Aspectos inovativos do Bitcoin, microestrutura de mercado e volatilidade de retornos

Bruno Ferreira Frascaroli[1]
Thiago Carvalho Pinto[2]

Resumo: A presente pesquisa buscou analisar aspectos conceituais, inovativos, mercadológicos e quantitativos do Bitcoin (BTC) e como os mesmos se traduzem na volatilidade dos seus retornos. Após expostos conceitos basilares sobre o BTC, moeda e moedas digitais buscou-se contextualizar o BTC como inovação financeira. Foi usada como amostra os retornos das cotações do BTC/US$, do período de 13 de setembro de 2011 a 23 de junho de 2015 e, como subamostra, o período a partir de 10 de março de 2013 a 23 de junho de 2015. A partir desses conjuntos de informações, estimou-se a volatilidade associada aos retornos no BTC fornecidos pelos modelos ARCH, GARCH, EGARCH e TARCH para testar qual deles se ajustaram melhor a esta trajetória. Os resultados apontaram existência de volatilidade persistente e que mostra, possivelmente, que esses retornos tiveram duas fases: primeiramente um momento de 'euforia' e depois de 'convergência' para a média da volatilidade.

Palavras-Chave: Bitcoin; Inovação; M2L; Volatilidade; GARCH.

Abstract: The present essay studied the conceptual, innovative, market-oriented and qualitative aspects of Bitcoin (BTC) and how these aspects are presented on volatility of its returns. After presented aspects of BTC, currencies and digital currencies, we tried to understand the BTC as a financial innovation. It was used as sample the returns of BTC/US$, in the period between September, 13th of 2011 and June, 23th of 2015 and for subsample the period from March, 10th of 2013 to June, 23th of 2015. From this data sample, we estimate the volatility associated to BTC returns obtained by models of ARCH, GARCH, EGARCH and TARCH to test the better fit to the data. The results pointed to the existence of a persistent volatility which possible shows that the returns of the currency had two distinguish stages: firstly a period of 'euphoria' and after it, a period of ''convergence' to average of volatility.

Keywords: Bitcoin; Innovation; 2SM; Volatility; GARCH.

Código JEL: E51; G23; C58.

[1] Professor do Departamento de Economia da Universidade Federal da Paraíba, Cidade Universitária - João Pessoa – PB, CEP: 58051-900, frascaroli.b@gmail.com.

[2] Mestre em Economia pela Universidade Federal da Paraíba, thiagao.cp@gmail.com.

1. Introdução

É imprescindível um sistema de preços estável que possibilite o cumprimento de contratos a emissão de títulos (privados ou públicos) e mesmo a existência e o funcionamento do mercado financeiro. Neste sentido, as tarefas de regulação do sistema financeiro, emissão e manutenção do poder aquisitivo da moeda são tradicionalmente atribuídas ao Estado. Assim, políticas monetárias afetam o bem estar social ao alterar o poder fiduciário da moeda.

Contudo, o processo de globalização possibilitou a abertura de novos mercados, o fortalecimento de laços comerciais e a criação de zonas de influência. Novos produtos e mercados surgem com grande velocidade. Mercados mais interligados podem tornar o ambiente mais sensível a oscilações. Argumenta-se que crises financeiras apresentam crescente capacidade de contágio e a interdependência comercial entre países é fator preocupante. Por isso, defendem uma maior regulação desses mercados, com a criação de leis e organismos governamentais a fim de incutir disciplina ao sistema financeiro.

A ação dos governos pode comprometer a desejabilidade da moeda. Participação em conflitos, políticas de substituição de importações, regime de câmbio fixo, planos de resgate econômicos e a senhoriagem, são exemplos de estratégias que implicam ao menos momentaneamente, e independentemente do êxito, em algum grau de depreciação da moeda de modo a afetar o sistema de preços.

Os meios de troca refletem o nível de organização social e tecnológico. Por exemplo, o escambo já foi a principal forma de aquisição pacífica de bens e serviços, mas a dinâmica social foi gradativamente transformada por eventos e processos socioeconômicos, culturais e tecnológicos, de forma que com o decorrer do tempo a utilização de moedas dominou as demais formas e se tornou padrão. Cartões de crédito e débito representaram novo avanço técnico ao proporcionar facilidade, segurança e possibilitar alteração do comportamento de consumo. A proliferação de meios de pagamento digitais, como por exemplo, Pay pal, Google Wallet e MoneyGram conhecidos como *eWallets* facilitaram ainda mais as transações no comércio eletrônico.

As moedas digitais representam meios eletrônicos de troca com todas as funções e características das moedas tradicionais, exceto pelo fato de não serem fisicamente tangíveis. Algumas das características são ainda mais evidentes em moedas digitais que nas moedas físicas, tais como a homogeneidade, divisibilidade, transferibilidade e facilidade de manuseio e transporte.

Dentre as diversas moedas digitais existentes, o Bitcoin (BTC) é a que apresenta a maior liquidez e volume negociado diariamente nos mercados financeiros. Além disso, por ser a primeira moeda digital emitida, sua série de preços cotados possui maior número de observações e os movimentos da série refletem não apenas aspectos quantitativos, mas também adaptações sociais. O BTC é uma moeda criptografada[3], não centralizada, não regulada por legislação específica e de curso não forçado.

Apresentadas algumas das características sobre o tema abordado, este trabalho tem por objetivo geral estimar os padrões de volatilidade dos retornos da série de BTC/US$ levando em consideração fatores microeconômicos e macroeconômicos. Para tanto, contextualizou-se o BTC segundo conceitos e características de padrões monetários, de inovações financeiras e no âmbito microeconômico, usando a estrutura teórica dos Mercados de Dois Lados (M2L), de forma a identificar similitudes e diferenças com o sistema de crédito e débito tradicional.

Logo após, baseando-se na Hipótese de Eficiência de Mercados (HME), que postula que todas as informações necessárias para negociação do BTC já estão refletidas nas suas cotações, foram estimados modelos da família GARCH para mensurar a volatilidade associada aos eventos no âmbito global e intrínsecos ao mercado, como os ataques

[3] Criptografia é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário (detentor da "chave secreta"), o que a torna difícil de ser lida por alguém não autorizado. Assim sendo, só o receptor da mensagem pode ler a informação com facilidade.

hackers às bolsas que negociam esse ativo, ou pedidos de falências como o da Mt Gox, por exemplo. Os referidos modelos, amplamente utilizados para esse propósito, são indicados para lidar com processos históricos de natureza heteroscedástica. Com isso, foi possível observar qual o modelo se ajustou melhor à natureza do processo, o que forneceu informações empíricas de como é o processo de formação de clusters de volatilidade associadas às cotações do BTC.

Este trabalho encontra-se disposto da seguinte forma: além desta breve introdução, a seção 2 apresenta conceitos básicos sobre moeda, inovações financeiras e moedas digitais. Na seção 3 são apresentadas as características do BTC. A seção 4 expõe a estrutura teórica do Mercado de Dois Lados e aponta similitudes e diferenças entre o mercado de cartões de pagamentos e o de BTC. A seção 5 apresenta os procedimentos metodológicos. O planejamento amostral é descrito na seção 6. A análise dos resultados obtidos, por sua vez, é descrita na seção 7 e, por fim, as considerações finais seguem na seção 8.

2. Moeda

2.1. Funções e características

O surgimento das moedas se deu de forma espontânea. Em termos evolutivos, a viabilização de meios de troca intermediários se deu segundo a sua capacidade de liquidez. Posteriormente outras características se tornaram importantes, como a portabilidade, e, para além dessas características, a moeda possui funções. Entre elas, a função de *unidade de conta* é imprescindível para a realização de comparação, planejamento financeiro de famílias e empreendimentos.

A função de *meio de troca* permite incremento da atividade econômica, facilitando a produção, a aquisição e a distribuição de bens e serviços. A função de reserva de valor não é exclusiva da moeda, mas intrínseca a qualquer ativo financeiro. A diferença da moeda para os demais ativos é que a primeira é considerada de maior liquidez. Moedas, além das funções mencionadas, apresentam as seguintes características: *divisibilidade, facilidade de manuseio e transporte, homogeneidade, indestrutibilidade, inalterabilidade e transferibilidade*. É de importância fundamental a percepção de que tanto funções quanto as características da moeda são atendidas pelas moedas digitais.

As características da moeda não são relevantes para a função de reserva de valor. Reserva de valor trata-se de uma percepção individual baseada na suposição de que os demais indivíduos da coletividade apreciam de modo idêntico ou muito próximo o mesmo ativo. De modo semelhante, as funções de poder liberatório, *instrumento de poder e pagamento* diferido podem ser entendidas como gradações da percepção da função reserva de valor. Se entendido dessa forma as moedas digitais criptografadas, e em especial o BTC, são moedas *stricto sensu*.

