UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
INSTITUTO COPPEAD DE ADMINISTRAÇÃO

ANDRÉ FLUMINENSE CARNEIRO

A análise estatística de séries de criptomoedas

Mestrado em Administração
Orientadora: Beatriz Vaz de Melo Mendes

RIO DE JANEIRO
FEVEREIRO DE 2019

ANDRÉ FLUMINENSE CARNEIRO

A análise estatística de séries de criptomoedas

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Administração, Instituto Coppead de Administração, Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários à obtenção do título de Mestre em Administração.

Orientadora: Beatriz Vaz de Melo Mendes, Ph.D.

RIO DE JANEIRO
FEVEREIRO DE 2019

CIP - Catalogação na Publicação

F289a

Fluminense Carneiro, André
A análise estatística de séries de criptomoedas / André Fluminense Carneiro. -- Rio de Janeiro, 2019.
114 f.

Orientadora: Beatriz Vaz de Melo Mendes.
Dissertação (mestrado) - Universidade Federal do Rio de Janeiro, Instituto COPPEAD de Administração, Programa de Pós-Graduação em Administração, 2019.

1. Criptomoedas. 2. Séries temporais. 3. Risco. I. Vaz de Melo Mendes, Beatriz, orient. II. Título.

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos pelo(a) autor(a), sob a responsabilidade de Miguel Romeu Amorim Neto - CRB-7/6283.

ANDRÉ FLUMINENSE CARNEIRO

ANÁLISE ESTATÍSTICA DE SÉRIES DE CRIPTOMOEDAS

Dissertação de Mestrado apresentada ao Instituto COPPEAD de Administração, da Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários à obtenção do título de Mestre em Administração.

Aprovada por:

Beatriz Vaz de Melo Mendes, Ph.D
(IM/COPPEAD/UFRJ)

Otávio Henrique dos Santos Figueiredo, D.Sc
(COPPEAD/UFRJ)

Eduardo Fraga Lima de Melo, D.Sc
(UERJ)

Agradecimentos

Aos meus pais e meu irmão por todo o suporte, amor, carinho e dedicação que sempre tiveram por mim. Não teria conseguido chegar até aqui sem vocês. Meu eterno agradecimento pela formação do meu caráter e por tudo o que conquistei até hoje.

À minha orientadora, Professora Beatriz, pelos mais valiosos ensinamentos e paciência durante essa jornada, que foi muito além do nível acadêmico, chegando ao nível pessoal. Guardarei com carinho em minha memória todos esses momentos.

Ao COPPEAD e seus funcionários por exercerem papel crucial nesse caminho, sempre dando suporte quando necessário.

À minha namorada Karoline, pelo companheirismo e compreensão nos momentos difíceis dessa caminhada. Você fez com que meu caminho fosse mais leve. Te amo.

"A evolução do homem passa, necessariamente, pela busca do conhecimento."
Sun Tzu

Resumo

Desde o seu surgimento em 2009, as criptomoedas vem sido estudadas, sendo o maior foco do estudo o Bitcoin pelo seu pioneirismo como a primeira criptomoeda e também pelo seu tamanho de mercado. Ao contrário de diversos estudos já realizados na comunidade acadêmica, o foco desta dissertação vai além do estudo sobre o Bitcoin, incluindo outras criptomoedas que não são tão famosas, como por exemplo a Stellar e o Litecoin. Ao contrário de mercados maduros e já estudados por décadas, o mercado de criptomoedas começou a ser analisado no mundo acadêmico só recentemente, carecendo assim de uma maior atenção e estudo. Assim sendo, o primeiro objetivo deste estudo é realizar uma revisão bastante aprofundada sobre o conceito de criptomoedas, desde a sua criação até a atualidade, entrando desde conceitos básicos e gerais para todas as criptomoedas como forks, carteiras, mercados, além da abordagem de conceitos mais familiares ao mercado de ações como diferenças entre um Initial Coin Offering (ICO) e um Initial Public Offering (IPO), benefícios e riscos de um ICO e por fim entrando em conceitos específicos para cada criptomoeda, com suas particularidades e eventuais semelhanças até como essas criptomoedas pretendem ser em um futuro, dentre outros aspectos abordados. Em segundo lugar iremos efetuar uma análise estatística mais aprofundada sobre as séries de retornos e de preços das séries, analogamente ao que se fez nas últimas duas décadas sobre os retornos de ativos financeiros. A ideia seria verificar se, assim como no caso de carteiras e índices de ações, as séries das criptomoedas seguiriam os mesmos padrões já bem conhecidos, como os fatos estilizados sobre os preços, retornos e volatilidade, estudar o seu processo gerador não condicional, procurar pelos modelos condicionais adequados, especialmente para a volatilidade e acessar a representação do seu risco de mercado.

Palavras-chave: criptomoedas, séries temporais, risco

Abstract

Since its inception in 2009, the cryptocoins have been studied, being the main focus of the study Bitcoin for its pioneering as the first cryptocoin and also for its market size. In contrast to several studies already conducted in the academic community, the focus of this thesis goes beyond the study of Bitcoin, including other not-so-famous cryptocoins, such as Stellar and Litecoin. Unlike mature markets that have been studied for decades, the market for cryptocoins began to be analyzed in the academic world only recently, thus requiring more attention and study. Thus, the first objective of this study is to carry out a very thorough review of the concept of cryptocoins, from its creation to the present day, ranging from basic and general concepts to all cryptocoins such as forks, portfolios, markets, as well as the concept approach more familiar to the stock market as differences between an Initial Coin Offering (ICO) and an Initial Public Offering (IPO), benefits and risks of an ICO and finally entering into specific concepts for each cryptocoin, with their particularities and possible similarities to how these cryptocoins are intended to be in the future, among other aspects addressed. Second, we will carry out a more detailed statistical analysis on the series of returns and prices of the series, similarly to what has been done in the last two decades on the returns of financial assets. The idea would be to verify whether, as in the case of portfolios and stock indexes, the series of cryptocoins would follow the same well-known patterns, such as stylized facts about prices, returns and volatility, study their unconditional generating process, search appropriate conditional models, especially for volatility and access to the representation of their market risk.

Keywords: cryptocoins, time series, risk

Sumário

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

Desde o seu surgimento em 2009, as criptomoedas vem sido estudadas, sendo o maior foco do estudo o Bitcoin pelo seu pioneirismo como a primeira criptomoeda e também pelo seu tamanho de mercado. Ao contrário de diversos estudos já realizados na comunidade acadêmica, o foco desta dissertação vai além do estudo sobre o Bitcoin, incluindo outras moedas que não são tão famosas, como por exemplo a Stellar e o Litecoin. Ao contrário de mercados maduros e já estudados por décadas, o mercado de criptomoedas começou a ser analisado no mundo acadêmico só recentemente, carecendo assim de uma maior atenção e estudo. Como motivação pessoal, o autor despertou paixão pelo tema criptomoedas por conta de investimentos realizados e, consequentemente, conhecendo um pouco melhor sobre as tecnologias que suportam e viabilizam todo esse mercado, acreditando que, futuramente, uma parte dessas tecnologias estarão no dia a dia das pessoas e instituições.

Gervais, Karame, Capkun e Capkun (2014) levantam um estudo onde a ideia é averiguar se o Bitcoin é, de fato, descentralizado, sendo este o pilar do Bitcoin e uma das maiores motivações de seu criador Satoshi Nakamoto. É visto que várias funções essenciais para o funcionamento do Bitcoin não são descentralizadas, onde algumas entidades realizam o processo de tomada de decisão, controle dos serviços, mineração (abordado também neste estudo), entre outros. Por fim, são apresentadas propostas para fortalecer a descentralização no Bitcoin.

Croman, Decker, Eyal, Gencer, Juels, Kosba, Miller, Saxena, Shi, Sirer, Song e Wattenhofer (2016) abordam o problema da escalabilidade do Bitcoin, como isso afeta a rede e como esse problema deve ser tratado de maneira urgente. Reparametrização dos blocos e intervalos devem ser tratado como um primeiro incremento, porém soluções mais profundas requerem reavaliar abordagens técnicas. Ao final do artigo são apresentadas propostas para de ideias de protocolos e ideias para este problema.

Armknecht, Karame, Mandal, Youssef e Zenner (2015) estudam o atual sistema de pagamento da Ripple, abordando aspectos como segurança e privacidade em relação ao Bitcoin. Uma contribuição importante deste artigo está no fato da escolha dos parâmetros pela Ripple Labs não impede a ocorrência de *fork*, onde os autores propuseram quais seriam os parâmetros corretos para essa não ocorrência. Após esse artigo a Ripple reconheceu este erro e mudou os seus parâmetros para evitar um possível *fork*.

Snider, Samani e Jain (2017) realizam uma análise de mercado da Ripple, passando por pontos como o background da Ripple, protocolo de consenso, como funciona o mercado atual, como a Ripple pretende mudar este paradigma e os riscos relacionados.

Chohan (2017) aborda em seu artigo um problema já conhecido sobre as criptomoedas que inviabilizou por muito tempo o seu uso, como meio de pagamento, até a criação do Bitcoin que solucionou esta questão: o gasto duplo. Há outros artigos importantes que abordam diferentes aspectos do funcionamento deste ambiente, como por exemplo os *whitepapers*, que são documentos oficiais publicados por uma organização ou pessoa, a fim de servir de informe ou guia sobre algum problema e como enfrentá-lo. Há, por exemplo, *whitepapers* para Bitcoin, Ethereum e Ripple, os quais abordaremos mais a frente. Além desses, há inúmeras publicações que podem ser consultadas na Internet, como *Cointelegraph, CoinMarketCap, Coindesk*, dentre outros.

Todos os artigos citados abordam apenas uma ou outra característica de uma ou outra criptomoeda. Assim sendo, o primeiro objetivo deste estudo é realizar uma revisão bastante aprofundada sobre o conceito de criptomoedas, desde a sua criação até a atualidade, entrando desde conceitos básicos e gerais para todas as criptomoedas como *forks*, carteiras, mercados, além da abordagem de conceitos mais familiares ao mercado de ações como diferenças entre um *Initial Coin Offering* (ICO) e um *Initial Public Offering* (IPO), benefícios e riscos de um ICO e por fim entrando em conceitos específicos para cada criptomoeda, com suas particularidades e eventuais semelhanças até como essas criptomoedas pretendem ser em um futuro, dentre outros aspectos abordados. A ideia é que esse estudo possa ser base, servindo de material pronto para as próximas teses que podem se seguir a respeito do tema.

Alguns estudos recentes tratam de análises estatísticas de criptomoedas. Katsiampa (2017) procura o melhor modelo GARCH para a volatilidade do Bitcoin. Liu, Shao, Wei e Wang (2017) comparam a distribuição *normal reciprocal inverse Gaussian* (NRIG) com a t-student sob o modelo GARCH para ver qual performa melhor para os retornos diários do Bitcoin. Guo e Antulov-Fantulin (2018) tentam prever a curto prazo as flutuações do preço do Bitcoin em uma corretora americana de criptomoedas, se utilizando de *machine learning* e alguns métodos, dentre eles o modelo GARCH. Chan, Chu, Nadarajah e Osterrieder (2017) analisam algumas das maiores criptomoedas da época, realizando ajustes de distribuições paramétricas. Em outro artigo, Chan, Chu, Nadarajah e Osterrieder (2017) ajustam modelos GARCH para diversas criptomoedas. A maioria dos artigos listados foca apenas no Bitcoin. Os únicos que abordam outras criptomoedas (que são dos mesmos autores) naõ fizeram para Ethereum e Stellar. Além disso, os ajustes do modelo GARCH nos outros artigos não contemplam o FIGARCH e o GARCH-M, contemplados aqui, além de não abordar o teste mais famoso de cobertura que é o de Kupiec (1995). Soma-se a isso o fato de nenhum deles possuirem uma revisão de literatura extensa sobre as criptomoedas presente aqui.

Assim sendo, em segundo lugar iremos efetuar uma análise estatística mais aprofundada sobre as séries de retornos e de preços das séries, analogamente ao que se fez nas últimas duas décadas sobre os retornos de ativos financeiros. A ideia seria verificar se, assim como no caso de carteiras e índices de ações, as séries das criptomoedas seguiriam os mesmos padrões já bem conhecidos, como os fatos estilizados sobre os preços, retornos e volatilidade, estudar o seu processo gerador não condicional, procurar pelos modelos condicionais adequados, especialmente para a volatilidade e acessar a representação do seu risco de mercado. Um resultado interessante a nível de mercado trazido por este trabalho é o cálculo da Perda Média Esperada (*Expected Shortfall*) para as séries, baseados nos melhores modelos não condicionais e condicionais, para t+1. Esta informação

é de grande importância para gestores que administram o risco diariamente, sendo uma informação de apoio à tomada de decisão gerencial.

Foi visto que diversos fatos estilizados foram também verificados para as séries sob análise. Vimos também que, ao contrário do que pensávamos inicialmente, em relação aos ajustes não condicionais, a distribuição t-assimétrica de Zhu e Galbraith (2010) não é um bom modelo para a distribuição subjacente dos retornos para todas as séries. Foi observado também que a GPD se saiu melhor no Teste de Kupiec de uma forma geral tanto para *in-sample* como *out-of-sample*. Já para os modelos condicionais, os modelos com GPD se saíram melhor para Ripple e Litecoin, ao passo que os modelos sem GPD se saíram melhor para Ethereum e Euro para o Teste de Kupiec fora da amostra. Para Bitcoin e Stellar, o desempenho foi igual. Os modelos condicionais EGARCH e GARCH-in-Mean para as séries analisadas não forneceram bons ajustes.

Vários artigos já mostraram empiricamente que geralmente basta um modelo GARCH$(1, 1)$ para capturar a dinâmica da volatilidade da série de retornos financeiros. Será que este fato também será observado para as criptomoedas? No que concerne à memória longa, como as criptomoedas se comportarão? Perguntas como estas e outras serão vistas no capítulo 4.

A revisão sobre as criptomoedas se encontra no Capítulo 2, a especificação da modelagem estatística, incluindo análises exploratórias, ajustes de modelos e testes, estão no Capítulo 3 e todas as análises efetuadas com o auxílio do pacote R estão no Capítulo 4. O Capítulo 5 discute os resultados obtidos e conclui dando sugestões para trabalhos futuros.

Capítulo 2

Criptomoedas e Conceitos Básicos

Antes de falarmos sobre as criptomoedas, alguns conceitos básicos sobre o funcionamento deste mercado serão apresentados.

2.1 Conceitos Básicos

2.1.1 *Soft fork, hard fork* e separação da cadeia (*chain split*)

As definições a seguir são voltadas para o protocolo do Bitcoin, mas em geral estas mesmas definições se aplicam também para outras Blockchains. Há dois tipos de *forks: soft fork* e *hard fork*. Além disso, *forks* podem gerar separação da cadeia (*chain split*) (https://medium.com/lightcoin/the-differences-between-a-hard-fork-a-soft-fork-and-a-chain-split-and-what-they-mean-for-the-769273f358c9. Consultado em 27 de março de 2018).

2.1.1.1 *Soft fork*

Um *soft fork* é uma restrição das regras de consenso do atual protocolo, reforçadas por nós que se atualizam para também reforçarem as novas regras vindas com o *soft fork*. Um bloco que antes era considerado válido nas antigas regras é considerado inválido pelos nós se o este bloco viola as novas regras impostas pelo *soft fork* após a ativação do mesmo. Um exemplo seria de um *soft fork* que restringe o limite do tamanho do bloco de 1 MB para 700 KB, por exemplo. Blocos que possuíam 1 MB eram considerados válidos antes do *soft fork*, porém após a ativação da nova regra nós não aceitarão nenhum bloco com tamanho superior a 700 KB (https://medium.com/lightcoin/the-differences-between-a-hard-fork-a-soft-fork-and-a-chain-split-and-what-they-mean-for-the-769273f358c9. Consultado em 27 de março de 2018).

2.1.1.2 *Hard fork*

Um *hard fork* é um afrouxamento das regras de consenso do atual protocolo, reforçadas por nós que se atualizam para também reforçarem as novas regras vindas com o *hard fork*. Um bloco que antes era considerado inválido nas antigas regras é considerado válido pelos nós se este bloco não viola as novas regras impostas pelo hard fork após a ativação do mesmo. Um exemplo seria de um *hard fork* que aumenta o limite do tamanho do bloco de 1 MB para 3 MB por exemplo. Blocos que possuíam 3 MB eram considerados inválidos antes do *hard fork*, porém após a ativação da nova regra nós aceitarão blocos

com tamanho até 3 MB (https://medium.com/lightcoin/the-differences-between-a-hard-fork-a-soft-fork-and-a-chain-split-and-what-they-mean-for-the-769273f358c9. Consultado em 27 de março de 2018).

2.1.1.3 Separação da cadeia (*chain split*)

Uma separação da cadeia pode ocorrer tanto em um *soft fork* quanto em um *hard fork*. Isso acontece quando duas ou mais versões da Blockchain compartilham a mesma história até o momento que as regras divergem entre si. É importante observar que quando ocorre *soft fork* ou *hard fork* não necessariamente ocorrerá uma separação da cadeia. A barreira para evitar uma separação de cadeia disruptiva é muito maior em caso de *hard fork*, por conta de sua incompatibilidade com nós antigos, mas é tecnicamente possível (https://medium.com/lightcoin/the-differences-between-a-hard-fork-a-soft-fork-and-a-chain-split-and-what-they-mean-for-the-769273f358c9. Consultado em 27 de março de 2018).

2.1.1.4 Separação sustentável da cadeia

Quando ocorre uma separação de cadeia, um cenário possível seria o seguinte: a maioria dos nós adota as novas regras do *soft fork*, por exemplo, porém a maioria dos mineradores continua a minerar os blocos de acordo com as regras antigas para uma minoria de nós. Em um lado você tem o *hashpower*, vindo dos mineradores e do outro o poder econômico, vindo dos nós. Em geral, os nós minoritários não suportam a demanda econômica dos mineradores, fazendo com que os mineradores atualizam o seu protocolo, a fim de poder minerar a maioria dos blocos que também atualizaram o seu protocolo e conseguindo assim maiores recompensas. Ao mesmo tempo, enquanto os mineradores não atualizam o seu protocolo, a maioria dos nós precisa estar disposta a esperar por mais tempo as suas transações serem concretizadas, visto que há poucos mineradores em sua Blockchain (https://medium.com/lightcoin/the-differences-between-a-hard-fork-a-soft-fork-and-a-chain-split-and-what-they-mean-for-the-769273f358c9. Consultado em 27 de março de 2018).

Com uma separação sustentável da cadeia, essa situação perdura por mais tempo, pois o poder econômico e o *hashpower* das Blockchains são mais equilibrados (em comparação ao desequilíbrio citado anteriormente) ao ponto de que cada uma consegue ser sustentável no seu próprio ecossistema. Grandes problemas que surgem com uma separação sustentável de cadeia está mais no âmbito social que técnico: qual das cadeias sustentáveis (que antes eram apenas uma) manterá o nome Bitcoin? Essa confusão entre Blockchains pode prejudicar a confiança do investidor para investir nesta moeda, por exemplo. Um grande exemplo dentro dos criptomoedas relacionado com separação de cadeia sustentável foi relacionado com o *hard fork* do Ethereum para Ethereum e Ethereum Classic, por conta do ataque hacker sofrido pela DAO (*Decentralized Autonomous Organization*), onde hackers invadiram o sistema e roubaram 55 milhões de dólares em moedas DAO. Este caso será abordado com mais detalhes na seção sobre possíveis falhas em *smart contract* no Ethereum (https://medium.com/lightcoin/the-differences-between-a-hard-fork-a-soft-fork-and-a-chain-split-and-what-they-mean-for-the-769273f358c9. Consultado em 27 de março de 2018). Para maiores informações sobre forks, onde é possível ver desenhos de vários cenários por exemplo, visitar o seguinte link: https://medium.com/lightcoin/the-

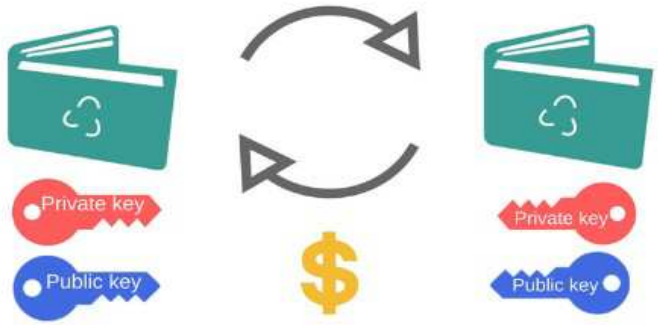

Figura 2.1: Transação entre carteiras digitais. Fonte: (https://blockgeeks.com/guides/cryptocurrency-wallet-guide/). Consultado em 27 de março de 2018

differences-between-a-hard-fork-a-soft-fork-and-a-chain-split-and-what-they-mean-for-the-769273f358c9.

2.1.2 Carteiras de criptomoedas (*cryptocurrency wallet*)

Carteira de moedas digitais é um *software* que guarda as chaves pública e privadas e interage com várias Blockchains para permitir que o usuário envie e receba moedas digitais, além de conseguir monitorar o saldo (https://blockgeeks.com/guides/cryptocurrency-wallet-guide/. Consultado em 27 de março de 2018).

