explica Carvalho *et al.* (2007), a não neutralidade da moeda, mesmo em longos períodos, é baseada na proposição de que a moeda e ativos não reprodutíveis são formas de acumulação de riqueza alternativas a acumulação de bens de capital, e, dessa forma, o agente que reter moedas (e outros ativos líquidos) na forma de ativo, e em um momento de maior incerteza, está agindo de forma racional. Uma vez que, quanto maior a incerteza, o agente pode (e muitas vezes prefere) aplicar seus recursos em ativos não reprodutíveis, como moeda e demais ativos líquidos, ao invés de aplicar em ativos reprodutíveis, como ativos de capital.

De acordo com a abordagem keynesiana o indivíduo consumirá parte da sua renda - situação denominada por Keynes de propensão a consumir - e reservará outra parte de alguma forma para consumo no futuro. Na situação onde o agente econômico

[6] *Coeteris paribus*, também grafado como *ceteris paribus*, é uma expressão do latim que pode ser traduzida por "todo o mais é constante" ou "mantidas inalteradas todas as outras coisas".

opta por poupar parte de sua renda para o futuro é relevante saber de que forma o mesmo irá querer fazer isso. Se deseja conservá-la de forma líquida (equivalente a dinheiro) ou se está disposto a alienar parte dessa renda, por determinado período, esperando alguma recompensa por tal situação (KEYNES, 1985).

De acordo com Keynes (1985) quem guarda as suas economias em forma de dinheiro líquido não ganha juros, mesmo que economize; e pelo contrário, quem renuncia a liquidez por um período determinado tem a recompensa dada pela taxa de juros aplicada sobre o montante.

Como salienta Carvalho *et al.* (2007), a taxa de juros é definida, na concepção keynesiana, como uma recompensa por abdicar da liquidez e, portanto, da riqueza na forma monetária, tendo em vista que a moeda é o ativo com o maior prêmio pela liquidez. A taxa de juros é apontada como a recompensa por não entesourar, é o que se ganha por aplicar esse ativo em outros ativos (ativos financeiros) que não a moeda. E não pelo adiamento do consumo.

Carvalho *et al.* (2007, p. 48) sintetiza explicando que para Keynes a moeda "é uma forma de riqueza e a taxa de juros o preço que guia a escolha entre as formas líquida e ilíquida de riqueza, ao invés da escolha entre consumo presente e consumo futuro, concebida pela teoria clássica".

Em contrapartida à Keynes, Milton Friedman aprimora o modelo da TQM em relação ao modelo tradicional de Fischer (ou à versão de Cambridge). Segundo Friedman (1997) a teoria quantitativa é primeiramente, uma teoria da demanda por moeda, e não uma teoria do produto, ou da renda monetária, ou do nível de preços. Friedman examinou mudanças que necessitavam ser feitas na teoria de demanda por moeda de Cambridge à luz da teoria de demanda por moeda de Keynes. Porém a teoria de Friedman difere da keynesiana em vários aspectos, pois Friedman considera a demanda por moeda estável, enquanto Keynes considera instável; Friedman inclui outras possibilidades de ativos, enquanto Keynes considerava basicamente títulos; além da divergência que ambos têm referente as políticas monetárias e fiscal, na qual Keynes apoia maior interferência e o Friedman não (FROYEN, 2013).

Após esse percurso de teorias da demanda por moeda que inicia nos quantitativistas clássicos, passa por Keynes e depois avança para os monetaristas, como o Friedman, ainda existem outros estudos que foram evoluindo a partir das teorias

consagradas até o momento, como as análises dos neo keynesianos, que avançaram nos estudos de Keynes após sua morte em 1946.

Existem diversos autores com diversos enfoques distintos, porém esse trabalho fará menção aos motivos de demanda por moeda propostos por Keynes, estes serão melhor analisados no item a seguir.

3.2 OS MOTIVOS PARA DEMANDAR MOEDA PROPOSTOS POR KEYNES

Em seu livro *"The General Theory of Employment, Interest and Money"* publicado em 1936 Keynes apresenta três divisões na preferência pela liquidez que são definidas como os "motivos que a governam", são eles:

(i) o motivo transação, isto é, a necessidade de moeda para as operações correntes de trocas pessoais e comerciais;
(ii) o motivo precaução, ou seja, o desejo de segurança com relação ao equivalente do valor monetário futuro de certa parte dos recursos totais;
(iii) o motivo especulação, isto é, o propósito de obter lucros por saber melhor que o mercado o que trará o futuro. (KEYNES, 1985).

Entretanto, Carvalho *et al.* (2007) acrescenta que, após o livro da Teoria Geral de Keynes e em resposta a uma crítica feita ao seu livro, Keynes publica na revista *The Economic Journal* em 1937 um quarto motivo: o motivo financeiro (*finance motive*). De acordo com o autor, os então quatro motivos de demanda por moeda, são explanados conforme segue:

a) Motivo transação: este motivo refere-se à retenção de moeda para o ato de compra em data definida. O motivo transação incorpora a visão de moeda com funções similares a da TQM, pois a moeda é demandada para fins de compra e venda de bens e serviços;
b) Motivo precaução: este motivo de retenção de moeda visa atender às contingências inesperadas e às oportunidades imprevistas na realização de negócios vantajosos. Via de regra esse motivo tem associação a gastos inesperados, como por exemplo, contas de hospital, porém Keynes ressalta também a retenção com a pretensão de aproveitar barganhas futuras. Esse motivo pode ser associado a incerteza, no sentido que, os

agentes irão demandar moeda a fim de obter segurança frente a dificuldades imprevistas no futuro;

c) Motivo especulação: este motivo está relacionado com a incerteza em relação ao comportamento futuro da taxa de juros, variando a demanda por moeda para atender esse motivo, de acordo coma variação da taxa de juros. Assim, de acordo com a preferência pela liquidez, a demanda por moeda aumenta à medida que a taxa de juros reduz. Entretanto, quando a taxa de juros se torna em algum patamar baixa, a demanda por moeda torna-se elástica, fenômeno que ficou conhecido como armadilha da liquidez. Desse modo, a incerteza em relação as variações futuras da taxa de juros é o fator determinante que explica a demanda especulativa por moeda, e justifica a conservação de recursos líquidos.
d) Motivo financeiro: o motivo financeiro diz respeito à demanda por moeda antecipada a alguma despesa discricionária planejada, não rotineira e de grandes proporções, como o investimento em bens de capital. Sendo assim, este motivo pressupõe um investimento planejado (*ex ante*) e que pode precisar de provisão financeira para garanti-lo, ocasionando a demanda temporária e excepcional por moeda. De acordo com a afirmação de Keynes, a demanda financeira fica entre a demanda transacional e as demandas precaucional e especulativa. (CARVALHO *et al*., 2007).

Após análise das características e da história da moeda e também dos motivos que geram a demanda por moeda, torna-se crucial conhecer as características da moeda Bitcoin, que é propósito desta monografia. Informações relevantes sobre o Bitcoin e serão analisadas no capítulo que segue.

4 ENTENDENDO O BITCOIN

O Bitcoin é uma criptomoeda que ganhou fama e melhor se inseriu no ramo de moedas digitais. Isso porque surgiu com a proposta inovadora de ser descentralizada, controlada pelos próprios usuários e totalmente digital, e com a possibilidade de ser transacionada ao redor do mundo com baixíssimos custos de transações.

Foi idealizada em 2008 por Satoshi Nakamoto[7] e é baseada no sistema *peer-to-peer*[8] (ou ponto a ponto), que é de grande relevância para a manutenção e sucesso da continuidade do Sistema Bitcoin.

Nesse capítulo será descrito o Bitcoin, o que é, como surgiu e como funciona, a fim de entender as características da criptomoeda que vem sendo, cada vez mais, transacionada no mercado. Seja para transações de compra e venda, seja para especulação ou seja como forma de driblar o sistema monetário tradicional que centraliza a emissão de moeda, ou por quaisquer demais motivos o Bitcoin, de alguma forma, passou a ser notícia e ganhar aceitação e, por isso, é interessante conhecer suas propriedades e particularidades. Além disso, será exposto o conceito de criptografia, essencial para entendimento de uma criptomoeda como o Bitcoin.

4.1 CRIPTOGRAFIA E CRIPTOMOEDA

O termo criptografia deriva-se de duas palavras de origem grega – *kryptós* e *gráphein* – que significam respectivamente, “oculto” / “escondido” e “escrita”.

A palavra criptografia designa a prática de se comunicar em código e possui origem do termo grego para “escrita secreta”, como demonstra Julian Assange em seu livro “Cypherpunks: Liberdade e o futuro da internet”. No qual o autor expõe como o grupo Cypherpunk[9] utiliza-se da criptografia para defender a liberdade e provocar

[7] Pseudônimo utilizado pelo (s) criador (es) do sistema Bitcoin, cujo nome e nacionalidade reais ainda são desconhecidos.

[8] *Peer-to-peer* pode ser traduzido como ponto-a-ponto e também é encontrado como P2P, refere-se aos sistemas que trabalham como uma organização coletiva, porém de forma descentralizada, permitindo que cada indivíduo interaja diretamente com outros. No caso do Bitcoin, a rede é construída de modo que cada utilizador transmite as transações a outros, mas sem a existência um servidor central.

[9] Cypherpunk é um grupo informal, que teve origem nos anos 1990, de pessoas interessadas em criptografia.

mudanças sociais e políticas na internet. Membros deste grupo, posteriormente, incitarão as ideias de Satoshi Nakamoto.

A criptografia utilizada para o Bitcoin (e para uso de criptomoedas em geral) não era uma ideia nova, pelo contrário, ela já havia sido explicitada por Wei Dai[10] em 1998, no grupo de discussão Cypherpunk, o qual o mesmo fazia parte. O autor foi motivado por Tim May (fundador do grupo) e demonstrou sua euforia pelo tema quando iniciava sua citação no grupo dizendo estar fascinado com a cripto-anarquia de Tim May. Wei Dai expõe as principais caracteríticas do protocolo de uma criptomoeda e o necessário para a mesma funcionar na prática. Nessa mesma discussão o autor propõe o *b-money*[11], que posteriormente vai inspirar Satoshi Nakamoto para a criação do Bitcoin.

Já a criptografia descrita especificamente para o Bitcoin pode ser avaliada como "o ramo da matemática que nos deixa criar provas matemáticas que fornecem um alto nível de segurança" de acordo com o Bitcoin.org (2017). Que também explica que a criptografia já vem sendo utilizada em comércios online e bancos, e que no caso do Bitcoin, "a criptografia é utilizada para fazer com que seja impossível para qualquer um gastar fundos da carteira de outro usuário ou corromper a *blockchain*[12]".

Por intermédio do livro "Descobrindo a Bitcoin" de Silva e Albuquerque (2017, p. 19) a definição de criptografia se dá pelo "[...] conjunto de regras que tem por objetivo codificar informações de modo que apenas o emissor e o receptor consigam decifrá-las.". A aplicação da criptografia é intrínseca à matemática e aborda duas chaves: a chave simétrica (chave única) – também chamada de chave privada - e a chave assimétrica (chave pública). As chaves criptográficas se baseiam em algoritmos para codificar ou decodificar informações.

Com base no trabalho de Araújo e Machado (2015) a criptografia também pode prover autenticação, integridade e a não rejeição da mensagem. O autor descreve e explica cada item como: a autenticação consiste em possibilitar que o receptor da mensagem possa averiguar se esta é original; a integridade permite saber se a mensagem

[10] Wei Dai é um engenheiro de informática e membro do grupo Cypherpunk. Estudioso da criptografia e com contribuições para a área. Também reconhecido por ser o criador do *b-money*.

[11] *B-money* é a proposta inicial criada por Wei Dai para um sistema eletrônico de caixa eletrônico anônimo e distribuído.

[12] *Blockchain* é uma tecnologia que utiliza a descentralização como forma de segurança. Funciona como um livro-razão, porém de forma pública, compartilhada e universal, que cria consenso e confiança na comunicação direta entre duas partes, e não possui intermediários. São bases de registros e dados distribuídos e compartilhados que possuem a função de criar um índice global para todas as transações que ocorrem em um determinado mercado.

foi alterada na transmissão e a não rejeição faz com que o remetente não possa alegar não ter enviado a mensagem depois que o fez.

Uma explicação de como funciona esse processo é dado por Skudnov (2012) no parágrafo a seguir:

> Se duas partes desejarem enviar mensagens de forma segura, eles precisam usar *encryption*[13] para esconder o conteúdo da mensagem *plaintext*[14] e transformá-la em *ciphertext*[15]. A parte receptora da mensagem pode realizar *decryption*[16] para reverter a mensagem para *plaintext.* Normalmente o algoritmo para realizar a *encryption* e a *decryption* são de conhecimento geral (chave pública), mas a chave para realizá-las é mantida em segredo (chave privada). (SKUDNOV, 2012 p. 8).

Ou seja, no caso de uma transação em bitcoins, a chave pública ficará disponível no *blockchain*, para que todos os usuários tenham acesso, entretanto a chave privada é de uso exclusivo do usuário que vai realizar a transação.

Nesse sentido, a criptografia é utilizada para proteger dados sigilosos armazenados em computadores, além de proteger backups contra invasões e proteger as comunicações feitas pela internet de forma geral, como e-mails e transações bancárias. Já a chave criptográfica é um valor secreto que modifica o algoritmo, de acordo com Silva e Albuquerque (2017). As autoras exemplificam a chave criptográfica da seguinte maneira:

> Por exemplo, podemos compará-la a uma fechadura que tem uma série de pinos em que cada um desses pinos tem múltiplas posições possíveis; quando uma chave é introduzida na fechadura, cada um desses pinos se move para uma posição imposta pela chave para que a fechadura seja aberta, podendo abrir ou não. Assim funciona uma chave criptográfica. (SILVA E ALBUQUERQUE, 2017, p.21).