Ressalta-se que o BTC apresenta todas as três funções elencadas, e também as características desejáveis. No entanto, as funções oriundas da percepção de reserva de valor somente são percebidas de forma inequívoca por seus utilizadores. Diferentemente das moedas de curso forçado, em que o estado incute por meio de leis regulamentos e eventuais punições a percepção de valor, nas moedas de curso não forçado ocorre o inverso. Primeiramente o indivíduo é convencido do valor intrínseco ou apenas fiduciário da moeda e somente posteriormente a adota. Dessa forma, sempre que o indivíduo opta por utilizar certa moeda digital verifica-se a clara manifestação de preferência enquanto que o contrário não é verdadeiro. A tabela a seguir compara as funções e características da moeda entre o BTC e moedas de curso forçado.

Tabela 1. Funções e características da moeda e do BTC

FUNÇÕES E CARACTERISTICAS	MOEDAS TRADICIONAIS	BTC
RESERVA DE VALOR	DEPENDE DE REFERENCIAL LOCAL E TEMPORAL	DEPENDE DE REFERENCIAL LOCAL E TEMPORAL
PODER LIBERATÓRIO	PERCEBIDO COMO MELHOR	PERCEBIDO COMO PIOR
INSTRUMENTO DE PODER	PERCEBIDO COMO MELHOR	PERCEBIDO COMO PIOR
PAGAMENTOS DIFERIDOS	PERCEBIDO COMO MELHOR	PERCEBIDO COMO PIOR
UNIDADE DE CONTA	PIOR	TECNICAMENTE MELHOR
MEIO DE TROCA	PIOR	TECNICAMENTE MELHOR
DIVISIBILIDADE	LIMITADA	TECNICAMENTE ILIMITADA
FACILIDADE DE MANUSEIO E TRANSPORTE	PIOR	MELHOR
HOMOGENEIDADE	PIOR	MELHOR
INDESTRUTIBILIDADE	DEPENDE DE REFERENCIAL LOCAL E TEMPORAL	DEPENDE DE REFERENCIAL LOCAL E TEMPORAL
INALTERABILIDADE E TRANSFERIBILIDADE	PIOR	MELHOR

Fonte: Elaboração própria.

O BTC tem se mostrado volátil e esta característica representa elevado custo de carregamento, o que compromete a percepção de ativo com característica de reserva de valor. Em contrapartida, moedas de curso forçado, por depender da conjuntura político-econômica, podem perder parcial ou completamente suas funções, de modo que a reserva de valor é, em última análise, relativa e mesmo subjetiva.

Quanto ao poder *liberatório*, instrumento de poder e pagamentos diferidos, claramente as moedas tradicionais são majoritariamente percebidas como melhor em relação ao BTC, isso ocorre porque há a percepção de um sistema legal de direitos e deveres e um sistema de crédito já estabelecido. A necessidade de assunção de todos os riscos por parte dos usuários de moedas digitais representa desestímulo ao uso, quanto maiores forem os valores transacionados. Isto implica considerável limitação quando comparado ao sistema tradicional.

Quanto à *unidade de conta, meio de troca e divisibilidade*, o BTC é tecnicamente superior pelas características atuais e possíveis. Quanto ao *manuseio e transporte*, o BTC torna possível a portabilidade e a movimentação de grandes valores, não implicando em custos extraordinários. Além disso, também não se faz necessária a reposição de cédulas desgastadas pelo tempo. Por ser digital, o primeiro é perfeitamente homogêneo e enquanto o código for seguro é indestrutível. O mesmo se verifica ao analisar os atributos de *inalterabilidade e transferibilidade.*

2.2. Inovações financeiras e moedas digitais

Inovações financeiras radicais possibilitam estender o gerenciamento de risco para além dos limites anteriores, abrangendo novas classes de riscos, modificando os pressupostos sobre seguros financeiros, estratégias de *hedge* e de diversificação. O mesmo processo de difusão propiciado por inovações em outros setores também é observado nos processos de inovação financeira. Schiller (2007, p. 306) argumenta que os processos de inovação financeira são contínuos e seguem tendência de difusão. O autor aponta o papel da tecnologia da informação, compreensão do comportamento e psicologia aplicada às finanças como determinantes da difusão.

Entende-se que um *risk sharing* pleno, em que existem mercados para cada preço, risco e para cada estado da natureza, inexistem na realidade, deixando espaço para mercados incompletos. Assim, problemas como assimetria de informação e suas manifestações na forma de *seleção adversa* e *risco moral,* associados ao gerenciamento

de riscos implicam em custos de transação, que podem ser reduzidos. Wonglimpiyarat (2011) obteve resultados que indicam que as inovações financeiras afetam o desempenho econômico, ao promover atividades empresariais. Trata-se de um importante setor do sistema de inovação que pode ser visto como elo de financiamento para a inovação.

O surgimento de moedas digitais, por exemplo, representa a possibilidade de desvinculação entre o sistema financeiro e objetivos políticos. Desse modo, permite autonomia ao usuário que pode evitar moedas que apresentem elevado potencial de perda de valor. As externalidades de rede são também relevantes para a maior adoção de moedas criptografadas por parte de usuários, pois constituem um tipo especial de externalidades na qual o grau de utilidade auferido por um indivíduo depende da quantidade de usuários do mesmo bem. Quando a disponibilidade a pagar dos indivíduos supera os custos, o mercado se expande e, dado que ao menos dois equilíbrios são possíveis em mercados que apresentam externalidades de rede, verifica-se a tendência de que o mercado atinja um equilíbrio com grande número de agentes.

Segundo Dosi (1988) mercados com características de externalidade de rede os produtores podem inicialmente causar perturbação com promoções, discriminação de preços e outras estratégias para atrair usuários para a rede. No caso das moedas digitais, ao menos três fatores podem ser determinantes possibilitar a atratividade da rede: a confiabilidade, a possibilidade de ganhos e a manutenção de uma taxa de entrantes até a formação de uma massa crítica, que é dada por um volume de usuários que ao ser atingido torna a rede atraente aos não participantes pela própria existência da rede.

Há atualmente um crescente número de moedas digitais além do BTC, cada uma delas privilegia certos aspectos que seus idealizadores entendem como mais desejáveis. Entre as mais populares destacam-se:

- *Litecoin* – Que em tudo se assemelha ao BTC, mas a emissão esta condicionada a 84 milhões de unidades monetárias e a dificuldade de mineração representa algo próximo à quarta parte o que possibilita o uso de equipamentos mais simples. O apelo inicial desta moeda estava na facilidade relativa de mineração. Vale destacar que o algoritmo de mineração é diverso do BTC;
- *Dogecoin* – Possui emissão ilimitada com o claro objetivo de evitar se tornar uma moeda com tendência deflacionária e também facilitar a eventual formação de um mercado de crédito;
- *PPcoin* – Apresenta oferta de moeda não determinística e possui vantagens com relação ao modulo de segurança. A recompensa a cada bloco minerado depende da dificuldade de mineração, com um novo bloco emitido a cada dez minutos;
- *Dash* (denominada antes como *Darkcoin*) – Objetiva tornar anônimas as transações ao implementar maior dificuldade de rastreabilidade por meio de transações fictícias.

Também a tecnologia dos protocolos nos quais se baseiam as moedas digitais aplicadas aos mercados financeiros é capaz de causar uma série de inovações marginais, possibilitando produtos mais seguros, ágeis e customizados, transformando gradualmente a estrutura corrente.

Desta forma, conforme Christensen e Raynor (2003) produtos que apresentam inovações disruptivas possuem preço menor e qualidades específicas não atendidas pelo mercado já estabelecido. Com o tempo e melhorias subsequentes acabam por substituir o antigo mercado dominante. São definidos três tipos de Inovação Disruptiva (ID): a chamada *Low Disruption* – Christensen e Raynor (2003); a do tipo *New Market Disruption* – Christensen e Raynor (2003); e a *High Disruption* – Govindarajan e Kopalle (2006).

A ID do tipo *low disruption* surgem em produtos mais baratos e, por vezes,

"incompletos" quando comparados aos produtos tradicionais. Mas, as inovações incrementais são incorporadas com o tempo e este produto torna-se o padrão por atender também aos clientes mais exigentes. Por outro lado, a ID *new market disruption* não competem com a indústria estabelecida, ao contrário, cria um novo mercado antes inexistente. Os produtos são mais simples, baratos e inicialmente relativamente inferiores de forma a capturar potenciais clientes que não participavam do mercado em razão de restrição orçamentária. Neste sentido, constitui de fato um novo mercado. Conforme Christensen e Raynor (2003) as estruturas inovativas *low disruption* e *new market disruption* podem coexistir quando ao mesmo tempo competem por preço e criam novos mercados.

Por fim a ID *high disruption* ocorrem por meio da vinculação de maior qualidade em características específicas do produto. Inicialmente o produto é mais oneroso e capta clientes que apresentam menor elasticidade-preço. Em comum todas as ID's acabam por substituir o mercado dominante, mas inicialmente atendem a uma pequena parcela de clientes ou potenciais clientes.

O BTC não apresenta características de *high disrupition*, mas que em qualquer dos três tipos de ID, inicialmente os produtos apresentam qualidade inferior com relação aos produtos *mainstream*. Dessa forma, inicialmente os mercados inovadores buscariam atender a nichos específicos e gradativamente ocorreria uma massificação do produto inovador. Salienta-se que a inserção do produto inovador está relacionada negativamente com o custo de produção.

