

FGV FUNDAÇÃO GETULIO VARGAS
ESCOLA DE PÓS-GRADUAÇÃO EM ECONOMIA
MESTRADO EM FINANÇAS

MARCOS PAULO SOARES

**BLOCKCHAIN COMO ALTERNATIVA NAS TRANSFERÊNCIAS
INTERNACIONAIS NO BANCO DO BRASIL**

RIO DE JANEIRO
2018

MARCOS PAULO SOARES

**BLOCKCHAIN COMO ALTERNATIVA NAS TRANSFERÊNCIAS
INTERNACIONAIS NO BANCO DO BRASIL**

Dissertação de Mestrado apresentada à Escola de
Pós-Graduação em Economia da Fundação Getúlio
Vargas como requisito para a obtenção do título de
Mestre em Finanças.

Área de Concentração: Finanças

Orientador: Rafael Chaves Santos

RIO DE JANEIRO
2018

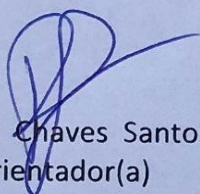
MARCOS PAULO SOARES

**“BLOCKCHAIN COMO ALTERNATIVA NAS TRANSFERÊNCIAS INTERNACIONAIS NO
BANCO DO BRASIL”.**

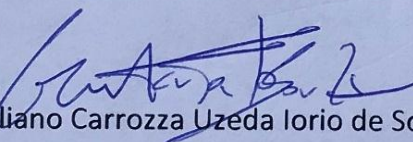
Dissertação apresentado(a) ao Curso de Mestrado Profissional em Economia Empresarial e Finanças do(a) Escola de Pós-Graduação em Economia para obtenção do grau de Mestre(a) em Economia Empresarial e Finanças.

Data da defesa: 26/12/2018

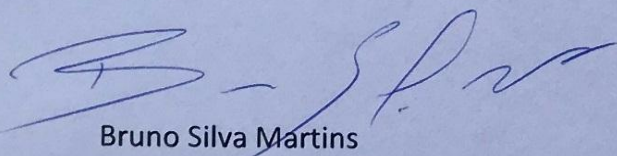
ASSINATURA DOS MEMBROS DA BANCA EXAMINADORA



Rafael Chaves Santos
Orientador(a)



Giuliano Carrozza Uzeda Iorio de Souza



Bruno Silva Martins

Soares, Marcos Paulo

Blockchain como alternativa nas transferências internacionais no Banco do Brasil / Marcos Paulo Soares. – 2018.
57 f.

Dissertação (mestrado) - Fundação Getulio Vargas, Escola de Pós-Graduação em Economia.

Orientador: Rafael Chaves Santos.

Inclui bibliografia.

1. Blockchains (Base de dados). 2. Inovações tecnológicas. 3. Banco do Brasil. I. Santos, Rafael Chaves. II. Fundação Getulio Vargas. Escola de Pós-Graduação em Economia. III. Título.

CDD – 332

AGRADECIMENTOS

À minha família, por todo apoio de sempre.

Ao meu orientador Rafael Chaves Santos, que me deu todo suporte necessário para que conseguisse concluir este trabalho com tema tão inovador e desafiador.

À monitora Letícia Nunes, por toda ajuda no desenvolvimento do modelo Garch e leitura atenciosa deste trabalho, sugerindo correções.

Aos amigos do Meetup Cripto, em especial ao Pedro Marins, que tirou dezenas de dúvidas em nossas reuniões mensais, além de revisar este trabalho, dando contribuições relevantes sobre a tecnologia Blockchain.

Ao meu chefe Francisco Roder, por me permitir tirar licença para concluir este trabalho.

À Gisele Gammaro, que me ajudou tantas vezes nas mais variadas situações.

Aos colegas de mestrado da FGV mais próximos Pedro Mello, Fátima Besada, Daphne Breyer, Frederico Papini, Filipe Bordalo e Viviane Ramos pela parceria.

À Consensys, e todo seu time, que me permitiu participar de um de seus encontros em São Francisco (CA), fazendo com que eu descobrisse um novo mundo de possibilidades com a tecnologia Blockchain.

À Ripple, que me permitiu conhecer suas instalações em San Francisco (CA) assim como todo material fornecido, sem o qual este trabalho estaria muito prejudicado.

Aos funcionários da Ripple Breno Araújo, que de Londres, foi o primeiro a me mostrar todas soluções em Blockchain que estavam sendo criadas pela Ripple; e Arthur Ware, representante da Ripple no Brasil, por todo suporte e esclarecimentos sobre a Ripple Net.

Resumo

A proposta deste trabalho é verificar a viabilidade da utilização do Blockchain para transferências internacionais, reduzindo custos e prazos. Para tanto, será utilizado o modelo GARCH (1,1) para examinar a volatilidade das principais criptomoedas comparando-as com moedas tradicionais como dólar, yen e euro, além de índices macroeconômicos, a fim de aferir a sensibilidade dessas moedas a fatores macroeconômicos. Além disso, uma vez verificado que a volatilidade das principais criptomoedas tende a se aproximar da volatilidade de outros ativos financeiros em breve, pretendemos mostrar quando essa variabilidade poderá ser assumida como semelhante a outros ativos financeiros. Por fim, este trabalho simulará a redução de custos nas transferências internacionais tendo como alternativa a solução Blockchain da Ripple e da IBM em contraste com a solução SWIFT, utilizando como referência o volume de transferências internacionais do Banco do Brasil.

Palavras-Chave: i) Blockchain ii) Inovação, iii) Criptomoedas iv) Custos de Transação, v) Ripple, vi) Banco do Brasil

Abstract

The purpose of this paper is to verify the feasibility of using Blockchain solution for international transfers, aiming reduce costs and deadlines. For this, the GARCH model (1.1) will be used to verify the volatility of the main crypto currencies, comparing them to traditional currencies such as the dollar, yen and euro, as well as macroeconomic indices. This approach will verify the sensitivity of these crypto currencies to macroeconomic factors. Furthermore, as the volatility of the main crypto-currencies tends is quickly trending towards the volatility of other financial assets, I intend to show how soon this volatility can be assumed to be similar to other financial assets. Lastly, this work will simulate the reduction of international transfer costs, by using the Ripple's and IBM's Blockchain solution versus SWIFT, using comparing them to the international transfers of Banco do Brasil.

Key Words: i) Blockchain ii) Innovation, iii) Crypto currencies iv) Transaction Costs, v) Ripple, vi) Banco do Brasil

Sumário

1. INTRODUÇÃO	11
2. O SISTEMA BLOCKCHAIN	17
2.1. A origem do Blockchain	17
2.1. Uma Breve História	17
3. PRINCIPAIS PROBLEMAS NA UTILIZAÇÃO DO BLOCKCHAIN	20
3.1. Escalabilidade	20
3.1.1. Lightning Network	21
3.1.2. SegWit	21
3.1.3. Flexcap	21
3.2. Segurança	22
3.4. Interface Pouco Amigável	24
3.5. Regulação	24
4. A VOLATILIDADE	27
4.1. Dados	27
4.2. Metodologia	32
4.2.5. Resultados	38
5. SWIFT VS. SOLUÇÕES BLOCKCHAIN	46
5.1. SWIFT	46
5.2. IBM Blockchain World Wire	49
5.3. Ripple Net	50
6. CONCLUSÃO	53
7. REFERÊNCIAS BIBLIOGRÁFICAS	55

Índice de Figuras

Figura 1 - Movimento dos Preços das 3 Principais Criptomoedas.....	27
Figura 2 - <i>Log Return</i> - Bitcoin, Ether e XRP	28
Figura 3 - Volume de Negociação Bitcoin por País - Principais Moedas	29
Figura 4 - Volume de Negociação Bitcoin - Principais Moedas (exceto CNY)	29
Figura 5 - Volatilidade Comparada de Bitcoin com Câmbio e Ouro	30
Figura 6 - Volatilidade Comparada de Bitcoin com Índice de Mercado de Ações	31
Figura 7 - Volatilidade Comparada de Bitcoin com <i>Bond</i> de 10 Anos	31
Figura 8 - Volatilidade Comparada de Ether com Taxa de Câmbio e Ouro	31
Figura 9 - Volatilidade Comparada de Ether com Índice de Mercado de Ações	31
Figura 10 - Volatilidade Comparada de XRP com Câmbio e Ouro	32
Figura 11 - Volatilidade Comparada de XRP com Índice de Mercado de Ações	32
Figura 12 - Volatilidade Comparada de XRP com <i>Bond</i> de 10 Anos	32
Figura 13 - Teste de Agrupamento de Volatilidade nos Resíduos – Bitcoin	34
Figura 14 - Teste de Agrupamento de Volatilidade nos Resíduos - Ether	35
Figura 15 - Teste de Agrupamento de Volatilidade nos Resíduos – XRP	35
Figura 16 - Distribuição dos Retornos.....	37
Figura 17 - Variância Condicional – Criptomoedas e VIX	42
Figura 18 - Tendência Variância Condicional – Bitcoin.....	42
Figura 19 - Tendência Variância Condicional – Ether	43
Figura 20 - Tendência Variância Condicional – XRP (a)	43
Figura 21 - Tendência Variância Condicional - XRP (b).....	44
Figura 22 - Usuários Ativos e Volatilidade Bitcoin	44
Figura 23 - Usuários Ativos e Volatilidade - Ether	45
Figura 24 – Usuários Ativos e Volatilidade - XRP	45
Figura 25 - Erros, Falhas e Reconciliações - SWIFT	48

Índice de Tabelas

Tabela 1 - Variáveis Macroeconômicas Escolhidas	30
Tabela 2 - Teste LM ARCH	35
Tabela 3 - Resumo das Estatísticas	36
Tabela 4 - <i>Market Share</i> das Criptomoedas (USD).....	39
Tabela 5 – Resultado da Regressão Garch (1,1) - Bitcoin.....	39
Tabela 6 - Resultado da Regressão Garch (1,1) - Ether	40
Tabela 7 - Resultado da Regressão Garch (1,1) - XRP	40
Tabela 8 - Os 10 Maiores Volumes de Transferências para o Exterior (USD) – Nov/2017 a Out/2018	46
Tabela 9 - Custos por Pagamento - SWIFT	48
Tabela 10 - Retorno do Investimento da Solução IBM Blockchain Wire.....	50
Tabela 11 - Custos Ripple Comparados com SWIFT	52

1. INTRODUÇÃO

Apesar dos grandes progressos tecnológicos alcançados com o avanço da computação e com o advento da internet, os sistemas de transações financeiras internacionais permanecem, em sua essência, os mesmos de séculos atrás, com a necessidade de cartas de crédito ao importador e dezenas de procedimentos feitos por muitos intervenientes, tornando o processo caro, demorado e ineficiente. O sistema atual é exclusivo, deixando milhões de pessoas sem acesso ao sistema financeiro; é centralizado, sendo exposto a ataques cibernéticos, vazamento de informações e violação de dados; e é oligopolista no Brasil, tendo nos cinco principais bancos brasileiros cerca de 80% de todas as operações de crédito e depósitos do sistema financeiro.¹

A necessidade de ter várias empresas/organizações foi explicada no trabalho seminal de Ronald Coase “A Natureza da Firma” (1937), onde o economista busca justificar porque existem empresas, se as pessoas poderiam transacionar seus serviços e mercadorias individualmente. O economista avança em seu estudo ao publicar “O Problema do Custo Social” (1960). Em ambos estudos surge a ideia dos custos de transação, mostrando a necessidade de existirem empresas, uma vez que estas reduzem os custos de cada indivíduo recorrer ao mercado a cada transação.

Williamson (1975 e 1987) formula a economia da organização a partir dos trabalhos de Coase, trazendo a ideia dos problemas para governança gerados pelas incertezas e racionalidade limitada, que por sua vez geram contratos incompletos. A continuidade dos investimentos, onde o pagamento depende dos investimentos dos outros, faz aparecer o oportunismo quando um agente pode renegar um contrato, modelado em teoria dos jogos. Dito de outra forma, o valor dos investimentos individuais depende da continuidade do relacionamento do grupo. Williamson defende que os riscos de oportunismos podem ser enfrentados com estruturas de governança eficientes. É a proteção contra o oportunismo que dá origem ao custo de transação.

Hayek (1945) acreditava que o caminho para uma economia em funcionamento era descentralizado e afirmava que uma economia descentralizada complementa a natureza dispersa da informação, espalhada por toda a sociedade. Foi um pioneiro em vislumbrar economias descentralizadas e processamento distribuído de informação. Tendo para muitos, no seu livro

¹ Conforme Relatório de Economia Bancária do Banco Central de 2017, disponível em https://ripple.com/pt_BR/insights/swell-2018-how-banco-santander-launched-a-payment-app-for-millions/ Acesso em 01/09/2018.

“*Denationalisation of Money*” de 1976, a ideia embrionária do Bitcoin, onde o autor pregava a privatização do dinheiro, onde moedas privadas competiriam até que o mercado escolhesse a moeda dominante no mundo. Hayek (1976) vai além ao arguir que mercado monetário seria a arma perfeita contra a inflação, com o argumento simples que o governo deveria manter a inflação baixa, ou as pessoas buscariam outras moedas. Parece que é exatamente o que vem ocorrendo na Venezuela, onde o crescimento do uso do Bitcoin tem sido recorde, devido à hiperinflação. Fazendo até com que o governo venezuelano criasse sua própria criptomoeda, o Petro².

Dessa forma, juntando os trabalhos de Coase (instituições eficientes), Williamsom (contratos incompletos) e Hayek (conhecimento distribuído e economias descentralizadas), há um arcabouço teórico aguardando o avanço da tecnologia para criar as condições em que se possa verificar suas ações na prática. Enxerga-se, assim, no Blockchain não apenas uma nova tecnologia, mas sim um novo tipo de economia.

A tecnologia Blockchain promete ser bastante disruptiva nos próximos anos, mudando toda uma gama de transações financeiras que carecem, até o momento, de entes centralizadores que tragam confiança para o sistema.

A internet, desde os anos 1990, nos permite mover dados para qualquer lugar no mundo de forma rápida, eficiente, padronizada e sem nenhum custo. O mesmo não ocorre para transferir valores, o que costuma ser caro, lento, ineficiente e pouco padronizado. A tecnologia Blockchain promete resolver esse problema. Ela pretende provocar uma grande mudança nas transações financeiras em todo o mundo, gerando possíveis desarticulações, assim como oportunidades. Promete, sobretudo, redução de custos de transação nas transferências internacionais.

Com a promessa do Blockchain, pela primeira vez na história, dois entes que não se conhecem, e, portanto, não confiam um no outro, poderão realizar negócios e fazer transações com segurança. Uma das funções mais importantes e que foi razão precípua de surgimento dos bancos, está sendo ameaçada pela primeira vez com o paradigma de consenso sobre demanda no Blockchain, onde não mais uma entidade centralizadora confiável é necessária. Surge uma rede P2P³ proporcionando um sistema distribuído confiável, seguro e imutável para realizar transações financeiras.

² Volume de negociação de Bitcoin bate recorde na Venezuela. Disponível em <https://criptoeconomia.com.br/venezuela-afetada-pela-inflacao-volume-de-negociacao-de-Bitcoin-registra-crescimento-recorde/> Acesso em 02/09/2018.

³ Do inglês “Peer-to-peer” – Rede de computadores ponto a ponto permitindo que pessoas possam compartilhar serviços e dados sem a necessidade de um intermediário.

A internet propiciou o surgimento de empresas com sistemas tecnológicos que permitiram a compra e venda de produtos e serviços entre indivíduos sem uma série de garantias e salvaguardas até então exigidas, viabilizando um sistema de confiança que estimula as pessoas se envolverem livremente umas com as outras. Seria inimaginável há 20 anos que entraríamos no carro de um estranho para nos deslocarmos, ou que abriríamos as portas de nossas casas para que viajantes de qualquer lugar do mundo pudessem passar alguns dias. Há alguns anos isso já é uma realidade com Uber e Airbnb. Ao que tudo indica parece ter chegado a vez dessas mudanças radicais chegarem aos sistemas financeiros.

A redução de custos de transações através da implementação do Blockchain promete ser uma grande ameaça ao modelo de negócio *mainstream* vigente. Com custos radicalmente mais baixos, será possível oferecer serviços financeiros a indivíduos que, até o momento, não são considerados pelos grandes bancos. Qualquer pessoa, em qualquer lugar, com um *smartphone* e acesso à internet poderá se conectar a todo um sistema financeiro mundial dentro do Blockchain. É o que preconiza Tapscot (2016).

