

UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
INSTITUTO DE ECONOMIA
MONOGRAFIA DE BACHARELADO

O BITCOIN PODE SER CONSIDERADO MOEDA?

RODRIGO MARTINS ALEXANDRE PINHEIRO
Matrícula nº: 112104201

ORIENTADOR: Prof. Fernando Carlos G Cerqueira Lima

MAIO 2017

UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
INSTITUTO DE ECONOMIA
MONOGRAFIA DE BACHARELADO

O BITCOIN PODE SER CONSIDERADO MOEDA?

RODRIGO MARTINS ALEXANDRE PINHEIRO
Matrícula nº: 112104201

ORIENTADOR: Prof. Fernando Carlos G Cerqueira Lima

MAIO 2017

As opiniões expressas neste trabalho são da exclusiva responsabilidade do autor

Dedico este trabalho aos meus pais: André Luiz Pinheiro e Maura Martins Alexandre, que tanto investiram na minha educação.

AGRADECIMENTOS

Agradeço a meus familiares: Brenda Gonçalves Dias, André Luiz Pinheiro, Maura Martins Alexandre, Gabriel Pinheiro, Nathalia Pinheiro, José Plínio Pinheiro, Neuza Pinheiro, Marcus Vinícius Alexandre e Eliete Martins Alexandre, por todo o apoio prestado durante toda minha vida. Agradeço também ao professor Fernando Carlos G Cerqueira Lima pela atenção dispensada na elaboração deste trabalho.

RESUMO

As moedas virtuais são um experimento monetário muito recente e sem precedentes na história. O Bitcoin foi a primeira e é a mais relevante dessas moedas. Visando o crescimento da sua utilização e suas características únicas em comparação com os sistemas monetários tradicionais, o objetivo desse trabalho é responder se o Bitcoin pode ser efetivamente considerado uma moeda. Para isso é analisado sua capacidade de exercer as três funções de uma moeda, também será explorado se suas características são compatíveis com as teorias monetárias metalista e cartalista. Para tanto é feita uma exposição sobre o funcionamento do sistema. Após análise do funcionamento e das principais características do Bitcoin, foi concluído que o mesmo não pode ser considerado moeda. Atualmente a moeda virtual exerce razoavelmente apenas a função de meio de troca, tendo em seu design obstáculos relevantes para exercer as outras duas. Também foi concluído que o Bitcoin não poderia ser considerado moeda a partir do arcabouço teórico das teorias monetárias metalista e cartalista.

ÍNDICE

INTRODUÇÃO

CAPÍTULO I- FUNÇÕES E ORIGEM DA MOEDA.....	08
--	----

I.1 FUNÇÕES E CARACTERÍSTICAS FÍSICAS.....	08
--	----

I.2 TEORIAS METALISTA E CARTALISTA.....	09
---	----

CAPÍTULO II- O BITCOIN.....	12
-----------------------------	----

II.1 DEFINIÇÃO E ORIGEM.....	12
------------------------------	----

II.1.1 Definição.....	12
-----------------------	----

II.1.2 Origem.....	13
--------------------	----

II.2 FUNCIONAMENTO.....	14
-------------------------	----

II.2.1 O Blockchain.....	14
--------------------------	----

II.2.2 Mineração e oferta.....	15
--------------------------------	----

II.2.3 Transações e Armazenamento.....	17
--	----

II.2.4 Anonimato e atividades ilegais.....	18
--	----

II.3 ECOSSISTEMA.....	19
-----------------------	----

II.4 SEGURANÇA.....	20
---------------------	----

II.5 REGULAÇÃO.....	22
---------------------	----

CAPÍTULO III- O BITCOIN EXERCE AS FUNÇÕES DA MOEDA?	23
---	----

III.1 CARACTERÍSTICAS FÍSICAS.....	23
------------------------------------	----

III.2 MEIO DE TROCA.....	24
--------------------------	----

III.3 RESERVA DE VALOR.....	27
-----------------------------	----

III.4 UNIDADE DE CONTA.....	29
-----------------------------	----

CONCLUSÃO

REFERÊNCIAS BIBLIOGRÁFICAS

INTRODUÇÃO

O desenvolvimento tecnológico permitiu o advento, nos últimos anos, de experiências monetárias sem precedentes na história. Iniciado há menos de uma década, o fenômeno das moedas virtuais tem se tornado mais relevante. Entre as moedas virtuais, a primeira e mais proeminente é o Bitcoin. O Bitcoin foi criado em 2009, e nos últimos anos tem sido alvo de maior atenção, seja por sua crescente utilização e valorização, por episódios negativos, e principalmente por sua tecnologia inovadora, o *Blockchain*, que tem potencial de gerar mudanças em diversos setores da economia.

Por ser uma experiência muito recente e envolver inovações tecnológicas, é muito comum o desconhecimento sobre as propriedades e o funcionamento do sistema. O Bitcoin possui características que diferenciam seu funcionamento de qualquer experiência monetária anterior, sendo portanto, necessário debater até que ponto ele pode cumprir as funções das moedas tradicionais. O objetivo desse trabalho é dar um panorama geral sobre o funcionamento do sistema Bitcoin e responder se o mesmo pode ser considerado moeda. Para isso será feita uma análise sobre sua capacidade de exercer as três funções de uma moeda. Também será analisado se ele poderia ser considerado moeda a partir do arcabouço teórico das teorias monetárias metalista e cartalista.

No primeiro capítulo são apresentadas as três funções de uma moeda e as características físicas necessárias para exercê-las. Também serão brevemente apresentadas duas teorias monetárias conflitantes, a metalista, que foca no papel do mercado na origem da moeda, e a cartalista, que foca no papel do Estado. No segundo capítulo é dado um panorama geral do Bitcoin, desde sua criação, seu funcionamento, até o estado atual de regulação. No terceiro capítulo é analisado se o Bitcoin possui as características físicas necessárias para exercer as funções, se ele efetivamente as exerce e os obstáculos que possam o impedir de exercê-las. Concluiremos com respondendo se o Bitcoin pode ser considerado uma moeda.

CAPITULO I – FUNÇÕES DA MOEDA

I.1 FUNÇÕES E CARACTERÍSTICAS FÍSICAS

Em uma economia não monetária, que funcionasse através de um sistema de escambo, os agentes incorreriam em custos muito elevados para recorrer ao mercado. Um indivíduo que produzisse um bem “A” e quisesse trocar pelo bem “B” necessitaria que outro indivíduo, ao mesmo tempo, possuísse o bem “B” e desejasse o bem “A”. Esse modelo só seria possível em uma economia primitiva, onde os indivíduos fossem quase autossuficientes, ou seja, onde não houvesse a disseminação da divisão do trabalho. (CARVALHO et al., 2012)

Em uma economia monetária, a moeda funciona como um intermediário entre as transações. Os agentes trocam sua produção por moeda, que a qualquer momento, pode ser trocada pelos bens e serviços produzidos por outros agentes, pois a moeda é aceita por todos. Isso reduz os custos de recorrer ao mercado pois dá velocidade e flexibilidade aos agentes. Funcionar como meio de troca é a primeira função da moeda.

A segunda função da moeda é servir como unidade de conta, ou seja, servir como medida de valor. Isso significa que os agentes expressam o valor de seus bens e serviços em determinada quantidade de moeda. Cotar os preços em moeda torna mais fácil o cálculo econômico dos agentes, pois simplifica a comparação dos preços dos bens. (KRUGMAN; OBSTFELD, 2003) A função de unidade de conta é também muito importante no estabelecimento de contratos entre os agentes, sendo a moeda corrente a forma de liquidar esses contratos. (CARVALHO et al., 2012)

A terceira função da moeda é servir como reserva de valor. A moeda pode ser usada para transferir poder de compra para o futuro, então deve poder ser estocada por longos períodos de tempo sem perda relevante do seu valor. Se os agentes não tivessem a flexibilidade de adiar seu poder de compra, teriam resistência em aceitar receber aquela moeda como forma de pagamento. Deste modo, o valor da moeda deve se manter estável ao longo do tempo para que cumpra corretamente sua função de reserva de valor.

Para exercer essas três funções, a moeda deve ter algumas características físicas. Carvalho et al. (2012, p .03) apresenta essas características e porque elas são necessárias:

“A moeda deve também possuir determinadas características físicas. Deve ser divisível, durável, difícil de falsificar, manuseável e transportável. A divisibilidade é necessária porque a moeda deve poder ser fracionada em múltiplos e submúltiplos, para que as transações que exigem valor fracionado ou transações que movimentem grandes valores sejam realizadas sem custos adicionais. A moeda deve ser durável, isto é, deve manter suas características físicas, para que a sua condição de ser aceita de forma generalizada seja mantida e não prejudique seu último detentor. A moeda deve ser, na medida do possível, difícil de falsificar – já que tal característica aumenta a confiança do público de que não há reprodução indevida – auxiliando conseqüentemente sua aceitação generalizada. A moeda deve ser manuseável e transportável, para que a função de meio de troca não seja prejudicada, impondo ao seu detentor custos de transação” (CARVALHO et al., 2012, p.03)

I.2 TEORIAS METALISTA E CARTALISTA

As teorias monetárias divergem a respeito de qual seria a principal função da moeda, estando o protagonismo atrelado a sua visão sobre a origem da mesma. A teoria metalista da moeda enxerga sua origem através do processo de mercado, sendo a função protagonista a de meio de troca. Já a teoria cartalista tem seu foco na função de unidade de conta, e considera a origem da moeda como um fenômeno inerentemente estatal. A contradição existente entre as teorias é um contraponto entre a análise “real” e a análise “monetária” dos fenômenos econômicos. (BELL, 1998)

Para os metalistas, a origem da moeda está relacionada com a redução dos custos de transação. Menger (1892) explica como a moeda se origina espontaneamente do mercado. Partindo de uma economia de escambo, as trocas seriam muito dificultadas, pois necessitavam da coincidência dupla de desejos. Menger afirma que os bens teriam diferentes graus de “vendabilidade”, ou seja, alguns bens teriam maior facilidade de serem trocados a preços de mercado. Então os agentes estariam dispostos a trocar seus bens não só por aqueles que necessitavam no momento, mas também pelos bens que poderiam ser trocados mais facilmente no futuro. Os bens mais “vendáveis” funcionariam como intermediários entre as transações, e conforme mais indivíduos os demandasse, maior seria sua “vendabilidade”. Então os bens seriam cada vez mais aceitos, até se tornarem aceitos por todos, dando origem a moeda.