3. Bitcoin

Desenvolvido por Satoshi Nakamoto (2008), possivelmente um pseudônimo utilizado por programadores, e implantado em 3 de janeiro de 2009, o BTC é a moeda digital criptografada mais popular. Conforme Nakamoto (2008) a utilização de rede P2P[4] possibilita operações sem a necessidade estrita de terceiros, as operações são registradas cronologicamente e as informações permanecem disponíveis.

A arquitetura P2P é a mesma utilizada em serviços de troca de arquivos em serviços como o antigo *Kazaa* e os atuais *Torrents*. Redes P2P permitem a transmissão de dados sem necessidade de um servidor central e apresentam capacidade de auto-organização tolerante a falhas. Os BTCs são validados por meio de algoritmos. Uma função *hash* é capaz de mapear dados de comprimento variável e retornar dados de comprimento fixo. Conforme Paar e Pelzl (2009) o hash é um conceito largamente utilizado. Trata-se de um identificador único de dados e necessariamente deve apresentar função unidirecional – sendo o hash produto da entrada de dados, não é possível obter os dados originários por meio do mesmo.

Cada um dos usuários do BTC possui duas "chaves", sendo uma delas pública e outra privada. A chave pública identifica o usuário na rede e utiliza um algoritmo de assinatura digital, denominado ECDSA[5] . Cada usuário pode possuir quantas chaves públicas desejar. A cada transação os usuários envolvidos precisam informar suas respectivas chaves públicas e estas podem ser checadas por quaisquer usuários da rede.

A emissão de BTC é limitada em 21 milhões e a taxa de emissão é decrescente ao longo do tempo. Taylor (2013) apontava que 58,8% da totalidade dos mesmos já havia sido emitida até 2013 e até 2032 a taxa será de 99%. Atualmente conforme gráfico abaixo, já foram minerados aproximadamente 14.357.900,00 BTCs. A transparência do sistema constitui fator capaz de agregar popularidade ao BTC. A qualquer tempo, é possível verificar as quantidades transacionadas, no entanto, não é possível acesso à identificação direta dos envolvidos nas transações.

[4] Redes do tipo P2P são popularmente conhecidas por facilitar troca de arquivos utilizando-se de *torrents,* neste sistema cada máquina funciona como servidor e usuário simultaneamente.

[5] Para detalhes sobre o protocolo de curva elíptica (ECDSA) ver: GOLDFEDER, Steven et al. (2014). No entanto, tal nível de especificidade foge ao escopo do trabalho.

A emissão inicial do BTC ao valor simbólico de US$ 0,01 foi entendida como sinalizadora de respeito irrestrito ao mercado, pois concede o poder completo para que os usuários lhe atribuam valor em razão das forças de oferta e demanda. Pode também ser encarada como estratégia de preço promocional, pois os dois entendimentos não são conflitantes. Preços iniciais promocionais, estratégias de divulgação e manutenção de uma taxa de crescimento da rede são estratégias frequentemente adotadas por empresas que atuam num mercado que apresenta externalidade de redes, como por exemplo, o mercado de softwares.

Ao se considerar o preço inicial de emissão e a menor dificuldade inicial de mineração, verificam-se estratégias similares àquelas adotadas por empresas que dependem da formação de uma rede para a maior penetração de seus produtos. Por ser um "produto" de potencial valor futuro, cada vez mais usuários são atraídos pela possibilidade de ganho formam a rede inicial, após divulgação nos meios de comunicação e a manutenção de uma taxa de crescimento da rede a apreciação ocorre, estes movimentos são realimentados até a formação de uma massa crítica com a qual se dá a consolidação do mercado.

Outra característica do BTC é a *irreversibilidade*, ou seja, os negociadores assumem todo o risco, se aproximando ainda mais de uma transação monetária tradicional. Os registros das transferências são mantidos permanentemente e, conforme Taylor (2013), estes registros podem comprometer o anonimato, mesmo para usuários que utilizam variadas contas, pois análise minuciosa pode evidenciar um mesmo operador com relativo grau de certeza.

A possibilidade da verificação dos registros das transações disponibilizados por alguns comerciantes, a fim de sinalizar credibilidade ao mercado também pode comprometer o sigilo dos usuários do BTC. Contudo, há serviços disponíveis que objetivam tornar menos claras tais evidências, utilizando-se de instrumentos de transmissão condicionada a futura devolução, mas envolvendo um número considerável de contas, funciona como um embaralhador virtual.

O BTC é muito utilizado como ativo financeiro, capaz de gerar retornos especulativos, mas também pode ser útil como instrumento capaz de tornar menos onerosas operações de câmbio. Mesmo com a popularização, verifica-se relativa relutância por parte de diversas redes comerciais em utilizá-lo, pois a maioria dos governos proíbe a livre circulação de outras moedas. Rússia e China já sinalizaram que têm intenção de proibir o uso de moedas digitais. Singapura Taiwan e EUA demonstram preocupação com atividades ilegais e defesa da moeda nacional. Além disso, os EUA, Japão, Alemanha e Finlândia criaram instrumentos para instituir a tributação.

May (1994) expôs os esforços dos governos em limitar o acesso de suas respectivas populações às ferramentas de criptografia e os efeitos adversos que esta tentativa causou, por exemplo, na França, nas Filipinas e nos EUA. Em suas conclusões, o estudo ressaltou a possibilidade de evasão fiscal, o que pode comprometer sensivelmente a capacidade de arrecadação por parte dos governos. O possível uso do BTC como salvaguarda de um mercado turbulento, como o observado por conta da crise financeira de 2008, a política adotada inundou o mercado de liquidez e expôs os efeitos adversos de uma politica expansionista, dentre estes aceleração inflacionária.

Esta moeda eletrônica pode vir a representar papel semelhante ao do ouro, posto que de antemão, a taxa de emissão é conhecida e inferior as de moedas tradicionais. Nesse caso, a valorização da moeda eletrônica frente outras moedas, muito provável mesmo em momentos não turbulentos, depende dos agentes aceitarem esse tipo de moeda.

Há basicamente três maneiras de se adquirir BTCs. A maneira mais comum no início das emissões era o processo de *mineração*. Não existia ainda um mercado estabelecido. Nakamoto (2009) justifica o termo mineração por analogia à atividade de garimpo

de ouro. No caso desta moeda, tal esforço é representado por maior dificuldade computacional e gastos com energia elétrica.

O BTC é minerado em blocos. O primeiro bloco minerado ficou conhecido pelo nome de *Genesis block* e gerou cinquenta BTCs. Vale destacar que cada hash é composto por 64 caracteres, além disso, cada bloco minerado informa o hash do bloco seguinte. O sucesso da mineração gera um registro na *blockchain*, que é um arquivo que registra todas as transações efetuadas em BTC. Cada BTC encontrado por um *minerador* deve ser validado por outros usuários de forma sistêmica e algorítmica.

A popularização da moeda, o maior número de mineradores e o crescente poder computacional exigido têm tornado menos interessante a mineração, e os usuários, na prática, atuam em grupos denominados *pools*, repartindo os ganhos entre o grupo conforme esforços individuais. Na realidade, exploradores com pouco poder computacional são compelidos a atuar em grupo para obter algum retorno. Quanto maior o poder de processamento, maior a probabilidade de sucesso de certo grupo de mineradores. O grau de dificuldade é regulado de forma autônoma de modo que seja possível manter a taxa de emissão decrescente relativamente constante.

A dinâmica temporal desenha um futuro com taxas cada vez menores de emissão, o que dificulta ainda mais a atividade de mineração para novos entrantes. É possível que até 2032 existam poucos e eficientes mineradores dado o maior poder computacional exigido e elevados custos de hardware. Nesse sentido, Taylor (2013) afirma que dois fatores são determinantes: o primeiro deles o acesso à energia e o segundo, possuir o hardware utilizado quitado, enquanto os retornos forem elevados.

Caso ocorra entesouramento por parte dos mineradores, os usuários finais podem desenvolver relativa aversão pela moeda. Mesmo considerando a extrema divisibilidade do BTC, os usuários estariam sujeitos a ataques monetários puramente especulativos. Mas, é pouco provável que processos dessa natureza sejam verificados por duas razões: a coordenação de grande parte de mineiros é impraticável e; mineradores têm um ponto de entrada não coincidente. Logo, o preço ótimo entre mineradores difere consideravelmente, mesmo se participarem do mesmo *pool*.

A depender do ponto de entrada, do investimento realizado e dos custos de operação que são individuais, se um grande número de mineradores decidir realizar lucros, muito possivelmente os preços jamais se tornarão inferiores ao custo de mineração, porque no momento em que o preço de mercado se igualar ao custo de mineração, os mineiros que ainda não alcançaram o ponto de saída passariam a adquirir BTC no mercado e manteriam o maquinário minerando.

O processo de mineração possibilita recompensar o minerador e também validar transações. Quando um comprador de bens ou serviços realiza uma ordem de pagamento com BTC a transação não é realizada instantaneamente. A carteira digital do comprador possui uma série de BTCs ou frações que foram previamente geradas por meio de esforço computacional. O objetivo dos mineradores é gerar novos blocos e estes são gerados após a "resolução" de uma função hash.