Em contraste com o conceito de carteiras tradicionais, uma carteia de moedas digitais não guarda nenhum tipo de moeda lá. De fato, moedas digitais não ficam guardadas em um único local ou existem de maneira física. O que realmente existe são os registros das transações nas Blockchains das moedas digitais que alguém possui. Por exemplo, quando alguém envia alguma criptomoeda, essa pessoa está basicamente assinando a propriedade desta criptomoeda transferida para a pessoa que está recebendo a criptomoeda. Para poder gastar essa criptomoeda e desbloquear fundos, a chave privada da pessoa que está recebendo deve corresponder à chave público que esta criptomoeda está atribuída. Caso isso aconteça, o valor da carteira digital naquela criptomoeda do destinatário irá aumentar pelo valor transferido e a do remetente irá diminuir na mesma proporção. Essa operação fica registrada na Blockchain. A Figura 2.1 ilustra um exemplo de transação entre carteiras digitais (https://blockgeeks.com/guides/cryptocurrency-wallet-guide/. Consultado em 27 de março de 2018).

Carteiras de criptomoedas podem existir na forma de *software* (computador, online e celular), *hardware* e papel. Carteiras digitais instaladas no computador são acessíveis apenas do computador onde o arquivo foi baixado e instalado. Fornece um nível de segurança alto, porém caso o computador seja hackeado, há um risco de perder tudo. Carteiras onlines rodam com a tecnologia nuvem e podem ser acessadas de qualquer aparelho em qualquer localização. Nesta modalidade a chave privada é guardada online, onde uma terceira parte controla, o que a torna mais vulnerável. Carteiras digitais no celular, através de aplicativo, podem ser utilizadas em qualquer lugar, inclusive em lojas. Por conta do tamanho, em geral, são menores e mais simples que as do computador. Carteiras digitais armazenadas em *hardwares* guardam as chaves privadas em dispositivos

Figura 2.2: Exemplo de um *hardware wallet*. Fonte: https://99bitcoins.com/wp-content/uploads/2017 /02/ledger-nano-s-review.png. Consultado em 27 de março de 2018

similares com *pendrive* USB. Elas também suportam diferentes tipos de moedas por conta da compatibilidade com diversas interfaces. Para realizar uma transferência basta apenas conectar o *hardware* em algum dispositivo que possua internet, entrar com uma senha, selecionar a moeda, quantidade e confirmar. É um método seguro. A Figura 2.2 mostra um *hardware wallet*.

A carteira papel fornece para o usuário um par de chaves (uma pública e uma privada) que posteriormente será impressa e guardada em algum lugar seguro, além de um endereço público. Para receber alguma moeda basta fornecer o endereço público e para gastar basta transferir os fundos da carteira de papel para alguma carteira digital através do uso da chave privada ou de escanear o QR *code* da carteira. Uma carteira de papel é basicamente um pedaço de papel com algumas informações. Este método para guardar moedas, mesmo que muito seguro por ser offline, está sujeito a perdas físicas, como perder o papel, destruí-lo, entre outros. Para diminuir as chances de se perder uma conta por completo, é recomendado realizar algumas cópias desta carteira e guardar em lugares seguros.

2.1.3 O mercado

No tempo desta escrita, o mercado de criptomoedas possui uma capitalização de 262 bilhões de dólares, um volume negociado de 10,9 bilhões nas últimas 24 horas e uma dominância do Bitcoin num patamar de 45,5%. Dominância é a relação entre a capitalização de uma moeda sobre a capitalização do mercado referido. Por exemplo, se a capitalização de mercado do Bitcoin é de 1000 dólares e a capitalização do mercado é de 2000 dólares, então a dominância do Bitcoin é de 50%.

Em janeiro de 2018, o Bitcoin atingiu a sua menor dominância de mercado, sendo inferior a 33%. Nesta mesma data, moedas como Ethereum e Ripple atingiram uma dominância de aproximadamente 12,5% e 19% respectivamente. Um movimento de mercado natural das criptomoedas é que, quanto menor a dominância do Bitcoin, maior é a dominância das criptomoedas conhecidas como *altcoins* (moedas alternativas). *Altcoins* são todas as criptomoedas que não são o Bitcoin. Portanto, se o Bitcoin possui uma dominância de 60%, as *altcoins* são responsáveis pelos 40% restantes. Atualmente, há 1594 moedas digitais listadas no site Coin Market Cap, onde 1593 são *altcoins*, onde o Bitcoin é o primeiro em capitalização de mercado com aproximadamente 119,7 bilhões

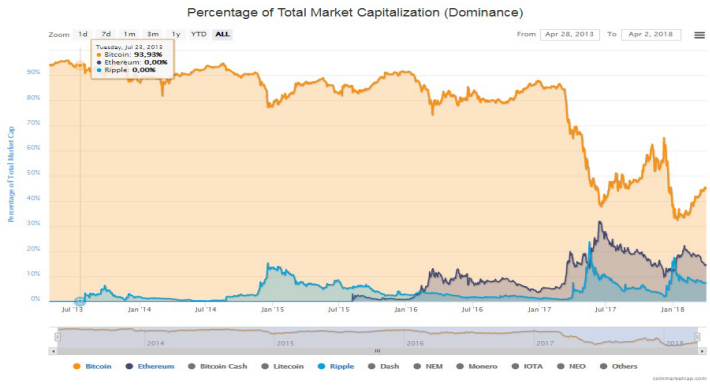

Figura 2.3: Dominância do Bitcoin, Ethereum e Ripple perante o mercado de criptomoedas. Fonte: https://coinmarketcap.com/charts/#dominance-percentage. Consultado em 2 de abril de 2018.

Figura 2.4: Evolução da capitalização total de mercado. Fonte: https://coinmarketcap.com/charts /#dominance-percentage. Consultado em 2 de abril de 2018.

de dólares e um valor unitário de 7064 dólares, seguido pelo Ethereum que possui uma capitalização de mercado de 37,9 bilhões de dólares aproximadamente e um valor unitário de 385 dólares e o Ripple em terceiro, com uma capitalização de mercado de 19,5 bilhões de dólares, negociado ao valor unitário de 0,49 dólares. Na Figura 2.3 podemos ver a dominância do Bitcoin e algumas altcoins.

Também em janeiro de 2018, a capitalização de mercado das moedas digitais alcançou o pico histórico, atingindo um patamar superior a 800 bilhões de dólares. Foi neste mesmo período de janeiro de 2018 que o volume de transação das últimas 24 horas foi o maior, um valor superior a 70 bilhões de dólares. Na Figura 2.4 é possível ver a evolução da capitalização de mercado das criptomoedas.

2.1.4 ICO

2.1.4.1 Definição

ICO (*Initial Coin Offering*), muitas vezes também referido como *crowdsale*, é uma forma de financiar projetos de criptomoedas. Uma companhia emite e vende a sua criptomoeda em troca de criptomoedas como Bitcoin, Ether ou moedas fiduciárias também para finan-

ciar o projeto que a mesma está desenvolvendo. Um exemplo famoso de ICO foi o do Ethereum (https://cointelegraph.com/explained/ico-explained. Consultado em 8 de abril de 2018).

2.1.4.2 Diferença entre ICO e IPO

Apesar de serem parecidos em alguns aspectos, há algumas diferenças relevantes entre ICO e IPO (*Initial Public Offering*). Uma delas é que o IPO denota uma fatia da companhia que o comprador possui (quanto mais ações o comprador tem, maior fatia da companhia ele tem e, consequentemente, maior poder de voto dentro da companhia ele tem). Isso não é verdade para a maioria dos casos das criptomoedas onde, em geral, elas funcionam como moedas que podem sem enviadas para outros usuários ou como troca por outras moedas. Outra diferença bem marcante é o fato da regulação. Um IPO é um processo fortemente regulado pelo governo, onde há a necessidade de uma extensa preparação de documentação antes que o IPO ocorra. Há diversas consequências para o caso de não conformidade. Já no caso de um ICO, onde não há toda essa regulação do governo, vários projetos podem lançar um ICO com pouca preparação, que pode representar um risco para o investidor (https://cointelegraph.com/explained/ico-explained. Consultado em 8 de abril de 2018).

2.1.4.3 Benefícios de um ICO

Do ponto de vista de um investidor, ICO's podem ser extremante lucrativos. Um exemplo que pode ser dado é do ICO do Ethereum, onde cada Ether foi vendido no ICO com um valor que variava entre 0,3 USD e 0,4 USD. Mais tarde, quando a plataforma principal foi liberada, cada Ether estava sendo negociado a mais de 19 USD e hoje é negociado com valores superiores a 300 USD (https://cointelegraph.com/explained/ico-explained. Consultado em 8 de abril de 2018).

2.1.4.4 Riscos de um ICO

Por conta da baixa regulação neste mercado, onde muitos projetos, com o intuito de serem fraudulentos, podem aparecer. São conhecidos na comunidade como *scams*. Algumas formas de identificar projetos fraudulentos são: os desenvolvedores não são conhecidos dentro da comunidade ou são anônimos, ausência de carteiras de custódia (carteiras onde para acessar os recursos nela são necessárias várias chaves privadas. Se todas as chaves estiverem concentradas nas mãos dos desenvolvedores do projeto, eles podem acessar esses recursos e roubarem tudo que há lá dentro), *whitepaper/roadmap* com metas irreais ou turvas (podendo significar que ou os desenvolvedores não fazem ideia do que estão fazendo ou não vão realizar de fato nada) e falta de transparência (não mostrar para a comunidade como está indo o progresso do projeto (através de versões demo ou beta do projeto ou qualquer outra ação que possa informar à comunidade que há algum trabalho realmente sendo feito) pode significar que na verdade não há trabalho algum realizado (https://cointelegraph.com/explained/ico-explained. Consultado em 8 de abril de 2018).

2.2 Criptomoedas

2.2.1 Bitcoin

O conceito de criptomoedas descentralizadas é antigo, primeiramente descrito por Wei Dai em 1998, onde ele sugeriu a ideia de uma moeda baseada em criptografia para controlar suas criações e transações em vez de uma autoridade central (https://www.weusecoins.com /en/questions/. Consultado em 11 de março de 2018). Inspirado por este conceito, Satoshi Nakamoto, pseudônimo de uma pessoa ou grupo de pessoas cuja a identidade não se sabe ao certo mas há muita especulação sobre, criou a moeda digital mais famosa hoje, o Bitcoin. O conceito de Bitcoin foi inicialmente publicado em um grupo de discussões chamado The Cryptography Mailing (https://www.mail-archive.com/search?l=cryptographymetzd owd.com&q=from:%22Satoshi+Nakamoto%22. Consultado em 3 de março de 2018), onde Nakamoto apresenta pela primeira vez o que seria o Bitcoin, o motivo pelo qual ele estava sendo criado e como funcionaria.

Whitepaper é um documento preparado por uma pessoa ou grupo de pessoas antes do lançamento de uma nova criptomoeda. Ele contém todo o detalhamento da moeda digital para que assim uma pessoa decida se quer de fato adquiri-la. Desdobramentos de cunho tecnológico, explicação da programação, aplicações comerciais, entre outros, podem estar presentes. Nakamoto afirma em seu *whitepaper* de 2009 (Bitcoin: A Peer-to-Peer Electronic Cash System, 2009) que o comércio na Internet depende quase que exclusivamente de uma instituição financeira atrás de todo o processo de compra e venda para garantir que essa transação ocorra com sucesso e não tenha problemas. Para isso, pelo menos uma das partes precisa confiar nessa terceira parte (as instituições financeiras). Porém Nakamoto aponta algumas falhas desse processo. Uma delas é que transações irreversíveis não são possíveis, e esta terceira parte precisa atuar como um mediador da disputa, caso ela ocorra. Além disso, estas mesmas instituições financeiras lutam contra transações fraudulentas. Tais fatos aumentam o custo de transação. A ideia de Nakamoto era eliminar a terceira parte da transação, onde se baseia em um sistema de confiança (as partes atuantes do processo de compra e venda precisam confiar nesta terceira parte) e passar a ser um sistema baseado em criptografia, onde transações onlines descentralizadas (sem a participação de instituições) possam ocorrer, ou seja, se valendo do conceito P2P (*peer-to-peer*), onde não há a necessidade de um servidor central, cada nó da rede funciona como cliente e servidor ao mesmo tempo (https://pt.wikipedia.org/wiki/Peer-to-peer. Consultado em 3 de março de 2018). Outros problemas, por exemplo, de se confiar em uma autoridade centralizadora para estes tipos de atividades transacionais seriam ficar à mercê desta instituição, que pode congelar toda a sua conta, como vimos no governo Collor aqui no Brasil, além do fato de que bancos são constantemente alvo de hackers para realizar operações fraudulentas e roubos. Fraudadores obtiveram 16 bilhões de dólares de 12.7 milhões consumidores americanos em 2014. A Figura 2.5 indica a evolução deste tipo de atividade ao longos dos anos de 2010 e 2014 nos EUA (https://www.nasdaq.com/article/credit-card-fraud-and-id-theft-statistics-cm520388. Consultado em 3 de março de 2018).

A moeda eletrônica (no caso o Bitcoin), como o *whitepaper* de Nakamoto próprio define, é uma cadeia de assinaturas digitais. Cada dono da moeda transfere a mesma para o próximo nesta cadeia utilizando uma assinatura eletrônica (*hash*) da transação realizada anteriormente e também informa a chave pública do destinatário (que seria o endereço de recebimento do próximo usuário). O destinatário desta moeda pode verificar

Figura 2.5: Fraude Cartões de Crédito nos EUA. Fonte: https://www.nasdaq.com/article/credit-card-fraud-and-id-theft-statistics-cm520388. Consultado em 3 de março de 2018

a autenticidade da mesma, porém não há como este destinatário verificar se foi gerado um problema de gasto duplo.

Esta questão do gasto duplo sempre foi uma preocupação que permeou o ambiente de transações digitais e por isso sempre houve a necessidade de uma terceira parte para evitar isso. O gasto duplo é uma possível falha no sistema de transações digital, onde a mesma moeda pode ser utilizada duas vezes, visto que essa moeda digital é um arquivo digital que pode ser corrompido ou falsificado. O gasto duplo gera um problema inflacionário, criando novas moedas que não haviam sido previstas antes (Chohan, Usman, The Double Spending Problem and Cryptocurrencies (December 19, 2017). Available at SSRN: https://ssrn.com/abstract=3090174 or http://dx.doi.org/10.2139/ssrn.3090174). Introduzir uma autoridade central para realizar esse controle resolveria a questão, porém em um ambiente descentralizado como é o do Bitcoin, não há nem é a intenção ter esta figura. O destinatário precisa ter a certeza de que o remetente não enviou esta mesma moeda anteriormente para outro endereço. Então, na verdade, as transações que contam para a rede do Bitcoin são as que foram realizadas mais cedo, logo tentativas de gasto duplo após essa primeira transação desta mesma moeda são desconsideradas pela rede. Para isso, é necessário estar ciente de todas as transações que ocorreram na rede, ou seja, elas precisam ser publicamente anunciadas e os participantes precisam concordar com um único histórico de todas as transações que foram recebidas. O destinatário precisa da prova de que, em cada transação, neste momento a maioria dos nós da rede concordou que foi a primeira recebida.

Todas essas transações anunciadas publicamente (e seus desdobramentos, como endereço de remetente e destinatário, valor, horário, entre outros) compõem o livro-razão

(ledger em inglês) conhecido como Blockchain. Apesar de não constar a expressão Blockchain em seu *whitepaper* de 2009 (apenas *blocks*), esta ideia foi concebida por Nakamoto e em 2009 o código foi lançado como código aberto. (https://bitcoin.org/en/faq#who-created-bitcoin. Consultado em 3 de março de 2018).

A solução proposta por Nakamoto começa com o Servidor de Carimbo de Tempo (*Timestamp Server*). A ideia é estampar digitalmente horário e data de cada transição ocorrida na Blockchain. Feito isso, todos os usuários da rede podem ver esta informação. Isso é a prova de que a operação ocorreu e foi validada pelo sistema. Cada *timestamp* atual inclui o *timestamp* anterior na sua *hash*, formando a cadeia (Blockchain), onde cada *timestamp* atual reforça o *timestamp* anterior. Com isso, a Blockchain e o histórico de transações contido nela também aumentam. É por esse motivo que hoje em dia para minerar Bitcoins é preciso muito poder de processamento e computação, algo que antigamente era feito facilmente com um computador de casa. Para que cada *timestamp* seja implementado, é necessária uma prova de trabalho (*proof-of-work*) para autenticar a transação, para provar que uma quantidade de trabalho foi desempenhada pelo sistema. Basicamente cada número do *hash* possui um problema matemático que precisa ser resolvido. A resposta desse problema é então passada para o nó destinatário da transação que vai checar se a resposta está correta. Para checar, o receptor coloca esta resposta no *hash* (que possui um número aleatório produzido pelo próprio *hash*, quando o mesmo é criado pelo *timestamp* e é identificado na Blockchain através deste número gerado), que vai informar se ela está correta ou não. Caso esteja correta, esta transação é finalizada na Blockchain e a mesma aumenta de tamanho. Em caso de resposta incorreta, a transação é invalidada. Isso fornece uma maior segurança ao sistema, pois para modificar um determinado bloco, é necessário desfazer toda a prova de trabalho dos blocos que surgiram depois desse que alguém deseja modificar, necessitando de uma quantidade muito grande de energia e CPU. A Figura 2.6 explica o motivo pelo qual é difícil burlar a Blockchain do Bitcoin, baseado em prova de trabalho.

No que tange à rede, há uma ordem de passos a ser seguida:

1. Novas transações são anunciadas para todos os nós.
2. Cada nó recolhe novas transações para um bloco.
3. Cada nó trabalha para resolver a prova de trabalho do seu bloco.
4. Quando um nó resolve esta prova de trabalho ou enigma, ele transmite o bloco para todos os nós.
5. Os nós aceitam o bloco somente se todas as transações nele forem válidas e se não existirem problemas de gastos duplos.
6. Os nós expressam sua aceitação do bloco trabalhando na criação do próximo bloco na cadeia, usando o *hash* do bloco aceito como o *hash* anterior.

Os nós sempre consideram as maiores cadeias como sendo as corretas e vão trabalhar para aumentá-la. Caso dois nós transmitam informações diferentes do próximo bloco simultaneamente, blocos que receberam essa próxima informação vão considerar, baseado no *timestamp*, a maior cadeia. Se um nó se desconectar da rede e acabar por não receber o próximo bloco, ele será atualizado quando retornar à rede.

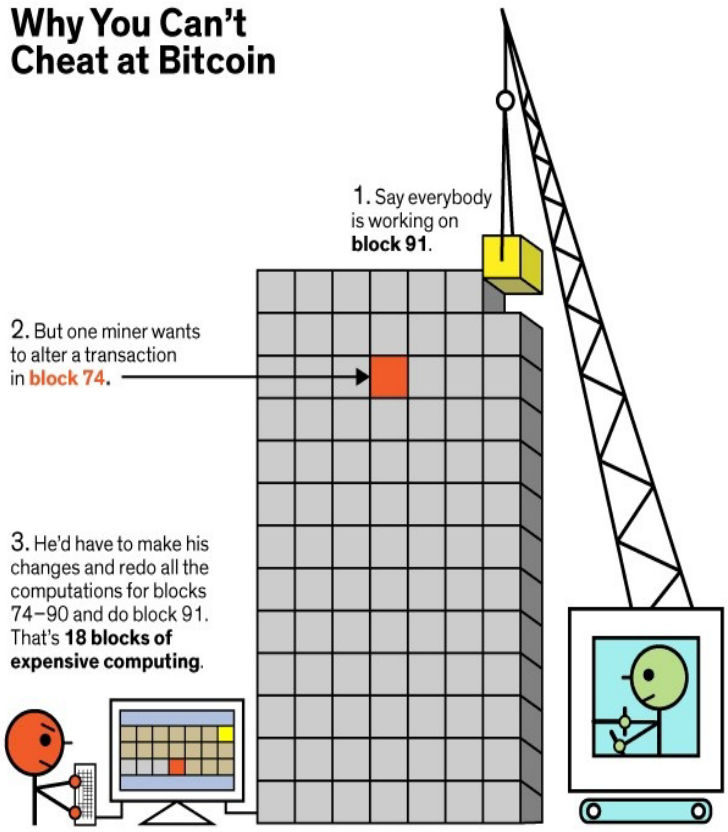

Figura 2.6: Exemplificação da dificuldade de burlar a *p*roof-of-work. Fonte: https://www.weusecoins .com/en/questions/ Consultado em 12 de março de 2018

Os incentivos por trás da criação de novos blocos e transações pela rede (feitas pelos mineradores) ocorre de duas formas: a primeira transação de cada bloco gera um Bitcoin para o criador daquele bloco e a segunda forma de incentivo é através de taxas de transação. Quando todas as moedas já tenham sido mineradas (21 milhões de Bitcoins), os incentivos vão girar em torno das taxas de transação. Nakamoto compara o trabalho das pessoas criam novos blocos aos mineradores de ouro, onde os mesmos gastam recursos para colocar o ouro em circulação e aqui para colocar o Bitcoin em circulação é necessário tempo de CPU e eletricidade para tal. A cada 10 minutos em média, um novo bloco é minerado pelos mineradores.

Para fins de espaço em disco, a raiz de qualquer transação é mantida na Blockchain de tal forma a mantê-la intacta, porém transações antigas que estão no interior do bloco são descartadas para que espaço em disco seja salvo, mas de qualquer forma o rastro é mantido ali através do *hash* raíz (*root hash*). Nakamoto afirma que de acordo com a Lei de Moore, que afirma que o poder de processamento dos computadores dobraria a cada 18 meses pelo mesmo custo (https://pt.wikipedia.org/wiki/LeideMoore. Consultado em 11 de março de 2018), o crescimento da Blockchain não seria um problema visto a capacidade das novas memórias que estariam por vir.