Devido a suas características físicas, os metais preciosos foram geralmente adotados como moeda. Porém utilizar o metal em sua forma natural geraria custos elevados de transação, pois

seria muito difícil identificar a quantidade e a qualidade do metal. Portanto, se passou a utilizar moedas cunhadas, que podiam garantir a qualidade e a quantidade do metal. A atividade da cunhagem foi historicamente desenvolvida por instituições governamentais, o que se tornou uma crítica à origem da moeda como um fenômeno espontâneo do mercado. Os metalistas responderam a essa crítica afirmando que a atuação do Estado foi posterior e apenas encorajou a continuidade da utilização dos metais como moeda, sendo assim, foi limitada apenas a dar suporte à vontade dos agentes privados. Para eles, as moedas cunhadas só eram aceitas devido ao seu conteúdo metálico. (BELL, 1998)

Para os metalistas, o valor da moeda é derivado do seu valor intrínseco, ou seja, de seu valor como commodity, independentemente de seu funcionamento como moeda. Isso seria necessário para que ocorresse a análise “real”, ou seja, todos os bens deveriam ter uma taxa de câmbio independente em relação a todos os outros bens, incluindo a própria moeda. Com a evolução dos sistemas monetários, as moedas metálicas foram substituídas por papel moeda, então os metalistas apontaram que o papel moeda somente tinha valor, sendo assim aceito, pois era lastreado em metais preciosos. Porém com o fim do padrão ouro, e o surgimento das moedas sem lastro em nenhuma commodity, a teoria metalista não foi capaz de explicar porque os indivíduos continuavam a aceitar uma moeda que teoricamente não teria valor algum. (BELL, 1998)

A teoria cartalista da moeda surgiu após mais de um século de predominância da teoria metalista. Os cartalistas rompem com os preceitos básicos da teoria de seus antecessores. A moeda passa a ser definida primariamente por sua função de unidade de conta, o conteúdo material da moeda não é mais considerado a fonte de seu valor e o Estado passa ter papel central na sua origem e desenvolvimento.

A teoria cartalista separa a função de unidade de conta da função de meio de troca, com o protagonismo da primeira. De acordo com Aschheim e Tavlas (2006) uma economia monetária não pode existir sem uma unidade de conta (dólar, euro etc.), mas pode existir sem um meio de troca. Isso porque sem a unidade monetária, seria impossível o cálculo econômico das taxas de câmbio entre os bens, assim como o registro de débitos e créditos. Por conseguinte, uma commodity pode ser a origem de uma moeda, mas não pela função de meio de troca. É sua função de unidade de conta que lhe permite se tornar moeda.

Portanto, uma commodity pode surgir do mercado como unidade de conta, transformando a economia de um estado de escambo para uma economia monetária. Porém, essa moeda é

considerada embrionária, e para que seja um sistema monetário completo, é necessário que exista aceitação generalizada dessa unidade de conta.

Para se obter a aceitação generalizada é necessária a definição pelo Estado de qual é essa unidade de conta. Porém, a simples declaração não é suficiente, o Estado tem que usar seu poder de cobrar impostos para gerar a adoção da moeda. Se o Estado definir que as obrigações legais dos contribuintes só podem ser pagas utilizando determinada unidade de conta, os indivíduos irão aceitar receber a mesma como pagamento, e pelas externalidades de rede, a moeda se tornará geralmente aceita por toda sociedade. (ASCHHEIM; TAVLAS, 2006)

Então, segundo essa teoria, o Estado tem a capacidade de tornar moeda aquilo que desejar, seja um metal, uma outra commodity, ou até mesmo papel inconvertível. Pois o valor da moeda é oriundo de sua utilidade para saldar as dívidas com o Estado. Assim sendo, a teoria cartalista pode ser aplicada em qualquer tipo de sistema monetário, desde as antigas moedas metálicas até as modernas moedas fiduciárias. As antigas moedas metálicas cunhadas pelo Estado eram um exemplo de moeda cartalista. Conforme argumentado por Bell (1998):

“When the coins are initially struck, and for some time thereafter, they will retain their original metal weight. After some time in circulation, however, they will begin to wear down and their weight will diminish. Knapp points out that if their continued use requires "weighing at the time of payment in order to establish their validity", then this is evidence of a "pensatory practice" and these pieces are not Chartal. If, however, their validity is retained after their wearing down has been noticed, then their continued use is in accordance with proclamation and they are Chartal”¹ (BELL, 1998, p.10)

O Estado declarava que determinada moeda possuía determinado valor, e mesmo perdendo parte do metal em sua composição, a moeda continuava a ser trocada normalmente pelo seu valor de face. Deste modo, seu valor era oriundo da declaração do Estado e não do seu valor intrínseco em metal, como defendido pelos metalistas.

No próximo capítulo serão expostas as características do Bitcoin. Após essa exposição, será analisado se o Bitcoin exerce as três funções de uma moeda, e se ele poderia ser considerado moeda a partir do arcabouço teórico das teorias monetárias apresentadas acima.

¹ Tradução nossa: “ Quando as moedas são cunhadas, e por algum tempo depois, elas retêm seu peso metálico original. Entretanto, depois de algum tempo em circulação, elas começam a perder parte do metal e seu peso diminui. Knapp afirma que se a utilização dessas moedas requeresse uma pesagem no momento da compra para garantir sua validade, então isso é evidência de uma “prática compensatória” então essas moedas não são cartalistas. Entretanto, se sua validade é mantida depois de a perda de peso ter sido notada, então seu uso está de acordo com a proclamação e elas são cartalistas”

CAPITULO II – O BITCOIN

O propósito desse capítulo é expor o que é o Bitcoin, apresentar suas origens, e dar uma visão geral do funcionamento da rede e de seu ecossistema. Também será discutido sobre a sua segurança e o atual cenário regulatório.

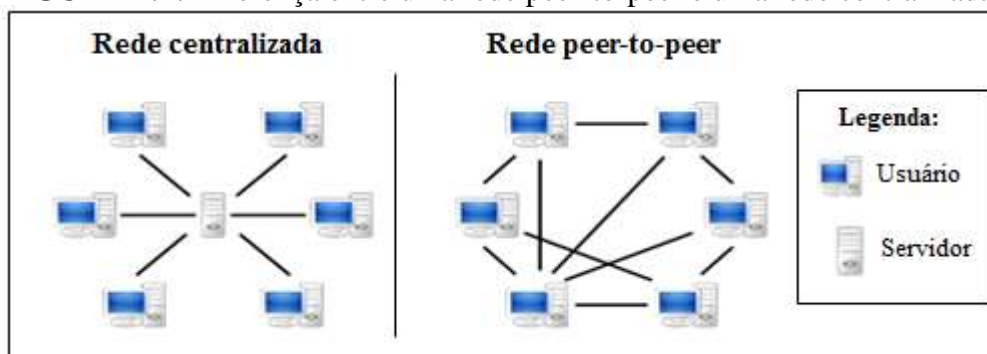
II.1 DEFINIÇÃO E ORIGEM

II.1.1 Definição

O Bitcoin é um protocolo online de comunicação que permite a utilização de uma moeda totalmente virtual. As unidades de bitcoin² são utilizadas para guardar e transferir valor entre os participantes de uma rede descentralizada composta pelos usuários do protocolo.

O Bitcoin é descentralizado porque é estruturado como uma rede *peer-to-peer*, ou par-a-par. Uma rede *peer-to-peer* significa que todos os computadores envolvidos na rede são iguais, não existindo nenhuma hierarquia entre eles, tampouco um servidor central. Os envolvidos na rede são, ao mesmo tempo, prestadores e consumidores de serviços. (ANTONOPOULOS, 2014) A figura 2.1 mostra a diferença entre uma rede peer-to-peer e uma rede centralizada.

FIGURA 2.1: Diferença entre uma rede peer-to-peer e uma rede centralizada



FONTE: Adaptado pelo autor a partir de: <<http://pt.wikipedia.org/wiki/Peer-to-peer>>

A descentralização é a principal inovação do Bitcoin, pois permitiu, pela primeira vez na história, realizar transações pela internet sem depender de uma terceira instituição de confiança, como um banco. A descentralização também torna o bitcoin a primeira moeda³ independente de qualquer autoridade central, uma vez que seu funcionamento independe de quaisquer instituições, privadas ou públicas.

² Utilizamos “Bitcoin” para fazer referência ao sistema e “bitcoin” à moeda.