Uma criptomoeda é, portanto, nada mais do que uma moeda digital criptografada. E o Bitcoin – e tantas outras moedas digitais – contam com essa tecnologia para funcionar. Mas além da criptografia o Bitcoin ainda soma a tecnologia *peer-to-peer* para o seu desempenho. Portanto, o Bitcoin é a junção da criptografia com a rede *peer-to-peer*. A primeira sendo bastante antiga, mas revelando um potencial superior após a era da computação e a segunda sendo possível somente após o advento da internet.

---

[13] Traduzido para o português significa criptografia.
[14] Pode ser traduzido como texto simples.
[15] Pode ser traduzido como texto criptografado.
[16] Pode ser traduzido como descriptografia.

Para Ulrich (2014) as duas tecnologias utilizadas para a criação da criptomoeda Bitcoin são essenciais e sem elas o Bitcoin não teria se tornado e ganhado as dimensões que possui hoje. O autor explica que a rede *peer-to-peer* difere das redes usuais, pois a mesma não possui um servidor centralizado, sendo que esse é o ponto chave dessa rede, e por isso da tradução (par a par ou ponto a ponto). As redes tradicionais possuem um servidor central o que facilita uma ameaça ao seu sistema. Na arquitetura do sistema *peer-to-peer* os dados são compartilhados sem a necessidade de um servidor central. Na verdade, a força computacional é distribuída por todos que a utilizam, e por isso ele á considerada descentralizada. O autor também reforça que essa ideia já vinha sendo desenvolvida pelo EUA desde os anos 1960, porém foi com o surgimento da internet que a rede passou a ganhar espaço e notoriedade.

Para o Bitcoin, Ulrich (2014, p. 45) demonstra que a rede *peer-to-peer* desempenha a fundamental função de "garantir a distribuição do *blockchain* a todos os usuários, assegurando que todos os nós da rede detenham uma cópia atual e fidedigna do histórico de transações do Bitcoin a todo instante.". Dessa forma, novas transações são transmitidas a todos os nós e registradas no log de transações único e compartilhado.

A fim de explicar a criptografia, segundo componente essencial ao funcionamento do Bitcoin, o antes citado autor complementa que tal tecnologia não é nova, pelo contrário, remonta a tempos passados, onde os primeiros registros datam ao redor de 2.000 a. C. A criptografia pode ser considerada a arte de cifrar mensagens, em que somente o remetente e o destinatário têm acesso ao conteúdo. Além disso, a criptografia é também uma ramificação da matemática e seu uso no mundo moderno se estende a aplicações presentes em nosso dia-a-dia, como sistemas de telecomunicações, comércio online e proteção de sites de bancos.

Para o autor quando aplicada ao Bitcoin a criptografia desempenha duas funções essenciais: a de impossibilitar que um usuário gaste os bitcoins da carteira de outro usuário (autenticação e veracidade das informações) e a de impedir que o *blockchain* seja violado e corrompido (integridade e segurança das informações, o que evita gasto duplo). Além disso, a criptografia pode também ser usada para encriptar uma carteira para que ela só possa ser utilizada com uma senha definida por seu proprietário. (ULRICH, 2014).

4.2 BITCOIN: DEFINIÇÃO E SURGIMENTO

Nesse item será exposto a definição, o surgimento e algumas características da moeda bitcoin com o objetivo de ilustrar e de entender esses conceitos e com a finalidade de contextualizar o Bitcoin, por se tratar de uma inovação monetária.

Iniciando pelo próprio nome, de acordo com o Bitcoin.org a palavra Bitcoin é formada pela junção dos termos *Bit* – que faz referência ao mundo digital, e corresponde ao dígito binário, a menor unidade de informação e é uma unidade comum para designar uma sub-unidade de bitcoin - 1.000.000 de bits é igual a 1 bitcoin (BTC) e *coin,* que vem do inglês e significa moeda.

Além disso, de acordo com o Bitcoin.org, a palavra Bitcoin, quando começar em letra maiúscula, visa descrever o conceito do Bitcoin, ou a própria rede por completa. Como por exemplo: "Eu estava aprendendo sobre o protocolo do Bitcoin hoje." Já a palavra bitcoin, em letra minúscula, é usado para descrever a unidade, ou seja, a quantidade de bitcoins movimentados em uma conta como no exemplo: "Eu enviei dez bitcoins hoje."

A abreviação ou sigla do Bitcoin é BTC ou mesmo XBT.

4.2.1 Definição: o que é o Bitcoin?

Bitcoin é uma moeda digital, não física, transacionada de forma eletrônica somente, que possui como característica marcante a descentralização, sendo assim, não é emitida por nenhuma autoridade monetária, Banco Central ou país específico. Tem origem recente, desde 2008 quando foi proposta, mas sua primeira moeda "minerada[17]" ou fabricada ocorreu no ano de 2009.

Fernando Ulrich (2014), autor do livro "Bitcoin – a moeda na era digital", explica o Bitcoin como:

[17] O termo mineração será esmiuçado mais adiante nesta monografia, mas refere-se ao processo de criação da mesma.

> BITCOIN É UMA MOEDA DIGITAL *peer-to-peer* (par a par ou, simplesmente, de ponto a ponto), de código aberto, que não depende de uma autoridade central. Entre muitas outras coisas, o que faz o Bitcoin ser único é o fato de ele ser o primeiro sistema de pagamentos global totalmente descentralizado. (ULRICH, 2014, p. 17).

De acordo com Silva e Albuquerque (2017, p. 15) "Bitcoin é uma moeda virtual, ou melhor, é uma moeda digital, uma criptomoeda que se baseia em uma tecnologia cujo objetivo é mudar a forma como são realizadas as transações monetárias.".

A Bitcoin é uma moeda digital descentralizada que só a partir de meados de 2010 começou a ser usada de forma mais generalizada e crescente. A ideia inovadora da Bitcoin trouxe uma nova perspectiva ao que conhecemos atualmente como moeda. A sua complexidade e aceitação a nível mundial fazem dela um fenômeno interessante de ser estudado (REGALADO, 2015).

De acordo com o *European Central Bank* (ECB):

> Bitcoin is probably the most successful – and probably most controversial – virtual currency scheme to date. Designed and implemented by the Japanese programmer Satoshi Nakamoto in 2009, the scheme is based on a peer-to-peer network similar to BitTorrent, the famous protocol for sharing files, such as films, games and music, over the internet. It operates at a global level and can be used as a currency for all kinds of transactions (for both virtual and real goods and services), thereby competing with official currencies like the euro or US dollar. The scheme maintains a database that lists product and service providers which currently accept Bitcoins. These products and services range from internet services and online products to material goods (e.g. clothing and accessories, electronics, books, etc.) and professional or travel/tourism services. Bitcoins are divisible to eight decimal places enabling their use in any kind of transaction, regardless of the value. Although Bitcoin is a virtual currency scheme, it has certain innovations that make its use more similar to conventional money. (ECB, 2012, p.22).[18]

[18] Livre tradução de citação: Bitcoin é provavelmente o mais bem-sucedido - e provavelmente o mais controverso - esquema de moeda virtual atual. Projetado e implementado pelo programador japonês Satoshi Nakamoto em 2009, o esquema é baseado em uma rede peer-to-peer semelhante ao BitTorrent, o famoso protocolo para o compartilhamento de arquivos, como filmes, jogos e música, pela internet. Opera em nível global e pode ser usado como moeda para todos os tipos de transações (tanto para bens e serviços virtuais quanto reais), concorrendo com moedas oficiais, como o euro ou o dólar dos EUA. O esquema mantém um banco de dados que lista os fornecedores de produtos e serviços que atualmente aceitam Bitcoins. Esses produtos e serviços variam de serviços de internet e produtos online para bens materiais (por exemplo, vestuário e acessórios, eletrônicos, livros, etc.) e serviços profissionais ou de viagens / turismo. Os Bitcoins são divisíveis em oito casas decimais, permitindo seu uso em qualquer tipo de transação, independentemente do valor. Embora o Bitcoin seja um esquema de moeda virtual, tem certas inovações que tornam seu uso mais parecido com o dinheiro convencional. (ECB, 2012, p.22).

Conforme as referências citadas, o Bitcoin surge como um meio alternativo de pagamento à moeda de curso forçado, porém descentralizado de qualquer banco central. Ela é criada pelos próprios usuários do Sistema Bitcoin, não possui intermediários e conta com o sistema *peer to peer* (par a par). Apesar de recente o Bitcoin vem ganhando espaço no mercado, com cada vez mais países e estabelecimentos aceitando o pagamento de seus produtos através dessa criptomoeda, o que faz o sistema ganhar confiança.

4.2.2 Surgimento

O Bitcoin foi inventado em 2008 com a publicação de um documento intitulado "Bitcoin: Um Sistema de Dinheiro Eletrônico Ponto-a-Ponto" em português, mas originalmente *"Bitcoin: A Peer-to-Peer Electronic Cash System"*, escrito por Satoshi Nakamoto, pseudônimo utilizado pelo autor (ou autores) – até a presente data a identidade de Nakamoto não foi confirmada - da obra que veio a gerar o criptomoeda Bitcoin. O autor do *paper* combinou diversas das invenções anteriores, pelas quais tomou como base e referência, tais como o *b-money*[19] e o *HashCash*[20] para criar um sistema de dinheiro eletrônico completamente descentralizado que não dependesse de uma autoridade central para a emissão de moeda ou para a liquidação e validação de transações (ANTONOPOULOS, 2016).

Satoshi Nakamoto em sua publicação de 2008, que deu origem ao Bitcoin, expõe os benefícios do sistema conforme o trecho a seguir:

> We have proposed a system for electronic transactions without relying on trust. We started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double-spending. To solve this, we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power. The network is robust in its

[19] Proposta inicial criada por Wei Dai para um sistema eletrônico de caixa eletrônico anônimo e distribuído.

[20] Hashcash é um algoritmo de prova de trabalho, que foi usado como uma técnica de medição de contador de negação de serviço em vários sistemas. Um selo de hashcash constitui uma prova de trabalho que leva uma quantidade parametrizável de trabalho para calcular para o remetente. O destinatário (e, de fato, qualquer pessoa que seja publicamente auditável) pode verificar selos hashcash recebidos de forma eficiente. Hashcash foi inventado por Adam Back em 1997.
É principalmente utilizado como a função de mineração do Bitcoin. Fonte: http://www.hashcash.org/.

> unstructured simplicity. Nodes work all at once with little coordination. They do not need to be identified, since messages are not routed to any particular place and only need to be delivered on a best effort basis. Nodes can leave and rejoin the network at will, accepting the proof-of-work chain as proof of what happened while they were gone. They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with this consensus mechanism. (NAKAMOTO, 2008, p.8).[21]

Fernando Ulrich (2014) também explica em seu livro o surgimento do Bitcoin, e acrescenta que a ideia do surgimento da criptomoeda foi divulgada ao mundo precisamente em 31 de outubro de 2008 no *paper* já mencionado de Nakamoto. Tal documento foi divulgado inicialmente em uma lista de discussão online de criptografia.

Para um leigo, a publicação de Satoshi pode parecer pouco esclarecedora e mais técnica do que conceitual, pelo fato da publicação não revelar as razões ideológicas por trás da criação do Bitcoin. Entretanto, o autor se colocou à disposição e respondeu diversas perguntas dos participantes da lista de discussões e nesse momento apresentou seu conhecimento de economia. Como salienta Ulrich (2014), uma das visões críticas mais interessantes de Nakamoto é acerca dos sistemas monetários e bancários.

No dia 3 de janeiro de 2009, nascia oficialmente o Bitcoin, com a criação do bloco gênese – considerado o primeiro bloco do *blockchain* e que daria origem a todos demais blocos da cadeia – criado justamente por Nakamoto, com a primeira transação da história da moeda digital e transmitida à rede por ele acompanhada da seguinte mensagem: "*The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"* (ULRICH, 2014).

Na percepção de Ulrich (2014) a postagem efetuada por Nakamoto faz uma alusão à manchete do jornal britânico *The Times* daquele dia de forma proposital. Indicando uma clara visão crítica de Satoshi sobre o sistema bancário e a desordem

[21] Livre tradução de citação: Propomos um sistema para transações eletrônicas sem confiar na confiança. Começamos com o quadro usual de moedas feitas a partir de assinaturas digitais, que proporciona um forte controle da propriedade, mas está incompleta sem uma maneira de evitar gastos duplos. Para resolver isso, propusemos uma rede peer-to-peer usando a prova de trabalho para registrar um histórico público de transações que rapidamente se torna computacionalmente impraticável para que um invasor mude os nós honestos que controlam a maioria da potência da CPU. A rede é robusta em sua simplicidade não estruturada. Os nós trabalham todos de uma só vez com pouca coordenação. Eles não precisam ser identificados, uma vez que as mensagens não são encaminhadas para nenhum local específico e só precisam ser entregues de acordo com o melhor esforço. Os nós podem sair e se juntarem à rede à vontade, aceitando a cadeia de prova de trabalho como prova do que aconteceu enquanto eles tinham desaparecido. Eles votam com o poder da CPU, expressando sua aceitação de blocos válidos trabalhando em estendê-los e rejeitando blocos inválidos, recusando-se a trabalhar neles. Quaisquer regras e incentivos necessários podem ser aplicados com este mecanismo de consenso. (NAKAMOTO, 2008, p.8).

financeira reinante. E como contraponto, nesse contexto de instabilidade econômica, o Bitcoin vinha como uma tentativa de resposta.