Além da redução de custos de transação, a utilização do Blockchain para transações financeiras internacionais promete aumentar a velocidade de transferência de dinheiro vertiginosamente. Onde atualmente leva-se de 3 a 5 dias para transferir recursos financeiros de uma empresa/indivíduo em um país para outra empresa/indivíduo em outro país, através da rede SWIFT que processa cerca de 30 milhões de transferências internacionais diariamente⁴; ou da Western Union que detém mais de 550 mil estabelecimentos, em mais de 200 países e que movimentou mais de US\$ 300 bilhões em 2017⁵, com a rede Bitcoin cada bloco é adicionado ao Blockchain a cada 10 minutos. Ou seja, a rede Bitcoin promete autorizar transações internacionais em qualquer lugar do mundo em minutos, substituindo um sistema que demora dias. Como será visto na quarta parte deste trabalho, outras iniciativas, como a xRapid da Ripple, já permitem reduzir a duração das transações para 3 segundos.

Observa-se que a mudança de um sistema que demora dias para processar uma transferência, para um sistema de transferência de alguns minutos, liberaria recursos represados, reduzindo drasticamente todos os ganhos com *float* que os intervenientes recebem.

A redução de custos de transação não se dá apenas com a redução de *float*, mas também com os elevados custos para se atestar a confiança em transacionar com entidades que não se conhecem. Segundo Tapscot (2016), verificar a identidade e estabelecer confiança não

⁴ Obtido em <https://www.SWIFT.com/about-us/SWIFT-fin-traffic-figures>. Acesso em 30/11/2018. Apresentou pico de 35 milhões de pagamentos diários em 31/05/2018.

⁵ Disponível em <https://corporate.westernunion.com/index.html>. Acesso em 30/11/2018.

é mais o direito ou o privilégio do intermediário financeiro. Os custos que todas as instituições financeiras têm para conhecer seus clientes, para manter uma estrutura responsável por autorizar transferências pode passar de US\$ 20 bilhões (TAPSCOT, 2016). Com a tecnologia Blockchain em um aplicativo, em qualquer *smartphone* conectado à internet, será possível fazer transferências internacionais para qualquer lugar do mundo de forma rápida e sem consumo de estrutura bancária. Há iniciativas como OmiseGo (troca de valores peer-to-peer), WeTrust (associações de crédito) e Humaniq (Blockchain com biometria para transações) que prometem conectar pessoas ao sistema financeiro com um *smartphone*. Como será visto na quarta parte deste trabalho, o Santander desenvolveu o aplicativo para celular chamado One Pay FX em que transferências internacionais envolvendo alguns países já é realidade.

O impacto da mudança de sistemas de transferência de recursos financeiros de forma instantânea daria uma enorme liquidez ao sistema financeiro e uma perda significativa de ganhos com *float* pelos intervenientes do sistema. Acrescenta-se a isso a redução de riscos, uma vez que em momentos de crises financeiras, não se sabe se as contrapartes irão honrar seus compromissos. A liquidação instantânea pelo Blockchain eliminaria esse risco, uma vez que todos os envolvidos acompanhariam o registro de cada transação na rede, no momento que desejarem.

A tecnologia Blockchain promete provocar uma grande mudança nas transações financeiras em todo o mundo, gerando possíveis desarticulações, assim como oportunidades. Aplicativos para transações financeiras pretendem oferecer seus serviços gratuitamente. Num primeiro momento não faz sentido oferecer serviços financeiros gratuitamente, mas se olharmos as empresas que mais cresceram nos últimos 10 anos no mundo, grande parte delas cresceram exponencialmente oferecendo produtos sem cobrar nada pelos seus serviços.

Se no século passado a ideia de grátis era dar algo para criar demanda para outro produto que era cobrado, como por exemplo dar aparelhos de barbear - que sozinhos não tinham utilidade - para vender lâminas de barbear. No século XXI, a nova forma de “grátis” que está mudando (e mudará) - ainda mais - a era atual, é impulsionada por uma habilidade incrível de reduzir os custos dos serviços a quase zero.

O site de buscas Google oferece um serviço de buscas inteiramente de graça, mas ao fazer pesquisas, sem saber, estamos melhorando seus algoritmos de localização de anúncios. Dessa forma, você está pagando com seu trabalho algo que recebeu, aparentemente, de graça.

A ideia de termos tantos serviços financeiros abundantes os leva indubitavelmente a serem oferecidos gratuitamente, como o sal que na Idade Média, chegou a ser usado como moeda, em partes da Europa distantes do mar. Atualmente o sal está em cada mesa de qualquer

restaurante sendo oferecido barato demais para ser cobrado. Com a internet o preço de consumir informação caiu até o custo marginal e esse custo on-line é tão próximo de zero que é cômodo arredondar para zero.

Com Blockchain tudo a leva a crer que acontecerá aos bancos, algo semelhante ao que está ocorrendo com o sistema operacional, de código aberto, Linux, que vem aumentando lentamente sua participação em sistemas operacionais de empresas, enquanto o Windows vem diminuindo sua participação. O Banco do Brasil é um exemplo de redução de custos com a utilização do software livre Linux, com estimativa de economia de custos de R\$ 50 milhões em licenças privadas⁶.

A tecnologia Blockchain nasceu com Nakamoto (2008), introduzindo o conceito de Bitcoin e seu registro público de transações. Passados dez anos de sua criação, embora tenha atingido aproximadamente 17 milhões de Bitcoins, o que dá um valor de mercado que ultrapassa 72 bilhões de dólares⁷, ainda não foi adotado em massa por vários motivos.

Dentre os principais motivos há o “trilema da escalabilidade” proposto por Vitalik Buterin, criador do Ethereum; e a alta volatilidade dos preços das criptomoedas. Ainda sem solução, o “trilema da escalabilidade” afirma que não é possível ter descentralização, segurança e escalabilidade ao mesmo tempo, numa solução Blockchain. Quando se tem um sistema descentralizado e com movimentação em escala, perde-se em segurança; quando se prioriza segurança e escalabilidade, não se tem um sistema descentralizado. Embora várias iniciativas, que serão explicadas mais à frente, busquem solucionar o problema, a solução Blockchain para sistemas financeiros que tem se mostrado mais promissor, abre mão de certa descentralização em prol da segurança e escalabilidade. Dentre essas soluções que mais se despontam citamos a Ripple Net da Ripple e IBM Blockchain World Wire da IBM.

Uma vez que os sistemas financeiros estão priorizando a segurança e escalabilidade em detrimento da descentralização, sobra-nos como principal entrave à adoção em massa do Blockchain a questão da volatilidade, utilizando-se criptomoedas para pagamentos e transações internacionais.

Um importante indício de que estaríamos perto da utilização cada vez mais intensa de Blockchain para transferências internacionais pelos agentes financeiros, seria a sinalização de que a volatilidade das principais criptomoedas esteja diminuindo. Três principais criptomoedas foram escolhidas, que representam 64% do valor de mercado das 2112 criptomoedas listadas

⁶ Disponível em <http://softwarelivre.org/fisl16/noticias/banco-do-brasil-comemora-transformacao-da-cultura-em-10-anos-de-software-livre>. Acesso em 10/10/2018.

⁷ Disponível em <https://coinmarketcap.com/>. Acesso em 01/12/2018

na coinmarketcap.com, para verificarmos se vem ocorrendo redução dessa volatilidade e em quanto tempo esperamos ter volatilidade semelhante ao de uma moeda fiduciária.

A estrutura deste trabalho, além desta introdução é organizada como segue: a segunda seção explica o que é Blockchain e mostra como surgiu no contexto histórico, a terceira seção busca identificar os principais obstáculos à utilização do sistema Blockchain em massa, a quarta seção aprofunda o principal problema encontrado no Blockchain para transferências internacionais que é a volatilidade, a quinta seção busca verificar as diferenças entre os sistemas SWIFT e soluções que utilizam Blockchain para transferências internacionais e na última seção concluímos este trabalho.

2. O SISTEMA BLOCKCHAIN

2.1. A origem do Blockchain

Blockchain foi mencionado pela primeira vez no fim de 2008, num artigo⁸ escrito por uma pessoa (ou um grupo) anônima, com o pseudônimo de Satoshi Nakamoto, que não foi mais ouvido desde abril de 2011. No artigo, Nakamoto (2008) traz a ideia de um sistema de pagamentos *peer-to-peer* descentralizado, através de uma moeda criptografada de nome Bitcoin. Ele foi o primeiro desenvolvedor a criar a possibilidade real de eliminarmos a necessidade de um intermediário para que seja efetuado um pagamento internacional, através do registro em um banco de dados público que ele denominou de Blockchain.

No Blockchain todas as transações são verificadas em “nós” da rede, que nada mais são que computadores conectados à rede e que validam as transações através de cálculos matemáticos complexos, sendo recompensados com criptomoedas e taxas por este trabalho. Esses “nós” também ficaram conhecidos como “mineradores”. O primeiro bloco foi adicionado em janeiro de 2009 à rede, lançando o Bitcoin, na prática, como software livre para uso de todos.

Cada bloco possui a assinatura *hash*⁹ do bloco anterior, criando uma “corrente” segura. O Blockchain é essencialmente um método de compartilhamento e registro de dados, transações ou qualquer ativo digital em um ambiente distribuído, ponto a ponto; usando criptografia e cálculos matemáticos para criar um banco de dados que seja aberto e descentralizado. Qualquer transação de qualquer valor pode ser registrada neste banco de dados. É construído de forma descentralizada, distribuindo informações e armazenando-as pela rede da Internet em vários computadores, sem um poder central que domine ou regule o sistema.

2.1. Uma Breve História

A ideia de Blockchain nasce com a moeda digital Bitcoin, mas a ideia de moeda digital não é nova. Pessoas que lidavam com criptografia lançaram moedas digitais independentes tais como Digicash em 1992, Cybercash em 1994, E-gold em 1996, Liberty Reserve em 2006 e

⁸ Também conhecido como White Paper. Disponível em <https://Bitcoin.org/Bitcoin.pdf>. Acesso em 01/09/2018.

⁹ Código com vários caracteres gerado por função matemática, que tem a função de resumir informações de arquivos para comparação, sem que se tenha acesso ao seu conteúdo.

Perfect Money em 2007¹⁰. Todas essas iniciativas não obtiveram sucesso por falta de transparência, segurança e descentralização; e por isso que a estrutura Blockchain é disruptiva. Ela foi criada para corrigir esses problemas em sua essência.

A primeira transação com o Blockchain do Bitcoin ocorreu em maio de 2010, quando um programador da Flórida enviou 10 mil Bitcoins (BTCs) para outra pessoa no Reino Unido que comprou 2 pizzas pelo valor de 25 dólares¹¹. Atualmente 10 mil BTCs valem R\$ 207 milhões.

O Bitcoin começa a ter um pouco mais de visibilidade quando nasce a primeira *Exchange* (corretora) de Bitcoin, a Mt. Gox. A partir desse momento pessoas com moedas fiduciárias poderiam comprar Bitcoin, onde antes apenas tinham Bitcoin quem tivesse “minerado” a criptomoeda.

A partir de 2011, o sucesso do Bitcoin ocorreu inicialmente para transações ilegais em mercados negros, para compra de drogas, armas e contrabando; dado suas características de ser global, anônimo, com baixíssimos custos de transação, impossível de serem bloqueadas e sem limites ou pré-requisitos. Neste mercado negro, desponta-se o site “Silk Road” para compras on line de drogas, que acabou sendo fechado pelo FBI em 2014, com a prisão, e posterior condenação à prisão perpétua de seu criador, Ross Ulbricht.

Em 2012, startups começam a surgir criando carteiras virtuais (*wallets*) mais simples de usar por usuários não técnicos, familiarizando-os com a tecnologia. Neste mesmo ano a Bitcoin-Central torna-se a primeira empresa autorizada a operar como um banco na França (SANTOS, 2012).

Em 2013, a corretora Mt. Gox era responsável por 70% das compras e vendas de todos os Bitcoins no mundo. A partir do início de 2014, por conta de má administração e fraudes, as pessoas começaram a perder a confiança na corretora, levando-a à ruína neste mesmo ano. Tendo sua sede no Japão onde não havia qualquer tipo de regulamentação, seus clientes ficaram sem proteção. A partir deste fato, muitos investidores perderam interesse na criptomoeda e o preço caiu.

Em 2013, também é colocado em operação o primeiro ATM para saque em Vancouver. Atualmente, há 3968 em todo o mundo segundo coinatmradar.com¹², com média

¹⁰ Disponível em <https://safehaven.com/article/45042/Before-Bitcoin-The-History-Of-Digital-Cash>. Acesso em 15/10/2018.

¹¹ Para comemorar a transação todo dia 22 de maio é celebrado o Bitcoin Pizza Day, onde fornecedores de pizza dão descontos para usuários da criptomoeda.

¹² Disponível em <https://coinatmradar.com/>. Acesso em 02/10/2018.

de 6 ATMs sendo instalados por dia. Há dois destes ATMs instalados no Brasil, ambos em São Paulo - SP.

3. PRINCIPAIS PROBLEMAS NA UTILIZAÇÃO DO BLOCKCHAIN

Para utilização do Blockchain no sistema financeiro como forma de pagamento, há que se superar quatro grandes obstáculos encontrados nos ativos digitais: escalabilidade, segurança/privacidade, interface pouco amigável e volatilidade.

Esse trabalho busca analisar opções que busquem inicialmente resolver todos os problemas citados acima, abrindo mão de certa descentralização, pois as soluções de Blockchain na área de transferências internacionais que mais têm avançado atualmente, abrem mão, em parte, de ter um sistema totalmente descentralizado em prol da segurança e escalabilidade.

3.1. Escalabilidade

O Blockchain do Bitcoin foi constituído por Satoshi Nakamoto (2008) para que cada bloco da corrente de blocos tenha no máximo 1 megabyte (MB – 1.000.000 *bytes*), visando segurança, tal restrição limita a no máximo 7 transações por segundo, enquanto infraestruturas como VISA permitem até 56 mil transações por segundo¹³.

Devido ao protocolo em que blocos são adicionados ao Blockchain a cada 10 minutos, sua capacidade máxima de transações é limitada pelo tamanho máximo do bloco, que no caso do Bitcoin é de 1 MB por esse intervalo. O tamanho máximo de um bloco é de 1 MB (e esse valor é uma constante *hardcoded* no software padrão que foi introduzida por Nakamoto em julho de 2010¹⁴. Considerando que uma transação tem em média 250 bytes e lembrando que é esperado em média 1 novo bloco a cada 10 minutos (600 segundos), tem-se: $1\ 000\ 000 / 250\ \text{bytes} = 4\ 000$ transações (tx) por bloco e então $4\ 000 / 600\ \text{s} = 6.6\ \text{tx/s}$.

Por ser de código aberto, o Blockchain tem uma comunidade engajada de desenvolvedores que não para de crescer e que de forma colaborativa vem mostrando que há várias soluções para o mesmo problema. Veremos algumas delas:

¹³ Disponível em <https://usa.visa.com/dam/VCOM/download/corporate/media/visa-fact-sheet-Jun2015.pdf>. Acesso em 02/10/2018

¹⁴ Disponível em <https://medium.com/@jcliff/understanding-the-block-size-debate-351bdbaaa38>. Acesso em 03/10/2018.

3.1.1. Lightning Network

Lightning Network é uma grande inovação para a escalabilidade do Blockchain, tendo como meta funcionar como um respaldo para canais de pagamentos entre usuários. Esses canais permitem que vários pagamentos sejam feitos fora do Blockchain e somente o pagamento resultante é então propagado para o Blockchain, representando o fechamento do canal, conforme Poon (2016).

3.1.2. SegWit

Termo que vem de Segregated Witness. Segundo Lambrozo, Wuille e Lau (2015), o sistema SegWit tem a ideia de que somente “nós” completos precisam manter uma cópia inteira do Blockchain para validar as transações. Desta forma, propõe que as assinaturas sejam desvinculadas da transação, sendo guardadas separadas, resultando em otimização e liberando cerca de 60% de espaço em disco para os “nós”.

3.1.3. Flexcap

Flexcap, como o próprio nome sugere, propõe uma flexibilização do tamanho máximo do bloco. Segundo Friendebach (2015) ele deve ser flexível, podendo ser aumentado ou diminuído através de um sistema de votação que é acompanhado de um custo para quem vota. Parte da ideia de que é impossível prever qual o melhor tamanho máximo para um bloco, mas que esse limite precisa aumentar ou diminuir para atingir a escalabilidade pretendida.

Na prática todas as criptomoedas lançadas a partir do Bitcoin, não limitaram o tamanho do bloco, trazendo maior capacidade de transações por segundo. Ademais, como esse trabalho tende a investigar, a capacidade de utilizar Blockchain como alternativa nas transferências internacionais, mesmo com um limite de 10 minutos para uma transação financeira no Blockchain do Bitcoin suplanta, em muito, as opções atuais como SWIFT ou Western Union onde transações demoram de 3 a 5 dias para confirmação.