³ Analisaremos nos próximos capítulos até que ponto o bitcoin pode ser considerado moeda

II.1.2 Origem

A origem do Bitcoin pode ser traçada para os primórdios da internet. Nessa época surgiram movimentos de criptógrafos de ideologia liberal que se dedicaram à criação de uma moeda livre do controle de bancos e do Estado. Nos anos 90 foram criadas algumas dessas moedas, porém todas falharam porque ainda dependiam de instituições privadas centralizadas. (WALLACE, 2011)

O Bitcoin foi criado no final de 2008 com a publicação em uma lista de e-mails, por Satoshi Nakamoto, de um paper chamado “Bitcoin: a Peer-to-Peer Electronic Cash System”, no paper é apresentado o funcionamento do protocolo. A verdadeira identidade de Nakamoto nunca foi revelada, especula-se que na verdade seria um pseudônimo para um grupo de pessoas.

Sua motivação para a criação do Bitcoin é incerta, mas uma mensagem enviada junto com a primeira transação da rede pode ser entendida como uma crítica ao sistema bancário. A mensagem: “The Times 03/Jan/2009 chancellor on brink of second bailout for banks” faz referência a uma matéria do jornal britânico sobre o resgate aos bancos ingleses impactados pela crise de 2008.

“A alusão à manchete do jornal britânico The Times daquele dia não é acidental. É, na verdade, um claro indicativo da visão crítica de Satoshi sobre o sistema bancário e a desordem financeira reinante.” (ULRICH, 2014, p.34)

Ao enviar a primeira transação à rede, no dia 03/Jan/2009, Nakamoto dava início a um experimento para tentar revolucionar o sistema bancário. O protocolo do Bitcoin foi disponibilizado como um software de código aberto⁴, o que permitiu seu desenvolvimento posterior através do trabalho de diversas outras pessoas. Também permitiu a criação de outras moedas virtuais baseadas no protocolo do Bitcoin.

Logo após seu surgimento, a utilização do Bitcoin foi muito restrita a um pequeno grupo de interessados em criptografia, sendo lentamente disseminada para outras pessoas. Os bitcoins não tinham nenhum valor até Abril de 2010, quando surgiram bolsas de bitcoins que permitiram troca-los por dólares. No início valiam poucos centavos, só atingindo a paridade em relação ao dólar em Fevereiro de 2011. (WALLACE, 2011) O posterior crescimento da

⁴ O Código Aberto é um termo que se refere a um software cujo código está disponível para download por qualquer pessoa e a uma filosofia de criação de aplicativos voltada para a colaboração entre desenvolvedores.

demanda pela moeda virtual fez sua taxa de câmbio disparar, encerrando o ano de 2016 cotado a US\$ 952. O gráfico 2.1 mostra evolução da taxa de câmbio do bitcoin em dólares.

GRÁFICO 2.1: Evolução da taxa de câmbio em dólares do bitcoin



FONTE: Criado pelo autor a partir de dados de: <https://www.quandl.com/data/BCHAIN/MKPRU-Bitcoin-Market-Price-USD>

II.2 FUNCIONAMENTO

II.2.1 O Blockchain

O maior desafio para a criação de uma moeda virtual se dá pelo problema do gasto duplo. Pela moeda não existir fisicamente, é necessário garantir que uma unidade da moeda não pode ser copiada e utilizada mais de uma vez, ou seja, garantir que a unidade monetária pertence, em um determinado momento, ao indivíduo A e não ao indivíduo B. As tentativas prévias de criar uma moeda virtual resolveram esse problema através de uma autoridade central que registraria todas as transações, como em um sistema bancário tradicional, porém isso tornava o sistema vulnerável a ataques e a manipulações. (ANTONOPOULOS, 2014)

A grande inovação do Bitcoin foi conseguir resolver o problema do gasto duplo mantendo um sistema monetário descentralizado, para isso foi utilizada uma engenhosa tecnologia. O *Blockchain* é uma espécie de livro razão, que é público e contém todas as transações já ocorridas, evitando assim, o problema do gasto-duplo, pois em um determinado momento apenas um usuário pode ser o dono de determinada unidade de bitcoin, e por ser público e distribuído, todos na rede tem essa informação, como explica Nakamoto:

“We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't

care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions. In the mint-based model, the mint was aware of all transactions and decided which arrived first. To accomplish this without a trusted party, transactions must be publicly announced”⁵ (NAKAMOTO, 2008, p.02)

O *Blockchain*, ou corrente de blocos, funciona através do agrupamento de diversas transações em blocos que são registrados, em média, a cada 10 minutos. Quando ocorre uma transação, em alguns segundos todos os usuários da rede são informados que determinada quantidade de bitcoins foi transferida de A para B, a partir desse momento, a transação já pode ser visualizada por todos na rede. Porém, essa transação só será confirmada, ou seja, o indivíduo B só poderá utilizar esses fundos, quando essa transação for verificada e registrada no *Blockchain*.

As transações são verificadas de forma independente. Diversos usuários irão verificar se as novas transações são legítimas e criarão o seu próprio bloco de transações. Os usuários então competem para registrar as transações no *Blockchain*, o primeiro que conseguir achar a resposta para um problema matemático, chamado de *proof-of-work*, registra o bloco e transmite para todos da rede. Esse problema matemático é gravado no bloco, então para que o bloco seja alterado ele teria que ser resolvido novamente. Se o bloco for reconhecido como legítimo, outros usuários criarão o próximo bloco conectado a ele, criando uma corrente de confiança e tornando as transações cada vez mais irreversíveis.

II.2.2 Mineração e oferta

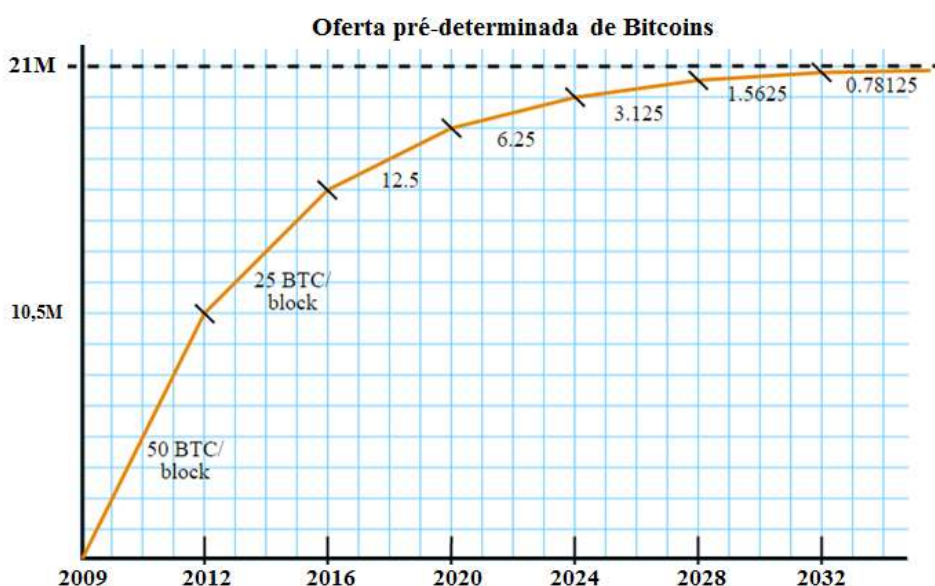
Os indivíduos que atuam na verificação das transações são chamados de mineradores. Os mineradores precisam utilizar equipamentos e gastar energia para manter o sistema funcionando. Seu incentivo econômico vem de duas formas: através de taxas de transação e por novas unidades de bitcoin, que são criadas a cada novo bloco registrado no *Blockchain*. Logo, o trabalho dos mineradores tem duas importantes funções no Bitcoin, garantir a segurança e a

⁵ Tradução nossa: “Precisamos que o beneficiário saiba que o antigo proprietário não efetuou transações anteriores. No nosso caso, a transação mais antiga é a que conta, então não nos importamos com as posteriores tentativas de gasto-duplo. A única forma de confirmar a inexistência de uma transação, é estar ciente de todas as transações. Em um modelo bancário, o banco estava ciente de todas as transações e decidiu qual ocorreu primeiro. Para conseguir isso sem um terceiro de confiança, as transações tem que ser anunciadas publicamente.”

validade das transações e criar novas unidades da moeda virtual, já que não existe órgão central que possa controlar a oferta da mesma.

Esses indivíduos são chamados de mineradores porque o Bitcoin foi criado de forma a simular a escassez de um metal precioso, como o ouro. Segundo Nakamoto: “The steady addition of a constant amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended”.⁶(NAKAMOTO, 2008, p.04). A oferta de bitcoins é programada para crescer de forma estável e decrescente até alcançar seu limite arbitrário de 21 milhões de unidades no ano de 2140. A partir desse momento os mineradores irão garantir o funcionamento da rede recebendo apenas as taxas de transação. O gráfico 2.2 mostra a quantidade ofertada pré-determinada de bitcoins.

GRÁFICO 2.2: Oferta total pré-determinada de bitcoins



FONTE: Adaptado pelo autor a partir de: <<http://www.lothar.com/presentations/bitcoin-brownbag/images/37-expansion.svg>>

Pode-se notar o retorno decrescente dos mineradores, pois a quantidade de bitcoins criados por bloco é dividida pela metade a cada quatro anos. O gráfico demonstra que no ano de 2032 quase todos os 21 milhões de bitcoins já estarão minerados.