Em 5 de outubro de 2009, após nove meses da rede Bitcoin ter iniciado suas operações, foi publicado o primeiro registro de preço de venda de um bitcoin. Equivalendo um centavo de dólar para 13 bitcoins (representado por 1.309,03 bitcoins por um dólar), calculado pelo ofertante com base em seus custos variáveis de mineração (ULRICH, 2014).

Não muito tempo depois, em maio de 2010, uma pizza foi vendida por 10 mil BTC, equivalente à época a 25 dólares. Em 17 de julho de 2010 ocorreu o primeiro registro de uma transação em uma casa de câmbio, a Mt. Gox. E a partir desse momento, diversas outras transações foram sendo realizadas e o preço do Bitcoin começou a ganhar mais valor (ULRICH, 2014).

O autor Fernando Ulrich (2014) elenca dois motivos fundamentais que impulsionaram a criação do Bitcoin: um sistema financeiro instável e com elevado nível de intervenção estatal e a crescente perda de privacidade financeira. Além de salientar que a rede mundial de computadores e o advento da internet, que viabilizaram a criação do Bitcoin.

4.3 COMO FUNCIONA - FUNCIONAMENTO TÉCNICO

Para que seja possível começar a utilizar bitcoins é necessário que o usuário crie uma carteira Bitcoin (*Bitcoin Wallet*), que é possível através do *download* do *software* gratuito de código aberto que pode ser baixado em um computador ou *smartphone*. Na Figura 1 é possível verificar a imagem de uma carteira *on line*.

Figura 1 – Carteira de bitcoins *on line*.

Fonte: Blockchain Info (2017).

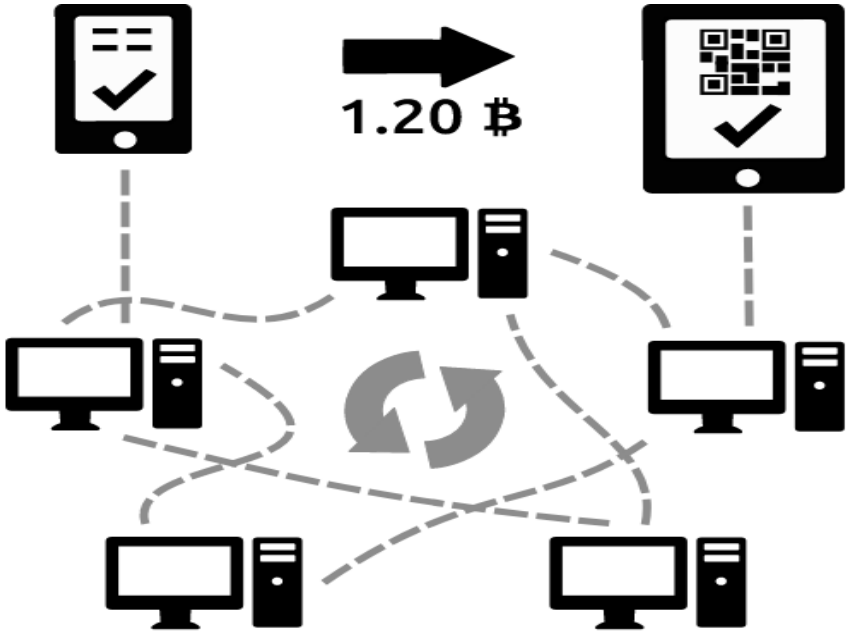
Um aspecto importante a ser analisado, para entender como o Sistema Bitcoin funciona, se encontra no fato desse sistema conseguir impedir o “gasto duplo”. Normalmente, esse problema é evitado nas transações cotidianas de transferências de valores através de um terceiro intermediário que acompanha e mantém os registros das transações e saldos das contas dos clientes. Mas como a proposta primordial do Bitcoin é justamente ser decentralizado, esse problema é resolvido de outra forma diferente.

Primordialmente, é preciso entender o que é o “gasto duplo” e Ulrich (2014) exemplifica esse processo de forma simples de entendimento conforme trecho a seguir:

> Até a invenção do Bitcoin, [...] as transações online sempre requereram um terceiro intermediário de confiança. Por exemplo, se Maria quisesse enviar 100 u.m. ao João por meio da internet, ela teria que depender de serviços de terceiros como PayPal ou Mastercard. Intermediários como o PayPal mantêm um registro dos saldos em conta dos clientes. Quando Maria envia 100 u.m ao João, o PayPal debita a quantia de sua conta, creditando-a na de João. Sem tais intermediários, um dinheiro digital poderia ser gasto duas vezes. Imagine que não haja intermediários com registros históricos, e que o dinheiro digital seja simplesmente um arquivo de computador, da mesma forma que documentos digitais são arquivos de computador. Maria poderia enviar ao João 100 u.m. simplesmente anexando o arquivo de dinheiro em uma mensagem. Mas assim como ocorre com um e-mail, enviar um arquivo como anexo não o remove do computador originador da mensagem eletrônica. Maria reteria a cópia do arquivo após tê-lo enviado anexado à mensagem. Dessa forma, ela poderia facilmente enviar as mesmas 100 u.m. ao Marcos. Em ciência da computação, isso é conhecido como o problema do "gasto duplo", e, até o advento do Bitcoin, essa questão só poderia ser solucionada por meio de um terceiro de confiança que empregasse um registro histórico de transações. (ULRICH, 2014, p.17).

Nesse sentido, a invenção do Bitcoin inova e revoluciona a solução do problema do gasto duplo, extinguindo a necessidade de um terceiro intermediário. Isso é feito através da distribuição do registro histórico a todos os usuários do sistema através da rede *peer-to-peer* (ULRICH, 2014). Na Figura 2 é possível visualizar como funciona a rede *peer-to-peer*, na qual não há uma rede centralizadora, pelo contrário, os diversos pontos da rede assumem o papel da força computacional necessária ao funcionamento do sistema.

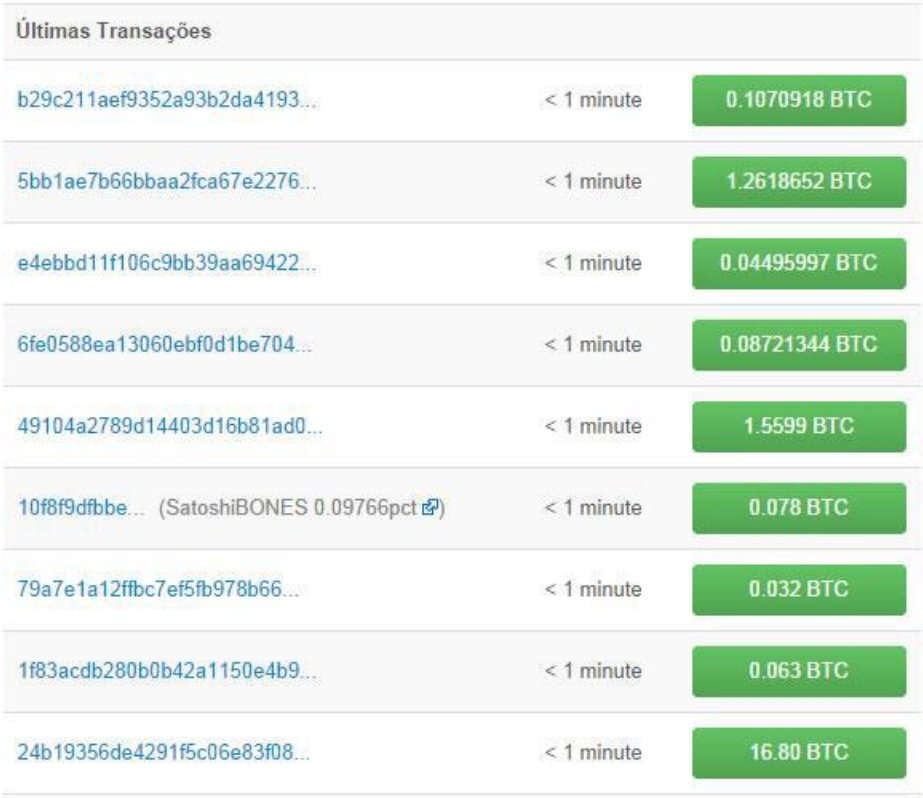
Figura 2 – Esquema do modelo *peer-to-peer* (P2P).



Fonte: BITCOIN.ORG (2017).

Ademais todas as transações ocorridas na rede Bitcoin são registradas em seu livro-razão público e distribuído chamado de *blockchain* (corrente de blocos ou simplesmente um registro público de transações), que pode ser considerado um grande banco de dados público, contendo o histórico de todas as transações realizadas. (ULRICH, 2014). Na Figura 3 é possível verificar as últimas transações efetuadas no *blockchain* que são de conhecimento público e na qual constam as chaves públicas de acesso dos usuários. As transações visíveis publicamente no *blockchain* são distribuídas através da rede *peer-to-peer*.

Figura 3 – Últimas transações registradas no *Blockchain.*



Fonte: Blockchain Info (2017).

Portanto, conforme explicam Silva e Albuquerque (2017), o *blockchain* é uma tecnologia que sustenta o Bitcoin e uma estrutura de dados que pode ser definida como um livro-contábil em que toda a movimentação financeira é registrada e cada transação é digitalmente assinada e autenticada, garantindo, dessa forma, que ninguém possa adulterá-la, mantendo toda a transação na íntegra.

Ainda segundo as autoras, o *blockchain* como uma "cadeia de blocos", funciona da seguinte maneira: quando uma transação acontece, o registro dessas entradas digitais é feito e as entradas digitais são distribuídas entre uma infraestrutura formada por nós ou blocos. Esses nós ou blocos na infraestrutura fornecem informações sobre o estado dessa transação a qualquer momento, e todos esses blocos tem cópias dos registros autenticados distribuídos entre eles (SILVA; ALBUQUERQUE, 2017).

Dessa forma, quando uma nova transação é recebida, os blocos do *blockchain* executam alguns algoritmos que avaliam o histórico do bloco individual que é objeto da proposta de transação e, chegando a um consenso, de que os históricos e as assinaturas

são válidas, permitem, então, que a nova transação seja aceita e que este novo bloco seja adicionado a esta cadeia de transação. Caso acorra algum erro, ou parte dos nós ou blocos não seja reconhecida para adição da entrada, essa entrada será negada e não adicionada à cadeia. Este modelo faz com que o *blockchain* funcione como um registro distribuído sem que seja necessária uma autoridade reguladora que informe e valide as transações (SILVA; ALBUQUERQUE, 2017). Na Figura 4, é possível verificar a criação dos últimos blocos minerados, informação que também é de conhecimento público.

Figura 4 – Carteira *Blockchain* com últimos blocos minerados.

ÚLTIMOS BLOCOS MAIS... →

Altura	Era	Transações	Total Enviado	Transmitido Por	Tamanho (em kB)	Peso (kWU)
497111	10 minutes	2309	7,123.69 BTC	BTC.com	1,028.59	3,992.64
497110	14 minutes	2831	9,698.48 BTC	BTC.TOP	1,049.81	3,992.81
497109	21 minutes	1683	4,807.30 BTC	BTC.com	1,092.64	3,992.83
497108	24 minutes	1725	10,157.34 BTC	BTC.TOP	1,052.13	3,992.83

Fonte: Blockchain Info (2017).

No caso do exemplo de João e Maria, exposto anteriormente, o gasto duplo é então prevenido por meio dos sistemas seguros do Bitcoin e através do uso da criptografia e da chave pública. Dessa forma, para cada usuário é atribuída duas “chaves”, uma privada e uma pública (conforme já explicado anteriormente). Ulrich (2014) exemplifica conforme segue:

> Quando a Maria decide transferir bitcoins ao João, ela cria uma mensagem, chamada de "transação", que contém a chave pública do João, assinando com sua chave privada. Olhando a chave pública da Maria, qualquer um pode verificar que a transação foi de fato assinada com sua chave privada, sendo, assim, uma troca autêntica, e que João é o novo proprietário dos fundos. A transação – e portanto uma transferência de propriedade dos bitcoins – é registrada, carimbada com data e hora e exposta em um "bloco" do *blockchain* (o grande banco de dados, ou livro-razão da rede Bitcoin). A criptografia de chave pública garante que todos os computadores na rede tenham um registro constantemente atualizado e *verificado* de todas as transações dentro da rede Bitcoin, o que impede o gasto duplo e qualquer tipo de fraude. (ULRICH, 2014, p.18-19).

Como o Sistema Bitcoin é uma rede *peer-to-peer*, que não necessita de uma autoridade central encarregada de criar as unidades monetárias e de verificar as transações realizadas, essa força computacional para manter a rede é provida diretamente pelos usuários. Os usuários, que proveem a força computacional do sistema, são conhecidos como "mineradores" (ou "*miners*"), justamente porque eles são recompensados por seu esforço na mineração de bitcoins recém-criados. Bitcoins são criados ou "minerados", à medida que milhares de computadores dispersos resolvem problemas matemáticos complexos que verificam as transações no *blockchain*. (ULRICH, 2014). Dessa forma:

> O protocolo, portanto, foi projetado de tal forma que cada minerador contribui com a força de processamento de seu computador visando à sustentação da infraestrutura necessária para manter e autenticar a rede da moeda digital. Mineradores são premiados com bitcoins recém-criados por contribuir com força de processamento para manter a rede e por verificar as transações no *blockchain*. E à medida que mais capacidade computacional é dedicada à mineração, o protocolo incrementa a dificuldade do problema matemático, assegurando que bitcoins sejam sempre minerados a uma taxa previsível e limitada. (ULRICH, 2014, p.20).

Antonopoulos (2016, p. 10), em seu livro *"Mastering Bitcoin"* acrescenta que o processo de mineração "consiste em competir para encontrar soluções para um problema matemático enquanto se processam transações de bitcoins". Além disso, afirma que qualquer participante na rede bitcoin, usando um dispositivo que execute a implementação completa do protocolo Bitcoin, pode ser um minerador, necessitando apenas utilizar o poder de processamento de seu computador para verificar e registrar transações.