As transferências monetárias são realizadas através de um hash, que carrega informações das transações anteriores e a chave pública do receptor da quantia. Quando algum minerador decifra o código e este é validado pela rede, o bloco é registrado na *blockchain*, e somente após esse processo os destinatários, vendedor e minerador recebem a quantia devida. Como o bloco contém as informações pretéritas e a chave pública do destinatário, todos os nós da rede podem se certificar de que a quantia que o comprador deseja dispor ainda pertence a ele. Este procedimento elimina a possibilidade de gasto duplo.

A segunda maneira de se obter BTC envolve trocas livres entre usuários. Em geral, este tipo de transação não incorre custo monetário, ou conforme Taylor (2013), o mesmo

é simbólico variando 0,0005 BTC a 1 *Satoshi*, que equivale a 0,00000001 BTC. Cada nó da rede possui uma cópia do blockchain, e dado que a cada transação a chave pública utilizada "assina" um hash, se faz possível a comparação da chave pública do fornecedor, eliminando a possibilidade de duplo gasto. Em outras palavras, caso o fornecedor já não seja possuidor dos BTCs transacionados, o histórico armazenado acusará tal diferença.

A constatação de posse por parte do emissor e a aceitação da transferência por parte do receptor são armazenados no blockchain e torna-se informação disponível e atualizada para cada nó da rede. Ressalta-se a transação será armazenada num novo bloco, portanto, necessária à atuação dos mineradores, pois, as transações não ocorrem de forma instantânea. Esta modalidade envolve os usuários finais de BTCs, comerciantes e consumidores de bens e produtos finais. Para realizar a transmissão de valores, o usuário precisa fazer uso de sua chave privativa.

Esta forma de aquisição, apesar de ser a menos custosa, é a mais arriscada. Aqueles que atuam como compradores de certo bem ou serviço não teriam a quem recorrer em caso de descumprimento de acordo. Na realidade esse é um fator determinante para a capacidade de penetração da moeda, posto que para assumir tal risco o valor do bem ou o serviço adquirido devem ser relativamente baixos. De outra maneira, alguma forma de garantia passa a ser desejada.

A forma de aquisição direta de moedas digitais possibilita o auxílio financeiro a causas e organizações criminosas. Estas possuem possibilidades mínimas de identificação e punição de responsáveis, caso os mesmos se utilizem de estratégias apropriadas de proteção à identidade. Grupos terroristas, paramilitares, cartéis interessados em evasão fiscal, e mesmo acordos tácitos, podem ser explicitados e não percebidos por meio dos instrumentos tradicionais de auditoria.

Em contra partida, auxílio humanitário, doações a pesquisas médicas e combate a excessos praticados por governos que restringem as liberdades individuais podem ser consideravelmente mitigados com o uso de moedas descentralizadas. Apesar disso é importante destacar que quando uma grande empresa decide adotar o BTC passa a gozar de credibilidade solidificada ao longo do tempo de atuação no mercado, tornando a negociação direta consideravelmente mais segura.

A terceira maneira de obter BTC, e atualmente a mais referida nos meios de comunicação, é a comercialização de moeda intermediada. Nesse caso, o usuário obtém moeda diretamente, nas diversas "bolsas" ou "bancos" de BTCs. Meiklejohn et al. (2013) ressalta que no inicio de 2012 dobrou de forma abrupta a porcentagem de transações para valores menores que a unidade monetária e triplicaram àquelas referentes a menos de um décimo da unidade. Não somente a comercialização de quantidades fracionárias torna-se mais popular, como também se observa aumento na velocidade da moeda[6] , que de fato é quantificada e não uma aproximação. Conforme os supracitados autores apenas uma parcela estimada em quatro milhões dos BTCs disponíveis é comercializada com frequência, mas a uma taxa de troca intensa.

A disseminação do BTC não é uniforme e muitos comerciantes evitam adotá-lo, por não haver regras claramente definidas, além de questões tributárias e da elevada volatilidade do preço da moeda. Permanecer por muito tempo com a moeda, pode significar expressivo ganho ou perda para aquele que transaciona respeitando a paridade verificada com sua moeda local no momento da compra. Em outras palavras, aumenta o *carrying cost,* como antes mencionado. Apesar do desejo de parte dos usuários para a legalização e regularização do BTC e de outras moedas digitais, esta iniciativa apresenta caráter destoante do ideal fundamental de não regulação e de assunção da totalidade dos riscos por parte de seus usuários.

As moedas digitais possibilitam oportunidade de crescimento de novos nichos de mercados, também conhecidos como *mercados de cauda longa*. Nestes tipos de

[6] A velocidade da moeda é definida como o número de vezes que o estoque de moeda circula entre os agentes num dado tempo. Vale ressaltar que a fórmula usual para estimar a velocidade da moeda considera a produção como aproximação para o número de transações. No entanto, o uso das moedas digitais, em especial o BTC, permite conhecer o real número de transações, uma vez que cada troca é registrada.

mercados a produção de certos bens e serviços, por vezes, se torna economicamente inviável, por dificuldades em atingir o mercado consumidor disperso geograficamente. Além de outras ferramentas de comércio eletrônico, as moedas digitais podem tornar tais atividades lucrativas, ao fazer menos burocráticos e custosos os processos de troca. O que possibilita o comércio de mercadorias de baixo custo, dado que praticamente inexistem taxas. Conforme White (1999, p.18) a transição monetária de analógica para digital não modifica o padrão fiduciário, nem tampouco a questão bancária.

Ao considerar o futuro das instituições financeiras o relatório do Fórum Econômico Mundial (2015, p.102-108) apresenta três possíveis cenários sobre o futuro papel de instituições financeiras, em resposta às contínuas mudanças nas preferências dos agentes do sistema financeiro internacional. No primeiro cenário, consideram um movimento de desconcentração do mercado, com o surgimento de novos agentes e de produtos financeiros mais flexíveis, intuitivos e personalizados. Nele os agentes atuais evoluem e se especializam, personalizando ao máximo seus respectivos produtos. São riscos apontados por este cenário: possibilidade de que o sistema se torne refém de desenvolvedores de tecnologia, comprometimento da capacidade de fidelização do cliente e incerteza quanto a aspectos reguladores.

O segundo cenário apresentado retrata a possibilidade de que os bancos tradicionais mudem de foco ao atuar como plataformas para conexão com produtos de nicho. Neste caso, também haveria menor grau de fidelização e, além disso, deveria ocorrer maior especialização, diminuindo a possibilidade da existência de subsídios cruzados. Como pontos críticos surgem: a dificuldade de seleção em razão da maior atomicidade, dificuldades de atribuir responsabilidades por falhas no serviço ou fraude, problemas de assimetria de informação e diminuição da lealdade do cliente.

Por fim, no terceiro cenário as instituições financeiras aumentariam os pontos de contato com os clientes por meio da tecnologia, emulando o relacionamento humano e objetivando a retenção e fidelização. Objetiva-se a superação das necessidades com a oferta de serviços não financeiros sem aumento significativo de custos. Sendo assim, é possível que as moedas digitais não centralizadas e não reguladas venham em pouco tempo ser consideradas como uma inovação radical, com características de inovação destruidora. Nesse caso, inovações incrementais poderão surgir, remodelando as formas tradicionais de comércio, tributação e legislação.

Todos os quatro tipos de inovação: comercial, organizacional, tecnológica e as institucionais podem ocorrer em maior ou menor grau a depender do grau de utilização de moedas descentralizadas. A inovação institucional está ligada aos meios considerados legais de atuação. Neste sentido, é imprescindível que o ordenamento jurídico e as instituições reguladoras da sociedade, em todos os aspectos, inclusive econômicos, sejam de fato efetivos e capazes de prover segurança jurídica aos agentes dos diversos tipos de mercados.

Caso o BTC se torne um ativo amplamente aceito como moeda, mas as legislações não acompanhem a sua evolução do ponto de vista do arcabouço legal aplicado aos incentivos econômicos corretos, tende em grande parte a tornar-se uma letra morta. Faz-se referência, neste caso, ao que na prática hoje ocorre em relação às leis de direito autoral e *copyright* na indústria do entretenimento de alguns países. Albuquerque e Callado (2015) reconhecem e exemplificam que a regulação é fraca, mas, a despeito de aspectos regulatórios, a bolsa de Nova York (NYSE) criou no dia 19 de maio de 2015 um índice oficial de conversão para valor em Dólar Americano. Evento que sinaliza que o mercado financeiro tradicional já assimila o mercado de moedas digitais como uma realidade.

4. Mercado de dois lados (M2L)

Esta seção define e caracteriza a teoria conhecida como Mercado de Dois Lados (M2L). Apesar da grande gama de configurações possíveis buscar-se-á comparar a estrutura do setor de cartões de pagamentos eletrônicos com a estrutura ainda em formação de um mercado de BTCs. Serão apontadas similitudes e diferenças fundamentais que impedem a total conformação do mercado de BTCs com a estrutura M2L.

4.1. Características gerais de mercado de dois lados

Modelos que descrevem o M2L possuem duas características: a existência de dois grupos distintos de participantes e a presença de externalidades positivas de rede. Essa estrutura se baseia numa plataforma que possibilita o encontro e a interação de dois tipos de usuários e deve ser capaz de propiciar que os grupos realizem o maior número de transações possíveis. A plataforma deve ser estruturada de modo a promover a percepção de vantagem de utilização por parte dos usuários finais.