Para garantir a liquidez e permitir transações de baixo valor, cada unidade de bitcoin tem oito casas decimais, podendo ser dividido em 100 milhões de partes. Caso o valor de um bitcoin

⁶ Tradução nossa: “A adição estável de uma quantidade constante de novas moedas é análogo a mineradores de ouro gastando recursos para adicionar ouro em circulação. No nosso caso, é gasto tempo de processamento e eletricidade”.

aumente muito e seja necessário aumentar a quantidade de casas decimais, isso pode ser feito por um consenso dos usuários da rede. (ULRICH, 2014)

II.2.3 Transações e armazenamento

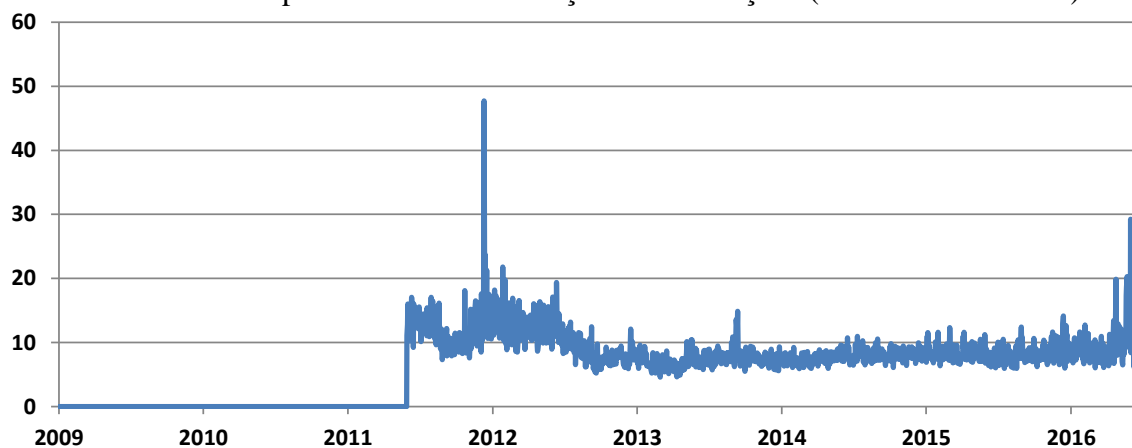
A rede bitcoin funciona através de um mecanismo de chaves. Os usuários criam endereços, e esses endereços são compostos de uma chave pública, e uma chave privada. As chaves são apenas uma sequência de números aleatórios. A chave pública funciona como um número de conta bancária, e a chave privada como uma senha. Para que ocorra uma transação, o usuário deve indicar a chave pública do endereço desejado e assinar a transação com a chave privada de seu endereço.

Não existem arquivos de bitcoins para serem armazenados, na verdade os bitcoins são apenas registros de transações. O que os usuários devem armazenar são as chaves privadas que permitem utilizar os bitcoins que foram transferidos para determinado endereço. As carteiras são a forma de armazenar as chaves privadas dos endereços. Existem diversos tipos de carteiras, com funcionalidades diferentes, mas em geral, elas são classificadas em dois tipos.

Hot wallets são carteiras cujas chaves privadas são armazenadas em um dispositivo com acesso à internet. São consideradas menos seguras, pois incorrem riscos de serem hackeadas. Porém são mais práticas de utilizar, pois permitem transacionar pelo navegador de internet e por aplicativos de celular. Já nas Cold wallets, as chaves privadas são armazenadas fora de um computador ou rede, por exemplo, em pendrives, em hardwares específicos e até mesmo em papel. São consideradas mais seguras, porém incorrem em riscos físicos, como a perda do papel com a chave, o que inutilizaria para sempre os bitcoins.

Por funcionar apenas no ambiente virtual, a rede Bitcoin funciona 24 horas por dia, todos os dias do ano, permitindo que transações sejam feitas em dias e horários no qual o sistema bancário tradicional não funciona. Adicionalmente, as transações no Bitcoin são processadas de forma bem rápida, levando em média dez minutos para serem confirmadas, o que as faz muito mais rápidas do que os serviços bancários tradicionais, principalmente em relação a transações internacionais. O gráfico 2.3 mostra o tempo médio de confirmação das transações do Bitcoin.

GRÁFICO 2.3: Tempo médio de confirmação das transações (valores em minutos)



FONTE: Criado pelo autor a partir de dados de: <<https://www.quandl.com/data/BCHAIN/ATRCT-Bitcoin-Average-Transaction-Confirmation-Time>>

II.2.4 Anonimato e atividades ilegais

O que é considerado uma vantagem para alguns usuários e ao mesmo tempo uma crítica ao Bitcoin, é a questão das carteiras não terem um nome vinculado a elas, o que tornaria o sistema completamente anônimo, e assim propenso à utilização para atividades ilegais.

Assim como o dinheiro físico, o Bitcoin não tem um intermediário que registra a identidade dos participantes de uma transação, porém todas as transações que já ocorreram no Bitcoin são públicas e podem ser rastreadas através da chave-pública do endereço. Portanto o Bitcoin não garante o anonimato, como destacado por Ulrich:

“Dessa forma, ainda que Bitcoin seja bastante semelhante ao dinheiro vivo, em que as partes podem transacionar sem revelar suas identidades a um terceiro ou entre si, é também distinto do dinheiro vivo, pois todas as transações de e para um endereço Bitcoin qualquer podem ser rastreadas. Nesse sentido, Bitcoin não garante o anonimato, mas permite o uso de pseudônimo.” (ULRICH, 2014, p.21)

O Bitcoin, assim como o papel moeda, já foi e provavelmente ainda é utilizado para atividades ilegais. O caso mais conhecido foi de um site chamado Silk Road. O Silk Road era um site onde usuários transacionavam itens ilegais. O site era mantido na deep web e aceitava apenas pagamentos em bitcoins. Em 2013 o site foi derrubado, seu criador foi preso e sentenciado a prisão perpétua⁷. A queda do Silk Road provou que as autoridades policiais podem rastrear e prender quem utiliza a rede para atividades ilegais. Um outro caso ocorreu

⁷ <https://www.theguardian.com/technology/2015/may/29/silk-road-ross-ulbricht-sentenced>

mais recentemente na Austrália, onde um traficante foi preso e seus bitcoins foram apreendidos e posteriormente leiloados⁸.

Existem formas que permitem identificar a identidade por trás de um pseudônimo da rede. As próprias bolsas de bitcoins, em muitos países, incluindo o Brasil, exigem dados pessoais de seus clientes, o que permitiria a identificação do mesmo em uma investigação. Ulrich argumenta:

“Vincular uma identidade do mundo real a um endereço Bitcoin não é tão difícil quanto se possa imaginar. Para começar, a identidade de uma pessoa (ou pelo menos informação de identificação, como um endereço IP) é frequentemente registrada quando alguém realiza uma transação de Bitcoin em uma página web ou troca dólares por bitcoins em uma casa de câmbio de bitcoins” (ULRICH, 2014, p.21)

II.3 ECOSSISTEMA

Após apenas oito anos da criação do Bitcoin, existem diversas empresas que atuam em seu ecossistema. Empreendedores que apostam no crescimento e consolidação da moeda virtual e de sua tecnologia, criam novos produtos e serviços para os usuários da rede. Empresas do ecossistema Bitcoin e de desenvolvimento da tecnologia do *Blockchain* já receberam um bilhão de dólares em investimento⁹. As principais empresas do ecossistema do bitcoin podem ser divididas em mineração, serviços de carteira, bolsas de bitcoins e processadores de pagamentos em bitcoins.

A mineração de bitcoins foi inicialmente feita por usuários utilizando seus computadores pessoais. Empresas surgiram para construir equipamentos específicos para a mineração de bitcoins¹⁰, que são mais eficazes na mineração e consomem menos energia. A atividade de mineração tem se tornado, com o crescimento da rede, cada vez mais competitiva, e por isso cada vez mais profissional. Foram criadas minas de bitcoins, que são imensos galpões repletos de equipamentos específicos para mineração, normalmente instalados em países onde o custo de energia é mais baixo, como na China¹¹. Existem também *mining pools*, que são empresas

⁸ <http://oglobo.globo.com/economia/australia-vai-leiloar-pacote-apreendido-de-bitcoins-de-42-milhoes-19403349>

⁹ <http://cointelgraph.com/news/1-billion-invested-so-far-in-bitcoin-blockchain-infrastructure>

¹⁰ <http://tecnologia.ig.com.br/especial/2013-09-02/conheca-as-maquinas-de-fazer-dinheiro-virtual.html>

¹¹ <http://www.infomoney.com.br/mercados/bitcoin/noticia/4018497/conheca-maior-mineradora-bitcoin-china-que-faz-milhao-por-mes>

para as quais diversos usuários “emprestam” seu poder computacional, e recebem uma proporção dos bitcoins mineirados.

As empresas que prestam serviços de carteira são muito importantes no ecossistema Bitcoin. Elas são a base de como os usuários se relacionam com seus saldos na moeda virtual. Inicialmente os bitcoins só podiam ser transacionados e armazenados utilizando um computador, o que era um entrave a sua popularização. Diversas empresas criaram seus serviços de carteira, tornando mais simples e seguro armazenar e transacionar com os bitcoins.

As bolsas de bitcoins são a principal interface entre o bitcoin e as moedas nacionais. Essas bolsas oferecem a plataforma para usuários trocarem bitcoins por moedas nacionais. Elas operam em um sistema de leilão duplo, com ofertas de compra e venda, como em um mercado financeiro tradicional. São financiadas a partir de comissões entre 0,2% e 2% do valor das transações. (BÖHME. et al, 2011) Outras empresas que atuam na interface entre o bitcoin e as moedas nacionais operam cartões de débito carregados com bitcoins¹² e caixas eletrônicos da moeda virtual, que estão sendo instalados em diversas cidades do mundo, incluindo São Paulo¹³.

Uma função extremamente importante no ecossistema do Bitcoin é das empresas que atuam como processadoras de pagamento. Essas empresas prestam serviços a comerciantes que desejam aceitar bitcoins de seus clientes. Elas recebem os bitcoins em nome dos comerciantes e lhes transfere o valor convertido para sua moeda local. Elas geram valor, pois tornam mais simples para os comerciantes aceitarem bitcoins e assumem o risco do preço flutuante da moeda virtual. Essas empresas foram responsáveis pelo aumento rápido no número de comerciantes que aceitam bitcoins, e serão muito importantes para seu crescimento futuro. (POLASIK, 2014)

II.4 SEGURANÇA.