3.2. Segurança

O sistema Blockchain vem desde 2010 sem que uma única fraude tenha ocorrido. A fraude no sistema é de difícil execução, tendo em vista que a própria essência do sistema foi desenvolvida para que a conferência seja por consenso, onde para se ter controle da rede, o fraudador deverá ter controle de 51% da rede, exigindo um poder computacional extremamente alto.

A principal forma de ataque é através do processo conhecido por “*Distributed Denial of Service*” (DDoS), onde quem está comandando a invasão se utiliza de computadores infectados com vírus ao redor do mundo para em determinado momento executar determinada ação.

Tendo em vista que atualmente há necessidade de computadores muito potentes para os cálculos complexos que são necessários para minerar um Bitcoin, grupos de pessoas se juntam colocando computadores juntos para aumentar a capacidade de processamento. A esses grupos deu-se o nome de “*mining pool*” e diversos estudos¹⁵ já foram feitos, inclusive utilizando *Game Theory* para verificar a possibilidade de estrategicamente conseguir controle da rede através de DDoS. E todos chegaram à conclusão da impossibilidade de se conseguir tal controle.

O sistema Blockchain é extremamente disruptivo no que tange principalmente segurança, pois sua concepção resolveu um problema bastante visto em aulas de computação e tido como sem solução: O Problema do Dois Gerais ou Problema dos Gerais Bizantinos. O problema está em conseguir achar uma maneira de chegar a um consenso para resolver uma questão. Lamport, Shostak e Pease (1982) foram os primeiros a formular tal problema que embora simples não trazia uma solução. Em resumo, o problema supõe uma situação hipotética onde dois generais planejam atacar uma cidade com seus exércitos. Cada general está em uma montanha, com um vale entre eles. Eles precisam trocar mensagens, mas a única forma de fazê-lo é através do vale que está cercado por forças inimigas, onde a chance do mensageiro ser capturado é muito grande. O problema então é conseguir chegar a um algoritmo que permita concluir, em consenso, a hora certa de atacar a cidade em conjunto, pois só juntos venceriam a batalha.

Digamos que um dos generais envie a mensagem “ataque dia 26 de dezembro às 8h”. Esse general não saberá se a mensagem foi entregue, e evitará atacar por causa do risco de ser o único atacante. O segundo general poderia confirmar que recebeu a mensagem concordando

¹⁵ Veja Johnson et al (2014) e Vasek et al (2015).

com o ato, mas também não atacaria por não saber se essa mensagem chegou ao destinatário. Isso gera uma incerteza que nem um número infinito de confirmações conseguiria eliminar. Esse era o principal problema que redes descentralizadas enfrentavam e que o sistema Blockchain solucionou.

Quando Satoshi Nakamoto (2008) criou o processo de mineração, além de estar resolvendo um dos grandes problemas da computação, estava também criando uma rede descentralizada extremamente segura.

O sistema de mineração faz com que seja criada uma rede de confiança onde blocos são adicionados aos blocos anteriores através de um código *hash* específico para cada transação e bloco. Caso haja algum indivíduo tentando incluir uma informação incorreta em um bloco, o sistema vai verificar o código daquele bloco e dos blocos antecedentes e verificar de qual corrente ele foi originado. O bloco validado será o que veio da cadeia mais longa, ou seja, o bloco reconhecido será o da rede que tenha o maior poder computacional. Um fraudador para obter sucesso terá que alterar todos os blocos anteriores ao que ele está tentando fraudar, fazendo isso muito rapidamente e com mais poder computacional do que toda a rede que continua validando a cadeia de blocos originais. Dito de outra forma, o fraudador terá que ter mais poder computacional do que todo o resto do Blockchain.

O sistema Blockchain já se mostrou extremamente seguro, contudo ainda há fragilidades no uso do sistema por conta dos usuários e corretoras que são atacadas por *hackers*, como o caso da Mt. Gox entre muitas outras¹⁶. Todas essas fraudes ocorreram por descuido das corretoras. Uma pessoa com sua chave privada guardada em lugar seguro não tem como sofrer ataques como os sofridos pelas corretoras.

A descentralização do sistema Blockchain traz muita segurança, por si só. Uma entidade centralizada com milhões de informações de clientes, torna-se um alvo para que milhares de hackers em todo o mundo tentem invadir seus bancos de dados e roubar informações, como o ocorrido com a Target onde hackers invadiram seu sistema e roubaram informações de cartão de crédito e débito de 40 milhões de pessoas, expondo todos a fraudes¹⁷.

Como este trabalho foca nas transferências internacionais envolvendo instituições financeiras que investem milhões em segurança, tal problema tende a ser minimizado.

¹⁶ Para as 5 maiores fraudes consulte <https://coinsutra.com/biggest-Bitcoin-hacks/>. Acesso em 05/10/2018.

¹⁷ Disponível em <https://money.cnn.com/2013/12/22/news/companies/target-credit-card-hack/index.html>. Acesso em 25/11/2018.

3.4. Interface Pouco Amigável

O sistema Blockchain criado até o momento, ainda não levou em conta a experiência de usuários não técnicos. Os aplicativos de criptografia ainda parecem aplicativos de criptografia. Para uma adoção em massa, a infraestrutura Blockchain ainda precisa de melhorias semelhantes às que já ocorreram com a Internet. Acessamos à internet sem nos darmos conta de códigos HTML, Javascript, TCP/IP. Abrimos um aplicativo e a internet está lá ao clicar de um botão.

A demanda pela criação de ferramentas de gerenciamento de senhas privadas de forma fácil e segura é de fundamental importância para adoção em massa da população mundial. Mais à frente neste trabalho, veremos que o Santander em conjunto com a Ripple criou o aplicativo One Pay FX que traz uma interface amigável para transferências internacionais, via *smartphone*.

3.5. Regulação

A construção da solução Blockchain por Nakamoto (2008), veio como uma alternativa aos serviços financeiros de até então, que mesmo com toda a regulação existente não impediu que os Estados Unidos e o mundo mergulhassem numa crise financeira bastante severa, tendo sido motivada, principalmente, pela concessão de créditos hipotecários arriscados (*subprime*), através de ativos financeiros que mascaravam o risco de crédito.

Com a crise de 2008 ficou claro, como afirma Tapscot (2016), que a velocidade e a complexidade do sistema econômico global tornam a criação e a aplicação de leis de forma tradicional e centralizada cada vez mais ineficazes.

O Blockchain tende a suprimir essas falhas de regulação do passado, uma vez que todos que acessam o sistema tomam parte na vigilância deste, através do consenso. Mas quem vai regular o próprio Blockchain?

O Parlamento da União Europeia, reunido em 15 de maio de 2017 para discutir sobre regulação do Blockchain no bloco econômico, entende que é cedo para legislar sobre o sistema, por não saber sobre quais questões deve haver intervenção, correndo o risco de qualquer ato inicial sufocar a inovação¹⁸.

¹⁸ Disponível em <https://www.coindesk.com/regulating-ethereum-eu-parliament-weighs-blockchains-big-issues>. Acesso em 20/11/2018

O Banco Central do Brasil (BCB) ainda não iniciou nenhum processo de regulamentação de criptomoedas, limitando-se a disponibilizar em seu portal respostas para perguntas frequentes sobre “moedas virtuais”. Respondendo “não” à pergunta se o BCB regula as moedas virtuais. Cabe destacar que o BCB proíbe transferências internacionais utilizando moedas virtuais, orientando que transferências internacionais devem ser feitas por instituições autorizadas pelo Banco Central a operar no mercado de câmbio.¹⁹

A CVM (Comissão de Valores Mobiliários) em comunicado de 11/10/2017²⁰ esclareceu que certas operações de ICO²¹ (*Initial Coin Offering*) podem ser caracterizadas como operações com valores mobiliários, e, portanto, já sujeitas à legislação e à regulamentação vigente, citando o art. 2º, da lei 6.385/76²² onde clubes de investimento em qualquer ativo (V) quando ofertados publicamente (...), quaisquer outros títulos que gerem direito de participação (...) ou de remuneração (IX).

A CVM ainda emitiu um ofício²³ dando orientações para os administradores de fundos de investimento, afirmando que criptomoedas não são ativos financeiros considerados pela Instrução Normativa CVM 555. Proibindo assim que fundos de investimento tenham em suas carteiras ativos digitais.

A Receita Federal orienta²⁴ a inclusão de moedas virtuais na declaração de Imposto de Renda de Pessoa Física como “outros bens”, uma vez que podem ser equiparadas a um ativo financeiro e que ganhos obtidos com a alienação de moedas virtuais, com ganhos mensais superiores a R\$ 35 mil são tributados como ganhos de capital, à alíquota de 15% e o recolhimento do imposto sobre a renda deve ser feito até o último dia útil do mês subsequente.

A evolução da internet cresceu, em grande medida, pela ausência de regulação/restrições no seu início. A internet democratizou a informação ao passo que o Blockchain democratiza valor, não restando dúvida que deverá ocorrer um papel regulador para que consumidores sejam protegidos no futuro.

¹⁹ Disponível em https://www.bcb.gov.br/pre/bc_atende/port/moedasvirtuais.asp?idpai=FAQCIDADA0. Acesso em 20/11/2018.

²⁰ Disponível em <http://www.cvm.gov.br/noticias/arquivos/2017/20171011-1>. Acesso em 21/11/2018.

²¹ ICOs são captações públicas de recursos, tendo como contrapartida a emissão de ativos virtuais, junto ao público investidor. Semelhante ao IPO para mercado de ações.

²² Disponível em http://www.planalto.gov.br/ccivil_03/leis/L6385.htm. Acesso em 21/11/2018.

²³ Ofício Circular CVM/SIN 01/18 disponível em <http://www.cvm.gov.br/legislacao/oficios-circulares/sin/oc-sin-0118.html>. Acesso em 21/11/2018.

²⁴ Disponível em <http://idg.receita.fazenda.gov.br/interface/cidadao/irpf/2018/perguntao/perguntas-e-respostas-irpf-2018-v-1-0.pdf>. Acesso em 21/11/2018.

O Fórum Econômico Mundial previu que até 2027, 10% do PIB Mundial estará armazenado no Blockchain. Estamos falando de USD 8 trilhões²⁵.

As regulamentações de épocas anteriores legislavam sobre novos comportamentos ou até mesmo inovações que demoravam anos para serem implementadas e mais anos para que a população passasse a adotá-las em larga escala. Essas regulamentações funcionavam bem na era industrial. Hoje a situação é totalmente diferente. As mudanças estão ocorrendo de tal forma que o crescimento é exponencial. As entidades regulatórias não estão conseguindo se adaptar ou se adaptando muito devagar a todo o avanço da era digital. A disrupção da atualidade é tão profunda e rápida que está indo além da capacidade de indivíduos, governo e entidades regulatórias compreendê-las e preverem seus impactos.

Dada a proibição de transferências internacionais envolvendo moedas virtuais, sem que se utilize uma instituição financeira autorizada pelo Banco Central, a questão “regulação” não tende a impedir a utilização de Blockchain nas transferências internacionais utilizando algum banco. Devido a isso, este trabalho dará foco a iniciativas como a da Ripple (xRapid) e da IBM (IBM World Wire) que utilizam instituições financeiras para transferências internacionais através de sistemas construídos com a tecnologia Blockchain.

Dos problemas enfrentados para utilização do Blockchain listados até o momento, não se observou impedimentos sérios pelas soluções colocadas em questão. Mas ainda há um problema de grande importância para utilização do Blockchain para transferências internacionais: volatilidade. Dada a relevância do tema, o mesmo será tratado na próxima seção.

²⁵ Disponível em http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf. Acesso em 17/11/2018

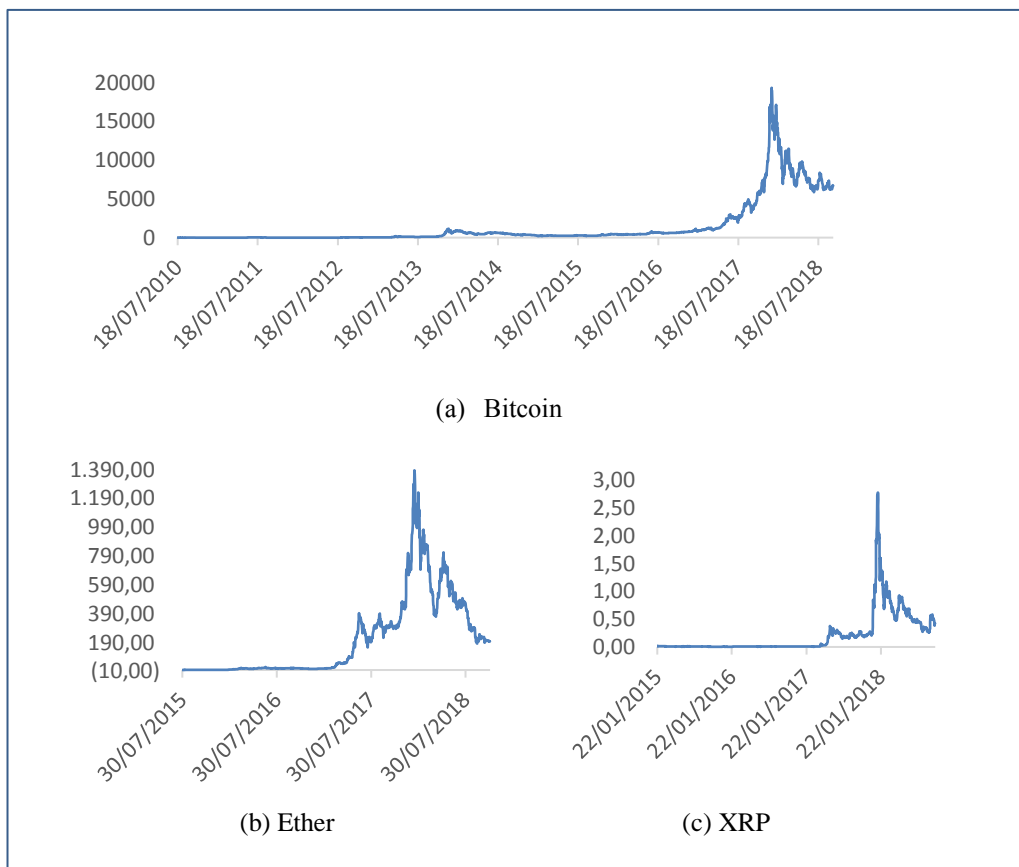
4. A VOLATILIDADE

4.1. Dados

As séries de dados dos preços das criptomoedas Bitcoin, Ether (Ethereum) e XRP (Ripple) foram extraídas do portal Coindesk²⁶. Coindesk usa um índice de preço para cada criptomoeda em dólares americanos, com a média das principais corretoras do mundo. Usando tais índices evitamos disparidades entre diferentes corretoras, mitigando o viés de escolher alguma *Exchange* específica.

O Bitcoin foi criado em 03/01/2009, o Ether em 01/08/2014 e o XRP em 01/07/2013. Optou-se por não buscar a série de dados desde a criação da moeda, por tratar-se de períodos iniciais com pouquíssima movimentação e valores insignificantes, onde há inclusive muitos dias sem precificação. Devido a isso para cálculo da volatilidade e regressão foram utilizadas as *ranges* de 18/07/2010 a 10/09/2018 para Bitcoin; de 09/08/2015 a 10/09/2018 para o Ether e de 01/02/2015 à 10/09/2018 para o XRP.

Figura 1 - Movimento dos Preços das 3 Principais Criptomoedas



²⁶ <https://www.coindesk.com/price>

Podemos observar claramente o aumento dos preços das três criptomoedas a partir do início de 2017, culminando no valor máximo no fim deste mesmo ano, para cair logo em seguida. Entretanto, a fase de maior estabilização dos últimos meses, estabeleceu-se em níveis mais elevados de preços.