Para a verificação de um pagamento, não é necessário rodar toda a rede em um só nó, basta apenas ter uma cópia da cadeia mais longa de prova de trabalho (onde é possível obter consultando nós da rede até que o usuário esteja convencido de que ele tem a cadeia mais longa) e o *hash* do bloco. Um único nó não pode checar a veracidade da transação, é necessário que ele se conecte a outro nó, conseguindo assim se conectar à Blockchain. Caso a versão do nó esteja desatualizada, uma atualização acontecerá para que assim possa dar prosseguimento à operação. Nakamoto afirma que este método de verificação é seguro desde que os nós honestos controlem a rede, mas é mais vulnerável em caso de a rede ser tomada por nós fraudulentos. Uma estratégia sugerida é que um alerta deve ser enviado pelos nós honestos que detectaram algum bloco inválido na Blockchain, informando aos outros nós que façam um *download* de uma cópia completa da Blockchain, confirmando assim a inconsistência dos blocos. Para fins de segurança e rápida verificação, Nakamoto acredita que negócios que recebem pagamento frequentes provavelmente vão querer rodar seus próprios nós.

No campo das transações, é possível combinar e dividir valores de uma transação, onde há a possibilidade de transferir cada centavo da transação que está sendo feita, porém isto é ineficiente. Na verdade, os valores da transferência são divididos e recombinados. Você pode ter um único input de uma grande transação anterior ou vários inputs combinando valores menores e no máximo dois outputs: um que seria o pagamento e outro que seria o troco para o remetente, caso haja algum.

A Figura 2.7 simula como a pessoa A compraria Bitcoins para negociar com a pessoa B através do processo de corretoras. A pessoa A transfere o seu dinheiro para um banco e depois troca esse dinheiro por Bitcoin em alguma corretora. Aqui no Brasil nós temos algumas corretoras que fazem esse tipo de serviço, como a Foxbit, por exemplo. Com essa transação de reais para Bitcoin, a pessoa agora pode transacionar nesta moeda digital, como por exemplo transferir os Bitcoins para a pessoa B em troca de um produto ou serviço prestado. A pessoa B ao receber esta quantia de Bitcoin através de uma corretora pode vender estes Bitcoins na corretora, enviar o dinheiro para um banco e depois fazer a retirada.

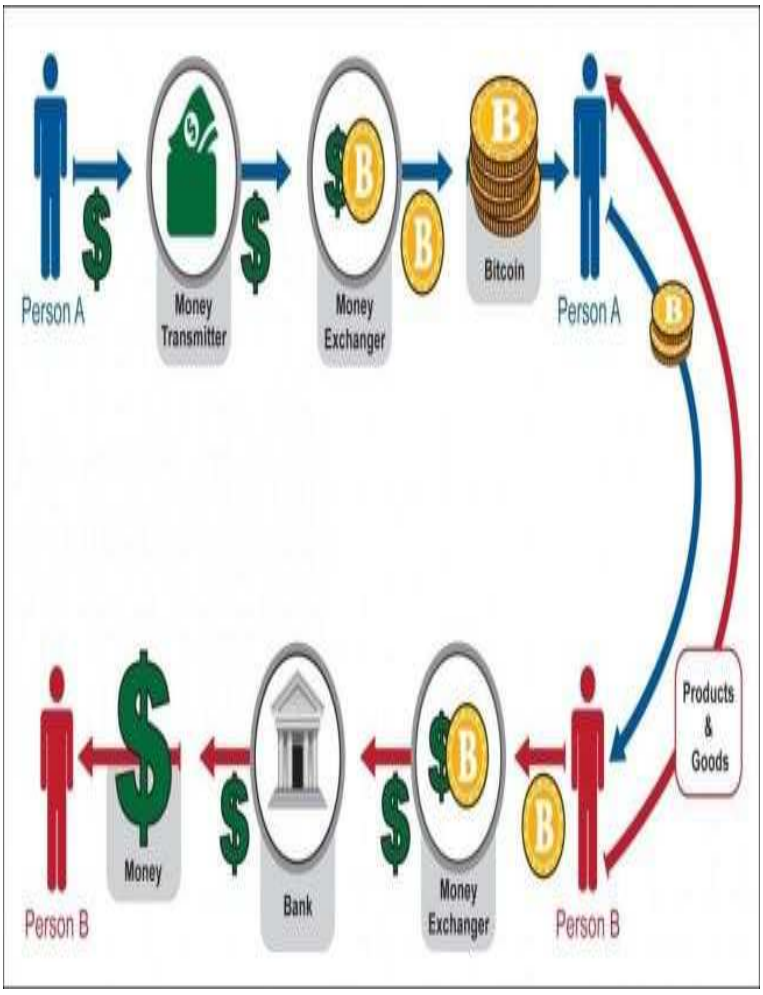

Figura 2.7: Exemplificação de transação entre duas pessoas A e B. Fonte: http://www.charteredonline .in/2017/02/bitcoins-india-mining-exchange-buy.html. Consultado em 11 de março de 2018

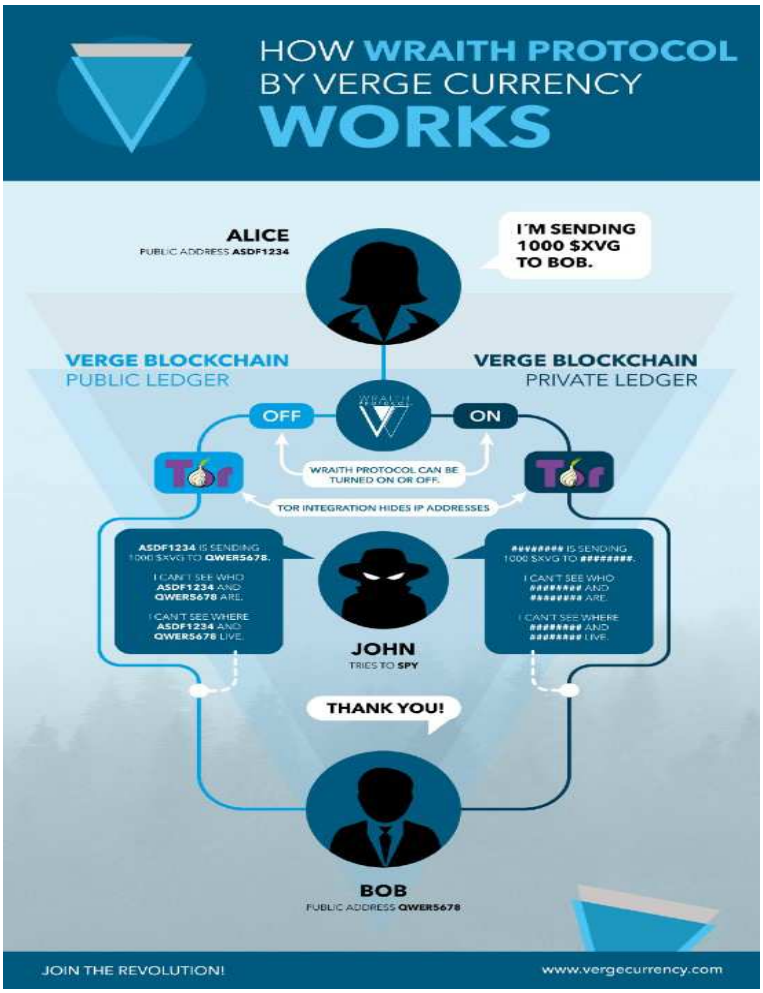

Figura 2.8: Exemplificação de transação entre duas pessoas A e B. Fonte: https://medium.com/verge-currency-xvg/what-is-the-wraith-protocol-bd1dfb289cda. Consultado em 11 de março de 2018

A privacidade é um ponto chave dentro do ecossistema do Bitcoin. Todas as transações são declaradas publicamente para toda a Blockchain, porém as chaves públicas, que seriam os endereços de cada usuário, não são conectadas com o dono do endereço. É possível saber que a pessoa A enviou 1 Bitcoin para a pessoa B ou quanto elas possuem nesses endereços, porém não é possível saber de fato quem é a pessoa A ou B. Há algumas criptomoedas, como a Monero ou a Verge que são mais focadas nesta questão da privacidade. A Verge, com o seu *Wraith Protocol*, promete levar ao usuário a escolha da privacidade e pode-se realizar uma comparação com a privacidade do Bitcoin na Figura 2.8, onde o Bitcoin seria o ramo da esquerda e no *Wraith Protocol* é possível escolher os dois ramos.

A parte de cálculos nos revela através de cálculos probabilísticos que há uma maior chance de um nó honesto alcançar um bloco antes de um nó frau-dulento. Se o nó fraudulento não der muita sorte no começo para achar os blocos, com o passar do tempo as chances dele diminuem drasticamente, para quase zero, pois ele ficará cada vez mais atrás do nó honesto no que concerne aos blocos, ou seja, quanto maior é a Blockchain, menor serão as chances do nó fraudulento de alcançar o nó honesto, onde os nós identificam

a maior cadeia de transações como sendo a verdadeira.

Nakamoto conclui o seu trabalho ressaltando os pontos mais marcantes de sua ideia, como um sistema de transações eletrônicos que não se baseia na confiança em um intermediário e sim na criptografia, assinaturas digitais que permitem um forte controle sobre a propriedade e gasto duplo, uso de uma rede *peer-to-peer* que se vale de prova de trabalho, entre outros aspectos.

Minerar é uma atividade muito competitiva entre os minerados, visto que minerar um bloco recompensa o minerador em Bitcoin. Para ser mais efetivo na mineração, novas tecnologias de *hashing* foram desenvolvidas, a fim de minerar com maior rapidez. Entre elas estão: *Graphical Processing Units* (GPUs), *Field Programmable Gate Arrays* (FPGAs) e *Application-Specific Integrated Circuits* (ASICs). Em 2014, a chance de minerar um bloco na primeira tentativa era de $7x10^{-20}$. Para garantir um pagamento regular aos mineradores, a capacidade computacional de cada minerador é unificada em centros de mineração (conhecidos como *pools* de mineração) que coordenam as atividades de mineração de cada minerador ali presente. O administrador deste *pool* de mineração terceiriza para os participantes do seu *pool* o problema ser solucionado na *proof-of-work* (PoW). Todos os participantes desse *pool* são remunerados em uma fração dos Bitcoins recebidos pelo esforço de minerar um novo bloco proporcional ao poder computacional oferecido por aquele minerador. Esta atividade gera uma centralização da mineração do Bitcoin, que pode ser perigoso para a rede. Caso alguns dos maiores *pools* se juntem, eles podem controlar a rede, como impedir transações de serem executadas, aprovar determinadas transações e gastos duplos (Arthur Gervais, Ghassan O. Karame, Vedran Capkun, and Srdjan Capkun. Is Bitcoin a decentralized currency? Disponível em https://eprint.iacr.org/2013/829.pdf). A Figura 2.9 ilustra como está a fatia de mercado dos maiores *pools* de mineração de Bitcoin para o período de 21 de março de 2018 até 24 de março de 2018. É possível ver que a soma dos quatro maiores pools de mineração representa quase 61% dos blocos minerados no período citado.

Atualmente, para uma transação entrar em um bloco, demora-se em média 10 minutos, que é a criação de cada novo bloco, isso sem contar o tempo de confirmação, que seria de aproximadamente uma hora (confirmação de 6 blocos). Soma-se a isso o fato do limite do bloco em 1MB. Essa combinação limita o número de transações que a Blockchain do Bitcoin processo por segundo, chegando até 7 transações por segundo no máximo (Croman, Kyle; Eyal, Ittay (2016). "On Scaling Decentralized Blockchains"). Em comparação a um meio comum de processamento de pagamento, a Visa lida com 150 milhões de transações diárias em média e é capaz de lidar com mais de 24000 transações por segundo (https://usa.visa.com/run-your-business/small-business-tools/retail.html. Consultado em 02 de abril de 2018). Com o Bitcoin se tornando cada vez mais popular, onde mais transações estão ocorrendo, problemas surgem. A Figura 2.10 ilustra a evolução do número de transações na Blockchain do Bitcoin confirmadas por dia.

O resultado de um tamanho insuficiente dos blocos é o aumento do tempo de processamento das transações e maiores taxas pagas por transação aos mineradores. Por conta do espaço limitado dos blocos, usuários precisam pagar tarifas mais altas para que suas ordens de transação sejam processadas e incluídas nos novos blocos pelos mineradores. Em suma, os usuários competem por um lugar dentro blocos e pagam por isso. (https://cointelegraph.com/explained/bitcoin-scaling-problem-explained. Consultado em 02 de abril de 2018).

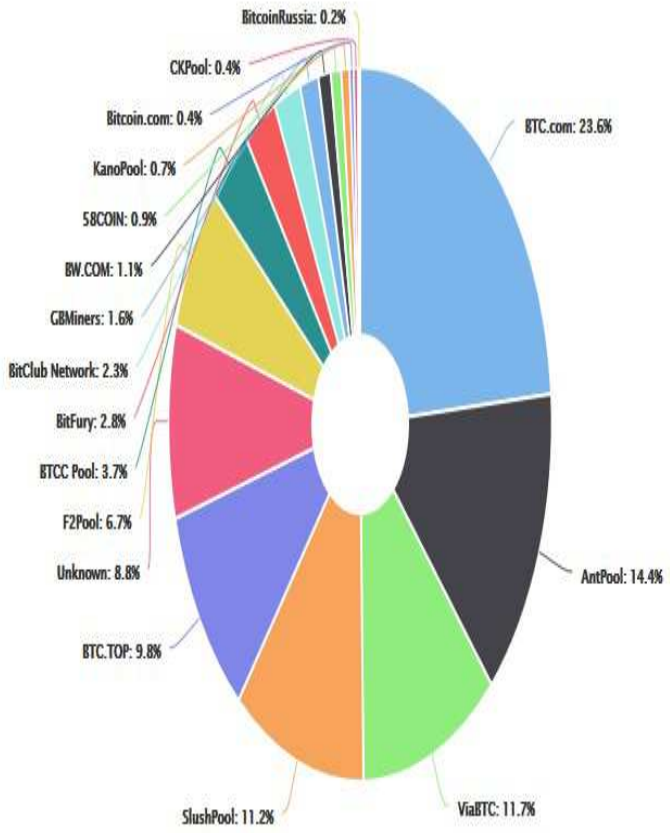

Figura 2.9: Fatia de mercado dos maiores pools de mineração de Bitcoin para o período de 21 de março de 2018 até 24 de março de 2018 (https://blockchain.info/pools?timespan =4days. Consultado em 24 de março de 2018)

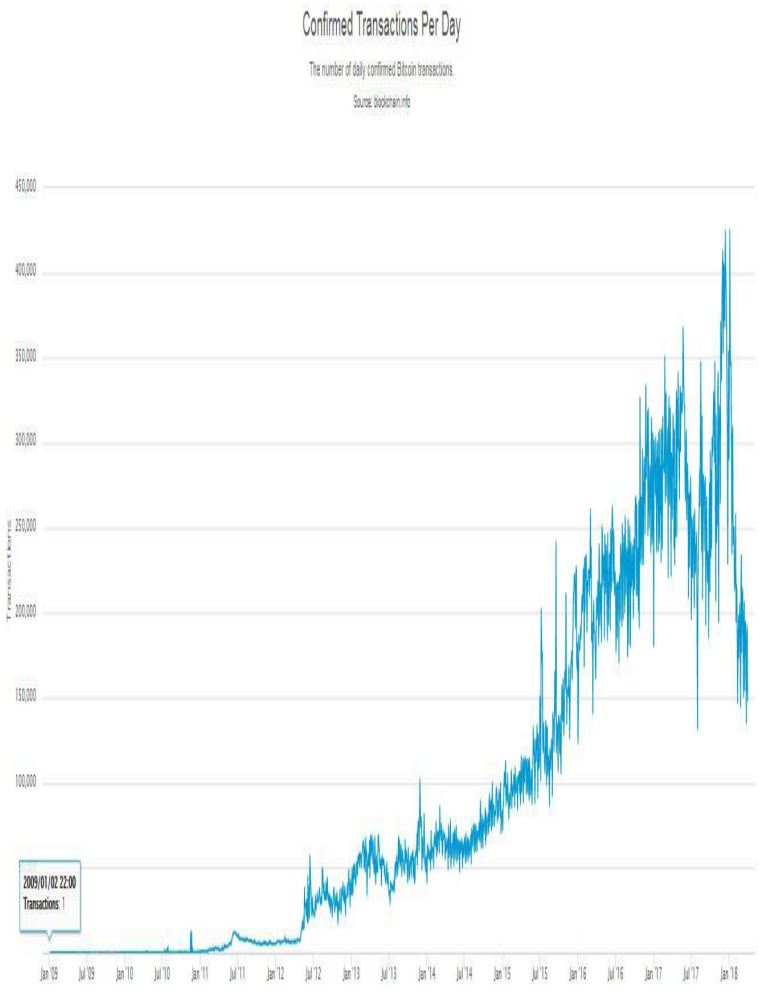

Figura 2.10: Evolução do número de transações na Blockchain do Bitcoin confirmadas por dia (https://blockchain.info/charts/n-transactions?timespan=all. Consultado em 02 de abril em 2018)

Uma das propostas rumo à escalabilidade do Bitcoin é de autoria do Dr. Pieter Wuille, onde ele propõe um método chamado *Segregated Witness* (SegWit). O que existe em um bloco é a informação da transação, na forma de script e de dados de assinatura. Enquanto a primeira inclui toda a informação como identidade de transação, valor, endereço de recebimento, entre outros, a segunda é uma chave única atribuída para cada usuário para performar transações e é utilizado para verificar se o usuário possui os recursos necessários para a transferência e a validade da conta (https://blog.unocoin.com/bitcoins-segwit-explained-5dc6b0afcb08. Consultado em 7 de abril de 2018). O problema é que os dados de assinatura são muito pesados, ocupando muito espaço dentro do bloco, além do fato de só ser necessário para o processo de verificação, não sendo necessário mais adiante (https://blockgeeks.com/guides/blockchain-scalability/. Consultado em 7 de abril de 2018). Com a implementação do SegWit, onde os dados serão transferidos para um bloco estendido paralelo ao bloco principal, espera-se aliviar espaço dentro do bloco (https://blog.unocoin.com/bitcoins-segwit-explained-5dc6b0afcb08. Consultado em 7 de abril de 2018). A Figura 2.11 é uma comparação da arrumação de blocos com SegWit e blocos sem SegWit.