No que tange aos riscos que afligem os usuários do sistema, o fato de não existir uma autoridade central, faz com que exista uma desconfiança muito grande a respeito da segurança do Bitcoin. O sistema Bitcoin e o *Blockchain* têm sua segurança baseada na sua construção engenhosa que é fundamentada pela criptografia.

O mecanismo de *proof-of-work* implantado na transmissão das transações ao *Blockchain* o faz muito seguro. Caso algum usuário malicioso resolva fraudar a rede, esse usuário teria que estar

¹² <https://bitcoinnewsmagazine.com/bitcoin-debit-card-options/>

¹³ <https://www.fiap.com.br/2015/11/11/fiap-disponibiliza-caixa-eletronico-de-bitcoins-no-campus-paulista/>

dotado de mais poder computacional do que todo o resto da rede somado, o que é extremamente improvável. Mesmo considerando essa possibilidade, seria mais lucrativo para esse usuário utilizar esse poder computacional para gerar novas moedas. Como explicado por Nakamoto:

“If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favor him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.”¹⁴ (NAKAMOTO, 2008, p.04)

O protocolo do Bitcoin é seguro, e já demonstrou isso em tentativas de ataque¹⁵. Porém, existem riscos relevantes na utilização do sistema, principalmente associados na forma como são guardadas as chaves privadas dos endereços e associados às empresas que compõe o ecossistema do Bitcoin. Por não existir uma autoridade central que possa atuar no caso de perdas ou roubos, a segurança dos bitcoins depende imensamente do usuário.

Existem diversos relatos de usuários que tiveram suas chaves roubadas por hackers que roubaram seus bitcoins, e também casos de empresas que perderam os bitcoins de seus clientes. O caso mais sério foi a quebra da corretora japonesa Mt.Gox em 2013. A Mt.Gox, na época a maior corretora do ecossistema Bitcoin, teve 400 milhões de dólares em bitcoins de clientes roubados, indo à falência logo em seguida¹⁶. O caso da Mt. Gox foi um exemplo emblemático dos riscos aos quais os usuários estão sujeitos se não utilizarem as melhores práticas de segurança.

Antonopoulos (2014), especialista em segurança do Bitcoin, recomenda práticas para armazenagem segura da moeda virtual. Em primeiro lugar, é recomendado que o usuário sempre mantenha os bitcoins sob seu controle, evitando riscos oriundos de terceiros. É recomendável também, guardar valores altos em carteiras não ligadas à internet. O autor também ressalta que já surgiram muitas inovações no âmbito da segurança do Bitcoin, e por se

¹⁴ Tradução nossa: “Se um agressor for capaz de conseguir mais poder de processamento do que todos os usuários honestos, ele teria que escolher entre usar isso para fraudar as pessoas roubando de volta seus pagamentos, ou usar para gerar novas moedas. Ele deve achar mais rentável seguir as regras que o favorecem com mais moedas do que todos os outros somados, do que minar o sistema e a validade de sua própria riqueza”.

¹⁵ <http://www.businessinsider.com/dan-kaminsky-highlights-flaws-bitcoin-2013-4>

¹⁶ <http://www.forbes.com/sites/cameronkeng/2014/02/25/bitcoins-mt-gox-shuts-down-loses-409200000-dollars-recovery-steps-and-taking-your-tax-losses/#451592327ed6>

tratar de um experimento muito novo, é provável que ainda sejam desenvolvidas novas práticas e ferramentas que tornarão mais fácil para os usuários manterem seus bitcoins a salvo.

II.5 REGULAÇÃO

Com a popularização do Bitcoin, e o conseqüente aumento dos riscos oriundos de sua utilização, autoridades governamentais ao redor do mundo passaram a estudar formas de regular o sistema. O desafio para os reguladores é atuar sobre os riscos e vulnerabilidades do sistema, sem comprometer as inovações proporcionadas pelo mesmo. Por ser um sistema inerentemente internacional, e ainda muito novo, o tratamento legal do Bitcoin varia muito ao redor do mundo. A maioria dos países não tem legislação específica, sendo permitida na maioria dos casos sua utilização, porém em países como Rússia, Bolívia e Equador vigoram proibições sobre sua utilização¹⁷.

A regulação do Bitcoin é um tema complexo porque ele contém elementos de uma moeda, um ativo e de um sistema de pagamentos. Definir como deve ser classificado é essencial para definir como deve ser regulado e até mesmo qual órgão regulador deve ser responsável por fazê-lo. Em diferentes jurisdições, e até mesmo dentro da mesma jurisdição, o Bitcoin foi categorizado de forma diferente. Nos EUA, a IRS, sua autoridade tributária, classificou o bitcoin como “propriedade” para fins de taxação, enquanto o Departamento do Tesouro o classificou como “valor” para fins de obrigações de combate à lavagem de dinheiro. (HE, Dong, 2016)

A descentralização é outro fator que dificulta a regulação do Bitcoin. O sistema não depende de intermediário central, que seria normalmente, o alvo da regulação. Redes com milhares de usuários independentes são naturalmente difíceis de regular. As empresas que atuam na interface entre o Bitcoin e as moedas nacionais, como as bolsas de bitcoins, têm sido o alvo mais comum de regulação, normalmente com o objetivo de evitar a lavagem de dinheiro, a evasão fiscal e o financiamento ao terrorismo.

Do ponto de vista tributário a tendência na maioria dos países tem sido o tratamento dos bitcoins como um ativo, sendo tributado nos casos de ganhos de capital. No Brasil, os usuários devem declarar os bitcoins como “Outros bens e Direitos”, estando sujeito a taxação de ganhos de capital caso o valor de bitcoins vendidos em um mês seja maior que R\$ 35 mil¹⁸.

¹⁷ <http://www.coindesk.com/bitcoin-legal-map/>

¹⁸ <http://www.infomoney.com.br/minhas-financas/impostos/noticia/4757581/bitcoins-nao-sao-consideradas-moedas-mas-devem-constar-declaracao>

CAPITULO III – O BITCOIN EXERCE AS FUNÇÕES DA MOEDA?

O objetivo desse capítulo é analisar até que ponto o bitcoin pode ser considerado moeda, analisaremos suas características físicas e sua capacidade de satisfazer as três funções de uma moeda.

III.1 CARACTERÍSTICAS FÍSICAS

Para analisar se o bitcoin pode ser considerado moeda, é preciso primeiro analisar se o bitcoin possui as características físicas necessárias para exercer as três funções da moeda. Conforme apresentado no Capítulo I, a moeda deve ser divisível, durável, difícil de falsificar, manuseável e transportável.

Conforme mencionado no capítulo anterior, atualmente cada unidade de bitcoin tem oito casas decimais, podendo ser dividido em 100 milhões de partes. No futuro, em caso de necessidade, pode ser dividido em quantas casas decimais forem necessárias. Por conseguinte, o bitcoin tem divisibilidade perfeita, não sendo um problema para funcionar como meio de troca.

O bitcoin não se manifesta fisicamente, então não está sujeito a questões físicas que podem degradar suas propriedades. O bitcoin existe apenas no ambiente virtual, portanto sua durabilidade é dependente somente da existência de energia elétrica e internet. Portanto, partindo do pressuposto que a internet continue existindo, o bitcoin tem durabilidade eterna.

Devido à construção de sua rede, a possibilidade de se falsificar bitcoins é nula. Não existem unidades de bitcoins para serem falsificadas, existem apenas registros de transações no *Blockchain*. Caso algum usuário malicioso conseguisse atacar a rede, ele poderia alterar o registro de transações, porém não poderia criar reproduções indevidas de um bitcoin.

Transportar os bitcoins é na verdade transportar as chaves privadas dos endereços onde os bitcoins estão armazenados. Essas chaves são apenas sequências de números, que podem ser armazenadas de forma muito simples. Podem ser armazenadas em computadores, celulares, servidores na internet e até mesmo em papel. Portanto, o custo de transportar essas chaves é muito baixo, mesmo transportando valores muito elevados.

Deste modo, o bitcoin possui todas as características físicas necessárias para exercer as três funções da moeda. Porém isso não é suficiente para garantir que as funções sejam exercidas, nas próximas seções analisaremos cada função separadamente.

III.2 MEIO DE TROCA

Para que o bitcoin exerça a função de meio de troca, precisa ser aceito como forma de pagamento por um número relevante de bens e serviços. O desafio inerente ao bitcoin é que ao contrário das moedas nacionais, não existe uma autoridade que obrigue sua aceitação. Portanto, a aceitação do bitcoin como forma de pagamento é voluntária e dependente da expectativa de que outros também aceitarão a moeda posteriormente. O principal fator que motiva os usuários a aceitarem a moeda virtual é o seu baixo custo de transação (LO; WANG, 2014)

A descentralização é um importante fator para a redução dos custos de transação. Por não existirem intermediários, as transações no Bitcoin podem ser feitas de forma mais barata. É possível realizar transações sem nenhuma taxa, ou pagando taxas muito pequenas. Por exemplo, no ano de 2016 a taxa média por transação foi de U\$ 0,16¹⁹.