Assim como Cermak (2017), e uma extensa literatura sobre cálculo de volatilidade de preços, acredita-se que preços são não-estacionários. Devido a isso, usar o *log return* faz os dados se tornarem normalizados e normalmente distribuídos. Os *log returns* são definidos como a primeira diferença do logaritmo natural dos preços, conforme equação abaixo:

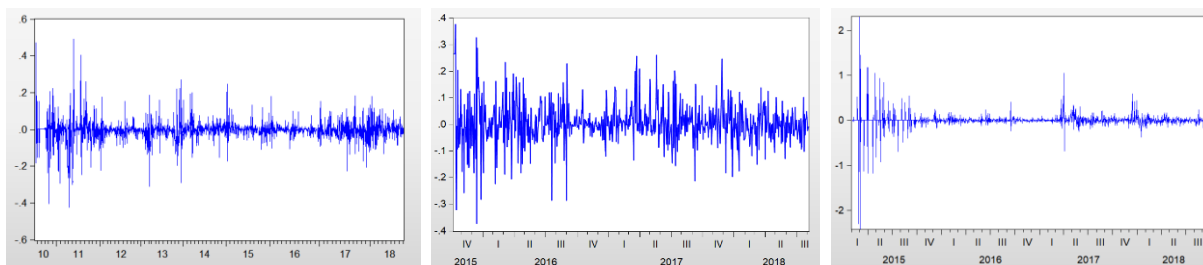
$$R_t = \ln(P_t) - \ln(P_{t-1}) \quad (1)$$

Onde:

R_t = log dos retornos no tempo t

P_t = preço da criptomoedas no tempo t

Figura 2 - *Log Return* - Bitcoin, Ether e XRP

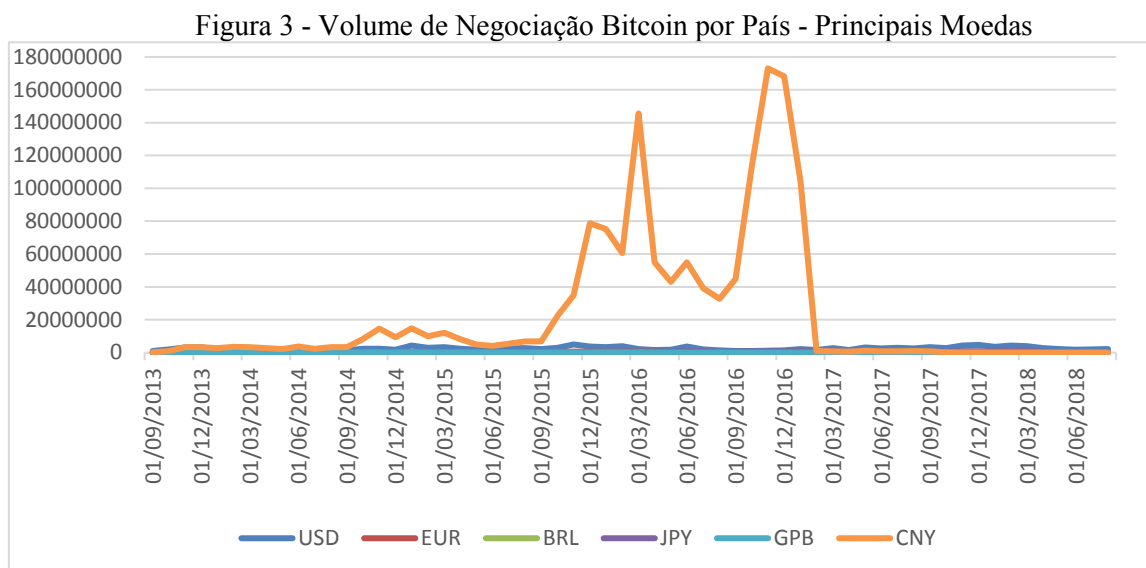


São muitos os fatores que afetam a taxa de câmbio de moedas fiduciárias, mas há certo consenso que variáveis macroeconômicas como taxa de juros, oferta de moeda nacional, exportação/importação, PIB, preço do petróleo, nível de protecionismo entre outros, afetam significativamente a taxa de câmbio²⁷.

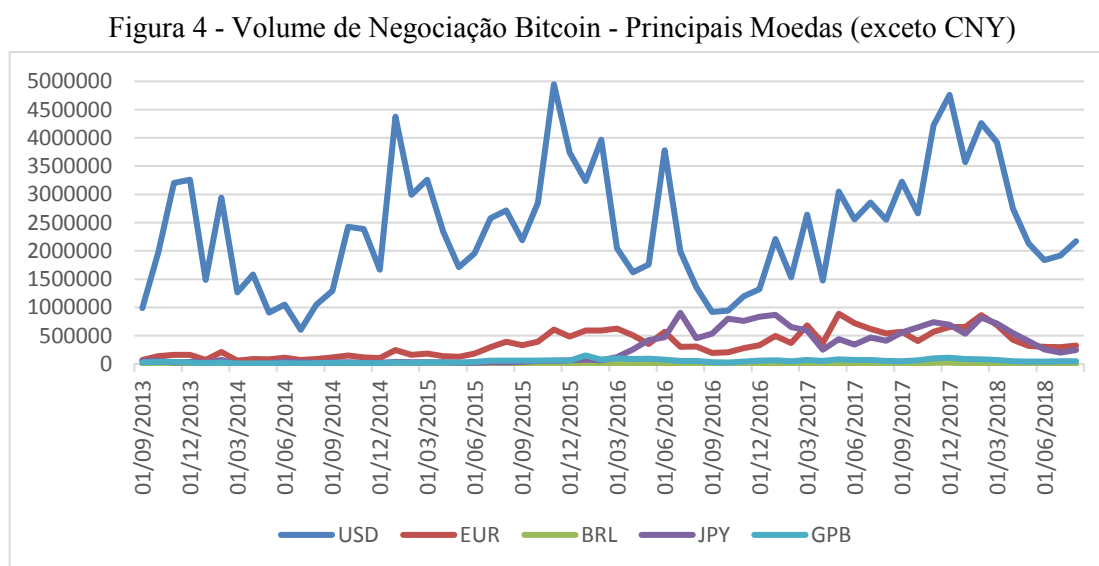
Tendo em vista as criptomoedas terem abrangência mundial, não faz sentido ter como referência um único país. Ao se pesquisar o volume de negociação das principais criptomoedas, tendo por base as moedas fiduciárias dos países, observa-se claramente um volume significativo

²⁷ (GRAW, 1988); (ANTONAKIS e DARBY, 2012).

da moeda chinesa (CNY), seguida, de longe, pelo dólar americano (USD), Euro (EUR) e a moeda japonesa (JPY), como demonstrado na figura abaixo:



Dado que o volume negociado pela China suplanta em muito o negociado por outros países, é necessário tirar a negociação em moeda chinesa (CNY) para ficar claro quais são os outros países que negociam criptomoedas.



Excluindo a moeda chinesa, desponta o dólar americano (USD) como a segunda moeda mais utilizada para negociar Bitcoin, seguida do Euro (EUR) e o Yen (JPY).

Com essas informações o modelo econométrico utilizará variáveis macroeconômicas da China, Estados Unidos, União Europeia (Alemanha) e Japão para estimar a volatilidade do Bitcoin, Ether e XRP.

Tendo em vista que as criptomoedas se assemelham ao ouro em determinados aspectos²⁸: quantidade limitada, fácil transporte e divisão, difícil falsificação, gasto de energia para obtenção (ambos são minerados, embora de forma bem diferentes), e alcance mundial; será usado o preço do ouro como controle para os modelos econométricos também.

Conforme Cermak (2017) os fatores macroeconômicos dos países escolhidos que são indicados para controle nos modelos econométricos para estudo da volatilidade das principais criptomoedas são a taxa de câmbio, o índice do mercado de ações e o *Bond* de 10 anos do título do governo.

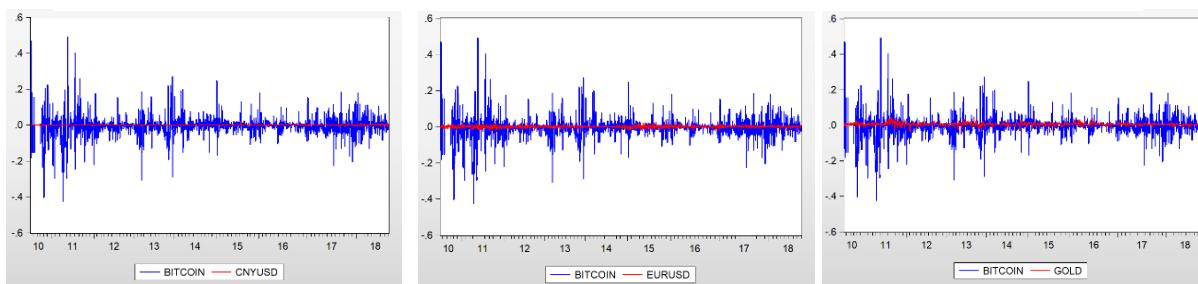
Tabela 1 - Variáveis Macroeconômicas Escolhidas

Variável	China	USA	Europa	Japão
Taxa de Câmbio	$\Delta \text{LnCNY}_{t-1}$		$\Delta \text{LnEUR}_{t-1}$	$\Delta \text{LnJPY}_{t-1}$
Índice do Mercado de Ações	$\Delta \text{LnShangayStock}_{t-1}$	$\Delta \text{LnSP500}_{t-1}$	ΔALEM_{t-1}	$\Delta \text{LnNIKKEI}_{t-1}$
Bond de 10 Anos	$\Delta 10\text{YRCHINA}_{t-1}$	$\Delta 10\text{YRUS}_{t-1}$	$10\text{YR}\Delta \text{ALEM}_{t-1}$	$\Delta 10\text{YRJAP}_{t-1}$

Dados extraídos do Federal Reserve Economic Data (FRED)²⁹ e Investing.com³⁰. Ao contrário das criptomoedas em que há negociação todos os dias, as variáveis macroeconômicas não apresentam dados para fins de semana e feriados.

Nas figuras a seguir, é demonstrada a volatilidade das criptomoedas Bitcoin, Ether e XRP em relação aos principais índices macroeconômicos escolhidos para se ter um parâmetro de comparação:

Figura 5 - Volatilidade Comparada de Bitcoin com Câmbio e Ouro



²⁸ Havendo inclusive artigos investigando se O Bitcoin pode ser considerado um novo tipo de Ouro, como análise de Klein et. Al de 2018: “Bitcoin is not the New Gold – A Comparison of volatility, correlation, and portfolio performance”.

²⁹ <https://fred.stlouisfed.org/>

³⁰ <https://www.investing.com/>

Figura 6 - Volatilidade Comparada de Bitcoin com Índice de Mercado de Ações

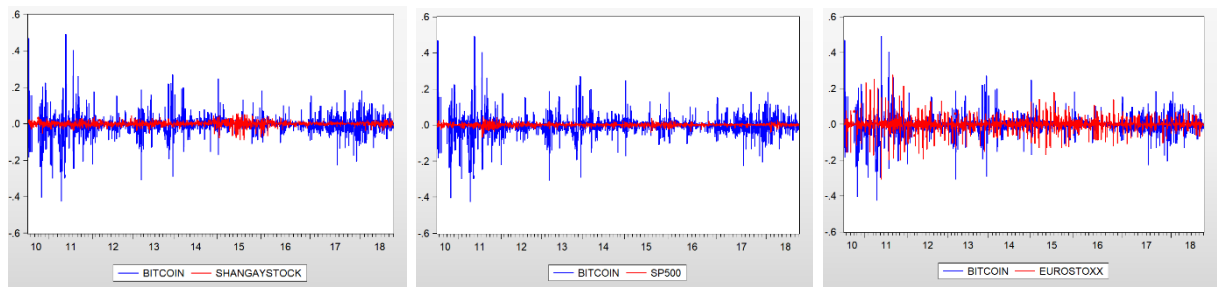


Figura 7 - Volatilidade Comparada de Bitcoin com *Bond* de 10 Anos

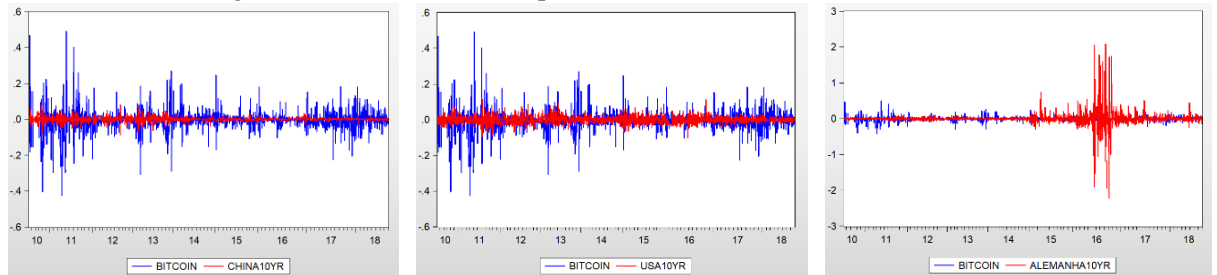


Figura 8 - Volatilidade Comparada de Ether com Taxa de Câmbio e Ouro

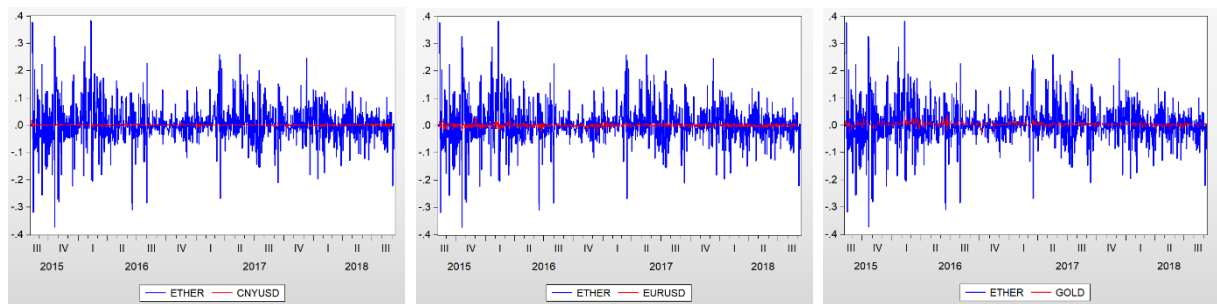


Figura 9 - Volatilidade Comparada de Ether com Índice de Mercado de Ações

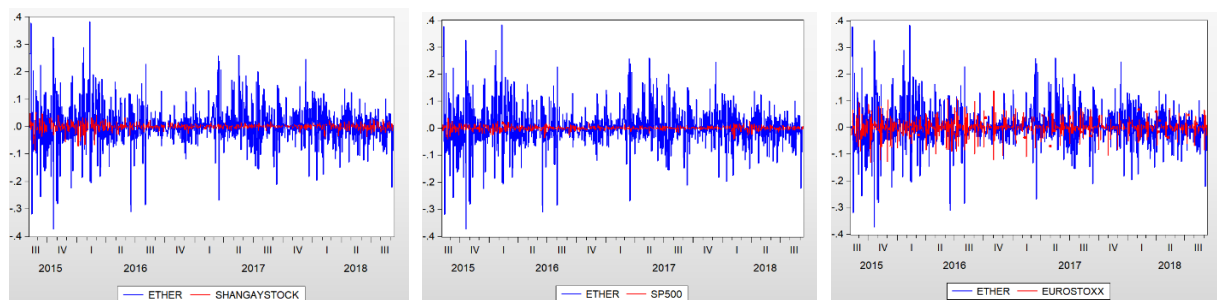


Figura 10 - Volatilidade Comparada de XRP com Câmbio e Ouro

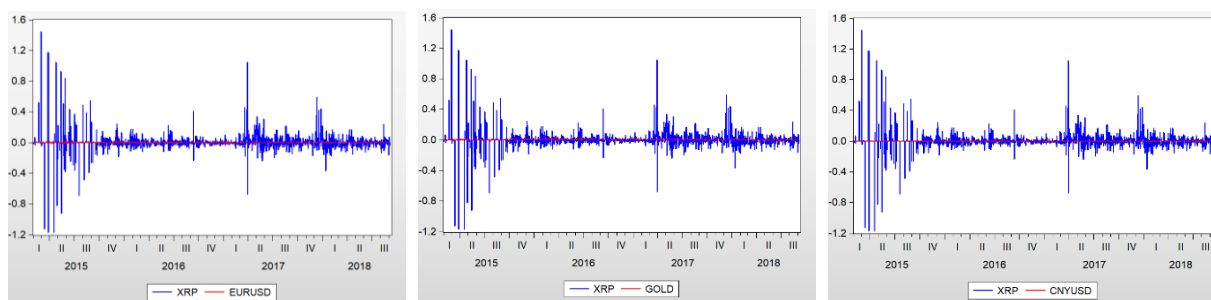
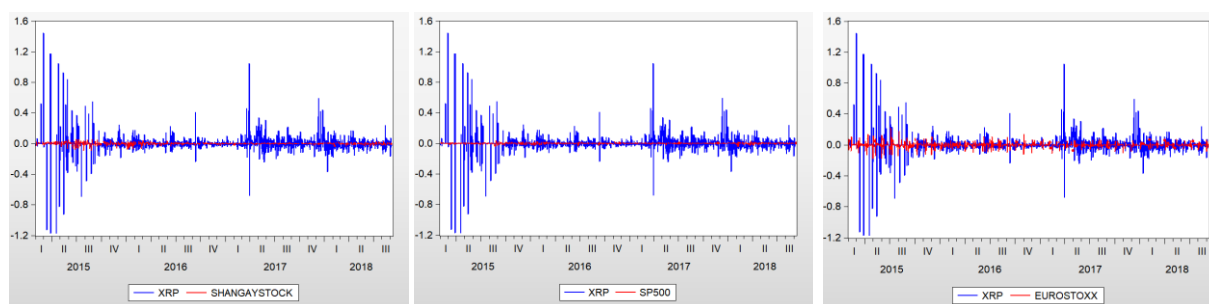
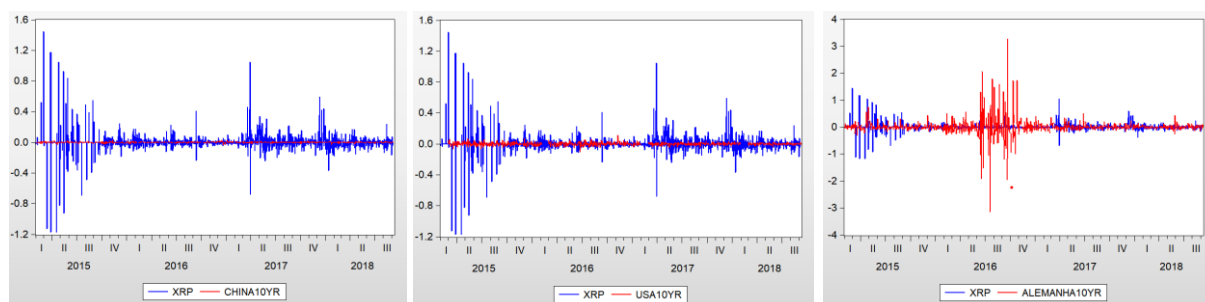


Figura 11 - Volatilidade Comparada de XRP com Índice de Mercado de Ações

Figura 12 - Volatilidade Comparada de XRP com *Bond* de 10 Anos

4.2. Metodologia

Há inúmeros modelos para estimar volatilidade de retornos financeiros, dentre esses os mais utilizados são os modelos auto regressivos com heterocedasticidade (ARCH – *Autoregressive Conditional Heteroskedasticity*) conforme proposto por Engle (1982) e sua extensão generalizada GARCH (*Generalized Autoregressive Conditional Heteroskedasticity*), proposta por Bollerslev (1986). O modelo GARCH leva em conta a volatilidade do período anterior e utiliza mínimos quadrados ponderados (WLS) para estimar a regressão, uma vez que a variância dos resíduos não é constante (heterocedástico) como é o caso do retorno do Bitcoin, Ether e XRP. O modelo GARCH então, transforma o método dos mínimos quadrados ordinários

(OLS) - que é usado em séries homocedásticas - em mínimos quadrados ponderados (WLS), usado em séries heterocedásticas.