Outra solução para o problema de escalabilidade, tanto para o Bitcoin como o Ethereum, é o *Off-Chain State Channels*. *State Channel* é uma comunicação em dois sentidos entre participantes que, em vez de ser realizada na Blockchain, vai ser realizada fora da Blockchain. Isso diminui o número de transações realizados na Blockchain, desafogando-a. Na verdade apenas duas transações são registradas na Blockchain: uma para quando o canal é aberto entre as diversas partes e uma para quando o canal é fechado. Realizar pequenas transações atualmente não é viável no sentido de rapidez e congestionamento da rede nem no sentido financeiro, pois uma taxa terá que ser paga aos mineradores por cada transação. Porém, neste tipo de transação *off-chain* isso é possível. Vamos supor que Bob, um cliente de uma cafeteria, quer comprar todo dia um copo de café e pagar em Bitcoin. As duas partes terão de abrir um canal de pagamento entre eles. Inicialmente, as partes depositam um valor de Bitcoin cada uma para realizar a transação. Vamos supor que Bob deposite 0,05 Bitcoin e a cafeteria nada, pois não há necessidade. Esses Bitcoins ficam guardados em endereço de assinatura múltipla, funcionando como se fosse um cofre que só pode ser aberto quando ambas as partes concordam em assim fazê-lo. Um balanço patrimonial também é feito onde, neste caso, consta que Bob possui 0,05 Bitcoin e a cafeteria nada. Este balanço patrimonial inicial é inserido na Blockchain para que haja transparência. Estabelecido o canal, Bob pode pedir o seu café diário, onde Bob receberá o café da cafeteria e terá de pagar um valor em Bitcoin para a mesma. Esta transação entre Bob e a cafeteria é atualizado no balanço patrimonial e validada por ambas as partes através das chaves privadas. Essa transação pode ser repetir várias vezes até que os recursos financeiros de Bob nesse canal acabem ou que qualquer uma das partes resolva fechar o canal de pagamento, sem ficar refém da decisão da outra parte. Para isso, basta transmitir o último balanço patrimonial validado entre as partes para a Blockchain. Mineradores irão validar as assinaturas no balanço patrimonial e, se tudo estiver correto, liberarão os fundos que estavam no cofre virtual baseado neste último balanço patrimonial e registrando esta última transação na Blockchain. O sistema garante que apenas o último balanço patrimonial assinado será considerado. Outra vantagem deste sistema é que, para realizar transações com outras partes, não é necessário abrir um canal de pagamento com todas elas: a rede irá conectar dois pontos que não possuem um canal de pagamento ativo

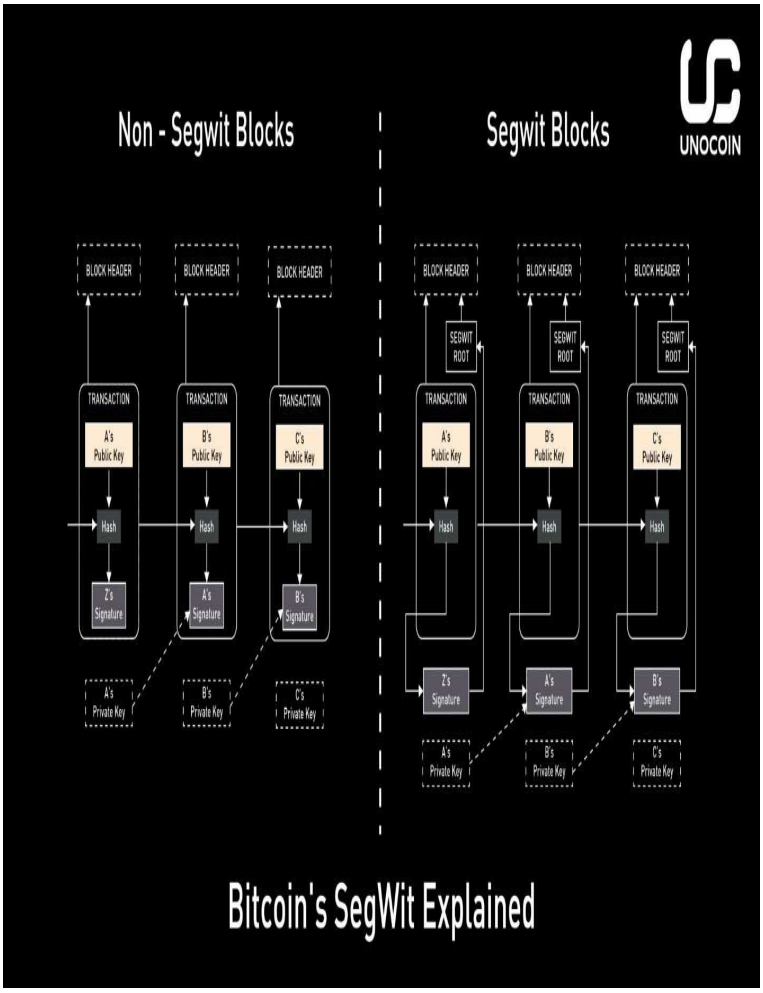

Figura 2.11: Comparação entre blocos utilizando SegWit e blocos sem SegWit (https://blog.unocoin .com/bitcoins-segwit-explained-5dc6b0afcb08. Consultado em 7 de abril de 2018)

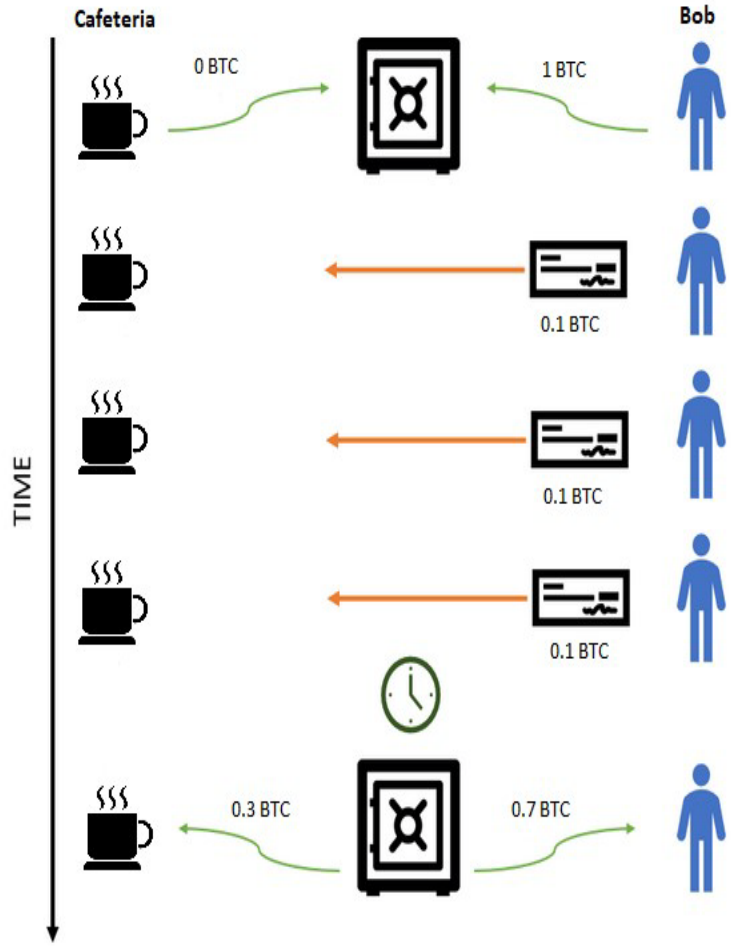

Figura 2.12: Transações realizadas entre Bob e a cafeteria (Fonte: Autor, adaptado de https://www.investinblockchain.com/lightning-network-bitcoin-scaling/.)

com outros pontos que possuem estes canais de pagamento, até que os pontos interessados se conectem. Voltando ao exemplo da cafeteria, se Alice quer comprar um café na mesma cafeteria que Bob compra, supondo que Alice e Bob tenham um canal de pagamento ativo e Alice e a cafeteria não tem esse canal de pagamento ativo, é possível que Alice envie a quantidade de Bitcoins necessária para a cafeteria se utilizando de Bob. Há desenvolvimento neste conceito de *Off-Chain State Channels* tanto para o Bitcoin (com a *lightning network*) como para o Ethereum (com o Raiden). Para maiores detalhes sobre a exemplificação de *Off-Chain State Channels* no caso da *lightning network*, consultar o seguinte link: https://www.youtube.com/watch?v=rrr_zPmEiME (Consultado em 7 de abril de 2018). A Figura 2.12 exemplifica as transações realizadas entre Bob e a cafeteria.

2.2.2 Ethereum

Após a introdução do conceito disruptivo causado pelo *whitepaper* de Nakamoto, muitas moedas digitais que surgiram com o passar do tempo foram inspiradas no Bitcoin. Atualmente, a moeda digital com o segundo maior valor de mercado é o Ethereum (58 bilhões de dólares), só perdendo para o Bitcoin (137 bilhões de dólares) (https://coinmarketcap.com/. Consultado em 15 de março de 2018.)

Em 2013, Vitalik Buterin, um programador russo-canadense, lançou o *whitepaper* do Ethereum (A next generation smart contract & decentralized application platform, 2013). Buterin já era conhecido na comunidade, tendo contribuído para a programação central do Bitcoin também (https://medium.com/FolusoOgunlana/cracking-the-ethereum-white-paper-e0e60c44126. Consultado em 16 de março de 2018). Ele começa o seu trabalho contando um pouco da história atrás do conceito das criptomoedas, onde começou na década de 1980 protocolos anônimos *e-cash*, porém estes falharam em conseguir tração do projeto pelo fato de ainda ter uma figura centralizadora no ecossistema. De fato, como citado anteriormente, a primeira ideia de uma moeda digital descentralizada veio com Wei Dai em 1998. Buterin continua esta seção falando um pouco sobre o Bitcoin e como essa nova tecnologia foi disruptiva, tanto em termos políticos de uma moeda sem uma figura de um banco central por trás, como também da volatilidade do preço, a programação atrás dessa plataforma, mineração nesta Blockchain, como é feito o *scripting* e por fim indica algumas limitações do Bitcoin.

Segundo o próprio *whitepaper* de Nakamoto, o Bitcoin é uma forma de transferência de dinheiro de A para B através de uma moeda digital onde não há a necessidade de uma terceira entidade para mediar a negociação. Ambas a moedas compartilham de características comuns, como resistente à censura, prova de violação, economicamente segura e descentralizada (https://medium.com/FolusoOgunlana/cracking-the-ethereum-white-paper-e0e60c44126. Consultado em 16 de março de 2018). Além desses traços compartilhados, o Ethereum pretende ir além: ser uma plataforma descentralizada para aplicações que funcionem da forma como foram programadas para tal, onde não há chance de fraude, censura ou alguma interferência de um agente externo. É importante frisar que Ethereum é o nome da Blockchain, enquanto Ether é a moeda digital. A principal função do Ethereum é permitir a criação dos *smart contracts*.

Um *smart contract* seria um contrato entre duas partes, programado na Blockchain, onde o acontecimento de algum evento ativa este mesmo contrato para fornecer os outputs já acordados anteriormente neste contrato. Esta plataforma trabalha com o conceito de *If-Then* (se-então) e é fiscalizado por muitos nós na Blockchain, o que gera uma maior segurança de cumprimento do acordado ou a não realização da transação. Um exemplo simples seria: no dia 15 de março de 2019, transfira 100 Ethers da pessoa X para a Y se a pessoa X tiver, no mínimo 100 Ethers na data da transação. Caso a pessoa X não tenha essa quantia na data da transação, não transfira. A Figura 2.13 ilustra um *smart contract*.

Smart contracts possuem vastas utilizações na vida real. Um exemplo seria a votação nos EUA. A votação ficaria mais segura, pois para fraudar uma eleição precisaria decodificar uma quantidade enorme de votos já contabilizados na Blockchain e, para isso, necessitaria de uma quantidade de processamento computacional enorme. Além disso, as taxas de participação poderiam ser elevadas, já que nos EUA o voto não é obrigatório, visto que as pessoas não precisariam sair de suas casas para votar. Outro exemplo se-

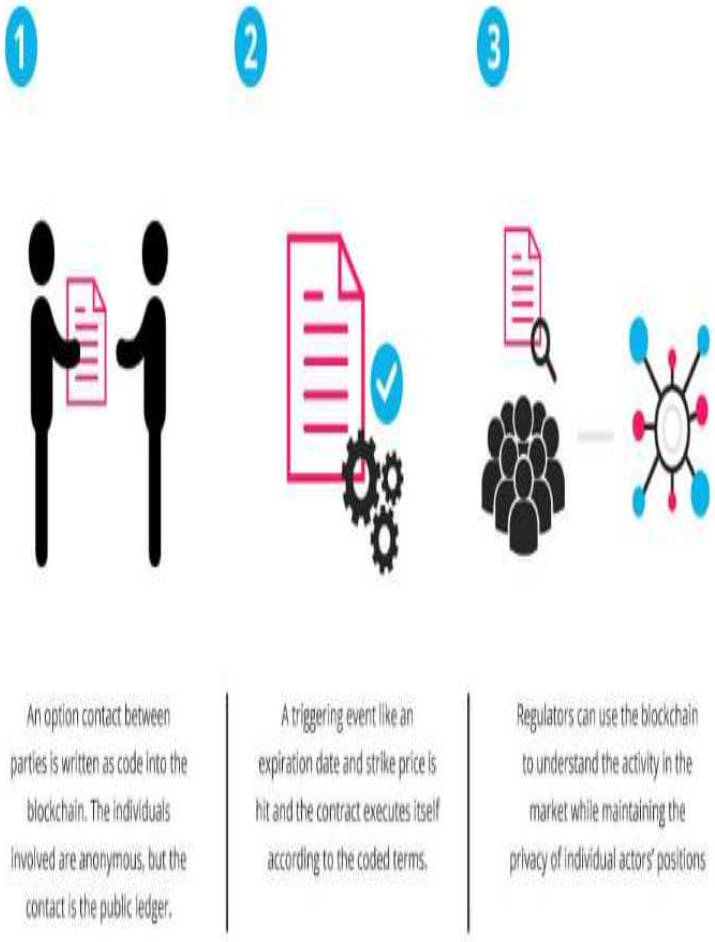

Figura 2.13: Explicação de *smart contract*. https://blockgeeks.com/guides/smart-contracts/ (Consultado em 15 de março de 2018)

ria a utilização para o campo logístico. A cadeia de suprimentos, em geral, é longa, onde cada nível necessita da aprovação do nível anterior para que o processo continue. Além de tomar tempo é improdutivo. Com *smart contracts*, é possível evitar perdas e fraudes ao longo do caminho, onde tarefas e pagamentos podem ser automatizados de acordo com o contrato. Áreas bancárias, gerenciamento, seguros, entre outros, podem se valer do benefício de *smart contracts* https://blockgeeks.com/guides/smart-contracts/ (Consultado em 15 de março de 2018).

Algumas das vantagens dos *smart contracts* seriam:

1. Segurança (pelo fato dele ser encriptado e distribuído ao longo dos nós, onde há a garantia de que nada é perdido ou modificado sem consenso da rede);

2. Rápido e econômico (pela automação dos processos e eliminação de quase todos os intermediários);

3. Padronização/customização (há vários tipos de *smart contracts* atualmente. É possível escolher o que mais se adapta para a realidade da situação e modificá-lo).

Porém, *smart contracts* também apresentam problemas como:

1. Fator humano - Visto que o código é desenvolvido por humanos, há a possibilidade de falha do mesmo. Um caso famoso de erro no código aconteceu em 2016 com DAO (*Decentralized Autonomous Organization*), onde hackers invadiram o sistema e roubaram 55 milhões de dólares em moedas DAO. Os hackers, devido a uma condição na programação da DAO de que retiradas só poderiam ocorrer após 34 dias após o pedido inicial, tiveram de esperar para realizar a retirada, caso assim desejassem. Ou seja, é como assaltar um banco e ter de esperar 34 dias para poder sair. O debate na comunidade foi tão grande que uma questão se colocou presente: desfazer, através de um *hard fork*, o ataque sofrido pela DAO ou continuar com a mesma Blockchain. Com o apoio do próprio fundador do Ethereum, Vitalik Buterin, a maioria dos nós concordou e o *hard fork* foi realizado, onde a ação dos hackers pode ser desfeita nesta nova Blockchain, conhecida hoje como Ethereum (o nome foi mantido ao original). Porém, algo curioso chamou a atenção: esperava-se que a Blockchain original do Ethereum, onde o ataque ocorreu, acabaria com o tempo, mas ela continuou transacionando e crescendo, onde viria a ser conhecida como Ethereum Classic (ETC). Nesta Blockchain do Ethereum Classic, os hackers ainda haviam o controle do que eles haviam roubado, graças ao fato da Blockchain se manter ativa. Defensores que viam *hard fork* como sendo uma violação dos valores fundamentais da Blockchain (não adulteração da mesma) apoiaram a continuação do Ethereum Classic (https://www.bloomberg.com/features/2017-the-ether-thief/. Consultado em 15 de março de 2018);

2. Incerteza do *status* legal - atualmente *smart contracts* não são regulados pelo governo e, consequentemente, passíveis de uma regulação, no sentido legal;

3. Custos de implementação - Custos de se criar um *smart contract* são altos, pois é preciso ter conhecimento em programação para fazê-lo de maneira correta e segura. Buterin sugere em seu *whitepaper* que o Ethereum aliado com outros sistemas pode fazer com que a programação seja facilitada para não-programadores;

4. Irreversibilidade do processo - uma ação realizada dentro da Blockchain não poderá ser revertida, a menos que haja um *hard fork*, o que não é um processo simples, pois a maioria dos nós da rede deve concordar com essa mudança (um dos desdobramentos do caso da invasão do sistema da DAO). https://cointelegraph.com/explained/smart-contracts-explained (Consultado em 15 de março de 2018).

A criação do Ethereum se dá pelo fato de ser muito complexo programar códigos mais rebuscados na Blockchain do Bitcoin, que viabilizariam os *smart contratcts*, por exemplo. Na Blockchain do Bitcoin, mais complexidade do código demanda maior espaço dessa transação no bloco. Logo, taxas mais altas seriam pagas aos mineradores, visto que os blocos do Bitcoin são limitados em 1 MB (antes da SegWit). Usuários pagariam mais caro para ter as suas transações efetuadas rapidamente pelos mineradores, aumentando a demanda e, consequentemente as taxas de transação. Essas limitações da Blockchain do Bitcoin a tornam mais complexa, porém não impossível, de realizar programações em um nível mais rebuscado, como seriam as dos *smart contracts*. Antes de criar o Ethereum, Buterin sugeriu modificações no protocolo do Bitcoin, mas não foi bem aceito pela comunidade pois, por ser um projeto nunca testado antes, havia um temor de que alguma mudança no código-fonte pudesse gerar problemas graves. E então ele resolveu criar o Ethereum (A next generation smart contract & decentralized application platform, 2013).

A mais significativa diferença entre o Ethereum e o Bitcoin é que o Ethereum utiliza uma linguagem de programação diferente, que é a Turing-Completo (nome dado em homenagem ao britânico Alan Turing, conhecido também como o pai da computação). De maneira simplificada, essa linguagem permite que pequenas transações podem descrever tanto operações mais simples como operações mais complexas. Olhar apenas para o tamanho da transação não é o suficiente para dizer a complexidade da mesma. O uso dessa programação na verdade é um *trade-off* entre Ethereum e Bitcoin. Se por um lado o Ethereum concede poder aos programadores, algo necessário para que os *smart contracts* sejam realizados, por outro lado esse mesmo poder é dado à hackers, que podem acabar atacando a rede, como visto no caso DAO. Já com o Bitcoin, por conta do limite dos blocos e quanto maior a complexidade maior a transação na Blockchain, isso limita tanto programadores quanto hackers que queiram se valer maliciosamente da rede (https://medium.com/FolusoOgunlana/cracking-the-ethereum-white-paper-e0e60c44126. Consultado em 16 de março de 2018).

A fim de evitar que o problema de hackers se aproveitarem do poder que a plataforma Ethereum concede para os seus usuários, para cada transação o usuário precisa gastar algo chamado *gas*. Mineradores podem não aceitar transações que não tenham *gas* suficiente para completar a transação, retendo o *gas* insuficiente para eles próprios. Um bom exemplo seria o de uma corrida de táxi. Você comunica ao taxista o quanto você vai pagar por quilometro percorrido (taxa) e o quanto estará trazendo consigo (limite). Caso o taxímetro chegue no seu limite antes de chegar no seu destino, o taxista pega o seu dinheiro, você é expulso do táxi e volta ao ponto inicial de onde pegou o táxi. No Ethereum, a taxa é o preço do *gas* e o limite é chamado de *gas limit*. Caso um hacker queira atacar a rede, ele provavelmente não terá *gas* o suficiente para realizar este ataque, ficando sem *gas* e o ataque não sendo concretizado. A Figura 2.14 nos mostra um gráfico com a média dos preços de gas ao longo dos anos em Wei (uma subdivisão do Ether) e o preço mais detalhado de 15 de março de 2018 (A next generation smart contract &

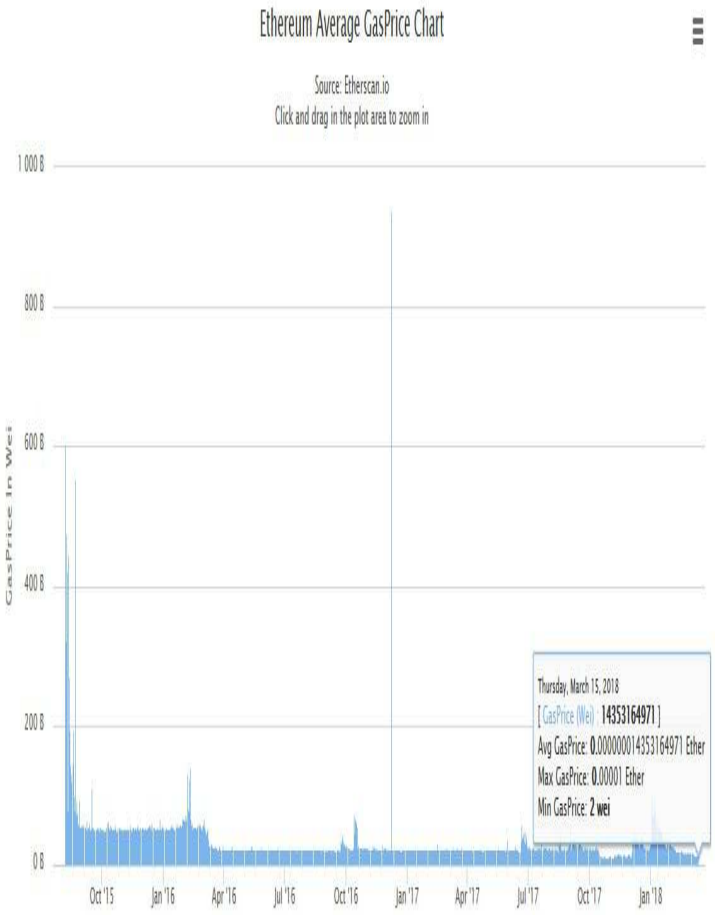

Figura 2.14: Média de preço do *gas* para o Ethereum. https://etherscan.io/chart/gasprice (Consultado em 17 de março de 2018).

decentralized application platform, 2013).

É fundamental que haja consenso descentralizado (grande número de pessoas separados geograficamente concordo em alguma questão). A Figura 2.15 ilustra uma rede descentralizada e diferentes distribuições de *ledgers*.