A irreversibilidade das transações é também um fator que possivelmente pode reduzir os custos de transação. Em um sistema de pagamentos tradicional, as instituições financeiras são responsáveis por mediar os conflitos, e o custo de mediar os conflitos aumenta os custos de transação. Os vendedores estão sujeitos à incerteza e a fraudes que em algum percentual são inevitáveis. (NAKAMOTO, 2008). A chamada fraude amigável, é um problema relevante para os vendedores, principalmente nas vendas pela internet. O consumidor estorna seu pagamento e ainda mantém o produto, forçando o logista a perder sua mercadoria e ainda pagar taxas para as operadoras de cartão de crédito. A fraude amigável representa 86% dos chargebacks, custando aos vendedores bilhões de dólares todos os anos nos Estados Unidos²⁰. Logo, a utilização do Bitcoin pode gerar economias consideráveis para as empresas, sendo um propulsor para o crescimento de sua aceitação.

O maior potencial de redução dos custos de transação está nas transações internacionais. O Bitcoin é por definição sem fronteiras, o que permite transacionar com um indivíduo a milhares de quilômetros de distância sem incorrer em custos adicionais. O Banco Mundial estima que em 2015, o valor das remessas internacionais foi de U\$ 600 bilhões²¹. Esses serviços tem um custo

¹⁹ Calculado com base no total de taxas de transação e na quantidade total de transações. Dados disponíveis em: <https://www.quandl.com/data/BCHAIN/CPTRA-Bitcoin-Cost-Per-Transaction> e <https://www.quandl.com/data/BCHAIN/NTRAN-Bitcoin-Number-of-Transactions>

²⁰ <http://www.forbes.com/sites/johnrampton/2015/04/14/how-online-fraud-is-a-growing-trend/#7bec5061349f>

²¹ <https://www.theguardian.com/global-development/2016/jun/16/remittances-mainstay-millions-worlds-poor-improve-them-dipti-pardeshi>

elevado, em média 7,6% do valor transacionado²². Portanto, o Bitcoin tem um potencial muito grande para crescer nesse mercado devido ao seu claro diferencial de custo.

Mesmo com seu claro diferencial de custo, a presença do Bitcoin no mercado de remessas é despresável. Um grande impedimento ao crescimento nesse mercado é o fato da imensa maioria das remessas serem para países em desenvolvimento. A população desses países, em geral, tem menos conhecimento sobre o Bitcoin, e menor acesso as tecnologias digitais que permitem o seu uso. (LO; WANG, 2014)

Durante os primeiros anos de sua existência o bitcoin era aceito apenas em pequenos sites, sendo muitos deles dedicados ao seu próprio ecossistema, como lojas de equipamentos de mineração. Nos últimos anos vem ocorrendo um crescimento de sua aceitação, expandindo para lojas físicas e para bens e serviços tradicionais. Atualmente é possível comprar um gama relevante de produtos e serviços utilizando a moeda virtual. Estima-se que mundialmente mais de 100.000 empresas aceitem bitcoins, incluindo gigantes como a Microsoft, Dell, Expedia Overstock entre outras²³.

Serviços de processamento de pagamento, como o Bitpay, foram responsáveis por boa parte do crescimento da aceitação do bitcoin, pois permitem a conversão imediata para a moeda local do comerciante, assumindo assim os riscos de sua alta volatilidade. Esses serviços exemplificam como o Bitcoin pode reduzir os custos de transação. Por exemplo, o Bitpay cobra taxas máximas de 1% do valor transacionado²⁴, sendo consideravelmente mais baixas que as taxas das operadoras de cartão de crédito. Em seu relatório sobre o Bitcoin, o banco Goldman Sachs estima que se todo o volume de pagamentos eletrônicos nos Estados Unidos fosse realizado utilizando serviços de processamento de pagamentos de bitcoin, os comerciantes poderiam ter economizado 211 bilhões de dólares em custos de transação, apenas no ano de 2013. A figura 3.1 mostra o detalhamento dessas economias.

FIGURA 3.1: Detalhamento das economias potenciais com o uso do bitcoin

Tamanho do mercado em 2013 (U\$bi)	Varejo	Comércio Eletrônico	Remessas
Volume em dólares por mercado	10.383	609	549
Taxas médias atuais	2,50%	2,90%	8,90%
Taxas Bitcoin	1%	1%	1%
Taxas atuais de transação(U\$ bi)	259,6	17,8	48,9
Taxas Bitcoin(U\$ bi)	103,8	6,1	5,5
Economias potenciais com Bitcoin	155,8	11,7	43,4

²² https://remittanceprices.worldbank.org/sites/default/files/rpw_report_june_2016.pdf

²³ <http://www.ibtimes.co.uk/bitcoin-now-accepted-by-100000-merchants-worldwide-1486613>

²⁴ <https://bitpay.com/pricing>

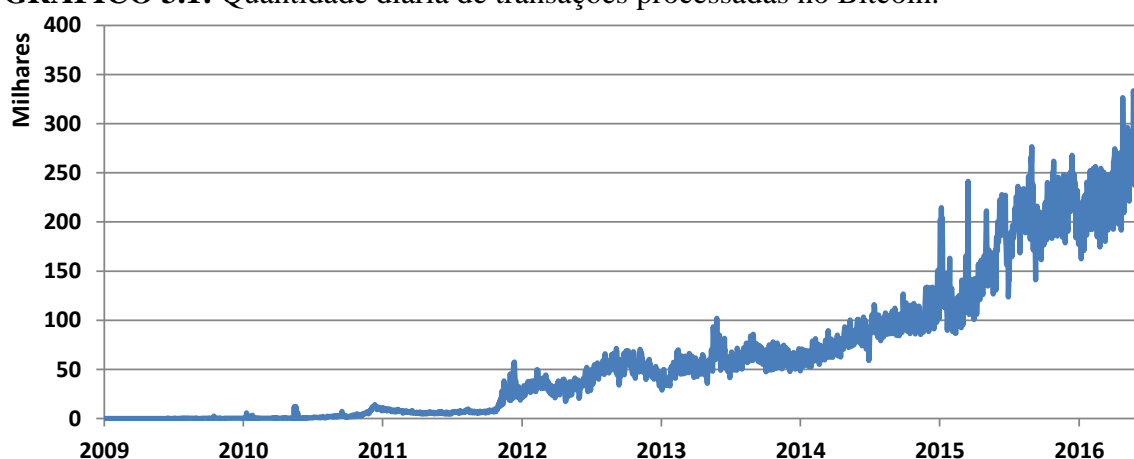
FONTE: Adaptado pelo autor a partir de:

<<http://www.paymentlawadvisor.com/files/2014/01/GoldmanSachs-Bit-Coin.pdf>>

Lo e Wang (2014) analisaram empiricamente se as empresas praticam preços melhores ou piores para pagamentos em bitcoins. A partir de amostras de preço de dois produtos em dois grandes vendedores online, concluíram que essas empresas não cobram mais caro para aceitar a moeda virtual e podem inclusive oferecer um pequeno desconto. Deste modo, aceitar bitcoins deveria ser pelo menos tão lucrativo quanto os sistemas de pagamento tradicionais.

Com a crescente popularização do Bitcoin, a quantidade diária de transações na rede tem aumentado. O gráfico 3.1 mostra quantidade de transações diárias na rede.

GRÁFICO 3.1: Quantidade diária de transações processadas no Bitcoin.



FONTE: Criado pelo autor a partir de dados de:

<<https://www.quandl.com/data/BCHAIN/NTRAN-Bitcoin-Number-of-Transactions>>

Apesar do seu forte crescimento, o Bitcoin continua sendo um meio de pagamento pouco relevante. Em 2016, o volume diário variou em torno das 250 mil transações, sendo apenas um percentual delas como forma de pagamento por bens e serviços. Em comparação, apenas nos Estados Unidos no ano de 2012 foram realizadas, em média, 72 milhões de compras por dia utilizando cartões de crédito²⁵.

Com a popularização da rede, o bitcoin tem exercido cada vez mais a função de meio de troca, porém ainda é pouco relevante comparado a outras formas de pagamento. Um obstáculo para a maior adoção da moeda virtual como meio de troca é a dificuldade na obtenção da mesma. Para obter unidades da moeda, os usuários precisam comprá-las em uma bolsa de bitcoins, que não estão disponíveis em muitos países e em geral tem baixa liquidez, e relevantes riscos associados

²⁵ https://www.frbervices.org/files/communications/pdf/research/2013_payments_study_summary.pdf

(YERMACK, 2014). Yermack também afirma que a inexistência de mecanismos de crédito ao consumidor é outro obstáculo a sua adoção generalizada:

“Finally, one cannot bypass the requirement of possessing bitcoins before procuring goods and services from a merchant. Being able to purchase goods without cash in hand occurs routinely in most retail markets, as customers frequently buy with consumer credit financed by the merchant or a third-party credit card vendor. These options are not available for bitcoins, as no bitcoin-denominated credit cards have yet been issued and consumer loans denominated in bitcoin appear to be unheard-of.”²⁶
(YERMACK,2014, p.11)

III.3 RESERVA DE VALOR

Para exercer corretamente a função de reserva de valor, o valor de um bitcoin deveria ser razoavelmente estável ao longo do tempo. A independência, a descentralização e suas características de oferta têm impactos relevantes sobre a capacidade da moeda virtual se tornar uma forma eficiente de reserva de valor.

O bitcoin não está atrelado a nenhuma commodity, nem a nenhum órgão central que possa atuar para garantir o valor da moeda. O valor do bitcoin é oriundo de sua escassez e é definido pelo mercado, ou seja, pela relação entre oferta e demanda. A oferta de bitcoins é limitada e conhecida por todos, portanto as flutuações em seu preço ocorrem quase exclusivamente por questões de demanda.