A fim de explicar como funciona efetivamente esse processo Antonopoulos (2016) acrescenta:

> Em média, a cada 10 minutos alguém é capaz de validar as transações dos últimos 10 minutos, sendo recompensado com bitcoins novinhos em folha. Essencialmente, a mineração de bitcoins descentraliza as funções de emissão de moeda e de compensação tipicamente atribuídas a um banco central, dessa forma substituindo a necessidade de qualquer banco central.
> O protocolo bitcoin contêm algoritmos que regulam a função de mineração através da rede. A dificuldade da tarefa de processamento que os mineradores devem realizar — registrar com sucesso um bloco de transações na rede bitcoin — ajusta-se dinamicamente de tal forma que, em média, alguém e bem-sucedido a cada 10 minutos, independentemente de quantos mineradores (e CPUs) estejam trabalhando na tarefa a qualquer momento. (ANTONOPOULOS, 2016, p. 10).

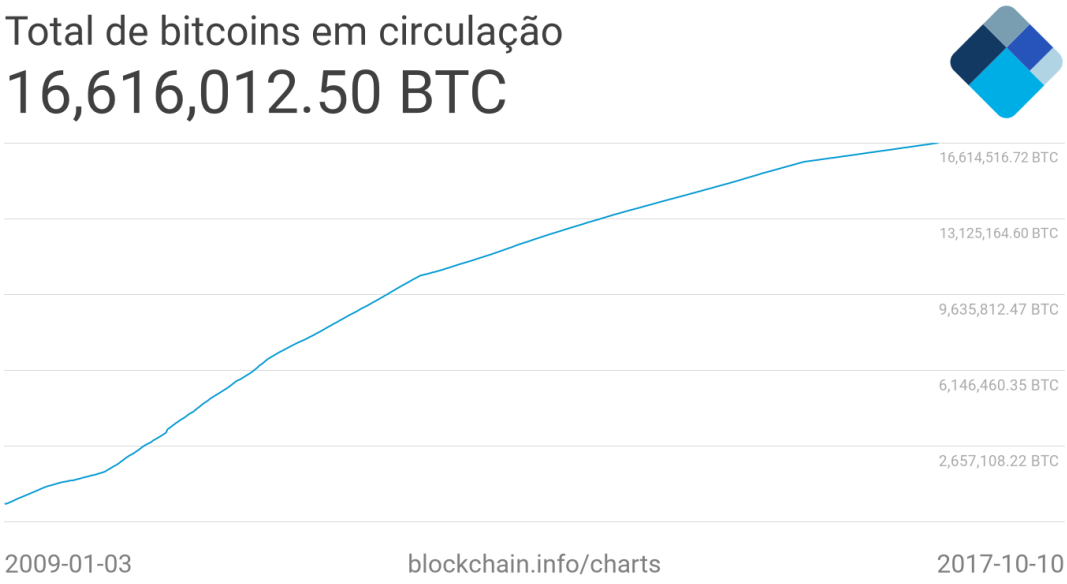
Assim sendo, o processo de mineração “remunera” os mineradores através de recompensas pelo seu esforço e dispêndio computacional e de energia elétrica. Esse esforço pode entendido como a *Proof-of-Work* (PoW) – ou prova de trabalho – que representa “uma parte de um dado que requer um esforço computacional considerável para ser encontrada”. Para criar o bitcoin os mineradores devem encontrar uma solução numérica para o algoritmo SHA-256 que esteja em conformidade com a meta da rede ou a meta de dificuldade. O protocolo também reduz à metade, a cada 4 anos, a taxa com que novos bitcoins são criados, limitando, assim, o número total de bitcoins que serão criados a um máximo de 21 milhões de moedas (ANTONOPOULOS, 2016).

Desde a sua concepção o Bitcoin foi projetado com um limite na sua criação de 21 milhões de bitcoins. Desse modo, o processo de mineração não continuará de forma indefinida. A proposta é de - reproduzir a extração de ouro ou outro metal precioso da Terra - assim sendo, somente o número limitado, já conhecido de bitcoins, poderá ser minerado. De acordo com Ulrich (2014), estima-se que os mineradores colherão o último "satoshi"[22], ou 0,00000001 de um bitcoin, no ano de 2140. Se a potência de mineração total escalar a um nível bastante elevado, a dificuldade de minerar bitcoins aumentará tanto que encontrar o último "satoshi" será uma empreitada digital consideravelmente desafiadora.

Atualmente a quantidade de bitcoins minerados, com data de referência de 10 de outubro de 2017, pode ser verificada no gráfico que segue.

[22] “Satoshi” é o nome dado à menor parte de um Bitcoin, ou a sua oitava fração.

Gráfico 1 – Total de bitcoins minerados.



Fonte: Blockchain Info (2017).

Como percebe-se pelo Gráfico 1 apresentado, até a data de referência de 10 de outubro de 2017, a quantidade de bitcoins minerados que estão em circulação é de mais de 16 milhões. Faltando pouco mais de 4 milhões de bitcoins a serem minerados para concluir o somatório final de 21 milhões estipulado pelo protocolo.

Uma vez que o último "satoshi" tenha sido minerado, os mineradores que direcionarem sua potência de processamento ao ato de verificação das transações serão recompensados com taxas de serviço, em vez de novos bitcoins minerados. Isso garante que os mineradores ainda tenham um incentivo de manter a rede operando após a extração do último bitcoin (ULRICH, 2014).

4.4 ENTRANDO NO MERCADO BITCOIN

Atualmente existem três formas possíveis para se adquirir unidades monetárias de bitcoins, conforme os sites oficiais do Bitcoin, ou Antonopoulos (2016).

Na primeira delas os bitcoins podem ser adquiridos através do processo de mineração (apresentado no item anterior). No qual os usuários “fabricam” suas próprias moedas utilizando como recurso, para tal feito, a sua força computacional e o dispêndio

de energia elétrica, sendo a recompensa para tal esforço frações da moeda bitcoin. A quantidade adquirida, como é de se imaginar, deve variar de acordo com a força de trabalho direcionada para tal fim.

Também existe a possibilidade de aquisição da moeda digital através da venda de bens e serviços, na qual se aceite bitcoins como meio de pagamento. Nesse caso, é feito a transferência de bitcoins de uma carteira para outra através do *blockchain*, ou seja, o comprador vai transferir da sua carteira para a carteira do vendedor. Nessa possibilidade ambos necessitam possuir uma carteira Bitcoin (ou *wallet*) para processar a transação, que será registrada no livro contábil do Sistema Bitcoin – o *Blockchain*.

Uma terceira possibilidade é a aquisição através de outros usuários ou de sites de câmbio virtual. Existem diversos sites que funcionam como uma casa de câmbio virtual e fazem a negociação de troca da moeda, sendo necessário criar uma conta em algum desses sites e fazer o processo de compra transferindo uma quantia em moeda corrente (por exemplo, o Real) para trocar por moeda em bitcoins. Nesse caso, o processo não será intermediado por um bem ou serviço, e será motivado somente pelo interesse em possuir bitcoins. O mercado de bitcoins é volátil e pode atrair o interesse de quem busca especular.

No decorrer do item quatro foi possível entender melhor sobre a moeda digital Bitcoin. E através deste capítulo foi demonstrado conceitos como o de criptografia, que está intrínseco às criptomoedas, além da definição, da história, do funcionamento e de informações referentes ao mercado do Bitcoin. Visando avançar nos conhecimentos sobre a moeda digital o próximo capítulo trará dados gráficos e empíricos a fim de verificar a evolução do Bitcoin no transcorrer do tempo.

5 ENQUADRAMENTO GERAL DA DEMANDA POR BITCOIN

Apesar de ainda se tratar de algo relativamente novo, o aumento do interesse pela moeda bitcoin é notório. Há quem se interesse pelo processo de fabricação da moeda (ou seja, a mineração), há quem se interesse pelo Bitcoin como forma de investimento (dado seu aumento de valor) e também há quem se interesse em apenas conhecer como funciona o Bitcoin, como curiosidade sobre o assunto. Seja qual for o motivo de interesse, é eminente o aumento da relevância que o tema ganhou nos últimos tempos, assim como as notícias veiculadas em diferentes mídias também aumentaram consideravelmente.

Precisamente devido a estas observações, este capítulo visa apresentar dados gráficos e numéricos evolutivos do Bitcoin, com a finalidade de verificar qual a dimensão nas mudanças referentes à sua utilização, sua demanda, seu preço e suas quantidades transacionadas. Também será analisado a demanda pela referida criptomoeda através dos motivos keynesianos de demanda por moeda, com o intuito de verificar se o Bitcoin atende a esses motivos.

5.1 ANÁLISE EVOLUTIVA DO BITCOIN

Neste item será avaliado a evolução do Bitcoin em relação ao seu preço, ao volume transacionado e à procura, a fim de identificar a dimensão do seu crescimento desde sua origem. Para tanto, o item 5.1 será subdividido para analisar de forma individual as variáveis de interesse que melhor apresentem informações para o tema da demanda pelo Bitcoin.

5.1.1 Preço

No que se refere ao preço da moeda bitcoin, estimado em dólares, é notável um expressivo aumento no preço da moeda desde a sua origem. Nos gráficos que seguem é possível analisar esse aumento.

Todos os gráficos deste item (5.1.1) foram acessados em 12/10/2017.

Gráfico 2 – Evolução do preço do Bitcoin em dólares.

Fonte: Blockchain Info (2017).

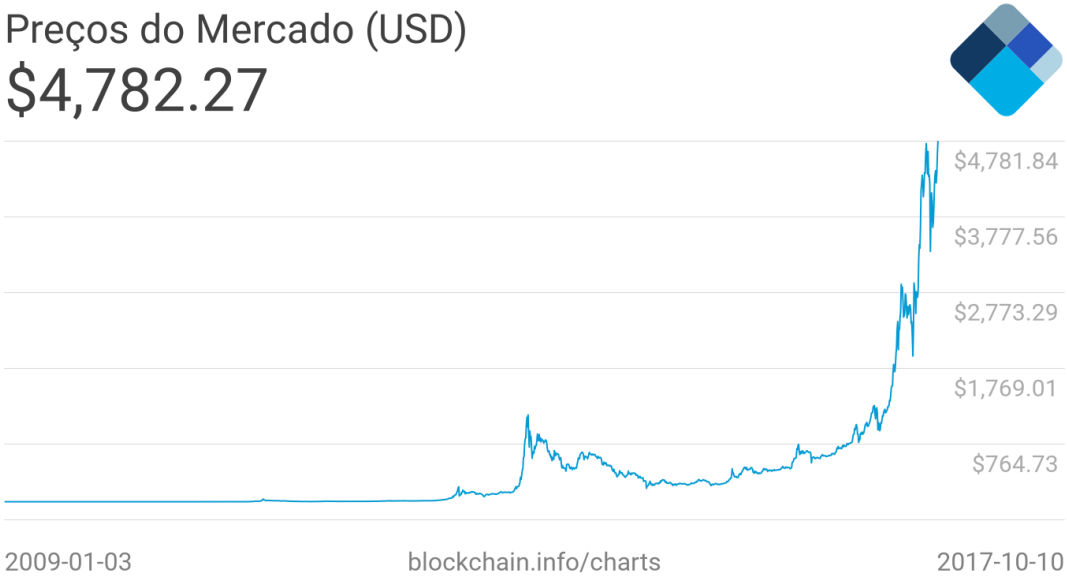
O Gráfico 2 apresenta a oscilação do valor monetário, representado em dólares, do preço de mercado da unidade de bitcoin. Conforme relata Ulrich (2014) o primeiro registro de venda de um bitcoin publicado foi em 5 de outubro de 2009, e na época 13 bitcoins equivaliam a um centavo de dólar (1 BTC = 0,000769 USD). A primeira compra em bitcoins se efetivou em maio de 2010, como já visto, e o produto em questão foi uma pizza, vendida na época por 10 mil BTC – pode se considerar a pizza mais cara do mundo, uma vez que trazendo a cotação atual (do gráfico 3) essa pizza custaria atualmente 47.822.700,00 USD[23]. Depois, em 17 de julho de 2010, ocorreu o primeiro registro de uma transação em bitcoin em uma casa de câmbio, a Mt. Gox, que negociou um bitcoin a US$ 0,05. Após esse período, de cotações de baixo valor, começa em 2011, algumas variações consideráveis, chegando a atingir US$ 22,5 em julho deste mesmo ano. Entretanto, é a partir de 2013 que o preço da Bitcoin começa a subir, tendo um pico entre dezembro de 2013 e janeiro de 2014 período no qual a cotação ultrapassou 1000 USD.

Apesar do aumento de preço no longo prazo, é possível verificar através do gráfico alguns períodos marcantes de oscilação, com destaque ao segundo semestre de 2013 e começo de 2014 e também ao longo do ano de 2017 no qual o preço já variou consideravelmente, em janeiro deste ano um bitcoin estava cotado na faixa de US$ 1000,00.

[23] Cotação datada em 10/10/2017 no valor de US$ 4.782,27 cada unidade de bitcoin.

No Gráfico 3 é possível verificar a cotação atual de uma unidade de bitcoin em US$ 4.782,27 cotado na data de 10 de outubro de 2017.