No caso das criptomoedas, seria concordar em quais blocos ou transações são válidos ou não para a rede) na Blockchain para as validações dos blocos. Os mineradores (validadores ou forjadores, no caso do *proof-of-stake*(PoS)) garantem as validações das transações ou dos blocos. Como citado anteriormente, o Bitcoin se utiliza da PoW como sendo uma peça extremamente importante para a sua Blockchain, onde um enorme esforço computacional é feito pelos minerados a fim de garantir a validação de determinados blocos e transações. Como recompensa, os mineradores ganham Bitcoins ao minerar um novo bloco, além das frequentes taxas de transação. Apesar do benefício de ser extremamente difícil e custoso um ataque em uma rede que se vale de PoW, há também pontos negativos como: a quantidade de energia para minerar Bitcoins é muito alta e, consequentemente, custosa, maior poder de computação necessário, que também é mais custoso, não há lealdade dos minerados à rede (eles podem minerar outra moeda caso essa ofereça maiores

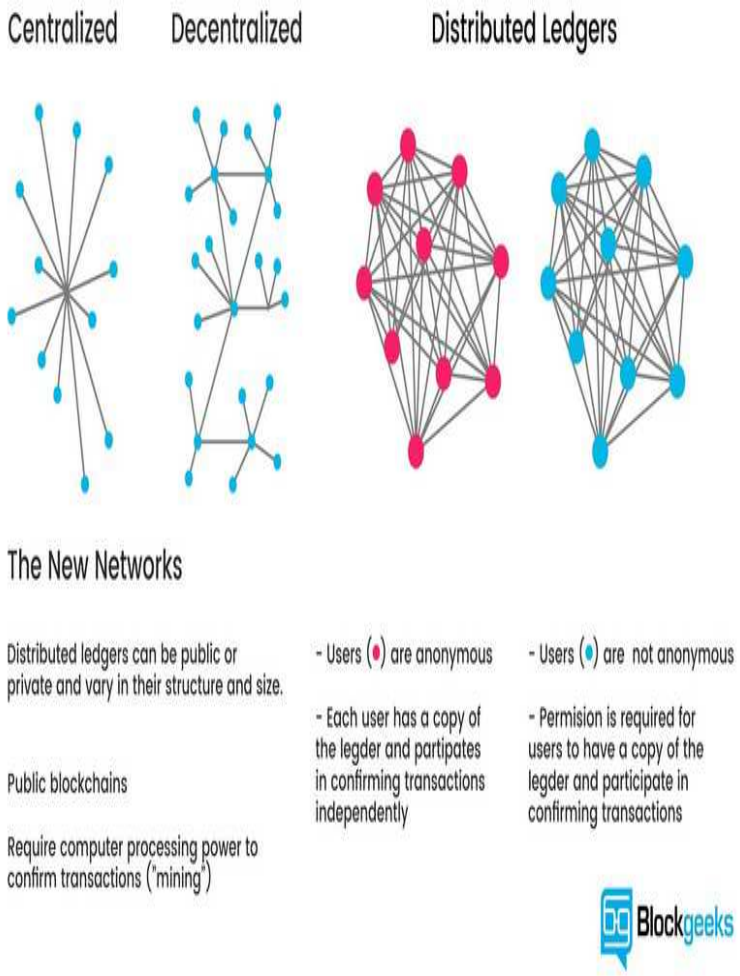

Figura 2.15: *Networks* e *ledgers*. https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/. Consultado em 18 de março de 2018

recompensas), entre outros. (https://medium.com/karthik.seshu/cryptocurrency-proof-of-work-vs-proof-of-stake-e1eee1420b10 . Consultado em 18 de março de 2018). No PoW, mineradores competem entre si para conseguir minerar um bloco primeiro e conseguir a sua recompensa. De maneira simples, o processo de mineração no PoW se dá por tentativa e erro de descobrir a senha de um cadeado complexo. Quanto mais mineradores na Blockchain, maior a capacidade computacional. Como a Blockchain do Bitcoin (utilizando seu algoritmo SHA-256), através de quer manter a criação o tempo de criação entre os blocos constante, a dificuldade para abrir este cadeado é aumentada (https://www.youtube.com/watch?v=apdQsrwAEXE. Consultado em 17 de março de 2018).

Atualmente o Ethereum também se vale de PoW, porém há uma pretensão em migrar para a PoS com uma *hard fork*, que seria o algoritmo Ethash sendo substituído pelo novo algoritmo Casper. Em geral, PoS funciona da seguinte forma: a Blockchain mantém registro de um conjunto de validadores, e qualquer pessoa que detém a moeda em questão (no caso Ethereum, Ether) pode se tornar um validador enviando um tipo especial de transação que bloqueia seu Ether em um depósito. O processo de criação e aceitação de novos blocos é feito através de um algoritmo de consenso que todos os validadores atuais podem participar (https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ. Consultado em 18 de março de 2018). Com esse depósito, Buterin espera minimizar ataques de hackers à rede, visto que um comportamento errado de um usuário poderá resultar em perder o dinheiro enviado por depósito e exclusão do *pool* de validadores (https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/. Consultado em 18 de março de 2018). Algumas das vantagens do PoS seriam: redução do consumo de eletricidade (em comparação ao Bitcoin, por não se valer de tanto poder computacional requerido pelo PoW), não há necessidade de comprar *hardwares* caros(ASICs, por exemplo ou qualquer outro para mineração), validadores mais leais (a lealdade deles está no fato dos critérios de seleção, como por exemplo ter uma moeda por mais tempo, em algumas Blockchains, conta como critério também para ser escolhido como validador, como é o caso da Peercoin) e Blockchains mais rápidas. Validadores não ganham recompensas por novos blocos validados, ganham como incentivo taxas de transação. Uma preocupação relacionada ao PoS é relacionada à centralização da mineração, onde o minerador que possuir mais moedas nessa rede terá uma vantagem sobre outros mineradores. A Figura 2.16 sumariza uma comparação entre PoW e PoS.

A Tabela 2.1 ilustra algumas das principais diferenças entre Bitcoin e Ethereum. É importante notar que, segundo o site etherscan.io, a média de criação dos últimos 5000 blocos foi de 13,9 segundos (consultado em 8 de abril de 2018).

Assim como no Bitcoin, o Ethereum atualmente não possui escalabilidade. Para o caso do Ethereum, cada bloco possui um limite de *gas*. A Figura 2.17 indica o número médio de limite de *gas* para o Ethereum.

Mineradores só podem incluir em determinado bloco o limite de *gas*, que seria o somatório de todo o gas utilizado nas transações. Isso é um limitante no que tange à escalabilidade do Ethereum. A Figura 2.18 exemplifica um do Ethereum com um limite de *gas* de 8.000.000.

Além da *Off-Chain State Channels* já citada anteriormente na seção sobre escalabilidade do Bitcoin (o Ethereum usará esse conceito com o Raiden), há outras formas de escalabilidade para o Ethereum, sendo uma delas o *sharding*. O maior problema

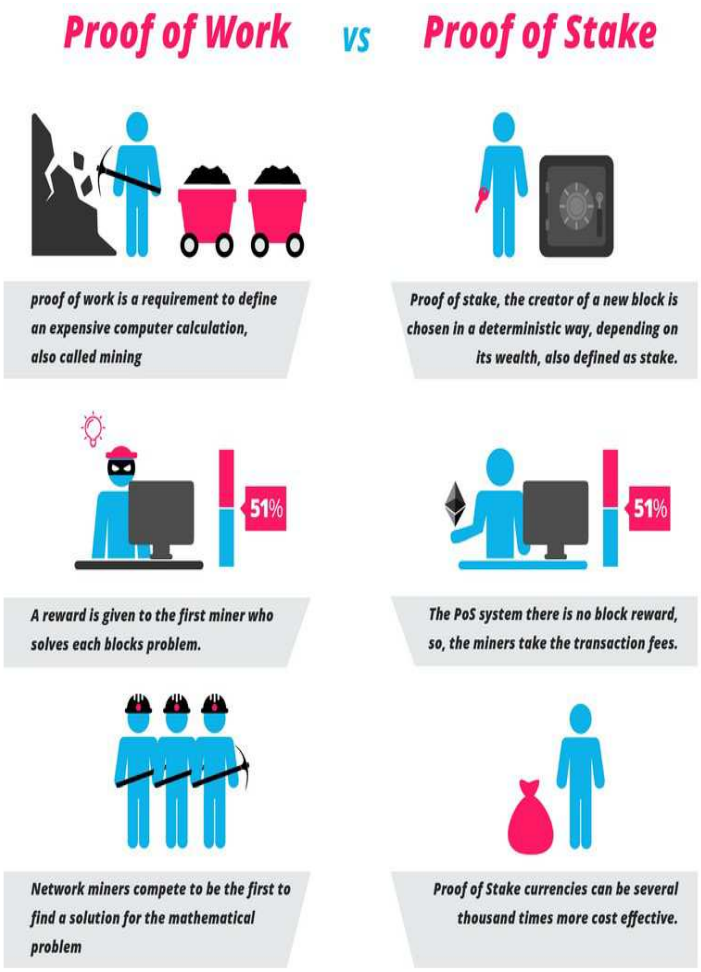

Figura 2.16: *Proof-of-work* (PoW) *vs* *Proof-of-stake* (PoS). https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/. Consultado em 18 de março de 2018

Tabela 2.1: *Principais diferenças entre Bitcoin e Ethereum.*

	Bitcoin	Ethereum
Criado por	Satoshi Nakamoto	Vitalik Buterin
Criado em	Janeiro, 2009	Julho, 2015
Modo de lançamento	Bloco Genesis	Pré-venda
Tipo de prova	Proof-of-work	Proof-of-stake
Uso	Moeda digital	Moeda digital e smart contracts
Criptomoeda	Bitcoin	Ether
Algoritmo	SHA-256	Ethash
Tempo médio de mineração	10 minutos	14.2 segundos
Possui Turing-completo?	Não	Sim

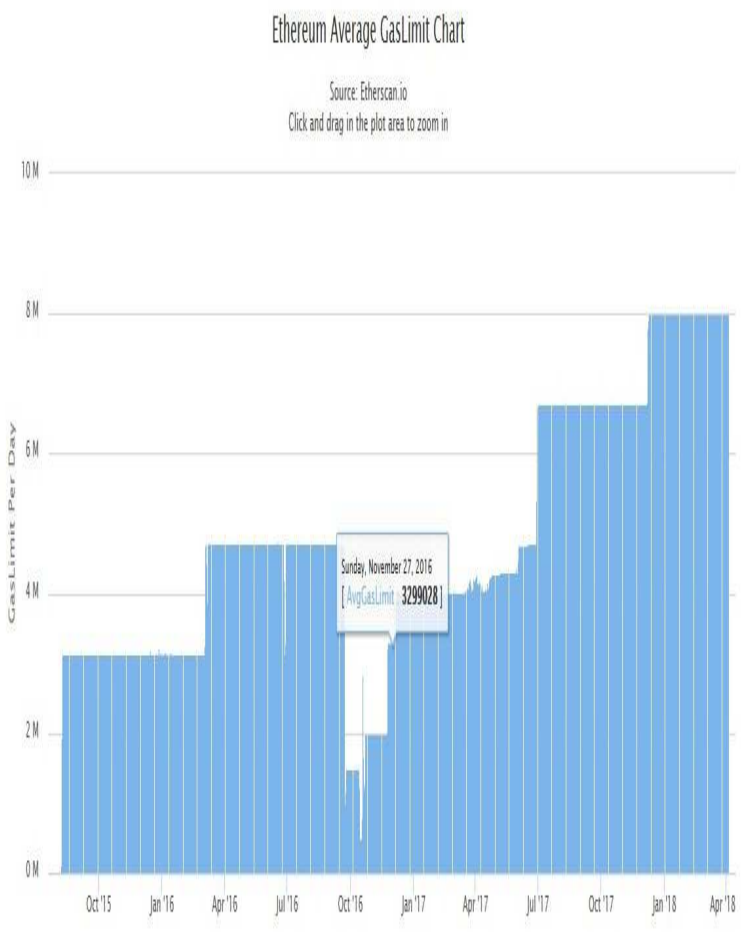

Figura 2.17: Número médio de limite de *gas* para o Ethereum. (https://etherscan.io/chart/gaslimit. Consultado em 8 de abril de 2018)

Figura 2.18: Exemplificação de um bloco com limite de *gas* de 8.000.000 para o Ethereum (Autor, adaptado de https://blockgeeks.com/guides/blockchain-scalability/. Consultado de 8 de abril de 2018)

que o Ethereum sofre atualmente é o tempo de verificação. Todos os nós da rede precisam fazer um *download* e salvar toda a blockchain. O que o método *sharding* faz é decompor a transação em fragmentos e espalha isso através da rede. Os nós trabalham em fragmentos individuais lado a lado, diminuindo assim o tempo total gasto (https://blockgeeks.com/guides/blockchain-scalability/. Consultado em 8 de abril de 2018). Se um nó necessita saber de transações ou blocos que não estão armazenados nele, então este nó irá procurar outro nó que possui a informação que ele necessita. O problema deste método é relacionado à confiança, visto que nós precisarão confiar na informação vinda de outros nós. O Ethereum quer resolver esta questão através de incentivos criptoeconômicos que levariam os nós a agir da maneira correta, ou seja, transmitindo informações válidas para outros nós (https://www.coindesk.com/information/will-ethereum-scale/. Consultado em 8 de abril de 2018).

Buterin conclui o seu *whitepaper* afirmando que a intenção do Ethereum é ser uma melhoria no quesito criptomoeda, mas não apenas isso: é ser um protocolo para aplicações descentralizadas como armazenamento de arquivos descentralizado, computação descentralizada, entre outras funções, onde a linguagem de programação Turing-completo significa que contratos podem teoricamente ser criados para qualquer tipo de transação ou aplicação.

2.2.3 Ripple

Ripple é uma Blockchain voltada para liquidações interbancárias. Ao contrário de muitas outras Blockchains, Ripple foi desenhado para trabalhar com instituições já existentes para facilitar a capacidade de transacionar qualquer ativo de maneira bem rápida em um nível global. A Blockchain da Ripple evoluiu completamente independente da Blockchain do Bitcoin e suas *forks*. Além da finalidade de ser utilizada como uma plataforma para facilitar a troca de ativos entre bancos, Ripple também possui a sua moeda digital, a XRP, que funciona além de uma transferência de valor (já que a moeda XRP possui um valor de mercado) também como uma taxa entre as negociações a fim de evitar o *spam* da *network* (Ripple ($XRP) Analysis, Multicoin Capital, 2017).

Ripple foi desenvolvida em um protocolo de consenso descentralizado de código aberto (*Ripple Protocol Consensus Algorithm* ou RPCA), onde o seu criador é a Ripple Labs. Foi fundada em 2012 por Chris Larsen e Jed McCaleb, tendo sua sede em São Francisco, Califórnia, Estados Unidos (https://en.wikipedia.org/wiki/Ripple_(company)). Consultado em 22 de março de 2018). Originalmente, a Ripple *network* foi criada com uma capacidade de suprimento de 100 bilhões de XRP, onde 20% foram alocados para os fundadores da Ripple, 25% para a Ripple Labs e os 55% restantes prontos para serem distribuídos para promover o crescimento da *network* (Armknecht, Karame, Mandal, Youssef e Zenner (2015)). Atualmente, a Ripple possui 61 bilhões de XRP contra 39 bilhões de XRP no mercado. Hoje, cada XRP tem um valor de mercado de 0,66 USD, garantindo o terceiro maior de valor de mercado, com 26 bilhões de dólares (https://coinmarketcap.com/. Consultado em 22 de março de 2018). Vale notar que o valor de mercado é sobre as moedas em circulação, não contando as represadas pela Ripple.

Para entender a proposição de valor da Ripple, é necessário antes entender o problema para o qual ela pretende solucionar. Ao depositar dinheiro no banco, é como se você estivesse concedendo uma linha de crédito para o mesmo, onde ele fica te devendo este valor e você pode solicitar o resgate, mesmo que parcial, a qualquer instante, acreditando que o banco cumprirá com as suas obrigações e te pagará. É simples transferir dinheiro de uma pessoa para outra dentro do mesmo banco. Há apenas uma atualização do *ledger* interno do banco, onde grava quanto o banco deve para cada um de seus clientes (Ripple ($XRP) Analysis, Multicoin Capital, 2017).

A situação fica mais complexa quando há a necessidade de transferência de um banco para o outro. É necessária uma relação de confiança entre os bancos participantes. Por exemplo, vamos supor que um cliente do banco A queira transferir dinheiro para um cliente do banco B. Este sistema só é válido se o banco B estiver disposto a receber uma IOU (*I Owe You* ou Eu Te Devo, traduzido) do banco A, mas isso nem sempre é o caso. Não é no caso anterior uma atualização do *ledger* interno de cada banco. Esses bancos, em algum momento, precisam realmente trocar dinheiro entre si. E este tipo de transação acontece periodicamente com quantias de dinheiro transferidas entre as partes. O sistema de IOU procura diminuir a ineficiência de ter que transferir constantemente dinheiro real entre os bancos. Porém, como dito anteriormente, nem sempre um banco confia no outro para cumprir as suas obrigações. Para isso, há a necessidade de esperar que o dinheiro seja de fato transferido de um banco para o outro ou que esta transação ocorra através de uma terceira parte de confiança para ambos os bancos envolvidos. Ambos os processos são mais lentos e custosos que a simples transação por IOU (Ripple ($XRP) Analysis, Multicoin Capital, 2017). Quanto mais intermediários no processo, mais lentos e custosos são os

Figura 2.19: Atual processo de transações entre bancos. https://ripple.com/files/ripple_vision.pdf. Consultado em 23 de março de 2018

processos de transferência, além de ter uma visibilidade obstruída e cada transação representa um possível ponto de atraso ou falha (https://ripple.com/files/ripple_vision.pdf. Consultado em 23 de março de 2018). A Figura 2.19 ilustra o atual processo de transações entre bancos que possuem uma linha de confiança entre si com a ajuda de outras partes que viabilizam o processo.

A rede desenvolvida pela Ripple elimina os problemas supracitados com Blockchain. O sistema tradicional é lento, custoso e propenso ao erro. Bancos precisam coordenar transferências de valor por diferentes bases de dados internas, fazendo assim com que as transações se concretizem de maneira devagar além do fato de aumentar o capital de giro necessário por parte do banco (bancos precisam abrir diversas contas ao redor do mundo e ter dinheiro em moeda local nessas contas para que as transações também sejam realizadas. Contas com essa finalidade são conhecidas como contas *nostro*. Ter quantias paradas de dinheiro nessas contas esperando para realizarem transações é ineficiente e, caso o banco precise realizar alguma transação em uma moeda que ele não possua conta e moeda local, precisará confiar em uma terceira parte, chamada de provedor de liquidez. Além de ser um risco, o capital do banco que necessita realizar a transferência pode ficar

preso, em trânsito, por dias. Ripple vem para mudar esse panorama, saindo de um sistema desconexo e baseado em confiança para uma base única, que seria o protocolo Ripple. Isso dá às transações fluidez, rapidez e libera capital de giro dos bancos. A rede da Ripple pode ser encarada como um mapa de linhas de confiança. Para realizar uma transação, duas partes não precisam estabelecer uma linha de confiança, o protocolo Ripple procura, para cada transação, o caminho mais rápido e curto (Ripple ($XRP) Analysis, Multicoin Capital, 2017).

Os nós podem assumir três distintos papéis no Blockchain da Ripple: usuários, que realizam e recebem transferências, *market maker*, que viabilizam as transações dentro do sistema e validadores, que executam o RPCA para certificar que todas as transações aderem aos pilares da exatidão, acordo e utilidade (estes pilares serão discutidos mais profundamente quando abordarmos mais o protocolo Ripple). Um usuário pode enviar recursos através da XRP ou de qualquer outro ativo. Para pagamentos realizados em outras moedas que não a XRP, a Ripple não possui uma forma de impor pagamentos, ela apenas registra os valores devidos de uma entidade à outra. Neste caso de transação em outras moedas, ela só é possível se B aceitar um IOU de A, ou seja, B confia em A e fornece para ele uma linha de crédito. O pagamento só terá sucesso se A quiser realizar este pagamento para B dentro do limite do crédito concedido. Um exemplo prático ilustrado pela Figura 2.20 seria a transferência de 100 USD de A para B. É possível realizar a transferências de duas formas: a primeira é pelo caminho A $\rightarrow$ U1 $\rightarrow$ U2 $\rightarrow$ U4 $\rightarrow$ B. Essa rota descrita possibilita a transferência do valor para linhas de crédito iguais ou superiores ao valor transacionado. Outra forma de concretizar a transação seria de realizar uma quebra entre os dois caminhos, onde 90 USD ou menos iriam por A $\rightarrow$ U1 $\rightarrow$ U3 $\rightarrow$ B e o restante por A $\rightarrow$ U1 $\rightarrow$ U2 $\rightarrow$ U4 $\rightarrow$ B (Armknecht, Karame, Mandal, Youssef e Zenner (2015)).

Outra forma de realizar esta transação seria utilizando a XRP em vez de uma IOU. Isso seria possível se os mediadores envolvidos na transação entre A e B estivessem dispostos a converter USD por XRP. A enviaria USD para U1, que converteria USD em XRP, XRP fluiria pela cadeia até chegar em U3 ou U4 (dependendo do caminho tomado) que converteria XRP em USD para B. Vale notar que esse método não é exclusivo com a XRP e pode ser realizado com outras criptomoedas, (Bitcoin ou Ether, por exemplo) funcionando como uma *bridge currency* (moeda-ponte), porém em suas respectivas Blockchains.

O Protocolo Ripple (RPCA) almeja ser um protocolo rápido, descentralizado e com baixos custos de transação. Em seu *whitepaper*, a Ripple Labs agrupa os problemas enfrentados para este objetivo em três principais categorias: exatidão, acordo e utilidade. (https://ripple.com/files/ripple_consensus_whitepaper.pdf. Consultado em 22 de março de 2018).