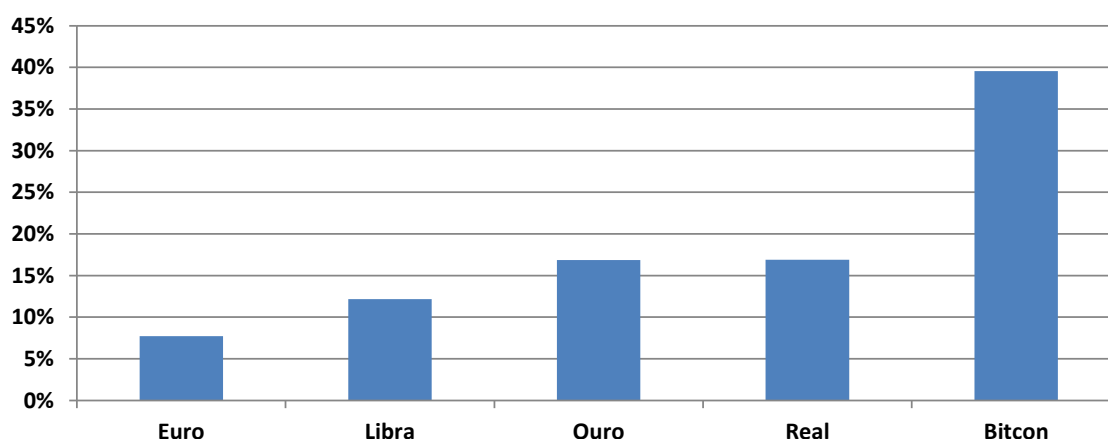
Os entusiastas do Bitcoin consideram sua independência e oferta limitada como uma grande vantagem da moeda virtual, pois protegeria os usuários dos males gerados pela inflação, e por controles de capitais. Não seria necessário confiar em um Banco Central, pois utilizando a moeda virtual o poder de compra poderia ser mantido, mesmo em países onde vigoram inflações elevadas. A Argentina é um bom exemplo, convivendo com inflação elevada e controles para a compra de outras moedas, o país se tornou líder na utilização do Bitcoin na América Latina²⁷.

²⁶ Tradução nossa: Não é possível evitar a necessidade de portar bitcoins antes de comprar bens e serviços de um comerciante. Poder comprar produtos sem ter dinheiro em mãos acontece rotineiramente na maioria dos mercados, pois consumidores frequentemente compram utilizando crédito financiado pelo comerciante ou por um operador de cartão de crédito. Essas opções não existem para bitcoins, pois ainda não existem cartões de crédito, nem empréstimos aos consumidores denominados em bitcoins

²⁷ <http://www1.folha.uol.com.br/tec/2016/07/1788250-com-crise-e-inflacao-buenos-aires-lidera-em-bitcoin-na-america-latina.shtml>

Como todo ativo financeiro, o bitcoin pode ser usado para investimentos especulativos. A falta de lastro e sua tendência a valorização devido a sua oferta limitada, tornam a moeda virtual muito suscetível a especulação e a formação de bolhas. Por ser também independente, não existe, como nas moedas nacionais, um órgão central que possa atuar para reduzir as flutuações de preço da moeda, o que acaba causando a volatilidade extremamente elevada da mesma. O gráfico 3.2 mostra a comparação da volatilidade anualizada²⁸ da cotação do ouro, da taxa de câmbio do bitcoin e de outras moedas em relação ao dólar no ano de 2016.

GRÁFICO 3.2: Volatilidade anualizada da cotação em dólares em 2016



FONTE: Criado pelo autor a partir de dados de <<https://www.quandl.com>> e <<https://www.bcb.gov.br/pt-br/#!/n/TXCAMBIO>>

O gráfico demonstra que o bitcoin é muito mais volátil que o ouro e que as moedas nacionais. A comparação da volatilidade do bitcoin com a de outras moedas e ativos demonstra que manter saldos em bitcoins é muito arriscado, mesmo em curtos períodos de tempo, o que impede a moeda de funcionar corretamente como reserva de valor.

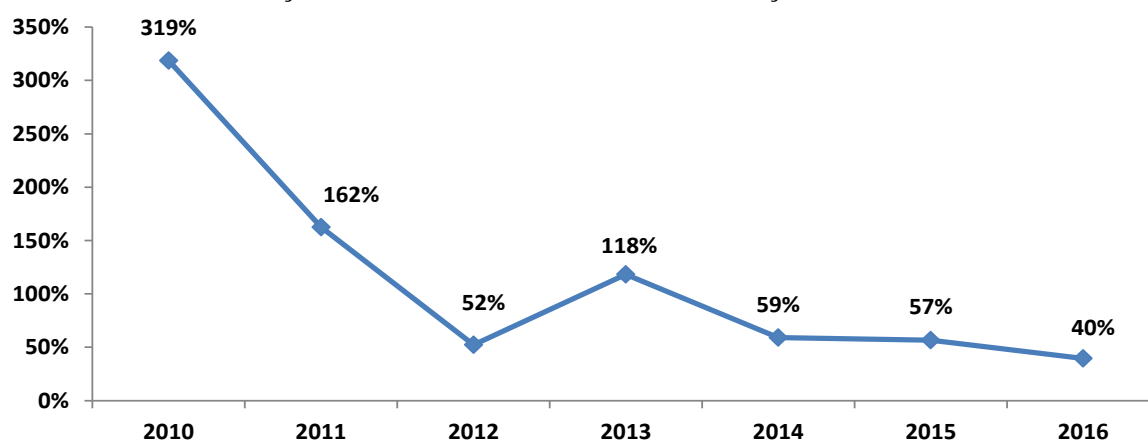
Yermack (2014) estudou a correlação entre a variação das taxas de câmbio em relação ao dólar das principais moedas, do ouro e do bitcoin. Seu trabalho mostra que existe forte correlação entre as principais moedas e também em relação ao ouro. Já o bitcoin não demonstra estar correlacionado com nenhuma moeda e tampouco com o ouro. Sua separação em relação a outros ativos demonstra que seu preço não é afetado por eventos macroeconômicos que afetam outras moedas, se comportando mais como um investimento especulativo do que como uma moeda. (YERMACK, 2014)

²⁸ A volatilidade anualizada foi calculada a partir do desvio padrão dos retornos diários multiplicado pela raiz quadrada de 252 (quantidade de dias úteis).

Polasik et al. (2014) analisou empiricamente fatores que afetam a formação do preço do bitcoin. Os fatores mais relevantes encontrados foram popularidade e o volume de transações. Foi percebido um forte aumento no preço da moeda com o aumento do número de pesquisas online e da quantidade de artigos publicados com a palavra bitcoin, o que sugere que a popularidade é um fator muito relevante. A correlação entre o aumento do preço do bitcoin com o aumento no volume de transações exemplifica o efeito das externalidades de rede, ou seja, os bitcoins teriam mais utilidade com o aumento generalizado em sua utilização (POLASIK et al., 2014)

Os entusiastas do Bitcoin afirmam que sua volatilidade é elevada devido a sua imaturidade e baixa liquidez. Com a maior adoção da rede e a maior utilização do bitcoin como forma de pagamento em detrimento de investimentos especulativos, a tendência seria a redução de sua volatilidade. Analisamos empiricamente se a volatilidade foi reduzida acompanhando o crescimento da utilização da rede nos últimos anos. O gráfico 3.3 mostra a evolução da volatilidade anualizada de 2010 até 2016.

GRÁFICO 3.3: Evolução da volatilidade anualizada da cotação em dólares do bitcoin



FONTE: Criado pelo autor a partir de dados de:

<<https://www.quandl.com/data/BCHAIN/MKPRU-Bitcoin-Market-Price-USD>>

Podemos perceber que efetivamente vem ocorrendo uma redução da volatilidade do preço do bitcoin. Porém, sua volatilidade ainda é extremamente elevada. Para que o bitcoin possa exercer corretamente a função de reserva de valor, a volatilidade ainda tem que ser muito reduzida, e o design da rede pode ser um obstáculo para tal redução.

III.4 UNIDADE DE CONTA

Para exercer a função de unidade de conta, os preços dos produtos vendidos pelos comerciantes que aceitam bitcoins deveriam ser cotados na moeda virtual. Em geral, essas empresas têm

cotado seus preços nas moedas nacionais, fazendo a conversão no momento da compra. Assim sendo, o bitcoin não tem desempenhado essa função.

A volatilidade de seu preço é um fator importante que impede o bitcoin de exercer a função de unidade de conta. Os preços dos bens cotados em bitcoins variam muito, mesmo em curtos espaços de tempo, o que gera inutilidade para os consumidores que não podem prever corretamente os preços. Essa variação também gera custos para que o comerciante atualize constantemente seus preços.

Outra questão para que o bitcoin exerça a função de unidade de conta, é a existência de diversas cotações da moeda virtual. Como as bolsas de bitcoins são independentes, o preço mais atual em cada uma delas é diferente. Isso dificulta para os consumidores e comerciantes terem um referencial para cotar seus preços (YERMACK, 2014). Em sua pesquisa feita em 2014, o autor encontrou preços variando quase 7% entre a cotação mais alta e a mais baixa entre as cinco bolsas de bitcoins com maior volume em dólares. Essa diferença parece ter diminuído²⁹, sugerindo uma redução desse problema com a crescente liquidez das bolsas.

Segundo Yermack (2014) outro obstáculo relevante oriundo do design da moeda virtual é o seu valor elevado. Por existirem poucas unidades da moeda, o valor de cada uma tende a ser muito elevado. Portanto, para realizar transações de baixo valor os consumidores precisam utilizar diversas casas decimais. Segundo o autor, os consumidores não estão acostumados a pensar em tantas casas decimais, que podem causar confusão e dificultar a diferenciação dos preços dos produtos. Os entusiastas do bitcoin tendem a negligenciar esse problema, pois argumentam que os usuários possam passar a transacionar em unidades menores, como por exemplo, micro-bitcoins. Reduzindo assim, o número de casas decimais utilizadas e facilitando o cálculo econômico.