No presente trabalho será usado mais especificamente o modelo GARCH (1,1) para buscar uma previsão do momento em que a volatilidade das principais criptomoedas chegará a um nível que seja possível utilizá-las como uma moeda ou um ativo financeiro.

Equação do GARCH, conforme Bollerslev (1986):

$$h_t = \alpha_0 + \alpha_1 \varepsilon_{t-1}^2 + \beta_1 \varepsilon_{t-1}^2 \quad (2)$$

Onde:

h_t = Variância condicional do período

α_0 = Variância média ponderada de longo prazo

ε_{t-1}^2 = Quadrado dos retornos dos resíduos do período anterior (termo ARCH)

ε_{t-1}^2 = Variância do período anterior (termo GARCH)

$\alpha_1 + \beta_1 < 1$ é a condição estacionária; $\alpha_1 > 0, \beta_1 > 0$

O modelo GARCH de ordem “p” e “q”, onde “p” significa quantos *lags* de retorno do resíduo e “q” quantos *lags* da variância. No caso em que será usado GARCH (1,1), o modelo levará em conta o retorno residual do período anterior, assim como a variância do período anterior. O modelo consiste de duas equações: a equação da média condicional e a equação da variância condicional.

Equação da Média Condicional (padrão):

$$r_t = \beta_0 + \beta_1 r_{t-1} + \varepsilon_t \quad (3)$$

Equação da Variância Condicional (padrão):

$$h_t = \alpha_0 + \alpha_1 \varepsilon_{t-1}^2 + \dots + \alpha_p \varepsilon_{t-p}^2 + \beta_1 \varepsilon_{t-1}^2 + \dots + \beta_q h_{t-q}^2 \quad (4)$$

Tendo em vista que queremos investigar se variáveis macroeconômicas afetam a volatilidade do Bitcoin, Ether e XRP, o modelo GARCH foi modificado para incluir essas variáveis de controle. A Equação da Média Condicional passa a ser como equação 4 abaixo:

$$\begin{aligned}
r_t = & \alpha_0 + \alpha_1 r_{t-1} + \alpha_2 \Delta \text{LnCNY}_{t-1} + \alpha_3 \Delta \text{LnEUR}_{t-1} + \alpha_4 \Delta \text{LnJPY}_{t-1} + \alpha_5 \Delta \text{LnGOLD}_{t-1} + \\
& \alpha_6 \Delta \text{LnShangayStock}_{t-1} + \alpha_7 \Delta \text{LnSP500}_{t-1} + \alpha_8 \Delta \text{LnALEM}_{t-1} + \alpha_9 \Delta \text{LnNIKKEI}_{t-1} + \\
& \alpha_{10} \Delta 10\text{YRCHINA}_{t-1} + \alpha_{11} \Delta 10\text{YRUSA}_{t-1} + \alpha_{12} 10\text{YR}\Delta \text{ALEM}_{t-1} + \alpha_{13} \Delta 10\text{YRJAP}_{t-1} + \varepsilon_t
\end{aligned} \quad (4)$$

O cálculo da equação da variância modificada será feito utilizando os seguintes parâmetros:

$$\begin{aligned}
h_t^2 = & \exp (\beta_0 + \beta_1 r_{t-1} + \beta_2 \Delta \text{LnCNY}_{t-1} + \beta_3 \Delta \text{LnEUR}_{t-1} + \beta_4 \Delta \text{LnJPY}_{t-1} + \beta_5 \Delta \text{LnGOLD}_{t-1} + \\
& \beta_6 \Delta \text{LnShangayStock}_{t-1} + \beta_7 \Delta \text{LnSP500}_{t-1} + \beta_8 \Delta \text{LnALEM}_{t-1} + \beta_9 \Delta \text{LnNIKKEI}_{t-1} + \\
& \beta_{10} \Delta 10\text{YRCHINA}_{t-1} + \beta_{11} \Delta 10\text{YRUSA}_{t-1} + \beta_{12} \Delta 10\text{YRALEM}_{t-1} + \beta_{13} \Delta 10\text{YRJAP}_{t-1}) + \\
& \omega_1 \varepsilon_{t-1}^2 + \varphi_1 h_{t-1}^2 + \varepsilon_t
\end{aligned} \quad (5)$$

Segundo Cermak (2017), há duas pré-condições que devem ser investigadas para se estimar o modelo GARCH (1,1): i) volatilidade de agrupamento e ii) efeito ARCH no resíduo. Para a primeira pré-condição os agrupamentos de volatilidade são mostrados nas figuras 14, 15 e 16 abaixo, respectivamente para Bitcoin, Ether e XRP. A figura mostra, para as 3 criptomoedas, que períodos de baixa volatilidade dos resíduos são seguidos de baixa volatilidade e vice-versa, ou seja, altos retornos são seguidos de altos retornos e baixos retornos são seguidos de baixos retornos; comprovando tratar-se de agrupamentos de volatilidade, o que significa que os resíduos são heterocedásticos. Devemos avaliar agora o efeito ARCH no resíduo.

Figura 13 - Teste de Agrupamento de Volatilidade nos Resíduos – Bitcoin

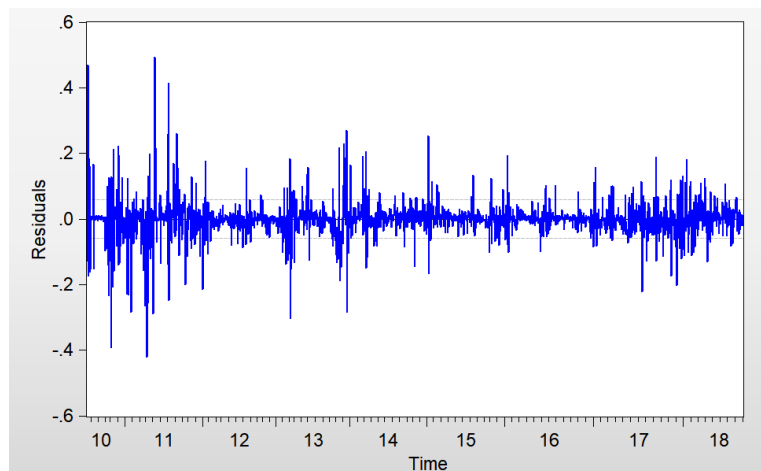


Figura 14 - Teste de Agrupamento de Volatilidade nos Resíduos - Ether

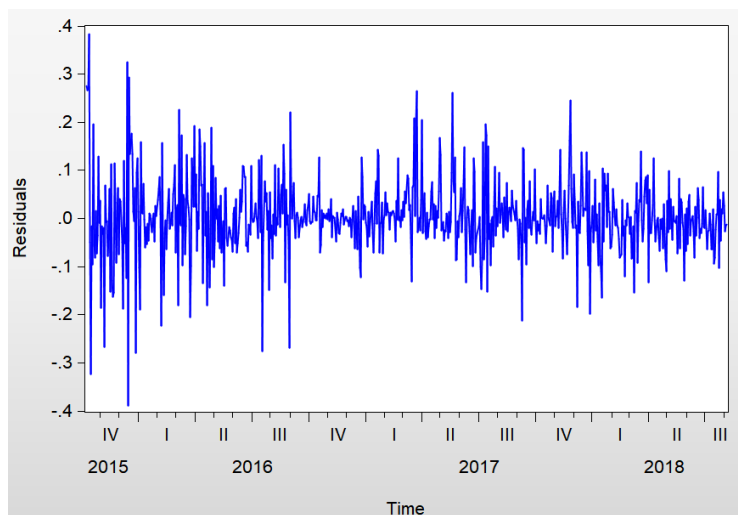
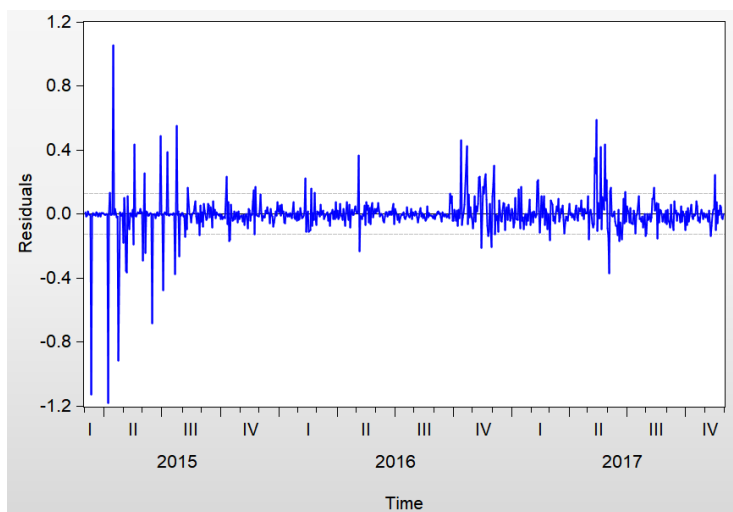


Figura 15 - Teste de Agrupamento de Volatilidade nos Resíduos – XRP



Para determinar se há um efeito ARCH no resíduo, ou seja, se há correlação serial da heterocedasticidade, conduzimos um LM ARCH *test*³¹. Com a hipótese nula que não existe efeito ARCH, contra a hipótese alternativa de que existe.

Tabela 2 - Teste LM ARCH

	Lags(p)	Chi2	df	Prob > Chi2
Bitcoin	1	105,5564	1	0,0000
Ether	1	102,0594	1	0,0000
XRP	1	23,11087	1	0,0000

H0: Sem efeito ARCH vs. H1: Caso Contrário

³¹ LM ARCH vem de Lagrange Multiplier ARCH. Um teste para verificar a heterocedasticidade condicional nos resíduos (Engle, 1982). Este teste começou a ser feito a partir da observação que em muitas séries financeiras a magnitude dos resíduos parecia estar relacionada com resíduos anteriores.

Os resultados mostrados na Tabela 2, mostram uma forte evidência que existe um efeito ARCH, o que nos permite rejeitar a hipótese nula. Com este segundo resultado podemos afirmar que as pré-condições foram atendidas e podemos utilizar o Modelo GARCH (1,1).

Segundo Cermak (2017) o ponto importante no modelo GARCH é a soma de α e β , que nos dá o parâmetro de persistência, o qual nos diz o quão rápido as altas volatilidades decaem após um choque.

4.2.4. Análise Descritiva

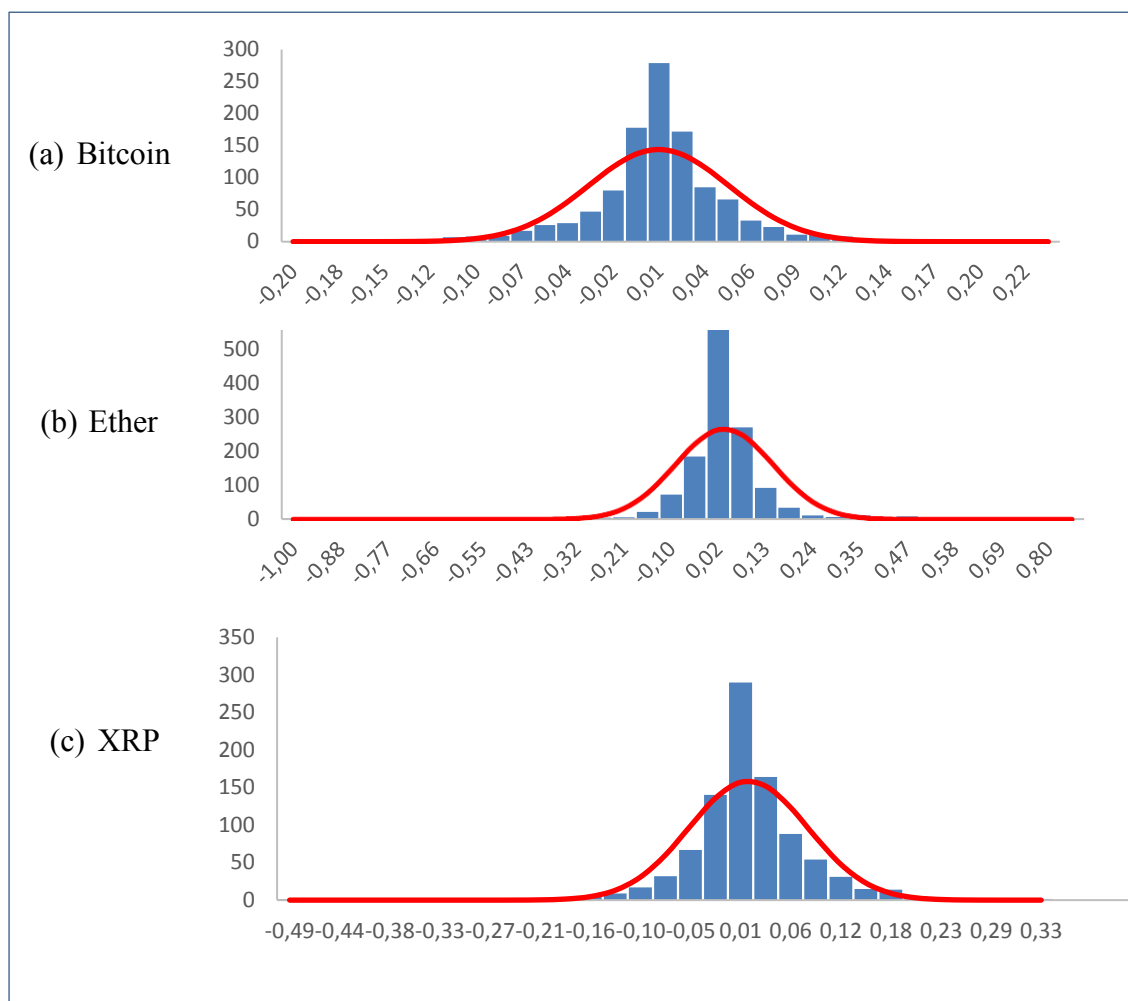
Tabela 3 - Resumo das Estatísticas

Variável	N	Média	Desvio Padrão	Mínimo	Máximo	Amplitude
Preço Bitcoin	1113	3632,75	3987,27	0,00	19187,00	19187,00
Preço Ether	1191	211,60	278,66	0,05	1385,02	1384,97
Preço XRP	1362	0,21	0,37	0,00	2,78	2,78
CNY/USD	1023	0,15	0,01	0,14	0,16	0,02
EUR/USD	1002	1,13	0,05	1,04	1,25	0,21
JPY/USD	1200	0,0089	0,0005	0,0080	0,0100	0,0020
Gold (USD)	930	1235,11	74,01	1050,60	1370,00	319,40
S&P 500	961	2302,72	280,30	1829,08	2914,04	1084,96
Shangay Stocks	901	3279,36	420,67	2655,66	5166,35	2510,69
Euro Stoxx	952	3341,27	246,35	2680,35	3828,78	1148,43
Nikkei	972	19596,76	2179,46	14952,02	24270,62	9318,60
USA 10YR	1183	2,27	0,42	1,36	3,23	1,88
China 10YR	982	3,38	0,37	2,66	4,07	1,41
Alemanha 10YR	1067	0,38	0,22	-0,18	0,99	1,17
Japão 10YR	1055	0,11	0,16	-0,29	0,53	0,83

Documentando as principais propriedades estatísticas das séries de tempo dos preços e dos retornos de Bitcoin, Ether e XRP, obtivemos algumas informações importantes para análise da volatilidade das criptomoedas

Quando analisamos a distribuição dos retornos, tendo a Curva Normal como parâmetro de comparação, verificamos o quão altas são as volatilidades.