Gráfico 3 – Preço atualizado de uma unidade de bitcoin



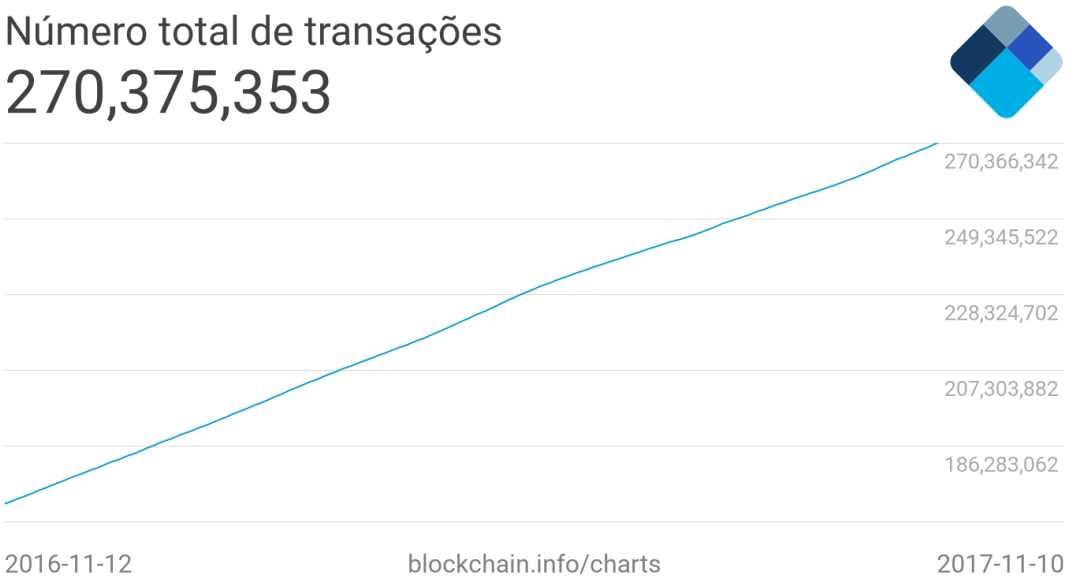
Fonte: Blockchain Info (2017).

De acordo com a tese de Regalado (2015) existe uma forte relação entre o preço da Bitcoin e o interesse manifestado pela moeda na internet. Sendo assim, com o aumento do preço que vem sendo demonstrado graficamente, mais pessoas demonstram algum interesse pelo Bitcoin.

5.1.2 Volume de transações

No Gráfico 4 é possível verificar o número total de transações com a moeda bitcoin desde sua criação até a data de referência do gráfico do dia 10 de novembro de 2017. Seguramente verifica-se uma evolução, pois o Gráfico 4 analisa as transações desde a origem da moeda, ou seja, de forma acumulada. Além de a quantidade monetária disponível em circulação de bitcoins estar aumentando com o processo de mineração pelo qual a unidade monetária bitcoin é criada.

Gráfico 4 – Número total de transações em bitcoins.

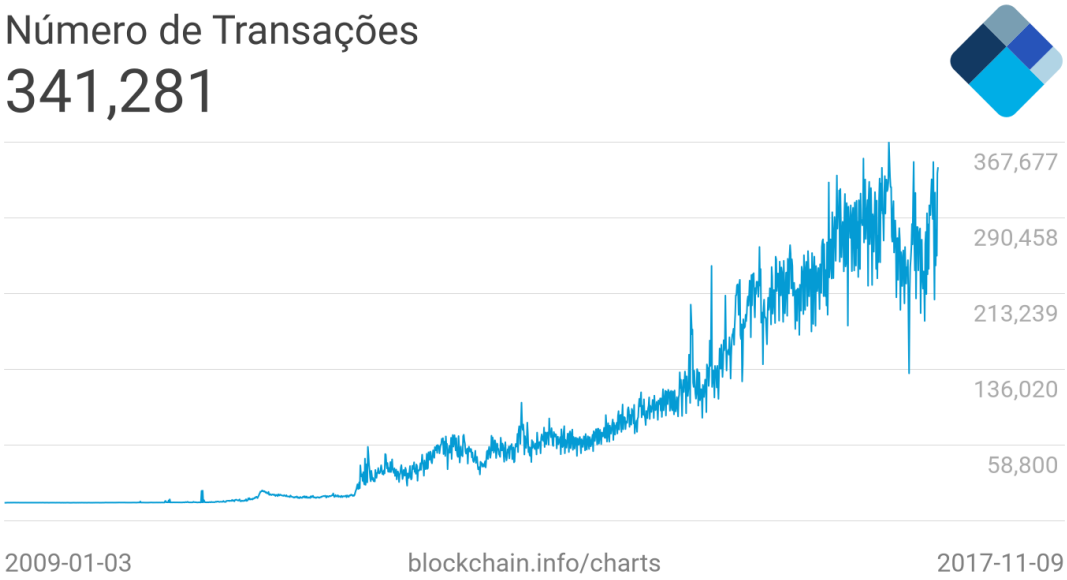


Fonte: Blockchain Info (2017).

No gráfico seguinte, de número 5, é possível verificar o volume de transações em bitcoins por dia, desde sua criação, além da forma como vem oscilando.

Na data de referência do Gráfico 5, de 9 de novembro de 2017, foram efetivadas 341.281 transações com a moeda.

Gráfico 5 – Volume diário de transações em bitcoins, medido em bitcoins.

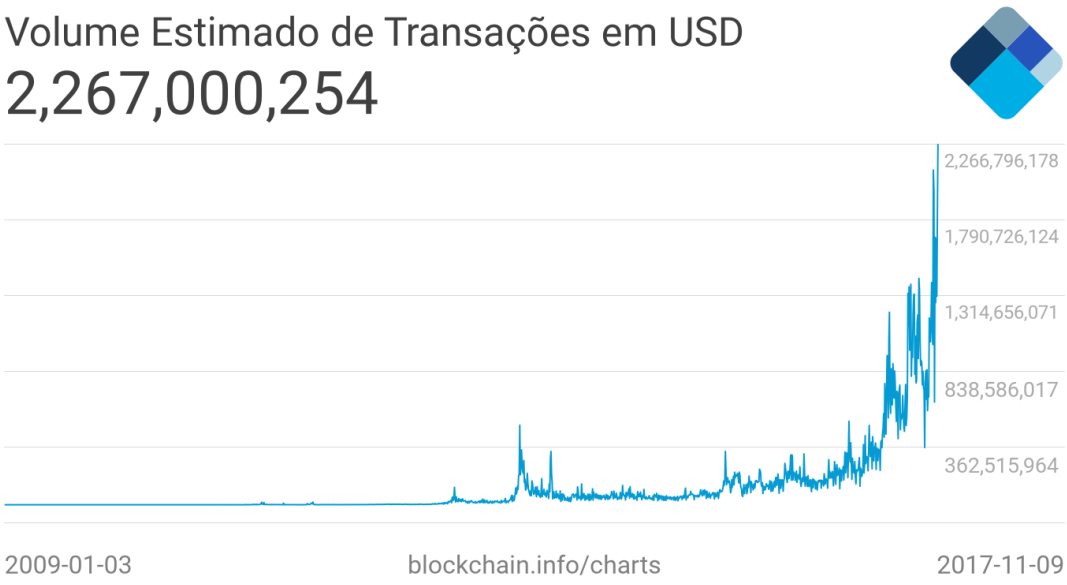


Fonte: Blockchain Info (2017).

É possível verificar no Gráfico 5 a oscilação no volume diário em transações com bitcoins, com alguns períodos demonstrando maior disparidade. Entretanto, ao longo do tempo o número de transações vem aumentando, observação manifestada na curva crescente representada no gráfico.

Contudo ao analisar o mesmo gráfico, porém considerando o volume de transações diárias medido em dólares, é possível verificar como o Bitcoin adquiriu valor. O Gráfico 6 faz menção ao volume de transações de uma unidade monetária de bitcoin por dia convertido ao seu valor de mercado cotado em dólares. Devido à grande valorização que o Bitcoin obteve ao longo dos anos - conforme já verificado no item anterior - é possível observar no Gráfico 6 uma movimentação expressiva cotada em dólares.

Gráfico 6 – Volume estimado de transações diárias medido em dólares.

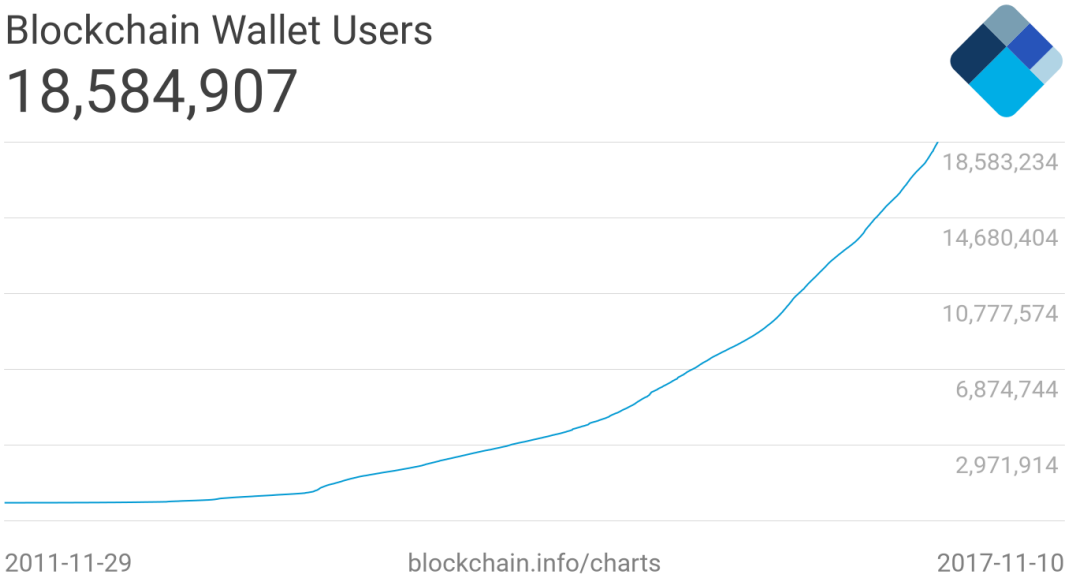


Fonte: Blockchain Info (2017).

5.1.3 *Downloads* de carteiras do *Blockchain*

Outro dado interessante que demonstra um incremento na demanda por bitcoins é o aumento do número de usuários da carteira digital do *Blockchain*[24]. Isso significa dizer que o número de pessoas que fizeram o *download* da carteira para poder trabalhar com bitcoins aumentou e pode-se concluir disso que o interesse também aumentou por consequência. No Gráfico 7 e Gráfico 8 é possível constatar o aumento de usuários da carteira do *Blockchain* no decorrer do tempo.

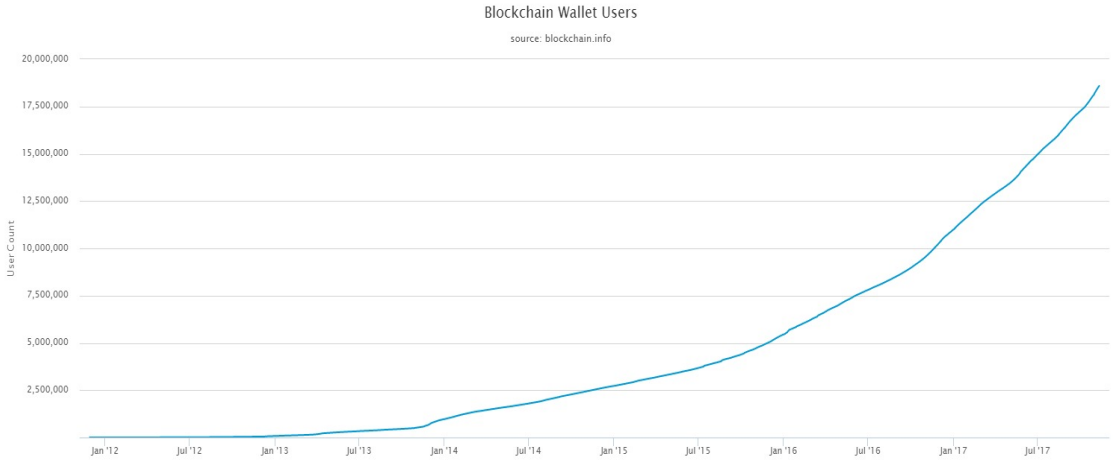
Gráfico 7 – Quantidade de usuários da carteira de bitcoins do *Blockchain*.



Fonte: Blockchain Info (2017).

[24] É o livro-razão público de todas as transações em bitcoins realizadas e que está em constante atualização à medida que novos blocos completos são adicionados. A carteira Bitcoin é mais ou menos o equivalente a carteira física na rede Bitcoin. Cada carteira Bitcoin pode mostrar o balanço de todos os bitcoins que controla, e deixa que sejam feitas transações de uma quantia específica a uma pessoa específica, exatamente como uma carteira real. É a carteira que controla as quantidades enviadas e recebidas dos usuários.

Gráfico 8 – Evolução da quantidade de usuários da carteira de bitcoins do *Blockchain*.



Fonte: Blockchain Info (2017).

Como demonstrado nos gráficos, como base na data de referência de 10 de novembro de 2017, a quantidade de usuários da carteira digital de bitcoins na *Blockchain* já é de 18.584.907. O número de utilizadores do Sistema Bitcoin não para de aumentar. É perceptível uma expansão significativa a partir do ano de 2014 com base nos gráficos.

5.2 VANTAGENS E DESVANTAGENS DO BITCOIN

O Sistema Bitcoin, por se tratar de uma proposta de moeda inovadora, traz consigo alguns questionamentos quanto a sua utilização e propósito. Para sanar possíveis dúvidas, nesse item serão analisados alguns riscos e benefícios desta criptomoeda.