Rochet e Tirole (2006) esclarecem que o M2L não se caracteriza apenas por conta da existência de uma plataforma que conecta dois usuários finais, mas sim o fato de que o volume total das transações depende principalmente da estrutura de preços, ou seja, como o preço é dividido entre os usuários finais. De acordo com Freitas (2007) no M2L a estrutura de preços e a definição de quem assumirá a maior parte dos custos da plataforma devem ser "desenhadas", de tal modo que incentive a participação dos dois lados do mercado. Disso resulta que o preço pago por determinado participante para fazer uso da plataforma não está necessariamente relacionado ao custo de sua entrada no sistema.

Evans e Schmalensee (2005) citam alguns mercados que, por sua natureza e características, estão organizados como M2L, tais como agências de encontro de casais, clubes noturnos, corretoras, agências de propaganda, jornais e revistas, sistemas operacionais de computadores, vídeo games, *shopping centers* e cartões de pagamento. Conforme os autores verificam-se três características fundamentais neste tipo de estrutura: a de preços diferenciada, os modelos de desenho do negócio e a existência de regras e regulamentos específicos.

Conforme Evans (2003) os preços finais são cobrados dos usuários finais, consumidores e comerciantes, a fim de se obter o equilíbrio das demandas. É importante não apenas manter, mas também atrair novos entrantes dos dois conjuntos de usuários na rede. O elemento-chave desse mercado, portanto, é o balanceamento das demandas dos usuários finais. As elasticidades-preço da demanda de cada de cada grupo exercem papel fundamental na determinação dos respectivos preços carregados por cada um deles. O lado mais elástico tende a ter seu preço reduzido, de forma a viabilizar a entrada de usuários deste lado da rede. Em geral, o lado com menor elasticidade tende a arcar com a maior parte dos custos da indústria.

O desenho do negócio é crucial na análise do M2L, devido não só à presença de externalidades de rede e das elasticidades-preço da demanda como também à necessidade de integração dos dois lados do mercado. Já a existência de regras e regulamentos específicos impostos pela plataforma faz-se necessária em razão da necessidade de construção de parâmetros que promovam as externalidades positivas e limitem as negativas, com vistas a produzir benefícios para os usuários finais (BANCO CENTRAL DO BRASIL; SECRETARIA DE ACOMPANHAMENTO ECONÔMICO; SECRETARIA DE DIREITO ECONÔMICO, 2010).

A estrutura de apreçamento deve promover estímulos para, pelo menos, um dos

lados, sem que isso resulte em uma punição muito severa ao outro, desestimulando sua participação. Este processo de fixação de preços em mercados de dois lados não reflete apenas a estrutura de custos dos participantes da indústria, mas também o excedente gerado para um dos grupos quando o mercado incorpora um usuário a mais no outro (ROCHET e TIROLE, 2002; 2003). Isto quer dizer que, na estrutura de apreçamento de um M2L, se todas as outras condições permanecerem constantes, o grupo que tiver obtido o maior excedente *subsidiará* o outro grupo. O lado que arca com os custos é chamado centro de lucro, o lado beneficiado é chamado de centro de perda.

4.2. Características do mercado de cartões

Na análise da estrutura de preços desse mercado duas características devem ser observadas. A primeira é a soma dos preços provenientes da estrutura de dois lados e a segunda é a repartição desses preços entre usuários finais de cada um dos lados. Os preços de cada lado do mercado dependem não só de seu custo marginal, mas da elasticidade-preço da demanda de cada lado do mercado, do valor que a entrada de um agente em um dos lados gera para aqueles participantes do outro lado (externalidade de rede), e do grau de competição interplataformas e intraplataformas (BANCO CENTRAL DO BRASIL; SECRETARIA DE ACOMPANHAMENTO ECONÔMICO; SECRETARIA DE DIREITO ECONÔMICO, 2010).

Fagundes, Ferrés e Saito (2009)[7] explicam que as externalidades de uso se verificam com aumentos das receitas por conta da difusão da ferramenta. A internalização de externalidades positivas para o comércio e consumidores pode ampliar o volume de transações e consequentemente ampliar as receitas, se o ônus da utilização for arcado majoritariamente pelo agente que apresenta menor elasticidade.

No caso tradicional da estrutura desse tipo de mercado, a tentativa de tornar o mercado mais competitivo com base em regulamentações apoiadas em estudos técnicos fortemente baseados na teoria microeconômica, que consideram a convergência de preços para patamar próximo aos respectivos custos marginais, poderia eliminar a característica de externalidade de rede e produzir efeitos outros de maior magnitude que o excedente gerado pelo corpo regulatório. Por exemplo, um nível maior de concorrência pode apenas ocasionar menor lucratividade para o proprietário do esquema. Entretanto, a literatura[8] aponta que estímulos à concorrência podem promover benefícios, quando um mesmo usuário tem acesso a diversos cartões indistintamente aceitos por parte dos comerciantes.

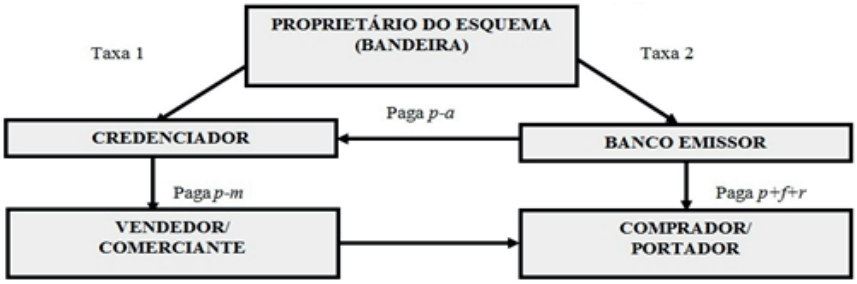
Poder-se-ia argumentar que independente das distintas elasticidades entre usuários finais, o custo poderia ser repassado em parte ou integralmente dos vendedores para os consumidores. Ou seja, por apresentar diferentes custos para diversas modalidades de pagamentos, se os comerciantes viessem a diferenciar e repassar aos clientes tais custos, mas existam cláusulas impeditivas impostas aos grupos de comerciantes, pode dificultar a diferenciação de preços. No entanto, a impossibilidade de diferenciá-los pode ocasionar subsídio cruzado punindo os usuários que optam pela forma de pagamento menos custosa.

Frequentemente, o mercado de cartões é estruturado sob uma plataforma contendo três ou quatro partes. Na plataforma de três partes o credenciador é também emissor do plástico. Na plataforma de quatro partes estes agentes não coincidem. A Figura 1 a seguir retrata uma plataforma de quatro partes:

[7] Os autores têm como escopo o mercado de cartões de crédito, mas raciocínio análogo aplica-se ao objeto do presente estudo, os BTCs.

[8] Ver mais sobre em Evans (2002), Frascaroli (2010) e Rochet e Tirole (2003).

Figura 1. Organização do mercado de cartões de pagamentos



Fonte: Frascaroli (2010).

onde *p* é o preço do bem ou serviço; *f* é a tarifa ao portador do cartão de pagamento, geralmente uma anuidade; *r* é a taxa de juros; *a* é a tarifa de intercâmbio; *m* é taxa de desconto.

Resumidamente, o mercado funciona da seguinte forma: o proprietário do esquema (bandeira do cartão) define a regras do negócio; os emissores são geralmente bancos que mantem contato direto com portadores de cartões definem: limites de crédito, encargos e taxas, vencimentos de fatura, programas de benefícios, etc; o credenciador, por sua vez, realiza a ponte entre estabelecimentos comerciais e proprietário de esquema por meio de contrato; o consumidor, do outro lado, é o portador de cartão; o vendedor é o agente que aceita o cartão como meio de pagamento; e os preços finais são compartilhados entre usuários finais, consumidores e vendedores, de modo a equilibrar as demandas dos dois lados.

5. Procedimentos metodológicos

Esta seção apresenta de maneira introdutória a estratégia empírica deste estudo. Conforme já mencionado, a presente pesquisa se dedicou a estimar a volatilidade associada aos retornos do BTC usando modelos GARCH. Mais precisamente, as estimações dos modelos da família GARCH tiveram como objetivo mensurar as mudanças nas volatilidades associadas aos eventos no âmbito global e intrínsecos ao mercado, como os ataques hackers às bolsas que negociam esse ativo, ou pedidos de falências como o da Mt Gox. Foram testados vários modelos a fim de testar qual deles representa melhor a trajetória da volatilidade do BTC.

O trabalho seminal de Engle (1982) introduziu a possibilidade de estimar modelos de *Hetorecedasticidade Condicional Autorregressiva* (ARCH). O modelo *Generalized Autoregressive Conditional Heteroscedaticity* (GARCH) formulado por Bollerslev (1986) é uma generalização do modelo ARCH. Ele permite a utilização de apenas dois parâmetros para captar simultaneamente a média e a variância de uma série temporal de um processo ARMA.