Exatidão se refere à necessidade de um sistema de distribuição identificar transações corretas das fraudulentas. No sistema tradicional isto é feito através de confiança entre instituições e assinaturas criptográficas para garantir que a transação é realmente da instituição que de fato fez a transação. Em sistemas de distribuição, não há esse tipo de confiança, visto que neste processo a identidade de todos os membros da *network* pode ser desconhecida. Logo, métodos alternativos precisam ser colocados em ação. (https://ripple.com/files/ripple_consensus_whitepaper.pdf. Consultado em 22 de março de 2018).

Acordo se refere ao problema da manutenção de uma verdade global através de uma

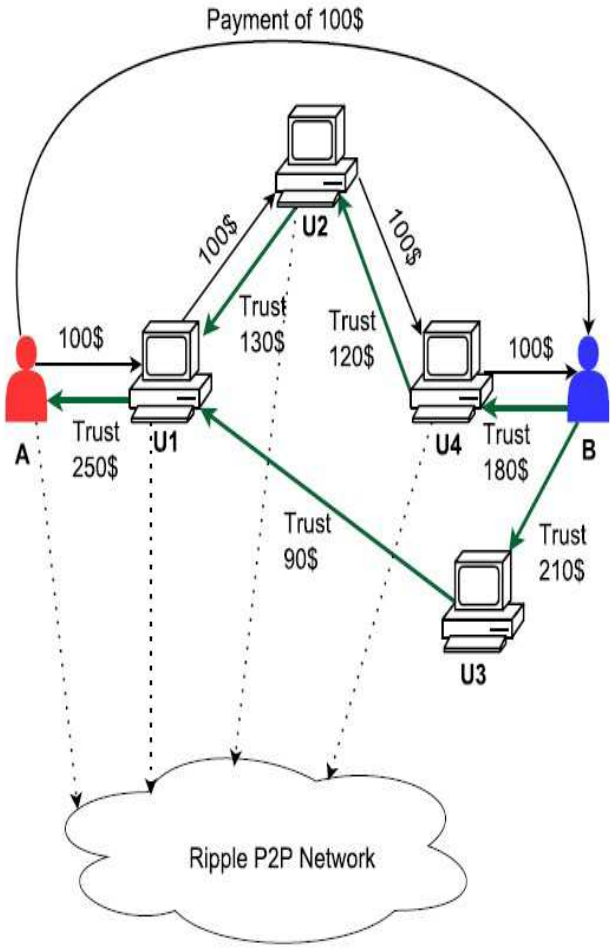

Figura 2.20: Exemplo de um pagamento IOU na rede Ripple (Armknecht F., Karame G.O., Mandal A., Youssef F., Zenner E. (2015) Ripple: Overview and Outlook. In: Conti M., Schunter M., Askoxylakis I. (eds) Trust and Trustworthy Computing. Trust 2015. Lecture Notes in Computer Science, vol 9229. Springer, Cham).

rede descentralizada. Mesmo que um hacker não crie transações fraudulentas, estando assim de acordo com o conceito de exatidão, ele pode criar várias transações corretas, onde estas transações não sabem da presença das outras transações criadas ao mesmo tempo. Um hacker pode criar, por exemplo, duas transações, onde há recursos suficientes para uma, mas não para duas. Basicamente, este é o problema do gasto duplo. Em suma, além de ser uma transação correta, ela também precisa ser a única reconhecida na Blockchain. (https://ripple.com/files/ripple_consensus_whitepaper.pdf. Consultado em 22 de março de 2018).

O último pilar trata da utilidade da rede. Este tópico é basicamente a viabilidade do processo no que concerne à velocidade. Uma transação que é correta (não fraudulenta) e reconhecidamente única na rede, que demora 6 meses para ser concluída não é útil no nosso sistema atual. Por isso, a velocidade das transações se faz tão crítica para a adoção e longevidade da rede quanto a certeza de que é uma transação correta e única reconhecida na Blockchain (https://ripple.com/files/ripple_consensus_whitepaper.pdf. Consultado em 22 de março de 2018).

O RPCA é um grupo de servidores (servidor é uma entidade que roda o *software* Ripple Server), onde cada servidor tem a sua própria UNL (*Unique Node List* ou Lista Única de Nós traduzido). Cada servidor S tem uma relação de outros servidores que S consulta para determinar consenso. Essa lista de servidores consultados é chamada de UNL. O servidor S estabelece uma relação de confiança com a sua UNL e só contabiliza os votos dos servidores da sua própria UNL. Isso foi desenvolvido para proteger a rede em um caso de tentativa de fraude. Na verdade, a UNL não é escolhida aleatoriamente, mas com a intenção de diminuir a probabilidade de um nó se juntar a um cartel com a ideia de fraudar a rede. Considerando que os nós não são anônimos, mas criptograficamente identificáveis, pode-se selecionar uma UNL com uma mistura de continentes, nações indústrias, ideologias, para diminuir a probabilidade de ocorrência de um cartel fraudulento (https://ripple.com/files/ripple_consensus_whitepaper.pdf. Consultado em 22 de março de 2018).

Inicialmente, cada servidor pega todas as transações válidas anteriores ao começo da rodada de consenso que não foram aplicadas e as torna públicas na forma de lista conhecida como *candidate set* (lista de candidatos). Cada servidor funde a lista de candidatos de todos os servidores dentro da sua UNL e vota sobre a veracidade dessas transações. Transações que recebem um número mínimo de "sims", que seriam a validação da transação, passam para a próxima rodada de validação, onde transações que não conseguirem esse mínimo podem ser descartadas ou colocadas na próxima lista de candidatos para serem novamente avaliadas no próximo *ledger*. A rodada inicial de validação se inicia com um requisito mínimo de 50% de consenso e aumenta em 10% para cada rodada, até chegar na rodada final. A rodada final requer um consenso mínimo de 80% a UNL dos servidores em uma transação. Toda transação que alcança esse requisito, é posta no *ledger* final e o *ledger* é fechado. A menos que tenha um número de interseções entre todas as UNL's da rede, várias UNL's podem chegar em um consenso de 80% individualmente. Isso significa que a rede pode chegar em consenso não único e, consequentemente, gerando um *fork* da rede. Logo, o RPCA necessita de interseções mínimas entre as UNL's (Armknecht, Karame, Mandal, Youssef e Zenner (2015)).

No começo, a Ripple defendia em seu *whitepaper* que o número mínimo de interseções necessárias para evitar um *fork* seria de 20% entre as UNL's. Porém, eu seu artigo de 2015,

Armknecht, Karame, Mandal, Youssef e Zenner provaram que o número mínimo para evitar um *fork* deveria ser de 40% de interseções entre as UNL's. A Ripple, posteriormente em seu site, concordou com a conclusão dos autores.

Uma das questões mencionadas anteriormente é que diferentes servidores possuem diferentes UNL's. E é necessário que haja uma interseção entre essas diferentes UNL's para evitar um *fork* da rede. Ao mesmo tempo que há uma motivação teórica para ter diferentes UNL's, para atingir a descentralização, há também motivação para convergência das UNL's a fim de evitar *forks*.

Outra questão é que há uma UNL padrão sob gerência da Ripple, onde novos servidores se inscrevem automaticamente. É possível mudar a UNL a qualquer momento para qualquer outra, porém há alguns problemas com isso: não há muito informação sobre em quais servidores confiar e, consequentemente, adicionar para a sua UNL. O segundo problema é que como uma maior divergência entre UNL's aumenta-se a probabilidade de gerar *forks*, onde empresas clientes terão mais motivos para escolher uma UNL que minimize esses problemas. Isso significa que nós estarão mais propensos a escolher os servidores sugeridos pela Ripple, gerando maior centralização. A Ripple fez algumas tentativas para minimizar os problemas acima descritos. A primeira medida informada pela Ripple é que a mesma anunciou, em maio de 2017, que iria de maneira gradual, começar a substituir uma parte dos validadores sob gerência da Ripple por validadores terceiros na UNL padrão. O segundo ponto, anunciado em julho de 2017, é que a Ripple aumentou o número de nós validadores para 55, um aumento de 120% desde maio de 2017, onde uma parte destes validadores são empresas e instituições terceiras além da própria Ripple. Mas, aparentemente, nenhum desses validadores foram incluídos na UNL padrão na época do lançamento da notícia pela Ripple (Ripple ($XRP) Analysis, Multicoin Capital, 2017).

É necessária uma quantidade mínima de XRP (20 XRP's) na carteira para que usuários possam participar da rede. XRP é a única forma de pagar por taxas de transação para evitar o spam da rede, conforme citado anteriormente. As XRPs que são utilizadas para pagar taxas de transação são queimadas. Isso significa que a XRP é uma criptomoeda deflacionária. Essas duas formas de uso da XRP possuem valor, porém a Ripple acredita que o real valor da sua moeda está em ser uma moeda liquidadora entre bancos. Enquanto bancos podem livremente trocar IOU's pelo protocolo, alguma hora essas IOU's precisam se liquidadas. Se essas liquidações forem feitas em moeda fiduciária (dólar, euro, real, etc.), essas mesmas liquidações estão sujeitas às ineficiências do sistema bancário atual que a Ripple procura substituir. Na Figura 2.21 é possível ver mais claramente isso. Um provedor de liquidez precisaria oferecer até 28 pares de moedas diferentes para poder participar de todas as transações de liquidação. Além do fato, já mencionado anteriormente, possuir contas e ativos em todas as instituições abaixo para as transações que o provedor de liquidez queira participar (Ripple ($XRP) Analysis, Multicoin Capital, 2017).

Em alguns casos, há a necessidade de vários provedores de liquidez envolvidos para que a transação ocorra, aumentando custos de transação, diminuição da velocidade além dos erros inerentes ao processo. A Figura 2.22 ilustra esse processo com o envolvimento de alguns provedores de liquidez (Ripple ($XRP) Analysis, Multicoin Capital, 2017).

Por outro lado, transacionar com XRP não necessita de contas bancárias, provedores de liquidez, custos adicionais de operação, entre outros. Na Figura 2.23, podemos ver que há a necessidade de apenas oito pares de moedas (contra 28 pares de moedas no exemplo anterior) para se conseguir realizar as mesmas transações (https://ripple.com/files/ripple_vision

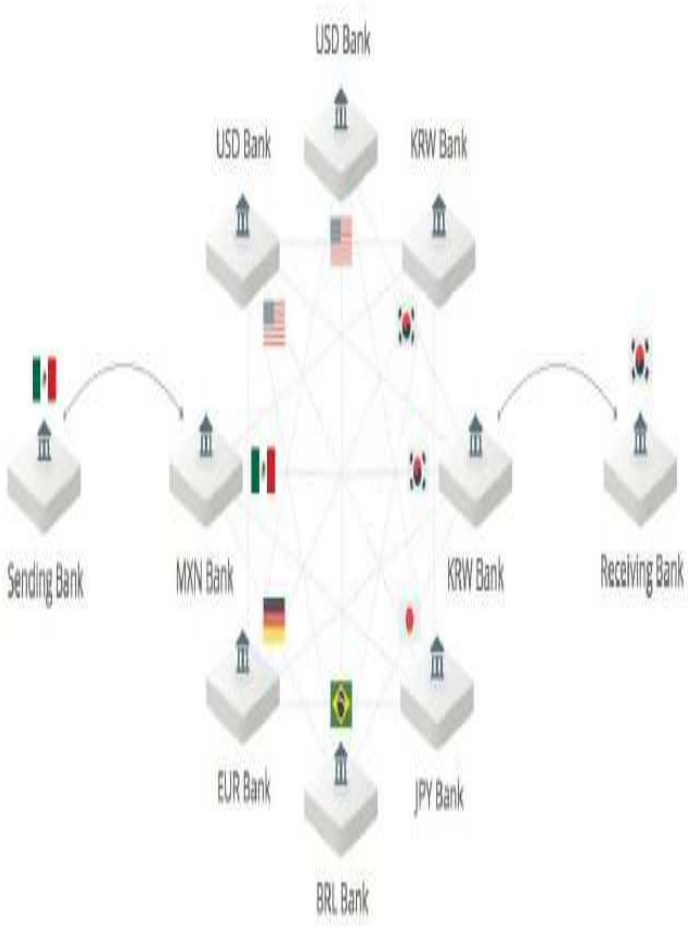

Figura 2.21: Exemplo de um provedor de liquidez participando de algumas transações interbancárias. https://ripple.com/files/ripple_vision.pdf. Consultado em 24 de março de 2018.

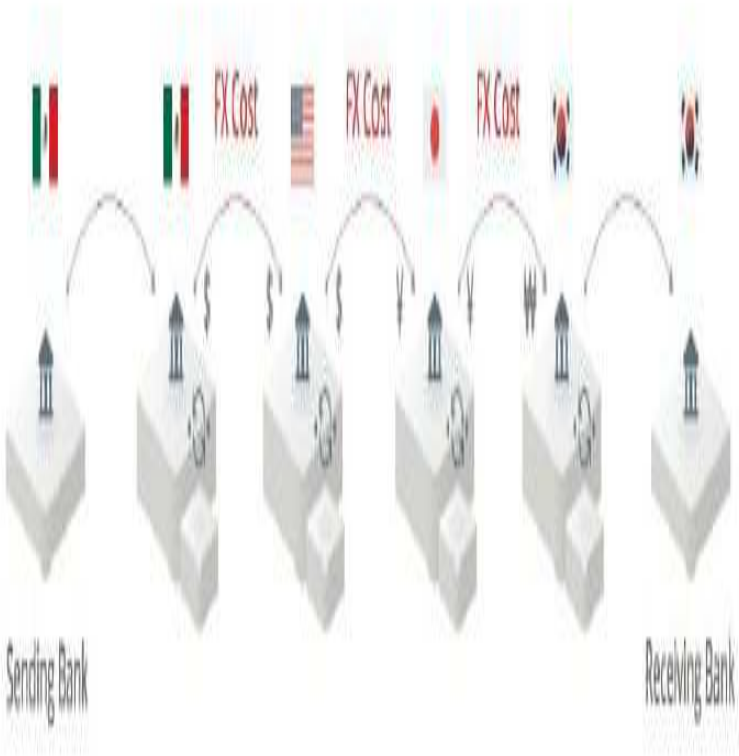

Figura 2.22: Exemplo de uma transação com mais de um provedor de liquidez. https://ripple .com/files/ripple_vision.pdf. Consultado em 24 de março de 2018.

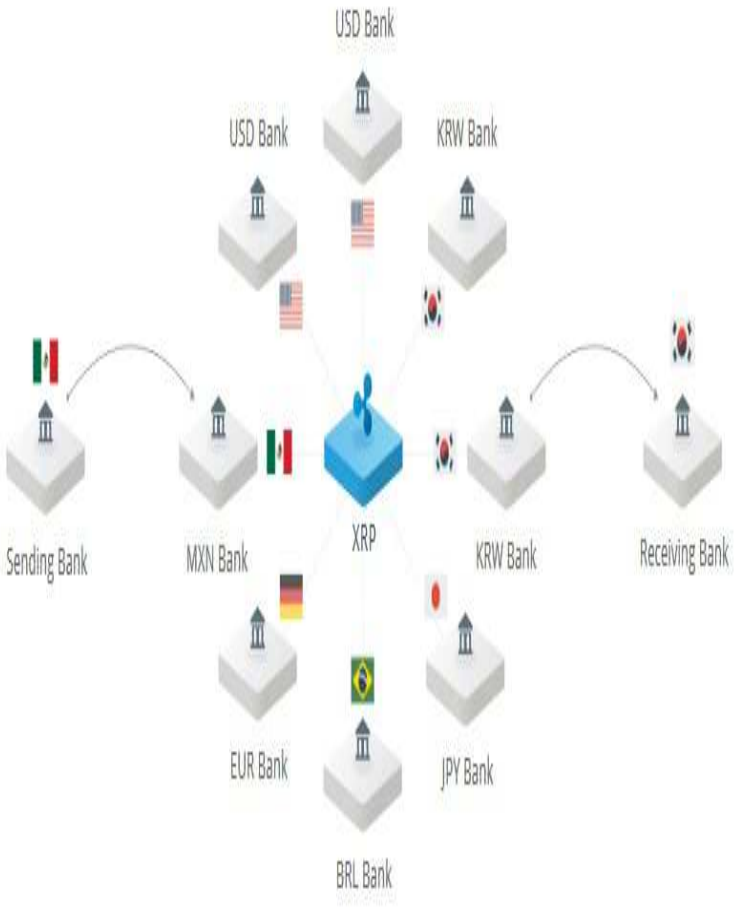

Figura 2.23: Novo ecossistema com o RPCA. https://ripple.com/files/ripple_vision.pdf. Consultado em 24 de março de 2018.

.pdf. Consultado em 24 de março de 2018).

E também não há a necessidade de vários provedores de liquidez. A XRP pode funcionar como uma moeda-ponte entre as partes envolvidas, diminuindo os custos de transação e aumentando a velocidade do processo, conforme apresentado na Figura 2.24 (https://ripple.com/files/ripple_vision.pdf. Consultado em 24 de março de 2018):

Conforme mostrado anteriormente, há uma centralização da rede da Ripple. A Ripple exerce grande influência sobre o protocolo através das UNL's padrão. Além disso, a Ripple opera a maioria dos servidores validadores (Ripple ($XRP) Analysis, Multicoin Capital, 2017).

Há uma incerteza no que concerne o RPCA. Por possuir grande controle sobre a rede, o protocolo precisa ainda ser testado com uma rede mais descentralizada, onde a chance de ter nós fraudulentos é maior. Os incentivos de ser um validador não são claros. Validadores não são recompensados pelo trabalho que exercem, ao contrário do que acontece com os mineradores do Bitcoin e Ethereum, por exemplo, o que pode levar a uma maior instabilidade e um aumento da centralização (Ripple ($XRP) Analysis, Multicoin Capital, 2017).

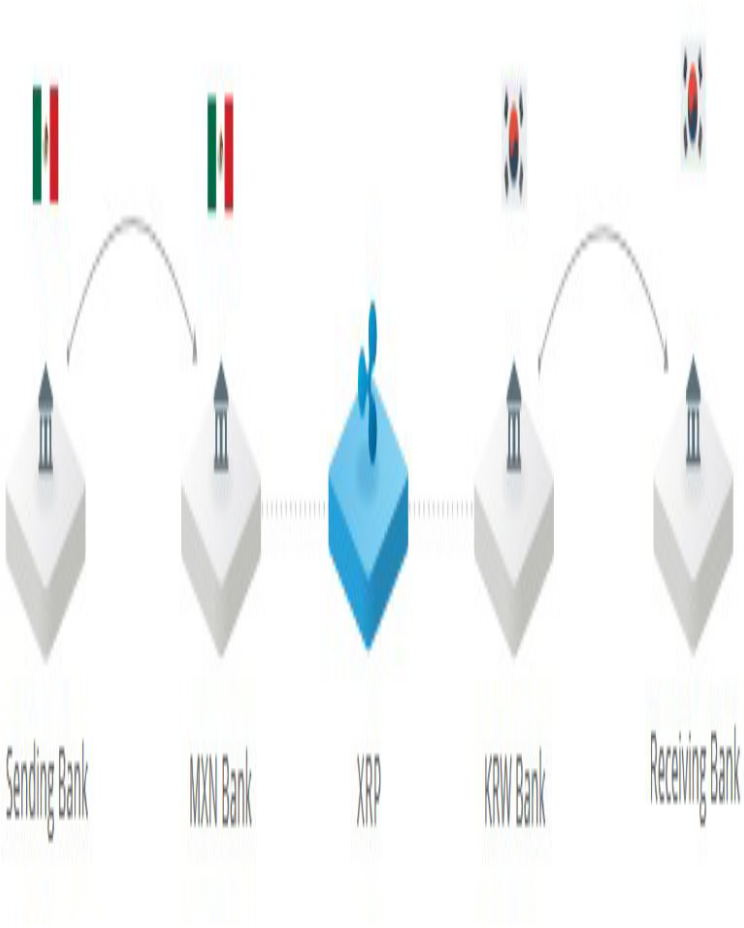

Figura 2.24: Proposição de transação interbancária com o RPCA . https://ripple.com/files/ ripple_vision.pdf. Consultado em 24 de março de 2018.

A principal proposta para a XRP é servir como uma moeda de liquidação nas transações bancárias. Isso é algo que outras criptomoedas podem fazer, não com a velocidade e escalabilidade da XRP atualmente, mas com os avanços em suas redes, plataformas como Bitcoin e Ethereum podem diminuir drasticamente essa diferença. Por ser muito focada nas transações bancárias, a XRP tem as suas funções limitadas quando se toma uma visão mais ampla do ecossistema de moedas digitais. Bancos terão uma motivação maior para realizar liquidações entre bancos utilizando os ativos que os seus clientes depositam, como Bitcoin, Ether ou futuramente moedas digitais emitidas por governos em detrimento ao uso da XRP. Bancos que optem por usar o XRP como uma moeda para liquidação precisarão ter uma reserva muito grande de XRP, visto que as obrigações são também enormes em valor. Isso é um problema visto a alta volatilidade do preço do XRP quando comparado a moedas digitais mais estáveis como o Bitcoin ou Ether ou moedas fiduciárias como o dólar (Ripple ($XRP) Analysis, Multicoin Capital, 2017).