5.2.1 Vantagens

Uma vantagem relevante do uso do Bitcoin é a redução nos custos de transações, que são inferiores a outros métodos. Como não há um terceiro intermediário as transações de Bitcoin são consideravelmente mais baratas e rápidas do que as feitas por redes de pagamentos tradicionais. O que, segundo a visão de Ulrich (2014, p.24), é uma forma de ajudar os pequenos comerciantes a reduzirem seus custos de transações – com

cartões de crédito, por exemplo. Além de ser uma grande promessa ao futuro das remessas de dinheiro, proporcionando “remessas baratas e instantâneas, e a redução de custo dessas remessas aos consumidores”.

Outra vantagem do Bitcoin colocada por Ulrich (2014, p.25) é que a moeda é uma potencial arma contra a pobreza e a opressão. Isso porque o Bitcoin “tem o potencial de melhorar a qualidade de vida dos mais pobres do mundo”; e “aumentar o acesso a serviços financeiros básicos” funcionando, assim como uma técnica antipobreza promissora. Segundo o autor, é o que vem acontecendo em países em desenvolvimento, onde os serviços bancários tradicionais em áreas pobres encontram diversos empecilhos para funcionamento.

Ademais, o Bitcoin pode proporcionar alívio às pessoas vivendo em nações com controle de capitais restritos, isso porque não há autoridade central que impeça a troca de bitcoins entre países. “O Bitcoin, dessa forma, proporciona uma válvula de escape para pessoas que almejam uma alternativa à moeda depreciada de seu país ou a mercados de capitais estrangulados” (ULRICH, 2014, p.26). Dessa forma, a vantagem do Bitcoin, pode ser comparada a privacidade usual que o dinheiro vivo proporciona, entretanto, com a conveniência da possibilidade de transferência digital (ULRICH, 2014). Em complemento, “não existe o risco de uma instituição congelar ou confiscar os fundos, além de que não há qualquer restrição quanto à quantidade que se pretenda transacionar.” (REGALADO, 2015, p.20). Apesar dos governos não terem acesso as contas de bitcoins dos usuários ou como bloquear o uso da rede, por ela ser descentralizada, governos autoritários - como o chinês - começam a querer impor limites a utilização dos usuários.

Um outro benefício possibilitado pelo Bitcoin, o de estímulo à inovação financeira. O autor refere-se a uma das aplicações mais promissoras do Bitcoin como uma plataforma à inovação financeira. Isso porque o protocolo Bitcoin contém um modelo de referência digital que possibilita uma grande quantidade de serviços financeiros, que pode ser facilmente desenvolvido por programadores, da mesma forma que a *web* e o correio eletrônico operam no protocolo da internet. Dessa forma, para o autor o Bitcoin “é a fundação sobre a qual outras camadas de funcionalidade podem ser construídas”. E muitas empresas já se interessam pelo tipo de tecnologia que o Bitcoin possibilitou (ULRICH, 2014, p.26).

A segurança do Sistema possui características positivas e negativas. No que tange aos benefícios é positivo pois o Bitcoin é baseado na rede *peer-to peer* (ponto a ponto) e utiliza a tecnologia do *Blockchain* (espécie de "livro-razão" que contabiliza as transações em bitcoins) e assegura a integridade dos dados utilizados, além de impossibilitar o gasto duplo. Seu caráter negativo refere-se à violação desse sistema de segurança, e será melhor abordado no item que segue.

5.2.2 Desvantagens

Uma desvantagem que o Bitcoin apresenta é a sua alta volatilidade. Tal volatilidade pode ser explicada devido a ajustes de preços que se assemelham a bolhas especulativas tradicionais. Como um excesso de imprensa publicando notícias otimistas, que provocam um aumento de procura por parte de investidores novatos que pressionam os preços para cima, até o ponto que atinge um ponto de inflexão e o preço despenca. O autor cita: "novos entrantes ávidos por participar correm o risco de sobrevalorizar a moeda e perder dinheiro em uma queda abrupta" (ULRICH, 2014, p. 29).

Regalado (2015, p.21) em sua tese explica que é um risco o Bitcoin ser muito volátil, e este risco "pode ser consequência de esta moeda ainda ser muito recente e de o seu mercado não possuir uma dimensão suficientemente alargada para que o preço estabilize". Além do mais, o autor também ressalta que a volatilidade pode resultar da utilização especulativa da moeda.

Outro ponto relevante a ser ressaltado é o que concerne a violação da segurança. Justamente por se tratar de uma moeda digital existe o desafio de reprimir invasões e ataques cibernéticos. Além do mais, Ulrich (2014) ressalta que as pessoas precisam ser cuidadosas para não perder ou apagar seus arquivos, e uma vez que, o arquivo digital esteja perdido, o dinheiro também está perdido, da mesma forma com dinheiro vivo de papel. Ademais, os bitcoins podem ser roubados por *malware*[25], e sofrer ataques de segurança por parte de *hackers*, conforme aconteceu com a Mt.Gox[26] em 2013, onde 24 mil BTC foram roubados.

[25] *Malware* é um termo proveniente do inglês *malicious software*; e é um *software* destinado a se infiltrar em um sistema de computador alheio de forma ilícita, com o intuito de causar algum dano, alterações ou roubo de informações (confidenciais ou não). (ULRICH, 2014).

[26] Mt. Gox é conhecida como a maior e mais famosa casa de câmbio de bitcoins.

Entretanto, uma das ameaças mais preocupantes do Sistema Bitcoin é o uso para fins criminosos. O Bitcoin permite o uso de pseudônimos e, portanto, existe o questionamento se criminosos podem fazer uso disso para atividades ilegais e lavagem de dinheiro.

O exemplo mais famoso de uso para esse fim foi o do site conhecido como *Silk Road*[27] que operava no mercado negro da *deep web*[28]. O site utilizava a tecnologia do Tor[29] para anonimato e a possibilidade do uso de pseudônimos do Bitcoin para disponibilizar um extenso mercado de produtos, em sua maioria ilícitos, e principalmente drogas ilegais. O fato de se usar pseudônimo no Bitcoin permitia que compradores adquirissem produtos ilegais *online*, reduzindo a chance de serem localizados, porém, da mesma forma que o dinheiro vivo possibilita de forma pessoal. A associação do *Silk Road* com o Bitcoin manchou sua reputação, mas o site foi encerrado em outubro de 2013 pelo FBI (ULRICH, 2014).

Por fim, outra possível situação de ameaça do Bitcoin, que parece estar ainda distante de ocorrer, é citada por Van der Laan (2014) em seu artigo no qual o autor expõe que as moedas virtuais no momento não representam um risco na economia real por seu sistema de pagamento funcionar basicamente dentro de comunidades virtuais específicas e não ser estendido a economia real. Entretanto, no caso de o advento do Bitcoin (ou demais moedas virtuais) adquirirem escala, isto poderia ocasionar perdas econômicas consideráveis e afetar os mercados financeiros, gerando risco sistêmico. Tal situação requereria regulação a fim de proteger a economia. Além do risco de afetar a eficácia e eficiência da política monetária, caso se chegue ao ponto em que o aumento no uso de moedas virtuais levaria ao decréscimo no uso da moeda soberana prejudicando, assim, o alcance das políticas monetárias.

---

[27] *Silk Road* foi um mercado operante através da Darknet que utilizava a rede Tor, assegurando assim o anonimato de compradores e vendedores no comércio de produtos ilícitos, particularmente estupefacientes. O site foi lançado em fevereiro de 2011 e em outubro de 2013 foi fechado pelo FBI. Na ocasião, Ross William Ulbricht, foi preso acusado de ser "Dread Pirate Roberts" ou DPR, o proprietário do site.

[28] *Deep web* se refere ao conteúdo da *World Wide Web* (WWW) que não é indexado pelos mecanismos de busca padrão, ou seja, não faz parte da *Surface Web* – comumente utilizada. É um compilado de páginas que não está presente nos mecanismos de buscas tradicionais (como o Google), mesmo que contenham a expressão ou palavra-chave pesquisada pelo usuário.

[29] Tor é um software livre e de código aberto que proporciona o anonimato pessoal ao navegar na Internet e em atividades online, protegendo contra a censura e principalmente a privacidade pessoal. O objetivo principal do projeto é garantir o anonimato, e consequentemente privacidade, ao usuário que está acessando a *web*.

Da mesma forma, o ECB (2012) traz alguns riscos e benefícios das moedas virtuais, salientado que atualmente não representam risco importante para a estabilidade monetária ou financeira, entretanto, esses riscos poderiam ser desenvolvidos ao longo do tempo no caso do estoque de moeda – hoje considerado pequeno – aumentar e ocasionar uma queda do preço dos ativos entre moedas digitais de livre flutuação que tivessem o potencial de afetar a estabilidade financeira. Os riscos potenciais para a estabilidade monetária só poderiam surgir uma vez que as moedas digitais conseguissem um uso substancial em toda a economia. Se um subconjunto de pessoas transacionarem exclusivamente em uma moeda digital, a capacidade do Banco para influenciar a demanda por este grupo poderia ser prejudicada.

5.3 O BITCOIN COMO UMA ALTERNATIVA MONETÁRIA

Muitos autores e autoridades são descrentes da possibilidade do Bitcoin se tornar de fato um substituto à moeda tradicional. Apesar disso, existem algumas situações em que o Bitcoin se tornou uma alternativa à moeda corrente. Este item do capítulo 5 tem a intenção de relatar tais casos a fim de refletir sobre o tema, pois, de acordo com essas situações, pode-se dizer que o Bitcoin teve demanda e supriu a necessidade por moeda por parte da população.

Nesse item será relatado três situações de países distintos e de continentes distintos – Argentina, Uganda e Grécia, no qual a criptomoeda bitcoin atendeu o anseio e a demanda dessas sociedades por moeda.

A Argentina é um caso peculiar do uso do Bitcoin. Isso porque o uso da criptomoeda aumentou consideravelmente como uma alternativa à crise vivida no país nos anos 2000. Problemas no que se refere à inflação e à depreciação da moeda doméstica tornaram difíceis a vida dos argentinos. A população argentina, que sofreu com a perda do seu poder de compra, passou a buscar novas alternativas que viessem a amenizar a situação. A compra de dólares, que era uma fuga da população à moeda doméstica desvalorizada, passou a ser controlada e proibida pelo governo, além do controle da taxa cambial de forma artificial. Tal situação gerou um mercado informal para a compra e venda do dólar por parte da população, e o dólar vendido de maneira informal passou a ser conhecido como o dólar “blue”, com uma cotação acima da cotação oficial do país.

Buscando contornar a crise e os empecilhos criados pelo governo surge o Bitcoin como uma alternativa ao país latino americano. As transações em bitcoins começaram a ganhar cada vez mais espaço, com diversos comerciantes aceitando a moeda como meio de pagamento na venda de seus produtos e serviços. O site Coinmap, que reúne os estabelecimentos que aceitam o Bitcoin ao redor do mundo, demonstra que a Argentina aumentou consideravelmente a quantidade de estabelecimentos que aceitam a moeda. A aceitação começou em fevereiro de 2013 com apenas 3 estabelecimentos aceitando a moeda digital e atualmente esse número já cresceu para 10.219 estabelecimentos, com base na data de consulta em 17 de outubro de 2017.

De acordo com Popper (2015) escritor da matéria do New York Times referente ao caso argentino, o Bitcoin passou a ser uma alternativa para driblar a crise no país. O jornal relata diversas situações de pessoas que passaram a intermediar as situações de câmbio entre as moedas bitcoin e o peso argentino ou dólar, profissionalizando pessoas nesse ramo. Além de reforçar que a volatilidade da moeda local e as disfunções dos bancos que proporcionaram tal situação. Outro documentário produzido pelo Bitcoinfilm também retrata a situação argentina e apresenta situações na qual os indivíduos fazem o câmbio trocando pesos argentinos por bitcoins como forma de se prevenir a crise do país. De forma a reter uma moeda que proporciona maior segurança do que a própria moeda nacional que está em crise.

Outro relato no qual o Bitcoin proporcionou melhoria na vida das pessoas, trata da facilidade e da redução de custos de transação no envio de valores entre países, neste exemplo a Uganda. De acordo com o Bitcoinfilm.org todo o ano são enviados cerca de US$ 700 milhões de diversos países do mundo a seus familiares que residem na Uganda. O filme retrata a situação de uma família na qual Nsubugar Ronald, que reside na Uganda, recebe valores de sua irmã, que mora nos EUA, para cobrir seus estudos. Até a facilidade do Bitcoin, os irmãos faziam uso dos sistemas tradicionais de envios de valores ao exterior como Moneygram e Western Union, que cobram tarifas altas (cerca de 10% a 20%) e demoravam cerca de dois dias a se efetivar. Além do mais, os bancos ugandeses também cobram tarifas altíssimas para a conversão dos valores enviados, fazendo com que Ronald receba cerca de 30% a 40% por cento a menos do total que sua irmã Ronah Nansubuga lhe mandava dos EUA, somando todas as taxas cobradas.

Ao descobrirem as transferências com bitcoins, conseguiram perceber os benefícios dessa opção. Pois quando Ronah enviava valores para o seu irmão em bitcoins a transação se efetivava rapidamente, em alguns minutos no máximo, e Ronald

podia converter seus bitcoins recebidos nos estabelecimentos que faziam o câmbio de bitcoins, além de ter suas taxas reduzidas a valores irrisórios de transação. Nesta situação o Bitcoin foi utilizado para atender à necessidade de transferência de recursos a baixos custos de transação e obteve êxito.

Uma terceira situação na qual o Bitcoin ganhou notoriedade foi na recente crise grega. Devido às dificuldades enfrentadas pelos gregos e por imposições que o governo implementou para movimentações dos euros, uma parte da população começou a converter seus euros por bitcoins por acreditar que dessa forma seus recursos financeiros ficariam mais seguros, visto que o governo não tem alçada para manipular ou mexer nos bitcoins da população.