O modelo GARCH assume que os mercados são eficientes e que os retornos seguem processos estocásticos. No entanto, este modelo apresenta algumas limitações e uma delas refere-se aos impactos de choques (negativos e positivos) na volatilidade, que são considerados simétricos, conforme já mencionado.

Assim, tentando resolver esta limitação, Nelson (1991) propôs o modelo Exponential Generalized Autoregressive Conditional Heteroscedasticity (EGARCH), que consiste em captar os impactos assimétricos nas séries de dados, além da não concessão de coeficientes negativos no modelo. Se esses coeficientes fossem negativos, isto significaria

que a série de dados não seria estacionária.

Por conseguinte, com o propósito de capturar o efeito alavancagem e parte da hipótese de que informações negativas e positivas provocam impactos diferentes sobre a volatilidade, Zakoian (1994) desenvolveu o modelo Threshold Autoregressive Conditional Heteroscedasticity (TARCH). Com a utilização deste modelo é possível captar o efeito alavancagem e também captar o efeito assimétrico tanto pelo sinal do choque quanto pelo tamanho do choque de mercado.

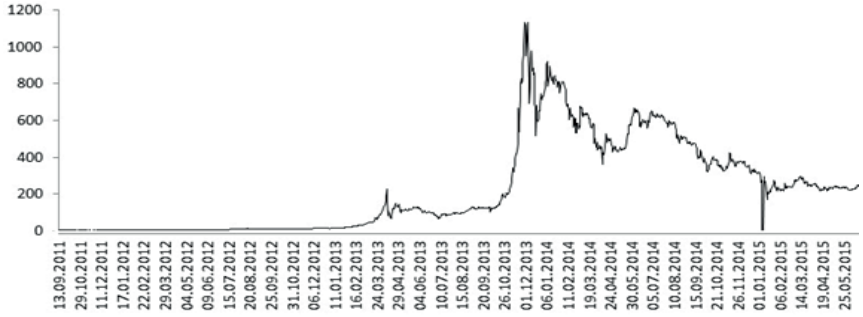
No presente trabalho, conforme já relatado, foi feito um esforço no sentido de ajustar o melhor modelo para estimar a volatilidade associada à série de retornos do BTC, respeitando critérios estatísticos, de parcimônia e aderência das mensurações à cobertura teórica dada. Mais informações sobre esses modelos podem ser consultadas em Tsay (2005).

6. Planejamento amostral

Todos os dados utilizados na pesquisa foram obtidos no sítio *br.investing*. Utilizou-se uma amostra composta de um total de 1.362 observações, e considera o período compreendido entre 13 de setembro de 2011 e 23 de junho de 2015. Além disso, para fins de testar a robustez das estimações, foi construída uma subamostra, que considera apenas os dados a partir de 10 de março de 2013, com 663 observações. Esta última é justificada por eventos e tendências que impactaram na série histórica de preços do BTC, conforme já discutido ao longo do texto.

Um dos instrumentos técnicos para justificar a necessidade de se analisar separadamente as amostras foi a modelagem MS-VAR. A mesma apontou a convergência da série histórica das variáveis considerando dois regimes, sendo que o regime 1 apresenta duração esperada de 75% do período de tempo e o regime 2 apresentou duração esperada de 25%. Ele foi utilizado para definir a janela temporal para a determinação da subamostra, isto é, além dos indícios visuais e históricos, foi estimado o modelo MS-VAR de dois regimes. A Figura 2 a seguir reforça as informações sobre a trajetória analisada:

Figura 2. Evolução da cotação BTC/US$



Fonte: *br.investing*.

Para fins analíticos ao nível microeconômico, recorreu-se aqui à teoria de M2L para explicar um dos possíveis fenômenos associados a essa fase. E uma segunda fase, de 'convergência' aos fundamentos que determinam as cotações da moeda. Esta fase persiste até o fim da série em que picos de mesma magnitude, já não são mais observados.

Em nível a série apresenta características indesejáveis, observa-se uma abissal

amplitude entre o valor máximo de US$ 1.132,01 e o valor mínimo de US$ 2,24. Ao se comparar visualmente os retornos da amostra com os retornos da subamostra, são claras as diferenças de magnitude. Séries denotadas na forma de retorno possibilitam mitigar efeitos persistentes de tendências, no entanto, a análise visual sugere períodos de acentuada volatilidade que possivelmente afetam a variância ao longo do tempo. Por essa análise, modelos da família GARCH são apropriados para uma tentativa de quantificar efeitos de variância condicional.

Nesse trabalho, a hipótese de normalidade foi rejeitada para todas as variáveis em quaisquer das amostras. Além disso, o excesso de curtose apontam séries léptocurticas, comum em séries financeiras de tempo, o que reforça o argumento para a utilização de modelos capazes de mensurar a volatilidade e estudar como elas de correlacionam. As estatísticas descritivas da amostra e subamostra estão dispostas na Tabela 2:

Tabela 2. Estatísticas descritivas da amostra e da subamostra

Variáveis	Média	Mediana	Máximo	Mínimo	Desvio-Padrão	Assimetria	Curtose
BTC Amostra	0,001256	0,000389	0,450252	-0,409647	0,0293	1,245677	89,84125
BTC Subamostra	0,000483	0,000211	0,066043	-0,130503	0,011374	-1,639805	30,0825

Fonte: Elaboração própria.

7. Análise dos resultados

A exposição mostrou a existência de antagonismos limitantes à operação com BTC. Verificou-se que as legislações mais restritivas são oriundas de localidades em que a moeda nacional apresenta desejabilidade fraca, sendo assim caracterizado como *inovação radical*, por não se conformar às estruturas observadas até o seu surgimento. Ao se considerar as tipificações conceituais de inovação disruptiva o BTC apresenta potenciais características dos tipos *low disruption* e *new Market.*

Contudo, o impacto de todos esses fatores sobre o ambiente econômico é de modo fundamental dependente da percepção do BTC como moeda. Sendo assim, ao longo da presente pesquisa argumentou-se que esta inovação concedeu-lhe a capacidade de competir com os mais rápidos e avançados mecanismos de transferência de recursos líquidos, como, por exemplo, o Pay Pal. Isso porque, conforme analisado no Quadro 1, o BTC possui vantagem comparativa como unidade de conta, meio de troca e, possivelmente, reserva de valor, em relação às moedas tradicionais.

A análise do BTC segundo a mecânica de funcionamento do mercado de cartões de pagamentos, tendo por base a estrutura de M2L, mostrou que a utilização de BTC para a obtenção de crédito não apresenta semelhança com o modelo tradicional. Contudo, quando considerado o sistema de débito a estrutura se mostrou adequada. Esse resultado aponta que o BTC é considerado como ativo quando incorporado ao sistema financeiro.

De maneira geral, todos esses fatores se manifestam do ponto de vista da HME, na formação de padrões referentes à volatilidade dos retornos do BTC/US$. A seguir são apresentados os procedimentos estatísticos até as estimações das medidas de volatilidade. Neste sentido, primeiramente, relata-se que os testes de estacionariedade de Dickey-Fuller aumentado (ADF) e Phillips-Perron (PP) e Kwiatkowski–Phillips–Schmidt–Shin (KPSS) indicaram estacionariedade das séries de retornos, dispostos na Tabela 3.

Tabela 3. Testes de Raiz Unitária

Testes de Raíz Unitária (Amostra)				Testes de Raíz Unitária (Subamostra)			
Variáveis	ADF	PP	KPSS	Variáveis	ADF	PP	KPSS
BTC	-8,301624*	-41,44987*	0.446490**	BTC	-28,14421*	-28,16805*	0.537775**

Fonte: Elaboração própria. Nota: * Rejeita a hipótese nula a 1%. ** Não rejeita a 5%.

Na referida tabela é indicado pelos testes que tanto para a amostra quanto para a subamostra, é possível rejeitar a hipótese nula de não estacionariedade para os testes ADF e PP. Já no teste KPSS a hipótese nula é de que não existe raiz unitária. Para ele, não rejeitamos a hipótese a 5%. Sendo assim, é possível observar que os retornos do BTC são estacionários e não dependem, portanto, do tempo.

A escolha do melhor modelo pelo grau de ajustamento baseou-se nos critérios *Akaike Information Criterion* (AIC) e *Schwartz Bayesian Criterion* (SBC). Segundo Tsay (2005), quanto menor o AIC e SBC melhor o ajustamento do modelo aos dados da série. Utilizando o critério da parcimônia, o modelo ARMA (0,2) foi o que melhor se ajustou e apresentou as seguintes características esperadas: retornos não correlacionados, mas com severa correlação nos quadrados dos retornos, o que justifica a estimação por modelos capazes de captar efeitos de volatilidade condicional.

Tabela 4. Melhor modelo ARMA ajustado

Modelo	Critério Schwarz	Critério Akaike
BTC AR(0) MA(2) Amostra	-4,31091	-4,318593
BTC AR(0) MA(2) Subamostra	-6,108152	-6,101125

Fonte: Elaboração própria.