Figura 16 - Distribuição dos Retornos



A volatilidade dos preços é uma das grandes fraquezas das criptomoedas. Por exemplo, no final de novembro de 2018, havia aproximadamente 16.250.000 Bitcoins em existência, com um valor da criptomoeda de 4.084 dólares americanos. Isso significa que o valor de mercado Bitcoin é de aproximadamente 72,4 bilhões de dólares, o que ainda é relativamente baixo quando comparado a moedas fiduciárias. Devido ao pequeno valor de mercado do Bitcoin, é fácil afetar o preço com grandes demandas de compra ou venda, tornando a moeda de natureza ainda bastante especulativa, onde sua volatilidade de preço é afetada principalmente por eventos, como fraudes em corretoras ou proibições de uso por determinados países. Os investidores reagem a esses eventos de forma positiva ou negativa, o que muitas vezes provoca uma venda em pânico ou compra em um movimento de manada. As grandes variações de preço são causadas principalmente pelas súbitas regulamentações governamentais e violações de segurança das carteiras de terceiros.

4.2.5. Resultados

A partir dos dados de volatilidade dos índices macroeconômicos dos países/regiões escolhidos e da volatilidade do Bitcoin, Ether e XRP; buscou-se estimar se a volatilidade do dia anterior seria estatisticamente significativa para explicar a volatilidade do dia seguinte (GRONWALD, 2014).

A China apresenta situação atípica, uma vez que vinha sendo o maior comerciante de criptomoedas do mundo, utilizando sua moeda fiduciária (CNY) para comprar ativos digitais até início de 2017, quando houve proibição pelo governo chinês. Dessa forma, a China tinha o maior peso no impacto do preço das criptomoedas até início de 2017, passando a não mais ter esse peso desde então.

Cemark (2017) faz um primeiro estudo comparando índices macroeconômicos com a volatilidade do Bitcoin, com a ideia de verificar se movimentos nos índices macroeconômicos nos países onde mais se comercializa Bitcoin, afetariam a volatilidade desse ativo digital. A confirmação de tal impacto, pode ser um forte indício que essa criptomoeda começa a se comportar como uma moeda tradicional.

No presente trabalho amplia-se o período de estudo incluindo todo o ano de 2017 e quase todo o ano de 2018. Há uma ampliação também das criptomoedas estudadas, fazendo análise do Ether e XRP, além do Bitcoin.

Foram escolhidas Bitcoin, XRP e Ethereum (Ether) por elas representarem 61,49% das 100 maiores criptomoedas listadas no Coinmarketcap³², e também porque as três reúnem características muito semelhantes às outras criptomoedas, podendo assim admitir, que o resultado encontrado neste estudo pode ser aplicado às demais criptomoedas³³.

³²Disponível em <https://coinmarketcap.com/pt-br/all/views/all/>. Acesso em 25/11/2018.

³³ No momento da pesquisa havia 2071 criptomoedas ativas.

Como era esperado, a equação média mostra que a maioria das variáveis explicativas não são estatisticamente significantes - com *lag* de 1 período - para as três criptomoedas, pois caso fossem estatisticamente significantes, seria possível que os agentes arbitrassem. No caso do Euro Stoxx, onde mostra-se significativo para o Bitcoin e Ether a 5%, em regressões feitas separadamente não se mostrou significância. Portanto, podemos concluir, que nenhuma das variáveis de um período são significantes para prever o período seguinte. Tal conclusão é semelhante à encontrada por Cemark (2017) para o Bitcoin.

Na equação da variância, por outro lado, a maioria das variáveis mostra-se estatisticamente significativa, indicando que o retorno de uma criptomoeda em um dia impacta a volatilidade da mesma no dia seguinte. Da mesma maneira, a volatilidade do dia anterior impacta a volatilidade do dia atual; sinalizando que a volatilidade passada pode ser usada para prever volatilidade futura. Na regressão do Bitcoin o câmbio da moeda chinesa não se mostrou significativa devido ao fato que a China, de 2010 a 2016, negociava Bitcoin com sua moeda (CNY) e a partir de 2017 proibiu seu uso. Dessa forma a regressão pegou muitos anos de uso da moeda com baixa movimentação, e excluiu os dois últimos anos de maior movimentação. Fazendo a regressão de 2010 a 2017, o regressor torna-se estatisticamente significativo. O *Bond* de 10 anos do Japão e da Alemanha não se mostraram significativos, a 5%, em nenhuma das criptomoedas. Era esperado que índices macroeconômicos do Japão tivessem pouco impacto uma vez que o crescimento de negociação com criptomoedas tenha começado realmente há menos de 2 anos, vide figura 5. No caso dos *Bonds* de 10 anos da Alemanha, percebe-se pouca relação com criptomoedas e significativa volatilidade por causas próprias, como pode ser visto nas figuras 8 e 13.

Quando se percebe a Variância Condicional, outra informação se confirma: a volatilidade das criptomoedas vem se reduzindo com o passar dos anos. Utilizando como referência para comparação o índice VIX³⁴ e descartando os dois primeiros anos de atividade das criptomoedas³⁵, percebe-se claramente a variância condicional das criptomoedas se comportando abaixo dos 4% na maioria dos anos, semelhante ao que ocorre no índice VIX. Adicionando uma linha de tendência para prever o nível de volatilidade futura, tendo por base os últimos anos, as criptomoedas tendem a ter o mesmo nível de volatilidade das moedas tradicionais por volta de 2019-2020. É bem verdade que qualquer evento negativo que envolva segurança nas *Exchanges*, por exemplo, pode levar a previsão de volatilidade para mais alguns

³⁴ O índice VIX (*Volatility Index*) mede a volatilidade das opções de ações do S&P 500. É considerado como "medidor de medo" do mercado.

³⁵ Para Bitcoin: 2010-2012. Para Ether e XRP: 2014-2015

anos à frente, contudo é inquestionável que a volatilidade vem diminuindo com os anos e essa redução de variabilidade tende a tornar os ativos digitais mais apropriados para transações internacionais.

Figura 17 - Variância Condicional – Criptomoedas e VIX

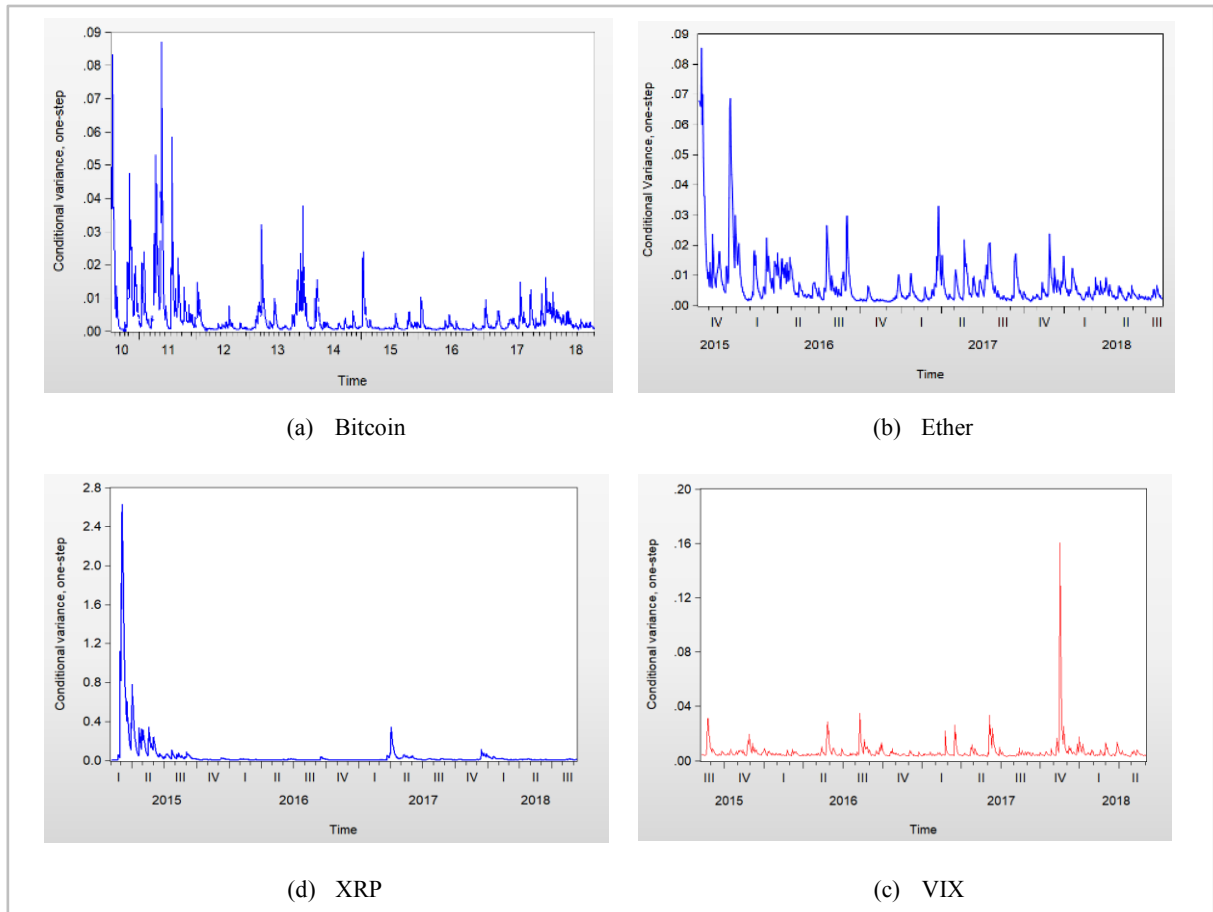


Figura 18 - Tendência Variância Condicional – Bitcoin

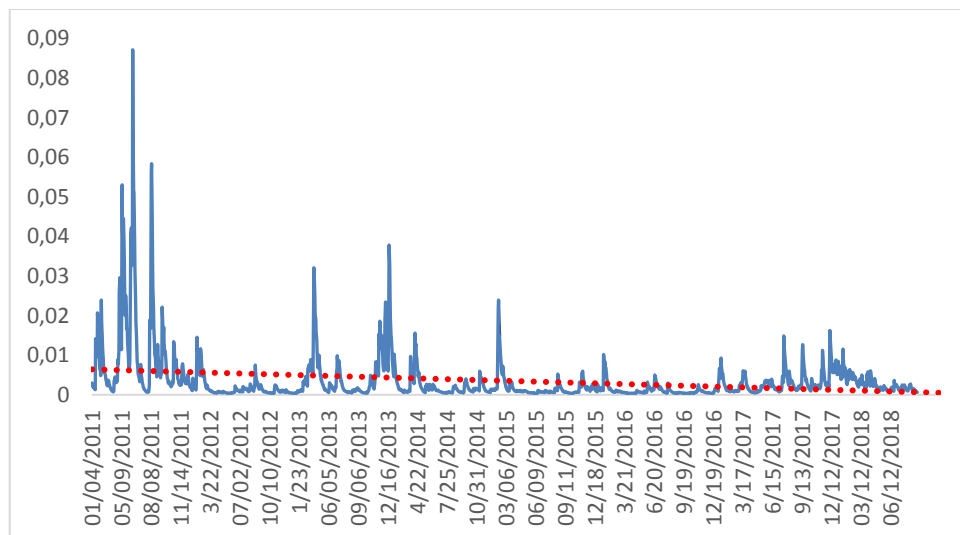


Figura 19 - Tendência Variância Condicional – Ether

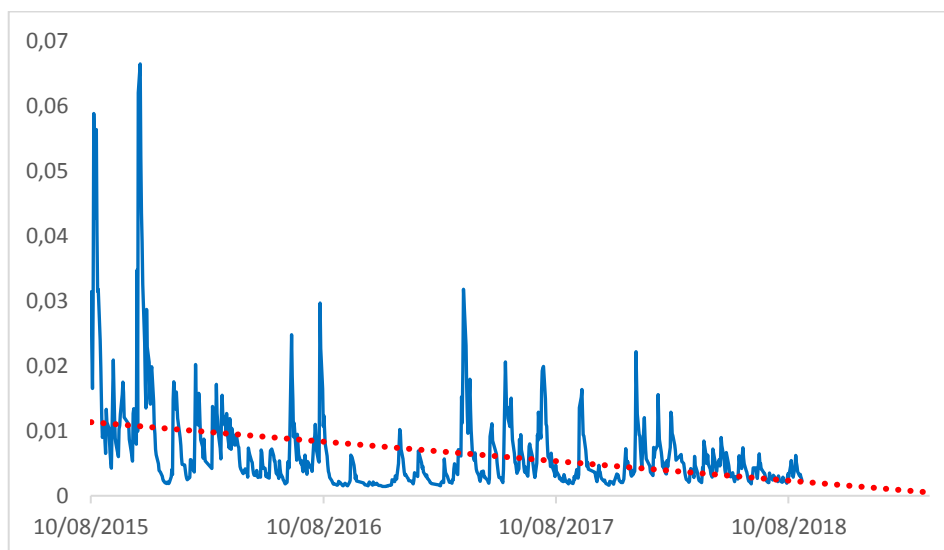
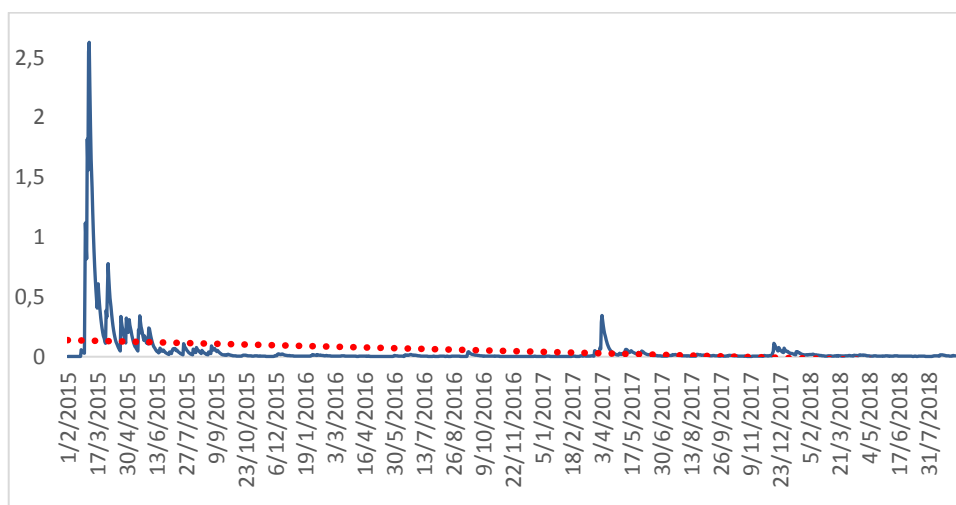
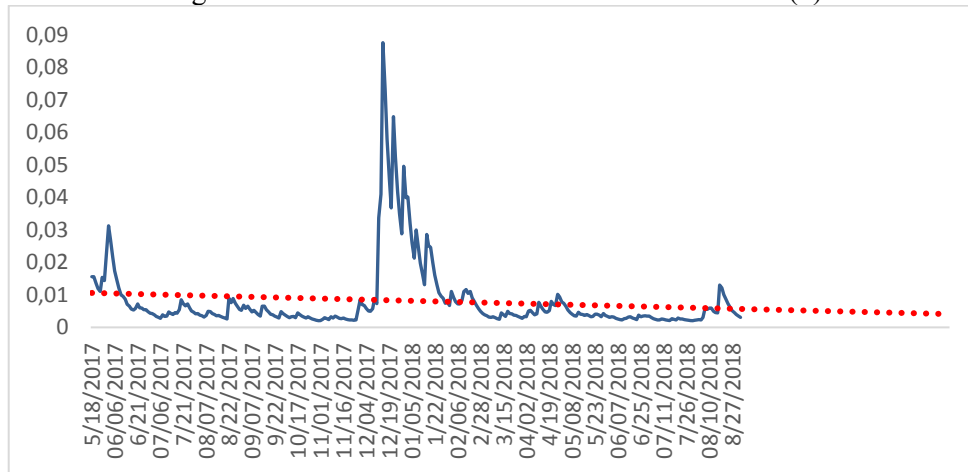


Figura 20 - Tendência Variância Condicional – XRP (a)



Tendo em vista que no início da série de variância do XRP (a) há uma volatilidade muito significativa, e que esta não voltou a se repetir com tamanha magnitude no restante da série, torna-se importante ter um outro recorte da série (b), a partir de 2017, que passa a ficar na mesma escala das outras criptomoedas.