De acordo com o Hern (2015) em manchete para o The Guardian, quando há instabilidade no país e turbulência no sistema financeiro isso pode acarretar o aumento da procura por moedas alternativas, como o Bitcoin. Isso deve-se a natureza descentralizada dessa moeda que permite a movimentação de valores dentro e fora do país sem que acarrete em represálias legais. A notícia, entretanto, não evidencia um aumento concreto na demanda pelos bitcoins mesmo com a crise, apenas sugere ser uma possibilidade plausível devido a situação do país.

Conforme a notícia do Coindesk, citando Miriam Liapi, fundadora do Bitcoin Community Greece - apesar das divulgações sugerindo o aumento na demanda pelo Bitcoin devido à crise e ao aumento da conscientização da população sobre o tema - Liapi acredita que esse aumento na procura se deu, na realidade, devido ao aumento no preço do Bitcoin, e, portanto, tem caráter especulativo.

Nas três situações colocadas pode ser verificado, de alguma forma, uma procura por bitcoins. Sugerindo que o Bitcoin pode suprir alguma necessidade da população que a moeda tradicional, naquele momento, não está suprindo.

5.4 A DEMANDA POR BITCOIN

Como o Bitcoin trata-se de uma tecnologia de criptomoeda relativamente nova, ainda existem poucas bibliografias sobre o tema. Muito se fala do Bitcoin na internet e nas mídias, porém de maneira informal. Em vista disso, torna-se um desafio evidenciar se o Bitcoin atende aos motivos de demanda por moeda, justamente devido seu caráter jovem e escassez de estudos.

Muitos dos trabalhos que se centram no Bitcoin focam-se no seu preço, na sua natureza volátil e nas suas características como moeda, mas pouco se refere as determinantes da sua demanda. E, portanto, justifica-se o desafio em conceituá-la.

Entretanto, é com base na literatura empírica incipiente que este estudo busca argumentos que evidenciem a demanda pelo Bitcoin, e corroborem com o problema exposto neste estudo.

Regalado (2015, p.64) em sua tese buscou demonstrar empiricamente, através de um estudo econométrico, as determinantes para a procura pelo Bitcoin, o autor utilizou diversas variáveis (como a taxa de câmbio entre bitcoin e o dólar e o índice Dow Jones, entre outras) e concluiu que "as estimações realizadas mostraram que as determinantes tradicionais da procura de moeda também explicam a procura de uma moeda digital como a Bitcoin". Além de "a taxa de câmbio da bitcoin face ao dólar afeta de forma significativa a procura da Bitcoin: uma depreciação do valor da bitcoin mostrou ter impacto negativo na procura desta moeda, indiciando um comportamento especulativo". O autor também utiliza em sua tese outros trabalhos que visam entender a demanda pelo Bitcoin que também chegam a conclusão do caráter especulativo ter grande influência na demanda pela moeda digital.

Para Surda (2012) a demanda por um meio de troca pode ser explicada por sua liquidez, sendo a liquidez do ativo um fator determinante para sua procura. O autor também acrescenta que o fator de custos de transação influencia a escolha de um meio de troca. Entretanto, em sua tese Surda (2012) conclui que o Bitcoin ainda não pode ser considerado dinheiro (podendo torna-se um dia) mas ainda não o é devido não ser um "meio de troca universalmente aceito", para o autor o Bitcoin é um "meio de troca secundário", uma quase-moeda, sendo questão fundamental, para tornar-se uma moeda, a liquidez; e para obter maior liquidez, é necessário à sua maior aceitação como meio de troca. Já no quesito custos de transação o Bitcoin apresenta superioridade em relação à moeda tradicional, pois não existem fronteiras ou intermediários, tornando seus custos inferiores.

Em seu artigo, Popper (2017), a fim de explicar o preço do Bitcoin, expõe que o mesmo se dá basicamente por oferta e demanda e faz uma analogia ao ouro explicando que o preço da Bitcoin flutua constantemente e é determinado pela oferta de mercado aberto nas trocas da Bitcoin, semelhante à forma como o preço do ouro são determinados por licitação nas bolsas. E também acrescenta que o Bitcoin pode ser

usado como precaução, em situações de países em crise e com a moeda doméstica depreciada, “pessoas em países com alta inflação, como Argentina e Venezuela, compraram bitcoins com sua moeda local para evitar a perda de suas economias na inflação”. O caso da Argentina e da Grécia já foram vistos na seção anterior e o autor complementa ainda a situação venezuelana.

De acordo com Hickey (2017), o preço do Bitcoin vem atingindo picos de crescimento apesar de sua alta volatilidade, esses elevados aumentos provocam uma maior procura, principalmente para investimento. Contundo, ressalta que muitas pessoas estão colocando todas as suas economias em bitcoins, o que pode ser muito arriscado devido às consideráveis oscilações da moeda e por ela não ter nenhum tipo de proteção típica que estão presentes nos demais investimentos. O autor, inclusive, faz uma comparação do Bitcoin com a bolha especulativa das tulipas, que ocorreu no século XVII nos Países Baixos. Nesta colocação verifica-se um forte comparativo do Bitcoin a um ativo de investimento apenas, sem lhe atribuir demais papéis.

Alemi (2017) descreve sobre as consideráveis valorizações que o Bitcoin obteve ao longo do ano de 2017, com um acumulado dos últimos doze meses de 1000%. E salienta que o novo recorde se deu devido à maior demanda institucional pela criptomoeda. Além do mais, reforça que o Chicago Mercantile Exchange Group (CME Group), maior bolsa de contratos futuros do mundo, relatou planos que irá começar a trabalhar com o Bitcoin, o que aumenta a credibilidade da moeda.

Ulrich (2014) também faz algumas colocações referente a demanda por bitcoins, o autor acrescenta que, quando da sua criação, de fato houve demanda real pelo bitcoin, no entanto que bitcoins foram adquiridos e preços formados para transações com bitcoins, independentemente do porquê isso ocorreu. Além do mais, o autor coloca o Bitcoin como um substituto de dinheiro, explicando que estes surgem e são demandados quando há a possibilidade de redução nos custos de transação, papel que o Bitcoin cumpre com maestria.

Outro aspecto ao qual Ulrich (2014) chama a atenção é para a suposição da demanda por bitcoins continuar crescendo. Como a oferta de bitcoins é dada pelo limite máximo de 21 milhões de unidades e cresce de forma gradativa, conforme estabelece o protocolo, um aumento na demanda por bitcoins ao longo dos anos acarretaria que a unidade de bitcoin iria valer cada vez mais, e por consequência, quanto maior a sua aceitação como moeda, maior será o seu poder de compra. Mas essa situação levou

alguns economistas a deduzir que seria inviável a utilização do Bitcoin para compras simples do cotidiano devido ao alto valor que a criptomoeda assumiria. Entretanto, a questão do aumento da demanda por bitcoins é resolvida por sua perfeita divisibilidade, pois a Bitcoin possui oito casas decimais (0,00000001 BTC), permitindo que os usuários realizem transações com as suas frações.

Entretanto, de acordo com Ulrich (2014) o que deve ser considerado não é o quanto vale cada unidade de Bitcoin, e sim que o Bitcoin possui um preço e está sendo utilizado por indivíduos que operam com a moeda. O preço no qual o Bitcoin é transacionado é algo que o mercado vem descobrindo, e sua evolução é difícil de ser prevista. Apesar da sua alta volatilidade - que agrada a especuladores - quando aumentar o número de adeptos ao Sistema Bitcoin para a sua aquisição e sua utilização, a tendência é aumentar a liquidez e reduzir a volatilidade da moeda, ampliando, por consequência, a sua aceitação no mercado. Portanto, pode-se interpretar disso que a demanda por transação seria melhor atendida.

Um comunicado feito pelo BACEN em 16 de novembro de 2017, alerta sobre os riscos em guardar e negociar bitcoins. Retrata também que o uso da moeda para fins especulativos está sujeito a ameaças de responsabilidade dos detentores da moeda. O comunicado reforça que o número de adeptos vem crescendo, mesmo que para fins especulativos. Segue um trecho do mesmo:

> Considerando o crescente interesse dos agentes econômicos (sociedade e instituições) nas denominadas moedas virtuais, o Banco Central do Brasil alerta que estas não são emitidas nem garantidas por qualquer autoridade monetária, por isso não têm garantia de conversão para moedas soberanas, e tampouco são lastreadas em ativo real de qualquer espécie, ficando todo o risco com os detentores. Seu valor decorre exclusivamente da confiança conferida pelos indivíduos ao seu emissor.
> A compra e a guarda das denominadas moedas virtuais com finalidade especulativa estão sujeitas a riscos imponderáveis [...]. (BANCO CENTRAL DO BRASIL, 2017)[30].

No mesmo comunicado o BACEN também destaca que o uso de moedas virtuais para fins ilícitos expõe seus detentores a penalidades por parte do poder público. E

[30] Documento eletrônico: Comunicado nº 31.379 BACEN, de 16/11/2017. Disponível em: <http://www.bcb.gov.br/pre/normativos/busca/normativo.asp?numero=31379&tipo=Comunicado&data=16/11/2017>. Acesso em: 24 nov. 2017.

reforça a falta de regularização e supervisão da moeda por parte do Sistema Financeiro Nacional.

Uma outra comparação que pode ser feita em relação à procura por bitcoins é comparando-o às demais criptomoedas disponíveis no mercado. O Bitcoin não é a única moeda digital existente, na realidade, existem centenas de moedas digitais disponíveis, as chamadas *altcoins*[31], mas o Bitcoin é a mais famosa e com maior aceitação. Além do mais, o Bitcoin possui o maior *market cap*[32] dentre todas as *altcoins* disponíveis. Na figura 5 é possível verificar a relação das quinze criptomoedas com maior *market cap*, com base na data de pesquisa de 18 de novembro de 2017, e como é bem superior o destaque do Bitcoin em relação às demais. Dessa forma, é possível verificar que, através do Sistema Bitcoin, diversos outros surgiram, provavelmente devido a repercussão que o Bitcoin teve e ainda está tendo.

Figura 5 – Relação das quinze *altcoins* com maior *market cap*.

#	Name	Symbol	Market Cap	Price	Circulating Supply	Volume (24h)	% 1h	% 24h	% 7d
1	Bitcoin	BTC	$130,448,323,863	$7817.21	16,687,325	$3,725,580,000	-0.35%	1.01%	24.57%
2	Ethereum	ETH	$33,352,489,697	$348.11	95,810,478	$608,791,000	1.24%	4.71%	11.24%
3	Bitcoin Cash	BCH	$21,114,753,760	$1256.11	16,809,638	$3,114,590,000	1.24%	7.09%	-11.66%
4	Ripple	XRP	$8,810,461,113	$0.228115	38,622,892,459 *	$146,916,000	-0.21%	0.72%	8.94%
5	Litecoin	LTC	$3,713,391,570	$68.91	53,885,133	$167,124,000	0.53%	1.49%	11.03%
6	Dash	DASH	$3,494,080,735	$453.97	7,696,654	$144,833,000	0.62%	6.13%	31.70%
7	NEO	NEO	$2,744,033,500	$42.22	65,000,000 *	$459,985,000	-1.11%	10.18%	49.15%
8	IOTA	MIOTA	$2,292,656,641	$0.824836	2,779,530,283 *	$58,077,900	1.07%	3.19%	40.15%
9	Monero	XMR	$2,012,642,440	$130.95	15,369,784	$62,902,200	-0.37%	4.40%	9.07%
10	NEM	XEM	$1,766,484,000	$0.196276	8,999,999,999 *	$6,995,840	0.42%	1.15%	4.16%
11	Ethereum Classic	ETC	$1,734,258,715	$17.77	97,572,238	$160,236,000	0.15%	3.16%	-8.56%
12	Lisk	LSK	$1,063,396,735	$9.24	115,041,032 *	$29,469,900	1.38%	9.05%	61.47%
13	Qtum	QTUM	$1,028,027,012	$13.95	73,670,984 *	$118,639,000	-0.19%	6.14%	20.68%
14	EOS	EOS	$940,122,432	$1.94	484,576,711 *	$52,737,200	-1.21%	11.92%	67.89%
15	Hshare	HSR	$867,442,414	$20.52	42,266,637	$39,762,300	0.39%	-2.46%	99.66%

Fonte: COIN MARKETCAP (2017).

[31] *Altcoin* ou *alternative coin* são criptomoedas alternativas ao Bitcoin que, em sua maioria, surgiram a partir de bifurcações (ou *fork* em inglês) do protocolo Bitcoin, com o intuito de modificar alguns parâmetros internos da rede do Bitcoin ou adicionar novas características.

[32] *Market cap* é a abreviação de *market capitalization* é a estimativa do valor total do ativo com base na sua cotação no mercado. É estimada através da multiplicação entre o volume de moeda disponível no mercado e o seu preço de cotação.

Com base nos estudos apresentados torna-se perceptível a relação do Bitcoin principalmente com o motivo de especulação de demanda por moeda, possivelmente pela evolução no aumento do seu preço, conforme demonstrado graficamente. Além do mais, como relata Ulrich (2014) a mídia favorável e que destaca a alta valorização da moeda, tende a influenciar a procura pela mesma.

Apesar dos outros motivos estarem presentes, algumas vezes em situações esporádicas e em momentos específicos, o que fica mais evidente é que as pessoas estão demandando o Bitcoin principalmente para especular, por acreditar no seu aumento de preço, apesar das oscilações, conforme pesquisas relatadas.

O Bitcoin também atende aos demais motivos de demanda, pois transações são feitas com a moeda - conforme informação gráfica do aumento do número de transações – e também cada vez mais estabelecimentos o aceitam como meio de pagamento. Porém, o uso para transação não é cotidiano para um grande número de pessoas, ocorrendo em pequenos grupos e não de forma disseminada como na moeda tradicional.