O terceiro passo na construção do modelo ARCH foi tentar ajustar o modelo ARMA usando a amostra, para verificar a correlação serial da série. Ressalte-se que os dados apresentam memoria longa, assim o teste ARCH somente captou a volatilidade a partir da segunda defasagem residual. A Tabela 5 traz os resultados do teste:

Tabela 5. Estatística F – ARMA (0,2)

Teste: ARCH – Modelo ARMA (0,2)			
Estatistica – F Amostra	8,098550	Prob. F(4,1348)	0
Obs* R^2	31,75133	Prob. Chi-Quadrado (4)	0
Estatistica – F Subamostra	52,71409	Prob. F(4,819)	0
Obs* R^2	168,7086	Prob. Chi-Quadrado (4)	0

Fonte: Elaboração própria. *A série apresenta volatilidade

O melhor modelo ajustado para a amostra com 1.357 observações, dentre os modelos estimados, foi o GARCH (1,1), conforme o critério de *Schwartz*. O modelo corrigiu completamente a autocorrelação residual e ao se repetir o teste ARCH se constatou a inexistência de volatilidade condicional. O modelo estimado resultante é dado por:

$$h_t = 0,00000346 + 0,220539 X_{t-1}^2 + 0,800577 h_{t-1} \quad (8)$$

A Tabela 6 e 7 sintetizam os resultados do modelo e a Estatística F do mesmo, respectivamente:

Tabela 6. Resultados do modelo GARCH (1,1) - Amostra

Variável	Coeficientes	Erro-Padrão	Estatística - Z	P Valor
Intercepto	0,000114636	0,00029024	0,39497012	0,69286494
MA (2)	0,055499339	0,027560405	2,013734487	0,044037417
Equação da Variância				
Intercepto	0,00000346	0,00000217	15,93489162	0
Resíduos (-1)^2	**0,220539029**	0,012605408	17,49558823	0
GARCH (-1)	**0,800576674**	0,008196231	97,67619844	0
R^2	-0,037313333			
R^2 ajustado	-0,038078878			
SQR	1,207575369		Critério de Akaike	-6,039195489
Estatística DW	2,103768306		Critério de Schwarz	-6,019987561

Fonte: Elaboração própria.

Tabela 7. Estatística F – GARCH (1,1) - Amostra

Teste: ARCH Modelo GARCH (1,1)			
Estatística - F	0,004481	Prob, F(1,1354)	0,9466
Obs* R^2	0,004488	Prob, Chi-Quadrado (4)	0,9466

Fonte: Elaboração própria.

Ao observar os valores em destaque dos parâmetros dispostos na Tabela 4, pode-se notar que primeiramente são significativos estatisticamente a 1%, e que a reação da volatilidade a choques é relativa, α_1=0,220539029. No que se refere à persistência da volatilidade aos choques ao longo do tempo, é β_1=0,800576674, o que indica, entre os parâmetros obtidos, relativa persistência. Isto é, percebe-se que tanto o choque imediato quanto à persistência são bastante representativos, mas há preponderância da persistência, o que corrobora com a elevada instabilidade dos valores cotados do BTC, sobretudo a partir de 2013.

Logo após, testes de autocorrelação dos resíduos dos retornos e do quadrado dos resíduos dos retornos – Estatística Q – foram realizados com o objetivo de afastar dúvidas sobre a robustez dos resultados alcançados. A Tabela 8 traz o resultado do teste:

Tabela 8. Teste de autocorrelação dos resíduos e do quadrado dos resíduos – Estatística Q - Amostra

Autocorrelação	Autocorrelação parcial	t	AC	PAC	Q-Stat	Prob*
| |	| |	1	0,047759972	0,047759972	3,102185399	
| |	| |	2	-0,018341142	-0,020669303	3,560024346	0,059186871
| |	| |	3	0,032210437	0,034184226	4,973127558	0,083195354
...	...	...	...	...	...	...
|* |[1]	|* |	7	0,097656629	0,093272095	22,84401255	0,000850442
| |	| |	1	0,001819164	0,001819164	0,004500734	0,946512036
| |	| |	2	0,006343791	0,006340502	0,059272623	0,970798538
|* |[2]	|* |	3	-0,023150262	-0,023174272	0,789221532	0,852043326

Fonte: Elaboração própria. [1] Resíduos. [2] Quadrado dos resíduos.

A Tabela 9 resume a comparação entre as estimações dos modelos GARCH, EGARCH e TARCH. O melhor modelo foi destacado em negrito:

Tabela 9. Modelo de melhor ajuste - Amostra

GARCH	BTC AR (0) MA (2)	Schwarz	-6,019988	Akaike	-6,039195
TARCH	BTC AR (0) MA (2)	Schwarz	-6,019542	Akaike	-6,046433
EGARCH	BTC AR (0) MA (2)	Schwarz	-5,990469	Akaike	-6,01736

Fonte: Elaboração própria.

Sendo assim, possivelmente estes resultados captam o aspecto inercial da fase de 'euforia'. No início do período da amostra a moeda não era utilizada majoritariamente enquanto meio de troca, por fatores apresentados em relação à adaptação do BTC em relação ao M2L para o caso dos cartões. Sendo assim, é possível que a maior parte dos agentes demandasse BTC por motivo especulação, e percebessem todo e qualquer retorno negativo como oportunidade de compra, não como reversão de tendência nas cotações.

Com base em 663 observações da subamostra foram realizadas estimações análogas às anteriores e, como esperado, o modelo de melhor ajuste de volatilidade divergiu. O modelo ARMA (0,2) também resultou no melhor ajuste conforme o critério de Schwarz e igualmente o melhor ajuste da volatilidade para um modelo GARCH (1,1), ou seja, estrutura idêntica a observada anteriormente. No entanto, os coeficientes resultantes são essencialmente diferentes. O modelo ajustado é dado por:

$$h_t = (6,74)10^{-6} + (0,240146)X_{t-1}^2 + (0,698707)h_{t-1} \quad (9)$$

As tabelas 10 e 11 trazem os resultados do modelo e a Estatística F do mesmo:

Tabela 10. Resultados do modelo GARCH (1,1) - Subamostra

Variável	Coeficientes	Erro-Padrão	Estatística - Z	P Valor
Intercepto	-0,000348	0,000286	-1,214364	0,2246
MA (2)	-0,010033	0,041015	-0,244615	0,8068
Equação da Variância				
Intercepto	0,00000674	0,00000063	10,71209	0
Resíduos $(-1)^2$	**0,240146**	0,024194	9,926044	0
GARCH (-1)	**0,698707**	0,021892	31,91609	0
R^2	-0,04835			
R^2 ajustado	-0,006051			
SQR	0,107511		Critério de Akaike	-6,805601
Estatística DW	1,948503		Critério de Schwarz	-6,794671

Fonte: Elaboração própria.

Tabela 11. Estatística F – GARCH (1,1) - Subamostra

Teste: ARCH Modelo GARCH (1,1)			
Estatística - F	0,333927	Prob. F(1,825)	0,5635
Obs* R^2	0,334602	Prob. Chi- Quadrado (4)	0,5630

Fonte: Elaboração própria.

Na Tabela 10, analogamente para o caso da Tabela 6, pode-se observar que primeiramente são significativos estatisticamente a 1%, tal qual no primeiro modelo, e que a reação da volatilidade a choques é ligeiramente maior se comparado às estimativas com a amostra completa, α_1=0,240146. Ao contrapor os valores com a estimação anterior, percebe-se que o termo constante α_0 praticamente dobrou, o que pode apontar para a percepção de um mercado já não tão incipiente. Por outro lado, no que se refere à persistência da volatilidade aos choques ao longo do tempo, é menor, β_1=0,698707, o que

está em consonância com a hipótese de 'euforia' observada nos valores cotados do BTC.

Assim como no caso das estimações para a amostra, testes de autocorrelação dos resíduos dos retornos e do quadrado dos resíduos dos retornos – Estatística Q –foram realizados com o objetivo de afastar dúvidas sobre a robustez dos resultados alcançados. A Tabela 12 traz o resultado do teste:

Tabela 12. Teste de autocorrelação dos resíduos e do quadrado dos resíduos – Estatística Q - Subamostra

Autocorrelação	Autocorrelação Parcial	t	AC	PAC	Q-Stat	Prob*
| |	| |	1	0,063624561	0,063624561	3,363973072	0,024955675
| |	| |	2	0,037853145	0,033942462	4,556126953	0,032801171
| |	| |	3	0,027915075	0,023551218	5,205257526	0,074078587
...	...	...	...	...	...	...
|* |	|* |	6	0,11480386	0,108584665	18,26474391	0,002632269
|* |	|* |	1	0,02011261	0,02011261	0,336155164	0,562056987

Fonte: Elaboração própria.

Igualmente, o modelo de variância condicional GARCH (1,1) eliminou a correlação serial observada na modelagem ARMA (0,2) e o teste ARCH aponta a inexistência do efeito após a estimação apropriada. A Tabela 11 traz a comparação entre as estimações dos modelos GARCH, TARCH e EGARCH. Em negrito o melhor modelo ajustado, GARCH, apresentou as seguintes estatísticas:

Tabela 13. Modelo de melhor ajuste - Subamostra

GARCH	**BTC C AR (0) MA (2)**	**Schwarz**	**-6,777104**	**Akaike**	**-6,805601**
TARCH	BTC C AR (0) MA(2)	Schwarz	-6,769141	Akaike	-6,803336
EGARCH	BTC C AR (0) MA (2)	Schwarz	-6,766251	Akaike	-6,811845

Fonte: Elaboração própria.