O maior obstáculo para que a função de unidade de conta seja exercida no longo prazo é a tendência a deflação gerada pelo limite no número de moedas disponíveis. A combinação de uma oferta limitada e de uma demanda crescente, poderia gerar uma valorização constante da moeda virtual. A valorização reduziria o valor dos bens cotados em bitcoins, ou seja, geraria uma deflação crônica. Em uma moeda deflacionária, os agentes têm incentivo para manter a

²⁹ Por volta das 17hrs do dia 15/07/2016 foi encontrada uma diferença em torno de 2%, de acordo com o site: <https://bitcoincharts.com/markets/currency/USD.html>

moeda e adiar o consumo, gerando uma espiral deflacionária e provável queda na atividade econômica. (EUROPEAN CENTRAL BANK, 2012)

Segundo o relatório do Banco Central Europeu, para evitar os problemas econômicos derivados de uma moeda deflacionária, os preços em bitcoins poderiam ser adaptados aos preços cotados em outras moedas:

“Bitcoin is not the currency of a country or currency area and is therefore not directly linked to the goods and services produced in a specific economy, but linked to the goods and services provided by merchants who accept Bitcoins. These merchants may also accept another currency (e.g. US dollars) and therefore, the fact that deflation is anticipated could give rise to a situation where merchants adapt the prices of their goods and services in Bitcoins”³⁰ (EUROPEAN CENTRAL BANK, 2012, p.25)

Portanto, mesmo que o Bitcoin se desenvolva, consiga superar o obstáculo da volatilidade e se torne mais difundido, sua natureza deflacionária provavelmente o impediria de exercer a função de unidade de conta.

³⁰ Tradução nossa: Bitcoin não é a moeda de um país ou de uma área, e portanto não está ligado diretamente aos bens e serviços produzidos em uma economia específica, mas ligado aos bens e serviços fornecidos pelos comerciantes que aceitam Bitcoins. Esses comerciantes podem também aceitar outra moeda e portanto o fato de que a deflação é antecipada pode gerar uma situação onde comerciantes adaptam os preços de seus bens e serviços em Bitcoins

CONCLUSÃO

Neste trabalho buscamos analisar se o bitcoin pode ser considerado moeda, ou seja, se pode exercer as funções de meio de troca, reserva de valor e de unidade de conta.

Pode-se considerar que a função de meio de troca é razoavelmente bem atendida. Embora o número de transações e de empresas que aceitam bitcoins sejam ainda inexpressíveis, quando comparados aos meios de pagamento tradicionais, existe uma quantidade razoável de bens e serviços que podem ser adquiridos com a moeda virtual. Adicionalmente, transacionar com bitcoins pode ser mais vantajoso do que com os meios de pagamento tradicionais, devido a rapidez e os baixos custos de transação, o que pode permitir um crescimento futuro em sua aceitação.

A função de reserva de valor não é bem atendida. Sua alta volatilidade o impede de manter seu poder de compra ao longo do tempo. Efetivamente, o bitcoin só foi utilizado como reserva de valor em países que sofreram com hiperinflação ou controles de capital. Sua volatilidade vem sendo reduzida de acordo com o crescimento da rede, o que pode tornar o bitcoin uma reserva de valor no futuro. Porém, seu design descentralizado e seu uso para investimentos especulativos podem fazer com que a moeda virtual nunca tenha a capacidade de manter sua volatilidade nos níveis de uma moeda nacional bem administrada.

A função de unidade de conta também não é atendida. As empresas que aceitam bitcoins não costumam cotar os seus preços na moeda virtual. Existem alguns obstáculos para que essa função seja atendida. A alta volatilidade, a diversidade de cotações e o número de casas decimais, são fatores relevantes para que os preços não sejam cotados na moeda. É possível que no futuro, com o crescimento da rede, esses fatores sejam superados. Porém, a natureza deflacionária da moeda virtual é um fator que possivelmente nunca permitirá que a moeda seja utilizada como unidade de conta.

A partir do arcabouço teórico da teoria monetária cartalista, é evidente que o bitcoin não pode ser considerado moeda. Sua natureza inerentemente privada, e o fato de não ser adotado por nenhum Estado, impediriam o bitcoin de ter aceitação generalizada. O protagonismo que a teoria concede à função de unidade de conta contrasta com o fato de que o bitcoin atualmente não exerce, e provavelmente nunca vai exercer essa função.

Já em relação à teoria metalista, no primeiro momento o bitcoin poderia ser considerado uma moeda, devido a sua origem no mercado privado e do protagonismo da função de meio de troca. Porém, ao contrário dos pressupostos da teoria, o bitcoin não é atrelado a nenhuma commodity, ou seja, não possui valor intrínseco. Por conseguinte, de acordo com a teoria, o bitcoin não poderia ser considerado moeda, pois não teria nenhum valor.

Portanto, o bitcoin não pode ser considerado moeda. O mais provável é que em seu desenvolvimento futuro, o bitcoin continue atuando apenas como meio de troca, ainda que de forma limitada. Sendo os preços cotados nas moedas nacionais, e os saldos em posse dos agentes convertidos para as mesmas.

REFERÊNCIAS BIBLIOGRÁFICAS

ASCHHEIM, Joseph; TAVLAS, George.S. Money as numeraire: doctrinal aspects and contemporary relevance. **BNL Quarterly Review**, [S.l.] v. 59, n. 239, p. 333-361, 2006. Disponível em: <<https://ideas.repec.org/a/psl/bnlaqr/200642.html>> Acesso em: 30 ago.2016

BELL, Stephanie. **The hierarchy of Money**. The Jerome Levy Economics Institute WP No. 231, Kansas City, 1998. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=96845> Acesso em: 30 ago.2016

BÖHME, Rainer. et al. Bitcoin: Economics, technology, and governance. **Journal of Economic Perspectives**, [S.l.], v. 29, n. 2, p. 213–238, 2011. Disponível em: <<http://pubs.aeaweb.org/doi/pdfplus/10.1257/jep.29.2.213>>. Acesso em: 18 jul.2016.

CARVALHO, Fernando J. Cardim. et al. **Economia monetária e financeira: teoria e política**. São Paulo: Campus, 2012. p. 1-4.

EUROPEAN CENTRAL BANK. **Virtual currency schemes**. Frankfurt, 2012. Disponível em: <<https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>>. Acesso em: 18 jul.2016.

GOLDMAN SACHS. All About Bitcoin. **Global Macro Research: Top of mind**, [S.l.], v. 21, 2014. Disponível em: <<http://www.paymentlawadvisor.com/files/2014/01/GoldmanSachs-Bit-Coin.pdf>>. Acesso em: 18 jul.2016.

GRINBERG, Reuben. **Bitcoin: An innovative alternative digital currency**. [S.l.], 2011. Disponível em: <<http://www.scienceandtechlaw.org/wp-content/uploads/2015/10/Bitcoin-An-Innovative-Alternative-Digital-Currency.pdf>>. Acesso em: 18 jul.2016.

HE, Dong. et al. **Virtual currencies and beyond: Initial considerations**. IMF Staff Discussion Note No.16/03, [S.l.], 2016. Disponível em: <<http://www.imf.org/external/pubs/cat/longres.aspx?sk=43618>>. Acesso em: 18 jul.2016.

KRUGMAN, Paul R.; OBSTFELD, Maurice. **International economics: theory and policy**. Boston, 2003. p. 357-359. Disponível em: <www.course.sdu.edu.cn/G2S/eWebEditor/uploadfile/20120417191243_590081573385.pdf>. Acesso em: 18 jul.2016.

LO, Stephanie; WANG, Christina. **Bitcoin as money?**. Federal Reserve Bank of Boston Current Policy Perspectives No. 14-4, [Boston], 2014. Disponível em: <www.bostonfed.org/economic/current-policy-perspectives/2014/cpp1404.pdf>. Acesso em: 18 jul.2016.

MENGER, Carl(1892). **On the Origins of Money**. Tradução de C.A. Foley, Auburn: Ludwig von Mises Institute, 2009.

NAKAMOTO, Satoshi. **Bitcoin: A peer-to-peer electronic cash system**. [S.l.], 2008. Disponível em: <www.bitcoin.org/bitcoin.pdf>. Acesso em: 18 jul.2016.

POLASIK, Michal. et al. **Price Fluctuations and the Use of Bitcoin: An Empirical Inquiry**. [S.l], 2014. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2516754>. Acesso em: 18 jul.2016.

ULRICH, Fernando. **Bitcoin: a moeda na era digital**. São Paulo: Instituto Ludwig von Mises Brasil, 2014. Disponível em: <http://www.mises.org.br/files/literature/MisesBrasil_BITCOIN_BROCHURA.pdf>. Acesso em: 18 jul.2016.

WALLACE, Benjamin. **The rise and fall of Bitcoin**. WIRED.[S.l], 2011. Disponível em: <www.wired.com/2011/11/mf_bitcoin>. Acesso em: 18 jul.2016.

YEAGER, Leland. Unit of Account or Medium of Exchange?. **BNL Quarterly Review**, [S.l] v. 60, n. 241, p. 195-205, 2007. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2065311> Acesso em: 30 ago.2016

YERMACK, David. **Is bitcoin a real currency? An economic appraisal**. NBER Working Paper No.19747, Cambridge, 2013. Disponível em: <www.nber.org/papers/w19747.pdf>. Acesso em: 18 jul.2016.