O motivo precaução pode ser encontrado quando relacionado às incertezas dos agentes em relação ao futuro das políticas econômicas de seu país, como na relação feita com Argentina, Grécia e Venezuela. Nessas situações o Bitcoin surgiu como uma opção à moeda tradicional, que não estava atendendo ou estava aquém das expectativas da população em um dado momento.

6 CONCLUSÃO

Com a finalidade de entender a demanda pela criptomoeda Bitcoin este trabalho se apoiou em análises empíricas, além de material teórico da literatura econômica para dar base e fazer o comparativo entre a moeda virtual Bitcoin e a moeda tradicional.

A primeira análise objetivando tal resposta ocorreu por meio da explicação e da conceituação de moeda, além de informações relevantes como a sua evolução, sua história, suas funções e suas características. Posteriormente, foi relevante explicar os motivos que levam os agentes a demandar moeda, no qual o foco foi a teoria keynesiana. Contudo, como o objeto dessa pesquisa foi o Bitcoin mostrou-se crucial também a descrição mais detalhada desta criptomoeda, explicando sua definição, sua origem, seu funcionamento, sua tecnologia inovadora e sua forma de aquisição.

Não obstante, elementos relevantes desde sua criação foram necessários para explicar a evolução desta moeda contemporânea. Para tanto, dados gráficos, relacionando oscilação de preços, de volumes de transações e de quantidades disponíveis da moeda foram essenciais para entender mais sobre a mesma. O comparativo entre suas vantagens e desvantagens também foram de suma importância para a decisão de aquisição de uma moeda digital, e situações históricas, onde a moeda repercutiu de maneira positiva, ajudam a entender a validade de uma proposta à moeda tradicional.

A utilização de tal embasamento teórico foi essencial para atender aos objetivos específicos, e, por meio deles, poder avaliar a demanda pelo Bitcoin – objetivo principal deste trabalho. Para tanto, também foram utilizadas análises empíricas para avaliar a demanda pelo Bitcoin e, através delas, foi possível verificar que o Bitcoin atende aos motivos keynesianos de demanda por moeda denominados de: transação, precaução e especulação, contudo com ressalvas e em determinadas situações específicas.

Muitas das pesquisas feitas revelam o motivo especulação de demanda fortemente presente na moeda digital, levando a crer que o interesse para muitos agentes é a lucratividade desse novo sistema, e não por sua proposta libertária e revolucionária de descentralização, pela qual originalmente a moeda foi criada por Satoshi Nakamoto.

O motivo precaução de demanda por moeda, foi verificado em situações de crises e de redução do poder de compra, ou seja, em situações pontuais, nas quais a

moeda soberana encontrava-se abalada e, portanto, sem a confiança dos agentes econômicos. Nessas situações a população fez uso do Bitcoin como recurso para fugir da crise que desvalorizava a moeda local e impunha restrições monetárias. O Bitcoin então, apresentava maior segurança que a moeda doméstica, sendo assim, mais demandado devido a essas circunstâncias.

O motivo de demanda para transação é visto no público que de fato compra e vende bens e serviços através do Bitcoin. Atualmente diversos estabelecimentos no mundo estão aceitando o Bitcoin como forma de pagamento e esse número vem aumentando, devido ao destaque que a moeda digital vem ganhando. Grandes empresas de porte como a Dell e a Microsoft já aceitam a criptomoeda e isso aumenta a credibilidade sobre a mesma. Além do mais, as transações com Bitcoin que envolvem divisas são muito vantajosas, no quesito custos de transação e rapidez de efetivação, podendo também ser demanda para tal fim.

Quando comparado à moeda soberana, o Bitcoin atende aos motivos de demanda por moeda de forma isolada, em determinado contexto e num dado período de tempo, principalmente para os motivos transação e precaução. O motivo especulação, entretanto, apresenta-se mais disseminado nas análises, principalmente quando da valorização do preço do Bitcoin, sendo visto como uma oportunidade de investimento e mostrando-se o motivo com maior representação aparente dentre os três, conforme as análises. Porém, esses números ainda são pequenos quando comparados às movimentações de valores com a moeda tradicional.

Conclui-se, portanto que o Bitcoin atende aos motivos de demanda por moeda, entretanto com ressalvas e com alertas. Instituições como Bancos Centrais não o recomendam, alguns analistas sugerem que se trata de uma bolha especulativa e outros reforçam seu caráter facilitador para usos ilegal e ilícito. Entretanto, mesmo com tais restrições a criptomoeda é demandada, ainda que para um grupo restrito. Uma possibilidade para a demanda pelo Bitcoin ainda ser reduzida, frente à moeda tradicional, pode estar na sua falta de liquidez, falta de conhecimento do público geral para seu uso e manutenção ou mesmo a falta de regulamentação governamental, que influenciam na confiança dos agentes e, consequentemente, na demanda pelo Bitcoin. Entretanto, indubitavelmente, é possível perceber demanda pelo Bitcoin, mesmo que para especulação. As estatísticas, os gráficos e as notícias veiculadas nas mídias e, até mesmo, pelos Bancos Centrais confirmam isso.

REFERÊNCIAS

ALEMI, F. **Bitcoin volta a quebrar recorde e acumula valorização de 1000% em 12 meses.** 2017. Disponível em: <http://economia.estadao.com.br/noticias/seu-dinheiro,bitcoin-volta-a-quebrar-recorde-e-acumula-valorizacao-de-1000-em-12-meses,70002091132>. Acesso em: 24 nov. 2017.

ANTONOPOULOS, A. M. **Mastering Bitcoin:** Unlocking Digital Cryptocurrencies. O'reilly Media, Inc: Copyright, 2016.

ARAÚJO, V. R. B. S. de; MACHADO, M. R. BITCOINS: An accounting perspective. In: INTERNATIONAL CONFERENCE ON INFORMATION SYSTEMS & TECHNOLOGY MANAGEMENT, 2015. São Paulo. **Anais…** CONTECSI, São Paulo. 2015. 38 f. Disponível em: <http://www.contecsi.fea.usp.br/envio/index.php/contecsi/12CONTECSI/paper/view/2551/2412>. Acesso em: 12 set. 2017.

ASSANGE, J. et al. **CYPHERPUNKS:** Liberdade e o futuro da internet. São Paulo: Bointempo Editorial, 2012.

BANCO CENTRAL DO BRASIL. Alerta sobre os riscos decorrentes de operações de guarda e negociação das denominadas moedas virtuais. **Comunicado nº 31.379**, de 16/11/2017 2017. Disponível em: <http://www.bcb.gov.br/pre/normativos/busca/normativo.asp?numero=31379&tipo=Comunicado&data=16/11/2017>. Acesso em: 24 nov. 2017.

BANCO CENTRAL DO BRASIL. Riscos decorrentes da aquisição das chamadas "moedas virtuais" ou "moedas criptografadas" e da realização de transações com elas. **Comunicado nº 25306**, de 19/02/2014**.** Disponível em: <https://www3.bcb.gov.br/normativo/detalharNormativo.do?method=detalharNormativo&N=114009277>. Acesso em: 22 jun. 2017.

BITCOINFILM. **Bitcoins in Argentina.** 2013. Disponível em: <http://bitcoinfilm.org/documentaries/>. Acesso em: 17 out. 2017.

BITCOINWIKI. **B-MONEY.** 2016. Disponível em: <https://en.bitcoin.it/wiki/B-money>. Acesso em: 13 set. 2017.

BITCOIN.ORG. **Criptografia.** Disponível em: <https://bitcoin.org/pt_BR/vocabulario#criptografia>. Acesso em: 13 set. 2017.

BLOCKCHAIN.INFO. **[Gráficos e dados].** 2017 <https://blockchain.info/pt> Acesso em: 11 jun. 2017.

CARVALHO, F. J. C. de et al. **Economia monetária e financeira:** teoria e política. 2. ed. Rio de Janeiro: Elsevier, 2007.

COIN MARKETCAP. **Cryptocurrency Market Capitalizations.** Disponível em: <https://coinmarketcap.com/all/views/all/>. Acesso em: 18 nov. 2017.

COINDESK. **Has the Greek Crisis Increased Bitcoin Awareness?** Elaborado por Yessi Bello Perez. Disponível em: <https://www.coindesk.com/has-the-greek-crisis-increased-bitcoin-awareness/>. Acesso em: 15 nov. 2017.

COINMAP.ORG. **Estabelecimentos que aceitam bitcoins na Argentina.** 2017. Disponível em: <https://coinmap.org/#/world/-36.02688935/-61.02905273/7>. Acesso em: 17 out. 2017.

DAI, Wei. **B-MONEY.** Disponível em: <http://www.weidai.com/bmoney.txt>. Acesso em: 12 set. 2017.

EUROPEAN CENTRAL BANK (ECB). **Virtual currency schemes** <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf> Acesso em: 05 jun. 2017.

FRIEDMAN, M. A Teoria quantitativa da moeda: reestabelecimento. In: CARNEIRO, R. (Org.). **Os clássicos da economia**. São Paulo: Ática, 1997.

FROYEN, R. T. **Macroeconomia:** Teorias e aplicações. 2. ed. São Paulo: Saraiva, 2013.

GALBRAITH, J. K. **Moeda:** de onde veio, para onde foi. 2. ed. São Paulo: Livraria Pioneira, 1983.

GREMAUD, A. P. et al. **Manual de economia.** 4. ed. São Paulo: Saraiva, 2003.

HASHCASH.ORG. **Hashcash.** Disponível em: <http://www.hashcash.org/>. Acesso em: 14 set. 2017.

HERN, Alex. Bitcoin fans eye potential in Greek crisis. **The Guardian**, 29 June 2015. Disponível em: <https://www.theguardian.com/technology/2015/jun/29/bitcoin-fans-eye-potential-in-greek-crisis>. Acesso em: 15 nov. 2017.

HICKEY, S. The Guardian. **Will bitcoin ever be a safe investment or always a gamble?** 2017. Disponível em: <https://www.theguardian.com/money/2017/oct/01/will-bitcoin-ever-be-safe-investment-gamble>. Acesso em: 19 nov. 2017.

HILLBRECHT, R. O. **Economia monetária.** São Paulo: Atlas, 1999.

KEYNES, J. M. **A teoria geral do emprego, do juro e da moeda:** inflação e deflação. 2. ed. São Paulo: Nova Cultural, 1985. (Os economistas).

LOPES, J. C.; ROSSETI, J. P. **Economia monetária**. 9. ed. São Paulo: Atlas, 2005.

POPPER, N. **Can Bitcoin Conquer Argentina?:** With its volatile currency and dysfunctional banks, the country is the perfect place to experiment with a new digital currency.. 2015. Disponível em: <https://www.nytimes.com/2015/05/03/magazine/how-bitcoin-is-disrupting-argentinas-economy.html?_r=0>. Acesso em: 17 out. 2017.

POPPER, N. **What Is Bitcoin, and How Does It Work?** 2017. Disponível em: <https://www.nytimes.com/2017/10/01/technology/what-is-bitcoin-price.html>. Acesso em: 18 nov. 2017.

REGALADO, J. M. S. **Determinantes da procura da Bitcoin:** um estudo econométrico, Porto. 2015. 73 f. Dissertação (Mestrado em Contabilidade e Finanças) - Instituto Superior de Contabilidade e Administração do Porto Instituto Politécnico do Porto, Porto, 2015. Disponível em <http://recipp.ipp.pt/bitstream/10400.22/6772/1/DM_JoaoRegalado_2015.pd>. Acesso em: 13 maio 2017.

ROTHBARD, M. N. **O que o governo fez com o nosso dinheiro?** São Paulo: Instituto Ludwig von Mises Brasil, 2013. Disponível em: <http://www.mises.org.br/Ebook.aspx?id=92>. Acesso em: 10 jun. 2017.

SENNA, J. J **Política Monetária:** ideias, experiências e evolução. Rio de Janeiro: FGV, 2010.

SILVA, S. F.; ALBUQUERQUE, V. G. **Descobrindo a BITCOIN.** São Paulo: Novatec, 2017.

SKUDNOV, R. **BITCOIN CLIENTS.** 2012. 38 f. Tese (Mestrado) - Curso de Tecnologia da Informação, Turku University Of Applied Sciences, Turun Ammattikoreakoulu, Turkia, 2012. Disponível em: <http://www.bitcointrading.com/pdf/Bitcoin_Clients_Thesis_Skudnov_Rostislav.pdf>. Acesso em: 12 set. 2017.

SURDA, P. **Economics of Bitcoin:** is Bitcoin an alternative to fiat currencies and gold? 2012. 93 f. Tese (Doutorado) - Curso de Economics And Business, Wu Vienna University Of Economics And Business, Vienna, 2012. Disponível em: <http://nakamotoinstitute.org/static/docs/economics-of-bitcoin.pdf>. Acesso em: 15 nov. 2017.

ULRICH, F. **Bitcoin – a moeda na era digital**. São Paulo: Instituto Ludwig von Mises Brasil, 2014. 138 p. Disponível em: <http://www.mises.org.br/Ebook.aspx?id=99> Acesso em: 22 abr. 2017.

ULRICH, F. **Por que precisamos entender o Bitcoin.** 2015. Disponível em: <http://www.mises.org.br/Article.aspx?id=2160>. Acesso em: 22 jun. 2017.

VAN DER LAAN, C. R. **É Crível uma Economia Monetária Baseada em Bitcoins? Limites à disseminação de moedas virtuais privadas.** Brasília: Núcleo de Estudos e Pesquisas/CONLEG/ Senado, dezembro/2014 (Texto para Discussão nº 163). Disponível em: <http://www.senado.leg.br/estudos>. Acesso em: 15 out. 2017.