Em resumo, as estimações mostram-se relativamente sensíveis a valores extremos. Nesta pesquisa, seguiu-se o critério da parcimônia, conforme pode ser observado. Na análise visual da série de retornos do BTC, Figura 2, foi possível perceber que a mesma apresentou uma tendência de apreciação em momentos de crises econômicas e políticas. Por outro lado, ataques às instituições financeiras resultam tendência contrária.

8. Considerações finais

Para atender ao objetivo geral foram analisados aspectos institucionais e operacionais do BTC. O estudo apontou que o período de surgimento do mesmo coincidiu com o período dos intensos reflexos da crise mundial originada nos EUA. Esse contexto histórico-social pode ter sido determinante para que a inovação proporcionada pelo BTC alcançasse popularidade. Em outras palavras, pode-se afirmar que crises parecem atuar como fator de expansão do mercado de BTC e moedas digitais de emissão descentralizada, em geral.

É possível que elas, aparentemente, estão sendo absorvidas pelo sistema financeiro de modo mais intenso não como moeda, mas como ativo financeiro. A grande variedade de moedas digitais propicia competição e a população pode ou não escolher um tipo dominante. A adoção do BTC por parte das instituições financeiras, apesar do potencial de destruição criativa, contrasta com a baixa quantidade de comerciantes dispostos a aceitá-lo.

Talvez as mesmas não sejam demasiadamente rígidas à adaptação de seus

de moedas digitais propicia competição e a população pode ou não escolher um tipo dominante. A adoção do BTC por parte das instituições financeiras, apesar do potencial de destruição criativa, contrasta com a baixa quantidade de comerciantes dispostos a aceitá-lo.

Talvez as mesmas não sejam demasiadamente rígidas à adaptação de seus respectivos serviços. Moedas digitais podem representar oportunidade de ganhos líquidos quando relativizadas com as possíveis perdas por possibilitar a oferta de novos produtos, e a captação de novos clientes que antes não participavam do mercado. Instabilidades jurídicas, custo de carregamento em função da oscilação de preços e irreversibilidade representam possíveis fatores que limitam a disseminação do BTC. O entendimento de que as moedas digitais não reguladas são na realidade ativos financeiros torna mais branda a potencial ameaça às moedas nacionais de curso forçado. Dessa forma, as legislações mais restritivas tendem ser mais rígidas para gestores financeiros e comerciantes.

Com a finalidade de compreender os processos de formação do preço do BTC e da volatilidade associada ao mesmo foram estimados modelos que consideram heterocedasticidade condicional. Cada um deles foi estimado para a amostra e para a subamostra, conforme descrito anteriormente. Seguindo o critério da parcimônia, as análises econométricas apontam que o modelo GARCH (1,1) foi o que apresentou melhor ajuste em quaisquer dos casos. No entanto, os resultados diferem consideravelmente ao se comparar os resultados em função da amostra, uma das hipóteses levantadas na presente pesquisa.

Ataques às instituições financeiras que transacionam BTCs também são elementos que afetam sensivelmente a volatilidade nos seus preços, mas em sentido contrário, afeta negativamente o preço. Em razão da relação entre picos na cotação do BTC e epicentros de crises político-econômicas sugere-se, para estudos futuros, que tenham por objetivo mensurar a volatilidade dos preços do BTC, a incorporação de variáveis numa abordagem multivariada capazes de apontar iminência de crises. Apesar da impossibilidade de previsão de ciclos econômicos de forma determinística, a análise de fundamentos macroeconômicos pode fornecer aos especuladores do BTC insumos para mudança de estratégia.

Referências

ALBUQUERQUE, Bruno Saboia de; CALLADO, Marcelo de Castro. Understanding Bitcoins: facts and questions. Revista Brasileira de Economia, v. 69, n. 1, p. 3-16, 2015.

ARROW, Kenneth. Economic welfare and the allocation of resources for invention. In: The rate and direction of inventive activity: Economic and social factors. Princeton University Press, 1962. p. 609-626.

BANCO CENTRAL DO BRASIL; SECRETARIA DE ACOMPANHAMENTO ECONÔMICO; SECRETARIA DE DIREITO ECONÔMICO. Relatório sobre a indústria de cartões de pagamentos. Brasília, 2010.

BOLLERSLEV, T. Generalized Autoregressive Conditional Heteroskedasticity. Journal of Econometrics, 31, pp. 307-327, 1986.

CHRISTENSEN, Clayton M.; RAYNOR, Michael E.; ANTHONY, Scott D. Six keys to creating

new-growth businesses. Harvard Management Update, v. 8, n. 1, p. 3-6, 2003.

DOSI, Giovanni. Sources, procedures, and microeconomic effects of innovation. Journal of economic literature, p. 1120-1171, 1988.

ENGLE, Robert F. Autoregressive conditional heteroscedasticity with estimates of the variance of United Kingdom inflation. Econometrica: Journal of the Econometric Society, p. 987-1007, 1982.

EVANS, David S. The antitrust economics of two-sided markets. Available at SSRN 332022, 2002.

EVANS, David S. Some empirical aspects of multi-sided platform industries. Review of Network Economics, v. 2, n. 3, 2003.

FAGUNDES, J.; FERRÉS, J.; SAITO, K. Indústria de cartões de crédito, regulação e concorrência. Revista do IBRAC, v. 15, n. 4, 2009.

FRASCAROLI, Bruno Ferreira. Uma investigação sobre moeda, meios de pagamentos e crédito no Brasil utilizando simulações nas taxas de juros: o que podemos dizer sobre as recentes contribuições em economia monetária? 2010. 162 f. Tese (Doutorado em Economia) UFPE.

FREITAS, P. S. Mercado de cartões de crédito no Brasil: problemas de regulação e oportunidades de aperfeiçoamento da legislação. Brasília, DF: Consultoria Legislativa do Senado Federal, 2007. Texto para discussão n. 37, Brasília, DF.

GOLDFEDER, Steven et al. Securing Bitcoin wallets via threshold signatures. 2014.

GOVINDARAJAN, Vijay; KOPALLE, Praveen K. Disruptiveness of innovations: measurement and an assessment of reliability and validity. Strategic Management Journal, v. 27, n. 2, p. 189-199, 2006.

LUNDVALL, B. Políticas de inovação na economia do aprendizado. Brasília: CGEE Parcerias Estratégicas. Nº. 10. mar. 2001.

MAY, Timothy C. Crypto anarchy and virtual communities. 1994.

MEIKLEJOHN, Sarah et al. A fistful of bitcoins: characterizing payments among men with no names. In: Proceedings of the 2013 conference on Internet measurement conference. ACM, 2013. p. 127-140.

NELSON, Daniel B. Conditional heteroskedasticity in asset returns: A new approach. Econometrica: Journal of the Econometric Society, p. 347-370, 1991.

PAAR, Christof; PELZL, Jan. Understanding cryptography: a textbook for students and

practitioners. Springer Verlag, 2010.

PAVEL, Ciaian; D'ARTIS, Kancs; MIROSLAVA, Rajcaniova. The Economics of BitCoin Price Formation. EERI Research Paper Series, 2014.

ROCHET, Jean-Charles; TIROLE, Jean. Cooperation among competitors: Some economics of payment card associations. Rand Journal of economics, p. 549-570, 2002.

ROCHET, Jean-Charles; TIROLE, Jean. Platform competition in two-sided markets. Journal of the European Economic Association, p. 990-1029, 2003.

ROCHET, Jean-Charles; TIROLE, Jean. Two-sided markets: a progress report. The RAND Journal of Economics, v. 37, n. 3, p. 645-667, 2006.

SATOSHI, Nakamoto. Bitcoin: a peer-to-peer electronic cash system. (2008). Disponível em:< https://bitcoin.org/bitcoin.pdf>. Acesso em 16 de Agosto de 2015.

SCHILLER, R. J.. Radical financial innovation. In: Entrepreneurship, Innovation, and the Growth Mechanism of the Free-Enterprise Economies. Princeton University Press, 2007, v. p. 306-323.

SCHMALENSEE, Richard; EVANS, David S. The economics of interchange fees and their regulation: An overview. 2005.

TAYLOR, Michael Bedford. Bitcoin and the age of bespoke Silicon. In: Proceedings of the 2013 International Conference on Compilers, Architectures and Synthesis for Embedded Systems. IEEE Press, 2013. p. 16.

TSAY, R. S. Analysis of financial time series. 2 ed. Hoboken, New Jersey: John Wiley & Sons, Inc., 2005.

WHITE, Lawrence H. The theory of monetary institutions. Oxford: Blackwell Publishers, 1999.

WONGLIMPIYARAT, Jarunee. The dynamics of financial innovation system. The Journal of High Technology Management Research, v. 22, n. 1, p. 36-46, 2011.

WORLD ECONOMIC FORUM and DELOITTE. The Future of financial services: how disruptive innovations are reshaping the way financial services are structured, provionad and consumed. 2015.

ZAKOIAN, J. M. Threeshold heteroskedastic models. Journal of Economic Dynamics and Control, v. 18, p. 931-944, 1994.