Figura 21 - Tendência Variância Condicional - XRP (b)



A principal razão para a diminuição da volatilidade das criptomoedas é o aumento de detentores de criptomoedas no mundo, conforme o volume de criptomoedas em existência e circulação aumentam. Outro fator que ajuda a limitar a volatilidade das criptomoedas é um surgimento das bolsas de derivativos de Bitcoin onde os clientes podem fazer *hedge* ou vender suas posições a descoberto usando contratos futuros.

Figura 22 - Usuários Ativos e Volatilidade Bitcoin

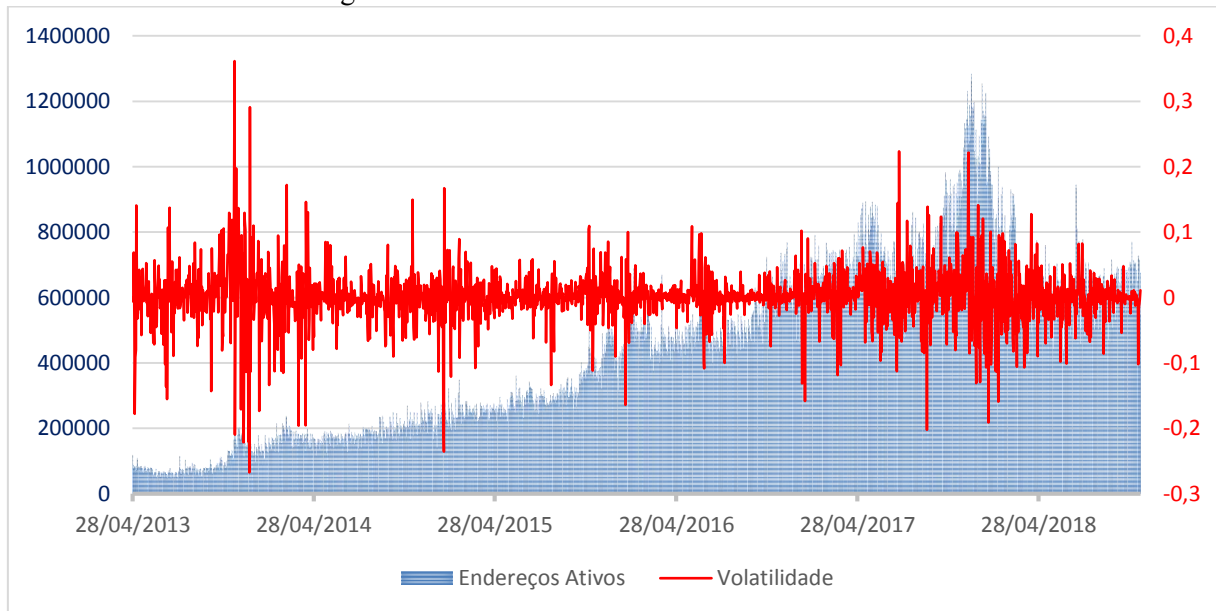


Figura 23 - Usuários Ativos e Volatilidade - Ether

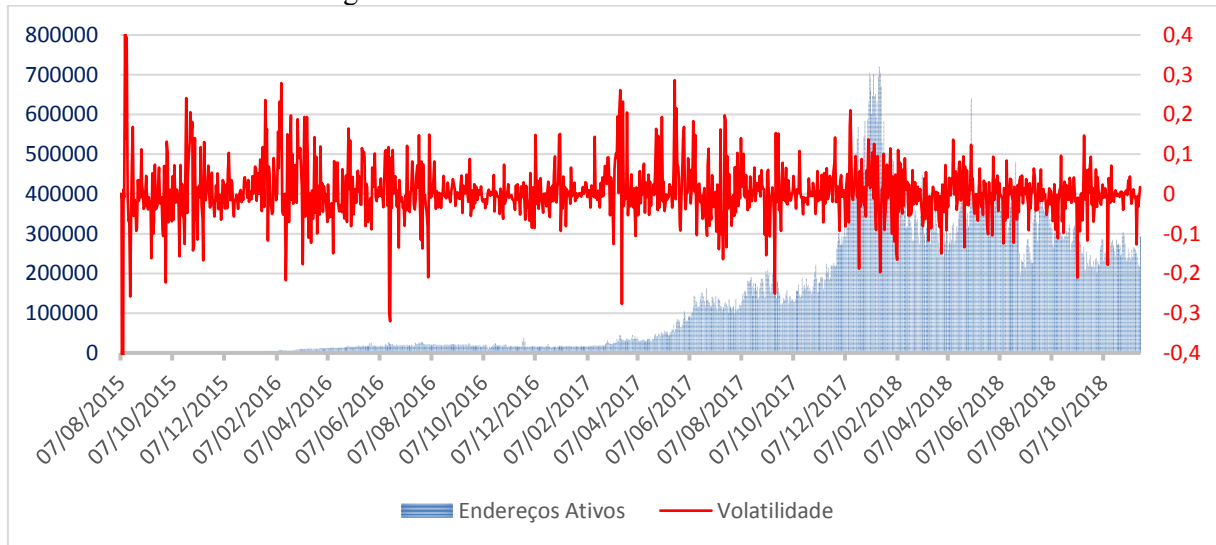
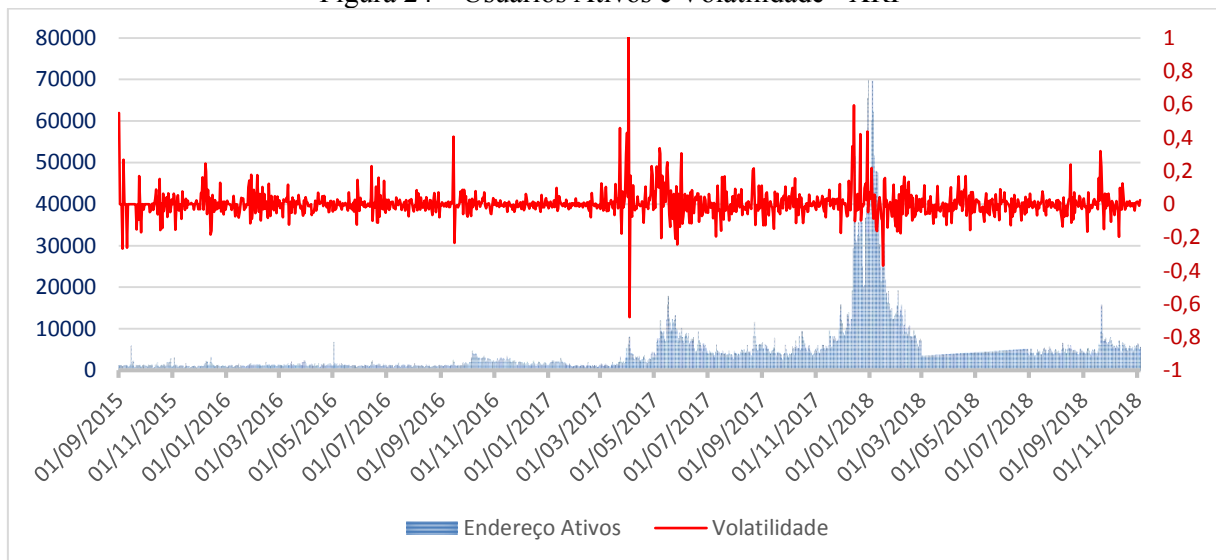


Figura 24 – Usuários Ativos e Volatilidade - XRP



5. SWIFT VS. SOLUÇÕES BLOCKCHAIN

Vimos até o momento que criptomoedas tendem a continuar diminuindo sua volatilidade nos próximos anos, e com isso, transferências internacionais, usando esses ativos digitais no Blockchain, passam a ser uma via bastante interessante, tendo em vista a segurança, agilidade e sensível redução de custos. Devido a isso, torna-se interessante comparar as diferenças entre o sistema amplamente utilizado no mundo há décadas com novas soluções utilizando Blockchain. Adotaremos os dados Banco do Brasil como *proxy* para as simulações.

Tabela 8 - Os 10 Maiores Volumes de Transferências para o Exterior (USD) – Nov/2017 a Out/2018

Ord.	Nome da Instituição	Qtde.	Valor	Ord.	Nome da Instituição	Qtde.	Valor
1	Citibank	117.038	89.476.473.013	1	Itaú Unibanco	375.945	46.910.189.190
2	Santander Brasil	350.657	70.748.557.319	2	Banco do Brasil	367.357	32.722.915.879
3	Bradesco	327.450	65.387.815.680	3	Santander Brasil	350.657	70.748.557.319
4	J. P. Morgan	23.292	55.618.297.180	4	Bradesco	327.450	65.387.815.680
5	Itaú Unibanco	375.945	46.910.189.190	5	MS Banco de Câmbio	305.738	1.202.188.070
6	Banco do Brasil	367.357	32.722.915.879	6	Citibank	117.038	89.476.473.013
7	Bank of America	21.144	24.772.034.867	7	Rendimento Banco	66.213	1.939.007.405
8	Societe Generale Brasil	4.506	20.749.328.433	8	Cotação Dist. de Títulos	62.959	728.337.415
9	BNP Paribas Brasil	19.368	18.521.593.408	9	Advanced Corretora	51.035	437.132.987
10	Morgan Stanley	6.157	12.004.512.684	10	Confidence Corretora	47.031	702.231.859

(a) Qtde.

(b) Valor

5.1. SWIFT

Os pagamentos internacionais atualmente se utilizam quase que em sua totalidade do sistema SWIFT (*Society for Worldwide Interbank Financial Telecommunication*). Um sistema de mensageria criado por um consórcio de bancos em 1973, que permite que instituições financeiras emitam instruções seguras entre elas em mais de 210 países. Por tratar-se de um serviço de mensagens, há necessidade de os bancos manterem contas³⁶ uns com os outros ou se utilizar de intermediários (uma vez que seria ainda mais oneroso ter conta em todos os países), o que torna o serviço lento, complexo, caro e sujeito a erros. Há ainda o enorme custo de oportunidade de ter que deixar recursos financeiros em bancos correspondentes para prover liquidez.

A fragmentada rede de pagamentos envolvendo milhares de bancos e correspondentes bancários ao redor do mundo é extremamente complexa. A SWIFT ajudou a organizar essa rede na década de 1970 com seu serviço de mensageria padronizada/normatizada, reduzindo o tempo

³⁶ Chamadas de Contas “*Nostro*” ou “*Vostro*”

de liquidação de um pagamento internacional de semanas para um intervalo de 3 a 5 dias. Contudo, há riscos de contrapartes ³⁷ (um dos bancos pode falir nesse meio tempo). Com a liquidação imediata de pagamentos transnacionais o risco de contraparte desaparece. Já há sistemas de liquidação imediata entre países como no caso da Europa com Target-2³⁸, criado pelo Banco Central Europeu e no Reino Unido com o Chapps³⁹ (*Clearing House Automated Payment System*) de responsabilidade do Banco da Inglaterra e com mais de 5000 instituições financeiras se utilizando do sistema, mas todas utilizando da mesma moeda fiduciária.

O sistema SWIFT funciona transferindo mensagens em ambiente seguro através de um sistema de códigos conhecidos como BIC (*Bank Identifier Code*) com 11 caracteres, onde os primeiros 4 caracteres são para designar a instituição financeira; os próximos 2 caracteres destinam-se ao código do país; os 2 caracteres seguintes são destinados ao código da cidade e o número da agência preenche últimos 3 caracteres. No caso de um envio de uma remessa do exterior para o Brasil, o Código BIC de destino pode ser BRASBRRJADR onde BRAS é o código do Banco do Brasil, BR é o código do Brasil; RJ é o código da cidade do Rio de Janeiro e ADR é o código da agência.

O sistema que trouxe padronização nos pagamentos internacionais sofreu pouca modificação em 45 anos, desde que foi implementado. Mesmo com o sistema de códigos, há muitos erros e falhas nas transferências internacionais, com custos elevados para reconciliação de lançamentos. Sem contar a necessidade de os bancos terem contas em outros bancos onde queira disponibilizar transferências para seus clientes, uma vez que a SWIFT é responsável apenas pelo serviço de mensageria.

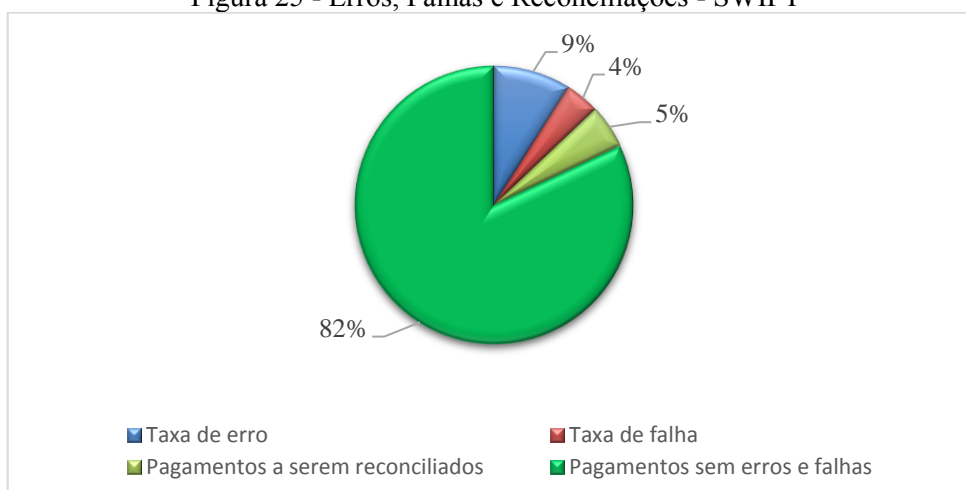
Em entrevista com representantes da Ripple, obtivemos a estimativa de custos para conciliação de pagamentos internacionais via SWIFT:

³⁷ Também chamado de Risco de Liquidação ou “Herstatt Risk” (devido ao caso da não liquidação de operações de câmbio pelo banco alemão Herstatt na década de 1970).

³⁸ Disponível em <https://www.ecb.europa.eu/paym/t2/html/index.en.html>. Acesso em 18/10/2018

³⁹ Disponível em <https://www.bankofengland.co.uk/payment-and-settlement/chaps>. Acesso em 18/10/2018

Figura 25 - Erros, Falhas e Reconciliações - SWIFT



Percebe que de todas as remessas processadas num dia, 9% são pagamentos que precisam ser reparados devido a entradas incorretas; 4% são lançamentos que não podem ser reparados e são devolvidos e 5% dos lançamentos são reconciliados, ou seja, exigem esforço de conciliação manual, após a demonstração do saldo da conta *nostro* no final do dia. Com uma média de 18% de erros, falhas e reconciliações nas remessas, são gastos cerca de 20 minutos para reconciliar cada lançamento.

Outro importante componente na estrutura de custos envolve o custo de oportunidade para prover a liquidez em contas internacionais e tarifas de contraparte. Estima-se em 50% o fluxo de pagamentos lançados em todo o sistema; 0,05% de custos na operação de câmbio na mesa de operações; 2% de taxa que a contraparte cobra para receber um pagamento e 2 dias, no mínimo, de float que os recursos precisam ficar na conta *nostro* para processamento dos pagamentos.

Tendo por base o volume de transações internacionais feitas pelo Banco do Brasil, conforme Tabela 8 anterior e aplicando os custos acima discriminados obtemos um valor de custos de USD 148,07 por pagamento no Banco do Brasil.

Tabela 9 - Custos por Pagamento - SWIFT

Custos	Valor (USD)
Taxas de Contraparte	2,00
Reconciliação	56,85
Tesouraria	84,49
Processamento	4,73
Total	148,07

5.2. IBM Blockchain World Wire

A IBM construiu sua solução para transferências internacionais utilizando Blockchain, chama-se IBM Blockchain World Wire. Tirando os intermediários que são utilizados pela SWIFT e unindo mensageria e transferência efetiva de recursos, a solução Blockchain da IBM promete fazer pagamentos internacionais em segundos com segurança e transparência.