Assim como o Bitcoin, a Ripple é um sistema de pagamento que é aberto, onde todas as transações e suas ordens de execução são abertas. É possível verificar se houve alguma tentativa de gasto duplo, por exemplo. Na rede Ripple, a validação é feita pelos validadores em um regime de votação, onde transações que receberem 80% ou mais de votos positivas no último *ledger* são validadas. Já o Bitcoin realiza a segurança com o PoW (*proof-of-work*). Para hackear a Blockchain do Bitcoin em determinado ponto, um hacker precisa ter uma capacidade computacional colossal, refazer toda a prova de trabalho daquele bloco, dos blocos subsequentes e passar, em tamanho, a Blockchain dos blocos honestos, algo que seria impossível, tanto financeiramente como computacionalmente. Para que a história da rede Ripple seja refeita, basta que a maioria dos servidores validadores sejam maliciosos (Armknecht, Karame, Mandal, Youssef e Zenner (2015)).

Os pagamentos através do Bitcoin precisam da confirmação de seis blocos, onde demora, em média, 10 minutos para um bloco novo ser minerado. Logo, necessita-se de uma hora, em média, para a confirmação de uma transação. No Ripple, pela velocidade de fechamento dos *ledgers* ser de segundos, em geral, pagamentos podem ser verificados rapidamente, não necessitando uma hora para confirmação, como é o caso do Bitcoin. Atualmente, o Bitcoin processa 10 transações por segundo, enquanto o Ripple pode processar 1500 transações por segundo (https://www.finder.com/se/bitcoin-vs-ripple). A Figura 2.25 ilustra quantos *ledgers* foram fechados em alguns intervalos de tempo para o período de janeiro e fevereiro de 2015 (Armknecht, Karame, Mandal, Youssef e Zenner (2015)).

No que concerne à privacidade, Ripple e Bitcoin são parecidas, onde todas as transações são públicas no *ledger*, porém não há nenhuma ligação com nome, região ou qualquer outro fato que ligue diretamente a transação com o real operador atrás. Porém, padrões de transferência como tamanho das transações, dia, horário, entre outros, pode servir como pistas para descobrir a real identidade do dono da transação (Armknecht, Karame, Mandal, Youssef e Zenner (2015)).

No campo de atualizações no protocolo, manutenção e *client*, por serem código-fonte aberto, qualquer entidade pode criar o seu próprio client, tanto para o Bitcoin quanto para o Ripple, porém os *clients* oficiais são mantidos pela Bitcoin Foundation e a Ripple Labs respectivamente. Todas as modificações no *client* do Bitcoin são amplamente discutidas em fóruns onlines, extremamente justificadas e votadas para adoção ou não entre os desenvolvedores do Bitcoin. Já para o Ripple, onde há uma empresa atrás do processo, a

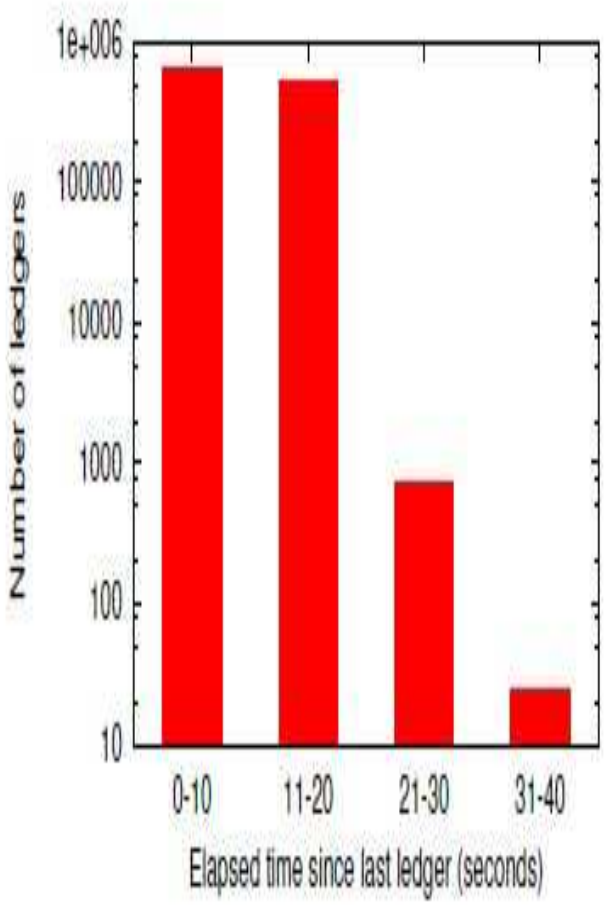

Figura 2.25: Quantidade de *ledgers* fechados por intervalos de tempo para o período de janeiro e fevereiro de 2015 (Armknecht F., Karame G.O., Mandal A., Youssef F., Zenner E. (2015) Ripple: Overview and Outlook. In: Conti M., Schunter M., Askoxylakis I. (eds) Trust and Trustworthy Computing. Trust 2015. Lecture Notes in Computer Science, vol 9229. Springer, Cham.

Ripple Labs, este processo não é tão transparente (Armknecht, Karame, Mandal, Youssef e Zenner (2015)).

Em termos de descentralização, os protocolos do Bitcoin e Ripple alavancam a descentralização, mas de fato há uma centralização em alguns processos de ambas as redes. Em janeiro de 2018, a maioria dos validadores do RPCA eram da Ripple Labs e a UNL padrão mantida por validadores da Ripple Labs (https://medium.com/tbis-weekly-bits/i-see-you-xrp-fcf151feb96d. Consultado em 25 de março de 2018). Isso significa que a Ripple pode controlar toda a segurança das transações da rede. Além disso, a Ripple possui uma enorme quantidade de XRP, como já citada anteriormente, podendo efetivamente controlar a economia desta criptomoeda. Conforme foi indicado na Figura 2.9, a mineração do Bitcoin é centralizada, mas as entidades que controlam a segurança das transações, a manutenção e atualização do protocolo e a criação de novas moedas são distintas.

2.2.4 Litecoin

Diferentemente das moedas vistas anteriormente, o Litecoin (LTC) não possui *whitepaper*. O Litecoin é baseado no Bitcoin e, por conta disso, são bem parecidas. Em um mundo onde o Bitcoin é o ouro, Litecoin seria a prata. Pela profunda abordagem realizada para o Bitcoin neste trabalho, seremos mais concisos para o Litecoin, nos focando mais nas diferenças entre ambas as moedas.

Criado pelo ex-engenheiro da Google Charlie Lee em outubro de 2011, o Litecoin se apresenta como uma opção ao Bitcoin, distinguindo-se em alguns pontos, porém muito parecido em diversos aspectos. Uma das principais diferenças entre Bitcoin e Litecoin diz respeito ao número total de moedas que cada criptomoeda pode produzir. A rede Bitcoin nunca pode exceder 21 milhões de moedas, enquanto que Litecoin pode acomodar até 84 milhões de moedas (https://www.investopedia.com/articles/investing/042015/bitcoin-vs-litecoin-whats-difference.asp).

Com relação às recompensas aos mineradores, Bitcoin e Litecoin seguem a mesma linha, porém com números diferentes. Hoje, cada bloco minerado no Bitcoin premia o minerador em 12.5 Bitcoins, ao passo que para o Litecoin esse prêmio por descoberta de bloco é de 25 Litecoins. Porém essas premiações mudam de valor gradualmente. A cada 210.000 blocos minerados para o Bitcoin, essa recompensa cai pela metade. Ou seja, o próximo nível de recompensa para o Bitcoin será de 6.25 Bitcoins por bloco descoberto. No momento desta escrita, há uma estimativa para que isso ocorra em 24 de Maio de 2020. Já para o Litecoin, essa recompensa cai pela metade a cada 840.000 blocos minerados, onde o próximo nível de recompensa será de 12.5 Litecoins. A previsão para que isso ocorra é 8 de Agosto de 2019. Todas essas informações e estimativas podem ser encontradas em https://www.bitcoinblockhalf.com/ e https://www.litecoinblockhalf.com/ para Bitcoin e Litecoin respectivamente.

O nível de dificuldade para a descoberta de um novo bloco para Bitcoin e Litecoin é revisto a cada 2016 blocos minerados. Para o Bitcoin isto representa, em média, 14 dias, por conta da velocidade de mineração. Já para o Litecoin isto representa, em média 3.5 dias. Ao final desse período, o sistema readapta o nível de dificuldade para a descoberta de novos blocos. Por exemplo, se 2016 blocos foram descobertos para o Bitcoin em 12 dias (ou seja, menos de 14 dias conforme previsto no algoritmo) o sistema aumenta o nível de dificuldade para que o período de 14 dias seja cumprido. Se os mesmos 2016 blocos forem descobertos em 16 dias, o sistema se reajustará diminuindo a dificuldade.

Embora tecnicamente as transações ocorram instantaneamente nas redes Bitcoin e Litecoin, é necessário tempo para que essas transações sejam confirmadas por outros participantes da rede. Conforme visto anteriormente, o tempo médio de confirmação de transação para o Bitcoin é de, em média, 10 minutos, embora isso possa variar muito quando o tráfego é alto. O valor equivalente para o Litecoin é de, em média, 2,5 minutos. Em princípio, essa diferença no tempo de confirmação pode tornar o Litecoin mais atraente para os comerciantes. Por exemplo, um comerciante que vende um produto em troca do Bitcoin precisaria esperar quatro vezes mais para confirmar o pagamento, como se o mesmo produto fosse vendido em troca do Litecoin. Por outro lado, os comerciantes podem sempre optar por aceitar transações sem esperar nenhuma confirmação. A segurança de tais transações de confirmação zero é objeto de algum debate (https://www.investopedia.com/articles/investing/042015/bitcoin-vs-litecoin-whats-difference.asp).

A maior diferença técnica entre Bitcoin e Litecoin está nos diferentes algoritmos crip-

tográficos que eles usam. O Bitcoin utiliza o algoritmo SHA-256 e o Litecoin emprega o Scrypt. Esses scripts diferentes são notáveis por causa da forma como eles afetam o processo de mineração de novas moedas. Tanto o Litecoin quanto o Bitcoin requerem um grande poder de computação para confirmar as transações. O SHA-256 é considerado mais complexo que o Scrypt, mas ao mesmo tempo permite mais processamento paralelo. Isso significa que os mineradores de Bitcoin agora podem usar métodos mais avançados de mineração de moedas. Mas isso também significa que a mineração de Bitcoin é difícil para usuários comuns. Em contrapartida, o Scrypt foi projetado para que não seja tão facilmente adaptado a soluções de hardware especializadas como a de mineração baseada em ASIC, o que torna as criptomoedas baseadas no Scrypt mais acessíveis aos usuários que desejam minerar e comprar criptomoedas. Mas, devido ao fato de algumas empresas do setor disponibilizarem ASICs para o Scrypt, a Litecoin pode não ser capaz de oferecer uma mineração tão acessível (https://medium.com/@BLMPNetwork/whats-the-difference-between-litecoin-and-bitcoin-6e9adb92a8b8).

A Tabela 2.2 sumariza as principais diferenças entre Bitcoin e Litecoin.

Tabela 2.2: *Principais diferenças entre Bitcoin e Litecoin.*

	Bitcoin	Litecoin
Limite de criptomoedas	21 milhões	84 milhões
Algoritmo	SHA-256	Scrypt
Tempo médio de mineração	10 minutos	2.5 minutos
Mudança de dificuldade	2016 blocos	2016 blocos
Recompensa atual	12.5 BTC	25 LTC
Criado por	Satoshi Nakamoto	Charlie Lee
Criado em	Janeiro, 2009	Outubro, 2011

2.2.5 Stellar

Analogamente ao citado na seção sobre Litecoin, a Stellar é similar à Ripple e terá uma abordagem mais concisa também, onde focaremos mais nas diferenças entre ambas as criptomoedas.

Após desentendimentos internos, um dos fundadores da Ripple, Jed McCaleb se juntou com Joyce Kim para criar a Stellar em 2014. Inicialmente, a Stellar era extremamente parecida com a Ripple no quesito código, porém isso foi mudando ao longo do tempo. Conforme dito na seção sobre Ripple, o seu protocolo de pagamento usa um mecanismo de consenso de correção com base na validação da maioria. O mecanismo é aplicado a cada poucos segundos por todos os nós para manter o acordo da rede. Enquanto isso, o protocolo de pagamento da Stellar, Stellar Core, é baseado no algoritmo Stellar Consensus Protocol. Isso usa um modelo de consenso chamado federated Byzantine agreement (FBA) e, de acordo com a Stellar, fornece um método de alcançar consenso sem depender de um sistema fechado para registrar com precisão as transações financeiras, como é o caso do Ripple. Para mais informações de como a Stellar atinge um consenso na rede, olhar o *whitepaper* da Stellar escrito pelo professor de Ciências da Computação da faculdade de Stanford David Mazières (https://www.stellar.org/papers/stellar-consensus-protocol.pdf).

Ripple e Stellar são construídos em filosofias separadas e estão focados em diferentes públicos. A Ripple é um órgão com fins lucrativos que visa criar uma rede de pagamentos com grandes instituições financeiras. Eles planejam conectar bancos, provedores de pagamento, trocas de ativos digitais e corporações através de sua própria rede, para fornecer uma experiência sem fricção para enviar dinheiro globalmente. Já a Stellar é uma organização sem fins lucrativos com objetivos altruístas incorporados ao seu mandato. A Stellar visa proporcionar maior acesso à população sem cobertura do mundo e promover a inclusão financeira. Outra diferença entre essas criptomoedas é com relação ao suprimento. A oferta máxima de XRP é de 100 bilhões. O fornecimento inicial de Lumens também foi de 100 bilhões, porém as similaridades acabam por aí. Para proteger o Ledger XRP contra spams e ataque de negação de serviço, uma pequena quantidade de XRP é destruída em cada transação. Este custo de transação significa que a oferta total de XRP diminuirá com o tempo. Por outro lado, a XLM (criptomoeda da Stellar) é projetada para ser inflacionária, com uma taxa de inflação fixa de 1% ao ano e todas as taxas de transação recicladas. Por fim, uma das diferenças mais marcantes entre as duas é com relação a descentralização. Abordamos este tópico na seção sobre o Ripple, onde ela acaba por possuir um grande poder sobre a rede. A descentralização é um dos fundamentos deste mundo criado por Nakamoto. A Stellar é vista como uma empresa que segue mais os princípios da descentralização que a Ripple. Sobre este tópico, a Ripple recebeu muitas críticas em 2015, quando a empresa congelou os fundos XRP (criptomoeda da Ripple) do fundador Jed McCaleb que havia saído da empresa, demonstrando assim o domínio da Ripple sobre sua rede. (https://www.investinblockchain.com/stellar-lumens-vs-ripple/)

Capítulo 3

Modelagem estatística

A maior preocupação dentro da área de risco é com fenômemos de baixa probabilidade, que possam vir a ocorrer e causar enormes danos para os *stakeholders*. Por exemplo, alguns dos *crashes* já ocorridos poderiam ter sido mensurados e não tratados como algo imprevisível. O risco sempre existirá e grandes perdas também. O importante é estar ciente destes riscos e de seus desdobramentos. Vários métodos podem ser utilizados para a modelagem de riscos, porém estas modelagens devem ser tratadas com muito cuidado para que as mesmas possam resultar em mensurações precisas. Métodos baseados em normalidade, por exemplo, apesar de serem de fácil cálculo, vão falhar nos momentos de maior necessidade, que seriam os momentos de crise. Vão falhar porque a distribuição Normal tem caudas leves e também pelo fato da mesma ser multivariada, implicando no fato dos quantis conjuntos de baixa probabilidade (isto é, perdas extremas simultâneas) terem probabilidade zero de ocorrência. Em outras palavras implica em independência assimétrica. Por isso a modelagem estatística é parte fundamental na vida dos administradores de risco. Neste capítulo daremos as abordagens utilizadas neste texto para modelar e analisar as séries de retornos das criptomoedas.

3.1 Retornos e fatos estilizados

3.1.1 Retornos financeiros

Denotaremos por P_t o preço de fechamento de um ativo no período t, onde o período pode ser semanal, diário, horário, etc. Em geral, séries de preços possuem tendência crescente e não são estacionárias, violando por isto a premissa básica para modelos de séries temporais que abordaremos mais à frente. Já as séries de retornos financeiros são, em geral, estacionárias sendo preferíveis para a análise.

A variação dos preços entre os instantes t e $t-1$, dado que não houve pagamento de dividendos, é definida como:

$$\Delta P_t = P_t - P_{t-1}. \tag{3.1}$$

O *retorno líquido simples de 1-período* deste mesmo ativo entre os instantes t e $t-1$ é definido como:

$$R_t = \frac{P_t - P_{t-1}}{P_{t-1}} = \frac{\Delta P_t}{P_{t-1}}. \tag{3.2}$$

A partir de (3.2) podemos chegar no *retorno bruto de 1-período* dado por:

$$1 + R_t = \frac{P_t}{P_{t-1}}. \tag{3.3}$$

O *retorno composto continuamente* ou *log-retorno*, r_t, é definido como o logaritmo natural do retorno bruto

$$r_t = \log(1 + R_t) = \log \frac{P_t}{P_{t-1}} = \Delta \log P_t \tag{3.4}$$

e portanto $\frac{P_t}{P_{t-1}} = e^{r_t}$.

Denotando $p_t = \log P_t$ temos que $r_t = p_t - p_{t-1}$. Notemos que R_t e r_t são em geral próximos, visto que $\log(1 + u) \approx u$ para u pequeno.

3.1.2 Conceitos estatísticos básicos para a análise de retornos financeiros

Seja r uma variável aleatória (v.a.) representando o log-retorno, F a sua função de distribuição acumulada (f.d.a.), isto é, $F(x) = P(r \leq x)$, e f a sua função de densidade. Podemos escrever $r \sim F$. Supomos ser r uma variável aleatória contínua. Denotaremos por $\mu = E[r] = \int_{-\infty}^{+\infty} rf(r)dr$ o valor esperado de r, ou *média* de r. O k-ésimo momento central de r é dado por $E[(r - \mu)^k]$. O segundo momento central de r é a *variância* de r, denotado por σ^2, onde a sua raiz quadrada, σ é o *d*esvio padrão de r. Apenas estes dois primeiros momentos são suficientes para definir uma distribuição Normal.

É importante abordar alguns conceitos estatísticos úteis para a análise de séries de retornos financeiros. As referências básicas são Mendes, B.V.M (2016) e Tsay, R.S. (2002). O primeiro conceito refere-se à estacionaridade da série. Uma série é estacionária de segunda ordem se todas as distribuições univariadas $\{r_t\}$ e bivariadas $\{r_t, r_{t+k}\}$, para todo k = 1,2,3... são invariantes ao longo do tempo. Isto faz com que, para todo t e $j \geq 1$

$$E(r_t) = E(r_{t+j}) \tag{3.5}$$

e

$$var(r_t) = var(r_{t+j}). \tag{3.6}$$

O terceiro momento central mede a simetria de $f(\cdot)$ em relação à sua média μ. O *coeficiente de assimetria* de r, $A(r)$, é dado por

$$A(r) = \frac{E[(r - \mu)^3]}{\sigma^3}. \tag{3.7}$$

Caso $A(r)$ seja igual a zero, significa que a distribuição é simétrica.

Já o quarto momento central mede a curtose, que seria o achatamento da função de densidade, e $C(r)$, o *coeficiente de curtose* de r, é definido como

$$C(r) = \frac{E[(r - \mu)^4]}{\sigma^4}. \tag{3.8}$$

$(C(r) - 3)$ é chamado de *excesso de curtose* e é zero para a distribuição Normal. Quando $C(r) - 3 > 0$ $(C(r) - 3 < 0)$ a distribuição do retorno tem excesso de curtose positivo

(excesso de curtose negativo) e, consequentemente, caudas mais grossas (caudas menos grossas) em comparação à distribuição Normal.

Os estimadores mais utilizados para μ e σ^2, $A(\cdot)$ e $C(\cdot)$ são as suas versões amostrais, ou estimadores empíricos. Seja $(r_1, r_2, \cdots, r_T)$ uma amostra aleatória de r. A média amostral $\bar{r}$ é definida por

$$\bar{r} = \frac{1}{T}\sum_{1}^{T} r_t \tag{3.9}$$

e a *variância amostral* S^2 é definida por

$$S^2 = \frac{1}{T-1}\sum (r_t - \bar{r})^2. \tag{3.10}$$

Estes são os estimadores de máxima verossimilhança (EMV) de μ e σ^2 sob normalidade. Estimadores empíricos para os coeficientes de assimetria e curtose são os coeficientes de assimetria amostral e de curtose amostral, definidos em (3.11) e (3.12) respectivamente, onde S representa o *desvio padrão amostral*:

$$\widehat{A(r)} = \frac{1}{(T-1)S^3}\sum_{1}^{T}(r_t - \bar{r})^3 \tag{3.11}$$

$$\widehat{C(r)} = \frac{1}{(T-1)S^4}\sum_{1}^{T}(r_t - \bar{r})^4. \tag{3.12}$$

No que tange a aplicações financeiras, é importante detectar se a série de retornos possui distribuição subjacente assimétrica. Por exemplo, sendo $\{r_t\}$ estacionária, é normal que investidores prefiram uma série assimétrica para a direita.

Pode-se testar a hipótese nula

$$H_0 : A(r) = 0$$

versus a hipótese alternativa $H_1 : A(r) \neq 0$ utilizando o valor absoluto da estatística teste $\widehat{A(r)}$ que converge em distribuição para

$$\widehat{A(r)} \rightarrow^d N(0, \frac{6}{T}) \tag{3.13}$$

quando $T \rightarrow \infty$.