As transferências ocorrem entre duas instituições financeiras que escolhem um ativo digital que servirá como ponte entre as duas moedas fiduciárias dos países envolvidos. A conexão do Blockchain IBM com as instituições financeiras é feita através de APIs⁴⁰ (*Application Programming Interface*) que convertem as moedas fiduciárias no envio e no recebimento dos recursos financeiros. Registrando todos os lançamentos e detalhes da operação em um Blockchain imutável.

A IBM traz como principal tecnologia a Stellar Lumens⁴¹ que além da criptomoeda Stellar (XLM) que está na quarta colocação em valor de mercado entre as criptomoedas (vide Tabela 4), também disponibiliza *stablecoins*⁴² como a Stronghold. Trabalhar com uma criptomoeda lastreada no dólar como é o caso da Stronghold pretende solucionar a questão da volatilidade que, conforme seção anterior, pretende atingir níveis mais estáveis para os próximos anos.

A IBM traz larga experiência em suporte computacional ao setor bancário e de pagamentos mundial, onde 97% dos maiores bancos do mundo são clientes da IBM e 90% das transações globais de cartão de crédito são processados em mainframes IBM⁴³. Além disso, traz parceiros como Stellar e Stronghold que possuem ativos digitais, retirando desconfiças sobre a manipulação dos ativos digitais quando a própria empresa tem ligação com a criptomoeda como é o caso da Ripple com a XRP.

De acordo com dados de consultoria da Forrester, o investimento na solução pode trazer 43% de retorno sobre investimento e retorno do investimento em 3 anos, conforme tabela abaixo:

⁴⁰ Padrões estabelecidos por um software para que outros aplicativos utilizem suas funcionalidades. Um bom exemplo é aplicativo da Uber que utiliza uma API do Waze para utilização de mapas digitais.

⁴¹ Tecnologia Blockchain criada por Jed Macted, um dos fundadores do XRP da Ripple. Ele ajudou a criar o XRP em 2013 e em 2014 criou a Stellar para servir como uma plataforma Blockchain para que países pudessem fazer a troca de moedas fiduciárias utilizando criptomoedas.

⁴² Criptomoedas que prometem estabilidade, geralmente lastreando seu valor a uma moeda fiduciária como o dólar.

⁴³ Disponível em <https://www.ibm.com/blockchain/solutions/world-wire> Acesso em 28/11/2018.

Tabela 10 - Retorno do Investimento da Solução IBM Blockchain Wire

Métricas	Baixa	Média	Alta
Custos	- 6.171.197,00	- 6.171.197,00	- 6.171.197,00
Receitas	8.840.088,00	24.263.375,00	42.582.438,00
Receitas Líquidas	2.668.891,00	18.092.179,00	36.411.241,00
ROI	43%	293%	590%
Payback	36 meses	16 meses	10 meses

A solução Blockchain da IBM ainda não tem um banco se utilizando do sistema para uma avaliação melhor do que está sendo prometido, o que não é caso da Ripple Net, que será explorado na próxima seção.

5.3. Ripple Net

A Ripple traz a ideia de que atualmente, com a internet, compartilhamos informação com facilidade, agilidade e segurança para qualquer parte do mundo, mas o mesmo não ocorre com recursos financeiros. A empresa pretende contribuir para que no futuro o dinheiro se movimente para qualquer parte do mundo com a mesma facilidade que se envia um e-mail. A essa possibilidade deram o nome de “Internet de Valor”⁴⁴.

À medida que o comércio fica mais globalizado a “Internet das Coisas” avança, a necessidade de micro pagamentos internacionais devem demandar serviços menos custosos e mais eficientes aos bancos. A mesma questão ocorre no caso de pequenas doações. O custo para enviar 10 dólares para outro país torna a doação inviável. Na prática, vivemos num mundo da internet que ainda funciona com um mundo de dinheiro pré-internet para transferências internacionais, e esses dois mundos não se encaixam.

Neste contexto, a Ripple criou serviços no Blockchain que permitem que pagamentos internacionais sejam feitos com custos reduzidos e em segundos. Chamado de Ripple Net, a rede global de pagamentos conectadas a uma rede que já conta com dezenas de bancos, tendo sua própria criptomoeda XRP e serviços de integração no Blockchain como xCurrent e xRapid.

A criptomoeda XRP foi criada em 2013 e hoje é a terceira maior criptomoeda em valor de mercado (vide Tabela 4) entre mais de 2000 criptomoedas existentes. Traz solução para questão da escalabilidade mencionada na seção 3.1, uma vez que processa 1500 transações por

⁴⁴ Disponível em <https://ripple.com/insights/a-vision-for-the-internet-of-value/>. Acesso em 28/11/2018.

segundo⁴⁵, e a validação de um bloco é feita no máximo em três segundos, enquanto no Blockchain do Bitcoin chega a 10 minutos.

E a escalabilidade conseguida pela XRP deve-se à forma como as transações são validadas no Blockchain, enquanto no Bitcoin a validação é feita por “*Proof-of-Work*”, ou seja, com cálculos matemáticos que demandam cada vez maior capacidade de processamento computacional e gasto de energia, a criptomoeda XRP usa a validação por consenso.

O algoritmo de consenso utilizado pela Ripple é aplicado a cada 2-3 segundos por todos os “nós”, quando o consenso é alcançado o “*ledger*” (registro) é fechado, o livro-razão de todos os “nós” torna-se idêntico ao último registro fechado, garantindo a fidedignidade das informações da rede. O consenso é alcançado por validadores que constroem reputações ao validar transações no Blockchain da Ripple.

A Ripple atualmente possui 60 bilhões de XRPs, o que representa 60% de todo o XRP que existirá no futuro. A Ripple bloqueou esses valores como garantia e há um cronograma para lançamento de 1 bilhão de XRPs pelos próximos 55 meses, sendo 1 milhão por mês.

A Ripple além da XRP tem os sistemas xCurrent e xRapid. O sistema xCurrent foi o primeiro protocolo a ser lançado, e que já está em pleno funcionamento há 2 anos. Ele é um sistema de liquidação que pode utilizar a criptomoeda XRP ou algum outro *token* digital, mas ainda necessita que os bancos mantenham uma conta *nostro* em outro país para que a operação ocorra. Traz ganhos significativos de eficiência por todo o processo ser gravado no Blockchain, mas ainda há os custos de liquidez, já mencionados. O sistema xRapid lançado em 01/10/2018⁴⁶, resolve a questão da liquidez efetuando pagamentos internacionais utilizando XRP, sem a necessidade de ter contas *nostros/vostros*.

Utilizando os valores de envio de remessas do Banco do Brasil conforme Tabela 8 e utilizando os custos calculados utilizando o Blockchain da Ripple, verificamos uma redução nos custos de 45,04%, o qual representa uma economia de 24,5 milhões de dólares.

⁴⁵ Disponível em <https://ripple.com/xrp/>. Acesso em 28/11/2018

⁴⁶ Disponível em <https://ripple.com/insights/ripple-highlights-record-year-xrapid-now-commercially-available/>. Acesso em 28/11/2018.

Tabela 11 - Custos Ripple Comparados com SWIFT

Custos	Valor (USD) Swift	Valor (USD) Ripple (USD)	Redução	Redução %
Taxas de Contraparte	2,00	2,00	-	-
Reconciliação	56,85	11,22	45,63	80,26%
Tesouraria	84,49	66,33	18,16	21,49%
Processamento	4,73	1,83	2,90	61,31%
Total	148,07	81,38	66,69	45,04%

A Ripple Net de todas as alternativas de Blockchain que podem ser utilizadas por instituições financeiras é claramente a que está mais avançada, já sendo utilizada por dezenas de instituições, como o MoneyGram, MercuryFX, IDT, Cullix, Western Union, Cambridge Global Payments, Currencies Directs, Santander, ATB Finantial, Reise Bank, entre outras. O banco ATB Finantial no Canadá, inclusive, fez sua primeira transferência para o Reise Bank na Alemanha utilizando o Ripple Net. Gravaram o episódio em vídeo, e ficaram surpresos por ter completado a transferência em apenas 8 segundos ao invés dos 4 dias habituais⁴⁷. O Santander inovou ao disponibilizar aplicativo no celular para uso da solução Ripple Net para seus correntistas no Reino Unido, Espanha, Brasil e Polônia.⁴⁸

⁴⁷ A transferência pode ser conferida em vídeo em <https://ripple.com/customer-case-study/reisebank/>. Acesso em 28/11/2018.

⁴⁸ Disponível em https://ripple.com/pt_BR/insights/swell-2018-how-banco-santander-launched-a-payment-app-for-millions/. Acesso em 28/11/2018.

6. CONCLUSÃO

Vimos que muitos economistas se dedicaram a estudar os custos de transação e seus impactos na economia no século passado, tendo na constituição de empresas a primeira solução para diminuir esses custos. Na década de 1990 a Internet começa reduzir custos, sobretudo na obtenção e compartilhamento de informação, mas ainda sem impacto na transferência de valores pelo mundo.

A tecnologia Blockchain, criada há 10 anos, tende a ser mais um importante componente na evolução tecnológica que reduz custos de transação, diminuindo a necessidade de intermediadores responsáveis por trazer segurança ao sistema. Tendo na função precípua dos bancos a intermediação financeira, entender as possibilidades de utilização dessa nova tecnologia nos serviços bancários é de vital importância para a economia brasileira, uma vez que se trata de ramo bastante oligopolizado.

O sistema Blockchain apresenta problemas, principalmente o Blockchain seminal do Bitcoin, quanto à escalabilidade, interface pouco amigável, questões de segurança, ausência de regulação e volatilidade. Observamos que a maioria dos problemas foram resolvidos com criptomoedas mais modernas, restando como problema principal a volatilidade ainda alta, quando comparada com moedas fiduciárias dos principais países. Dada a importância desse quesito foram feitas análises econométricas que demonstraram que há redução da volatilidade para as três criptomoedas com maior valor de mercado atualmente, e com tendência de queda para os próximos anos, chegando ao nível de moedas tradicionais no ano de 2019-2020. Vimos que essas criptomoedas ainda têm componentes bastante especulativos e que eventos externos ainda afetam sobremaneira seus preços, fazendo com que possa demorar um pouco mais para que a estabilidade se assemelhe às moedas fiduciárias.

É possível que o sistema Blockchain seja utilizado para quase todos os serviços financeiros no futuro, contudo algumas startups já veem no presente uma aplicabilidade imediata: transferências internacionais. Os bancos atualmente utilizam o sistema SWIFT, que é basicamente o mesmo há mais de 40 anos, para pagamentos internacionais. Caro, lento e complexo, o sistema SWIFT que reinou unânime por décadas, têm como ameaças, sistemas no Blockchain que devem ser considerados.

Avaliando os custos de se implementar dois dos mais promissores sistemas que se utilizam da tecnologia Blockchain para transferências internacionais, vimos que há redução de custos significativos, ganhos em segurança e eficiência com redução de prazo para conclusão

de uma transferência, que agora pode ser feita em segundos. Com o sistema da IBM vimos que há previsão de retorno sobre investimento de 43% (no pior dos casos), enquanto no sistema da Ripple, simulando com dados do Banco do Brasil, há redução de custos de 45%.

Como toda nova tecnologia, o Blockchain ainda tem muitas melhorias para serem efetuadas, sobretudo por ser baseada em criptomoedas que ainda são instáveis. Mas assim como o mundo nunca mais foi o mesmo depois do surgimento da Internet; com o Blockchain a transformação parece ser ainda mais profunda por tirar intermediários ineficientes do sistema. Sua utilização nas transferências internacionais será o seu primeiro grande teste.

7. REFERÊNCIAS BIBLIOGRÁFICAS

ANTONAKAKIS, N.; DARBY J. **Forecasting Volatility In Developing Countries Nominal Exchange Returns**, 2012. Disponível em https://mpa.ub.unimuenchen.de/40875/1/MPRA_paper_40875.pdf. Acesso em 21/09/2018.

BOLLERSLEV, T. **Generalized Autoregressive Conditional Heteroskedasticity**, 1986. Disponível em <https://pdfs.semanticscholar.org/7da8/bfa5295375c1141d797e80065a599153c19d.pdf>. Acesso em 01/10/2018.

CERMAK, V. **Can Bitcoin Become a Viable Alternative to Fiat Currencies? An Empirical Analysis of Bitcoin's Volatility Based on a GARCH Model**, Skidmore College. 2017.

COASE, R. H. **The nature of the firm**. Chicago: The University of Chicago Press, 1937. Disponível em <https://onlinelibrary.wiley.com/doi/epdf/10.1111/j.1468-0335.1937.tb00002.x>. Acesso em 05/09/2018

_____. **The Problem of Social Cost**. Chicago: The University of Chicago Press, 1960. Disponível em <http://www2.econ.iastate.edu/classes/tsc220/hallam/Coase.pdf>. Acesso em 05/09/2018

_____. **The Firm, The Market And The Law**. Chicago: The University of Chicago Press, 1992.

ENGLE, R.F. **Autoregressive Conditional Heteroskedasticity With Estimates Of The Variance Of U.K. Inflation**, 1982. Disponível em https://www.jstor.org/stable/1912773?seq=1#page_scan_tab_contents. Acesso em 15/10/2018.

FRIEDENBACH, M. **A Flexible Limit: Trading Subsidy For Larger Blocks**, 2015. Disponível em https://scalingbitcoin.org/hongkong2015/presentations/DAY2/3_tweaking_the_chain_2_friedenbach.pdf. Acesso em 07/11/2018.

GRAUWE, P. **Exchange Rate Variability And The Slowdown In Growth Of International Trade**, IMF Staff Papers (1988).

GRONWALD, M. **The Economics Of Bitcoins - Market Characteristics And Price Jumps**, 2014. Disponível em https://ideas.repec.org/p/ces/ceswps/_5121.html . Acesso em 09/10/2018.

GUO, Y; LIANG, C. **Blockchain Application And Outlook In The Banking Industry**, Springer Open, 2016.

HAYEK, F. **The Use of Knowledge in Society**. *The American Economic Review*, Vol. 35, No. 4. 519-530, 1945.

_____. **Denationalisation Of Money: An Analysis Of The Theory And Practice Of Concurrent Currencies**. Institute Of Economic Affairs, 1976. Disponível em <https://iea.org.uk/wp-content/uploads/2016/07/Denationalisation%20of%20Money.pdf>. Acesso em 28/10/2018

JOHNSON, B; LASZKA, A; GROSSKLAGS. J.; VASEK, M.; MOORE T. **Game-Theoretic Analysis of DDoS Attacks Against Bitcoin Mining Pools**, 2015. Disponível em https://fc14.ifca.ai/bitcoin/papers/bitcoin14_submission_16.pdf. Acesso em 21/08/2018

LAMPORT, L.; SHOSTAK, R.; PEASE, M. **The Byzantine General Problems**, 1982. Disponível em <https://people.eecs.berkeley.edu/~luca/cs174/byzantine.pdf>. Acesso em 10/08/2018.

LOMBROZO, E; WUILLE, P; JOHNSON, L. **Segregated Witness (Consensus layer)**, 2015. Disponível em <https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki>. Acesso em 12/11/2018.

MCMILLAN, J. **O Fim Dos Bancos: Moeda, Crédito E A Revolução Digital**. 1ª Ed. São Paulo, 2018. Disponível em Acesso em

MOUGAYAR, W. **Blockchain Para Negócios**. New Jersey: John Wiley & Sons, Inc., 2016. Disponível em Acesso em

NAKAMOTO, S. **Bitcoin: A Peer-to-Peer Electronic Cash System**, 2008. Disponível em <https://bitcoin.org/bitcoin.pdf>. Acesso em 11/08/2018

POON, J.; DRYJA, T. **The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments**, 2016. Disponível em <https://lightning.network/lightning-network-paper.pdf>. Acesso em 27/11/2018.

SANTOS, O.A. **Impactos Econômicos da Criptomoeda**, 2016. Disponível em <http://www.fecilcam.br/eventos/index.php/eaic/iieaic/paper/view/4279/1472>. Acesso em 01/12/2018.

TAPSCOTT, D; TAPSCOTT, A. **Blockchain Revolution: como a tecnologia por trás do Bitcoin está mudando o dinheiro, os negócios e o mundo**. São Paulo: SENAI-SP Editora, 2016. Disponível em Acesso em

TASCA, P; ASTE, T; P. LORIANA; PERONY, N. **Banking Beyond Banks and Money: A Guide to Banking Services in the Twenty-First Century**. London: Springer, 2016.

WILLIAMSON, O. E. **Market and Hierarchies: Analysis and Antitrust Implications**. New York: The Free Press, 1975.

_____. **Antitrust Economics: Mergers, Contracting, and Strategic Behavior**. New York: Basil Blackwell, 1987.

VASEK, M.; THORNTON, M.; MOORE, T. **Empirical analysis of denial-of-service attacks in the Bitcoin ecosystem**, 2014. Disponível em https://fc14.ifca.ai/bitcoin/papers/bitcoin14_submission_17.pdf. Acesso em 17/11/2018.