Pode-se testar a hipótese nula

$$H_0 : C(r) = 3$$

em um teste bilateral utilizando o valor absoluto da estatística teste $\widehat{C(r)}$ que converge em distribuição para

$$\widehat{C(r)} \rightarrow^d N(3, \frac{24}{T}) \tag{3.14}$$

quando $T \rightarrow \infty$.

Um teste bastante utilizado para testar se a distribuição subjacente dos dados é Normal é o teste Jarque-Bera. É baseado nas duas estatísticas acima

$$JB(r) = (\frac{T}{6})\widehat{A(r)}^2 + (\frac{T}{24})(\widehat{C(r)} - 3)^2 \tag{3.15}$$

e sob a hipótese nula de normalidade dos retornos tem distribuição *chi-quadrado* com 2 graus de liberdade (χ^2_2).

Já a covariância γ_k entre as v.a.'s r_{t-k} e r_t:

$$\gamma_k = cov(r_{t-k}, r_t) = E[r_{t-k}r_t] - E[r_{t-k}]E[r_t] \tag{3.16}$$

para $t, k \in \mathcal{Z}$, $\mathcal{Z} = \{0, \pm 1, \pm 2, \cdots\}$, é chamada de autocovariância de *lag* k de r_t. Em um processo estacionário a autocovariância depende apenas da defasagem k das variáveis no tempo e $cov(r_{t-k}, r_t) = cov(r_t, r_{t+k})$ para todo $t \in \mathcal{Z}$. Observe que $\gamma_0 = var(r_t)$.

O coeficiente da autocorrelação de *lag* k de r_t, ρ_k, é definido como

$$\rho_k = \frac{cov(r_{t-k}, r_t)}{(var(r_t)var(r_{t-k}))^{1/2}} \tag{3.17}$$

e portanto

$$\rho_k = \frac{\gamma_k}{\gamma_0} \tag{3.18}$$

para todo $k \in \mathcal{Z}$. Temos também que $\rho_k = \rho_{-k}$, $-1 \leq \rho_k \leq 1$, e $\rho_0 = 1$. Sendo ρ_k função do *lag* k, dá-se origem à *função de autocorrelação* (f.a.c.). Vale ressaltar que ρ mede o relacionamento linear e que uma série estacionária é dita não auto-correlacionada se e somente se $\rho_k = 0$ para todo k. Como ρ_k mede somente a força da dependência linear entre as variáveis envolvidas, a f.a.c. caracteriza a estrutura de dependência de processos lineares estacionários.

Dada uma série de T retornos, a *autocorrelação amostral* de *lag* k de r_t, $\widehat{\rho}_k$, é dada por

$$\widehat{\rho}_k = \frac{\widehat{\gamma}_k}{\widehat{\gamma}_0}, \quad k \in \mathcal{Z} \tag{3.19}$$

onde

$$\widehat{\gamma}_k = \frac{1}{T}\sum_{t=1}^{T-k}(r_t - \bar{r})(r_{t+k} - \bar{r}). \tag{3.20}$$

A função $\widehat{\rho}_k$ para $k = 1, 2, \cdots$ é a *função de autocorrelação amostral* (f.a.c. amostral) de r_t. Sendo $\{r_t\}$ uma sequência puramente aleatória, e se $E[r_t^2] < \infty$, então $\widehat{\rho}_1$ será assintoticamente Normal com média zero e variância $1/T$. Este resultado é utilizado para construir o intervalo de confiança mostrado na f.a.c. amostral. É importante salientar que a construção do intervalo é para todos os ρ_k (e não ρ_1 apenas). Como as suposições feitas em geral não se verificam para retornos financeiros, a construção do intervalo de confiança é aproximada, podendo não refletir de fato a confiança (95%) prevista pelo intervalo.

Dizer que o mercado não é previsível é dizer que não existe correlação serial. Porém, a forma como as ações são precificadas e os índices compostos, podem induzir algumas autocorrelações de curto prazo. A f.a.c amostral fornece uma ideia da extensão e do

grau da memória do processo, sendo assim uma ferramenta valiosa para a identificação do processo gerador de uma série temporal, além do fato de ser base para a construção de estatísticas teste. Para várias aplicações em finanças, é necessário testar se não existe memória curta, isto é, se as M primeiras autocorrelações $\rho_1, \rho_2, \cdots, \rho_M$ são zero. O teste de Ljung-Box (Ljung, G.M. e Box, G.E.P., 1978) usa a estatística teste

$$Q(M) = T(T+2)\sum_{k=1}^{M} \frac{\widehat{\rho}_k^2}{T-k}. \tag{3.21}$$

Escolher M é extremamente importante e, de uma forma geral, M é pequeno pois estamos testando se não existe memória curta. Simulações indicaram que $M \approx \log(T)$ é o valor que resulta em melhor performance do teste em termos de potência.

3.1.3 Fatos estilizados de séries de retornos

Fatos estilizados são características geralmente apresentadas por séries de retornos financeiros. São comprovados empiricamente e sugerem que séries de retorno:

1. São estacionárias.
2. Apresentam média amostral próxima de zero.
3. Apresentam distribuição (não condicional) aproximadamente simétrica.
4. Apresentam distribuição (não condicional) não Normal.
5. Apresentam excesso de curtose positivo (caudas pesadas).
6. Apresentam caudas com pesos diferentes. Podemos medir o peso da cauda através do *"tail index"* $\frac{1}{\xi}$, ξ parâmetro da distribuição de valores extremos.
7. Apresentam alguns pontos bem mais extremos que a maioria, os quais podem induzir assimetria para uma dada amostra.
8. Apresentam clusters de volatilidade (heteroscedasticidade condicional).
9. Apresentam alguma forma de não-linearidade (Pode surgir como consequência do fato de retornos financeiros reagirem diferentemente a choques positivos e negativos, ou a choques grandes ou pequenos, ou devido à dependência de cauda, etc.).
10. Não apresentam autocorrelação significativa. Quando existe, é pequena e significativa apenas para os primeiros *lags*.
11. Apresentam autocorrelação nos retornos ao quadrado significativa para vários *lags*. São todas positivas e podem decair lentamente.
12. Apresentam memória longa na média e na volatilidade (decaimento lento da f.a.c. amostral).

No Capítulo 4 iremos verificar se esses fatos estilizados também se verificam para as moedas que serão objeto de estudo.

3.2 Modelagem não-condicional dos retornos

Nesta seção iremos rever brevemente as distribuições usadas para modelar a distribuição subjacente das séries de retornos, assim como um resultado importante da Teoria dos Valores Extremos que foca na estimação das caudas da distribuição dos retornos. Iniciaremos dando um teste que será sempre aplicado para acessar a adequacidade da distribuição ajustada aos dados.

3.2.1 Teste de aderência

O teste de aderência (*goodness-of-fit*, GOF) testa quão bem uma amostra se encaixa dentro de uma distribuição dada (Normal, t-student, etc.). Seja F_0 a distribuição hipotética e F a verdadeira distribuição dos retornos r_t. A estatística de Kolmogorov para testar a hipótese nula $H_0 : F = F_0$ é definida por

$$D_T = \sup_{-\infty<x<\infty} \mid \widehat{F}_T(x) - F_0(x) \mid \tag{3.22}$$

onde $\widehat{F}_T$ representa a distribuição empírica dos dados (f.d.e.),

$$\widehat{F}_T(x) = (\sum_{t=1}^{T} \mathcal{I}_{(r_t \leq x)})/T, \tag{3.23}$$

$x \in \Re$, onde $\mathcal{I}_{(A)}$ é a função indicadora do evento A, isto é, $\mathcal{I}_{(A)} = 1$ se A ocorrer e zero caso contrário.

Pelo fato de $T\widehat{F}_T(x)$ ter distribuição Binomial com probabilidade de sucesso igual a $F(x)$, temos que $\widehat{F}_T(x)$ é um estimador não viciado de $F(x)$, com variância $F(x)(1 - F(x))/T$, além de ser consistente:

$$\widehat{F}_T(x) \xrightarrow{p} F(x) \tag{3.24}$$

e assintoticamente Normal para cada x. Pelo teorema de Glivenko-Cantelli, temos que para amostras grandes a f.d.e. se aproxima à verdadeira distribuição dos dados, isto é, $\sup_{-\infty<x<\infty} \mid \widehat{F}_T(x) - F(x) \mid \overset{q.c.}{\to} 0$ quando $T \to \infty$ (Bickel e Doksum, 1977).

3.2.2 Distribuição Normal

Muitas vezes é feita a suposição simplificadora de que os retornos sigam uma distribuição Normal com média μ e variância σ^2 constantes, $N(\mu, \sigma^2)$. No que concerne à estimativa, os parâmetros desconhecidos podem ser estimados através de estimadores de máxima verossimilhança sob normalidade, $\bar{r}$ e S^2, dados em (3.9) e (3.10).

3.2.3 Distribuição t-Student

Uma variável aleatória X que possui a seguinte função de densidade

$$f(x) = \frac{\Gamma[(\nu+1)/2]}{\sqrt{(\pi\nu}\Gamma(\nu/2)}(1 + \frac{x^2}{\nu})^{-(\nu+1)/2}, -\infty < x < \infty \tag{3.25}$$

tem distribuição t-Student padrão com ν graus de liberdade e denotaremos por $X \sim t(\nu)$. Neste trabalho, os três parâmetros da distribuição t-Student (μ,σ,ν) serão estimados simultaneamente por máxima verossimilhança.

3.2.4 Distribuição t-assimétrica

Como a primeira alternativa para a distribuição Normal, a distribuição t-student é comumente usada em finanças e gerenciamento de risco para modelar distribuições de retornos incondicionais e condicionais. Provavelmente a aplicação mais famosa é a modelagem de Bollerslev (1987) em distribuições condicionais em modelos GARCH. No entanto, medidas de risco mais precisas podem ser obtidas se formos capazes de distinguir o comportamento das caudas esquerda / direita na distribuição de retornos. Para este fim, as extensões de *skew* da distribuição t-student foram propostas, incluindo Hansen (1994), Fernandez e Steel (1998), Theodossiou (1998), Branco e Dey (2001), Bauwens e Laurent (2005), Jones e Faddy (2003), Azzalini e Capitanio (2003) e Aas e Haff (2006) entre outros.

Todas as referências acima, com exceção de Jones e Faddy (2003) e Aas e Haff (2006) têm duas caudas com taxa de decaimento polinomial idêntica, enquanto um parâmetro de assimetria controla a parte central da distribuição. Zhu e Galbraith (2010) propuseram uma nova classe de distribuições t-student assimétrica (AST), que tem um parâmetro de assimetria e dois parâmetros de cauda com o potencial de melhorar a aderência do modelo a dados empíricos. Eles derivaram suas propriedades discutindo métodos de estimação em particular as propriedades dos estimadores de máxima verossimilhança, destacando possíveis aplicações em econometria financeira. Adicionando os parâmetros de locação e escala, o modelo de cinco parâmetros resultante oferece potencial para ajustar características mais sutis da distribuição do que é possível com as versões anteriores de quatro parâmetros.

A distribuição t-student assimétrica de Zhu e Galbraith (2010) com locação zero ($\mu = 0$) e escala um ($\sigma = 1$) tem a função probabilidade densidade dada por

$$f_{AST}(y) = \begin{cases} \frac{\alpha}{\alpha^*} K(\nu_1)[1 + \frac{1}{\nu_1}(\frac{y}{2\alpha^*})^2]^{-\frac{\nu_1+1}{2}}, & y \leq 0 \\ \frac{1-\alpha}{1-\alpha^*} K(\nu_2)[1 + \frac{1}{\nu_2}(\frac{y}{2(1-\alpha^*)})^2]^{-\frac{\nu_2+1}{2}}, & y > 0 \end{cases} \tag{3.26}$$

onde $\alpha \in (0,1)$ é o parâmetro de assimetria, $\nu_1 > 0$ e $\nu_2 > 0$ são os graus de liberdade das caudas esquerda e direita respectivamente, $K(\nu) \equiv \Gamma((\nu+1)/2)[\sqrt{\pi\nu}\Gamma(\nu/2)]$ (onde $\Gamma(\cdot)$ é a função Gamma), e α^* é definido como

$$\alpha^* = \alpha K(\nu_1)/[\alpha K(\nu_1) + (1-\alpha)K(\nu_2)]. \tag{3.27}$$

A densidade da AST é contínua e unimodal com o modo em $y = \mu = 0$, e é em toda parte diferenciável pelo menos uma vez. No limite como $\alpha \downarrow 0$ a forma da densidade se assemelha a uma t-Student truncada no modo (inclinado para a direita), e como $\alpha \uparrow 1$ a forma do densidade se assemelha a uma t-Student truncada no modo (inclinado para a esquerda). O parâmetro α^* fornece ajustes de escala para garantir a continuidade da densidade sob alterações dos parâmetros de forma (α, ν_1, ν_2). Quando um dos parâmetros da cauda vai para o infinito, por exemplo, $\nu_1 \to \infty$, a AST se comporta como uma gaussiana no lado esquerdo (exponencial, cauda leve) e como uma t-Student no lado direito (cauda pesada). A forma geral da densidade da AST é dada por $\frac{1}{\sigma} f_{AST}(\frac{y-\mu}{\sigma}; \alpha, \nu_1, \nu_2)$. Deixe F_{AST} e F_{AST}^{-1} denotar respectivamente a função de distribuição cumulativa e a

função quantil da AST. Então temos $F_{AST}(\mu) = \alpha$ e $F^{-1}_{AST}(\alpha) = \mu$, portanto se $\alpha = 0.5$ a mediana é μ. Zhu e Galbraith (2010) também investigam propriedades assintóticas e amostras finitas dos estimadores de parâmetros de máxima verossimilhança.

A partir de agora iremos nos referir à t-assimétrica de Zhu e Galbraith com a seguinte denotação: t-ZG.

3.2.5 Modelagem das caudas

Excessos além de um limiar alto são muito importantes e utilizados em várias áreas, como por exemplo na medicina, seguros e resseguros e finanças. Em finanças, o valor médio dos retornos excedentes é conhecido como *shortfall*, também é importante e será tratado mais a frente. Iremos agora modelar separadamente as caudas das distribuições dos retornos das criptomoedas. Focando apenas nas caudas podemos estimar com maior precisão os quantis associadas à probabilidades muito pequenas.

Consideramos um retorno r, um limiar u, o excesso $Y = r - u$ e sua função de distribuição condicional F_u onde $F_u(y) = P(Y \leq y | r > u)$, $y \geq 0$. A função de sobrevivência condicional do excesso Y é dada por

$$\bar{F}_u(y) = P(r - u > y | r > u) \; = \; \frac{\bar{F}(u+y)}{\bar{F}(u)}. \tag{3.28}$$

Segue então que

$$\bar{F}(u+y) = \bar{F}_u(y)\bar{F}(u). \tag{3.29}$$

Resultados da Teoria dos Valores Extremos provam que a distribuição adequada para se modelar excessos além de um limiar alto é a *Generalized Pareto Distribution* (GPD) (De Haan, 1984). A f.d.a. da GPD padrão, denotada por P_ξ, é dada por

$$P_\xi(y) = \begin{cases} 1 - (1+\xi y)^{-1/\xi}, & \text{se } \xi \neq 0 \\ 1 - e^{-y}, & \text{se } \xi = 0 \end{cases} \tag{3.30}$$

onde $y \geq 0$ se $\xi \geq 0$, e $0 \leq y \leq -1/\xi$ se $\xi < 0$. Sua densidade é

$$p_\xi(y) = (1+\xi y)^{-(1+1/\xi)} \;\; \text{para} \;\; \begin{cases} 0 \leq y, & \text{se} \quad \xi \geq 0 \\ 0 \leq y \leq \frac{1}{|\xi|}, & \text{se} \quad \xi < 0 \; . \end{cases} \tag{3.31}$$

É possível obter a família de locação e escala $P_{\xi,\delta,\psi}$ substituindo-se o argumento y por $(y-\delta)/\psi$, para $\delta \in \Re$, $\psi > 0$. Neste caso, os suportes $D(\xi, \delta, \psi)$ da distribuição são: $D(\xi, \delta, \psi) = [\delta, \infty]$ se $\xi \geq 0$, e $D(\xi, \delta, \psi) = [\delta, \delta - \psi/\xi]$ se $\xi < 0$. Dentro da classe $P_{\xi,\delta,\psi}$ a distribuição de maior interesse nas aplicações práticas em finanças é a $P_{\xi,0,\psi}$ com $\xi \geq 0$ e y com suporte $D(\xi, 0, \psi)$. O valor esperado de uma v.a. GPD é dado por $\frac{\psi}{1-\xi}$. Observe que para $0 < \xi < 1$, quanto maior ξ maior será o valor esperado da GPD.

Podemos obter três submodelos de distribuições padrões ($\delta = 0, \psi = 1$) que são os tipos

Tipo I. Exponencial, $\xi = 0$, $P_I(y) = 1 - e^{-y}$, $\; y \geq 0$.

Tipo II. Pareto, $\xi > 0$, $P_{II,\xi}(y) = 1 - y^{\frac{-1}{\xi}}$, $\; y \geq 1$.

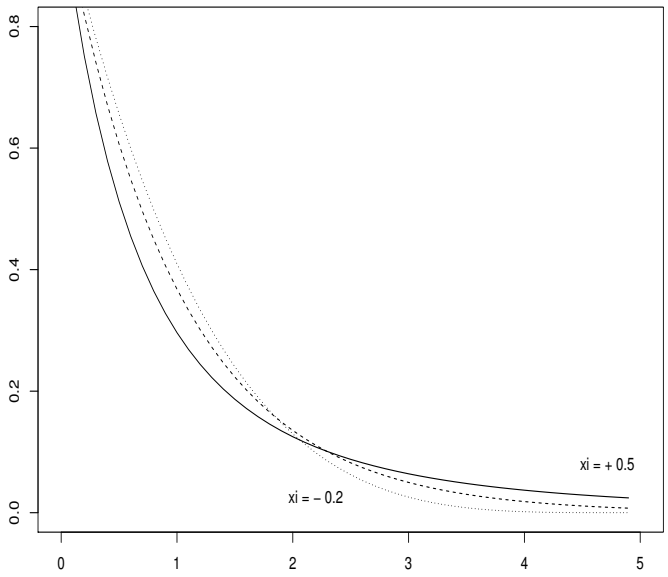

Figura 3.1: *Densidades: Exponencial (pontilhada); Pareto* $\xi = 0,5$ *(contínua); Beta* $\xi = -0.2$ *(tracejada). As três densidades possuem locação zero e escala um. Fonte: Modelagem do risco financeiro. / Beatriz Vaz de Melo Mendes. Rio de Janeiro: UFRJ/COPPEAD, 2016*

Tipo III. Beta, $\xi < 0$, $P_{III,\xi}(y) = 1 - (-y)^{\frac{-1}{\xi}}, \quad -1 \leq y \leq 0$.

P_I pode ser interpretada como o limite da P_ξ quando $\xi \to 0$. A Figura 3.1 compara os três tipos de densidades. Quando $\xi > 0$ têm-se caudas mais pesadas.

É necessário escolher um limiar ótimo, porém há um *trade-off* nessa escolha: um valor para u muito alto implicará em um número pequeno de observações na cauda, podendo resultar em uma maior variabilidade dos estimadores. Por outro lado, um limiar não suficientemente alto não satisfaz às suposições teóricas e pode resultar em estimativas distorcidas.

Diversos autores têm pesquisado sobre o problema da escolha do limiar u. Pickands, J. III (1975a) sugere um procedimento concomitante para a escolha do limiar e estimação dos parâmetros ξ e ψ da GPD. Pickands, J. III (1975b) propôs um método para a escolha das k estatísticas de ordem definindo o limiar ótimo. Outros trabalhos, como Mendes, B.V.M (2005a), não abordam explicitamente o problema da escolha do limiar, mas o obtêm como subproduto após o ajuste de um modelo de misturas.

Diversos procedimentos para estimar os parâmetros ξ e ψ da GPD têm sido propostos na literatura. Por exemplo, Pickands, J. III (1975a) sugere um método que também estima o limiar além de considerar estimadores de Bayes usando três estatísticas de ordem, inclusive o máximo. Pickands, J. III (1984) propôs uma abordagem não paramétrica. Hosking, J. R. M. e Wallis, J.R. (1987) consideram o método dos estimadores *Probability Weighted Moments* (PWM). Smith, R.L. (1987) propôs um estimador baseado nos estimadores de máxima verossimilhança que seria altamente eficiente se o limiar escolhido

fosse ótimo.

Iremos estimar os parâmetros da GPD pelo método da máxima verossimilhança. Considere os dados de excessos $y_1, y_2, ..., y_{N_u}$, onde N_u representa o número de excessos além de u, e a densidade da GPD com locação zero e escala ψ

$$p_{\xi,\psi}(y) = \frac{1}{\psi}\left(1 + \xi\frac{y}{\psi}\right)^{-(1+1/\xi)} \quad \text{se} \quad y \in D(\xi,\psi) \ . \tag{3.32}$$

Os EMV maximizam a função de log-verossimilhança

$$\mathcal{L}((\xi,\psi,u); y_1, ..., y_{N_u}) = -N_u \log(\psi) - \left(\frac{1}{\xi} + 1\right)\sum_{i=1}^{N_u} ln\left(1 + \frac{\xi}{\psi}y_i\right) \ , \tag{3.33}$$

onde $y_i \in D(\xi,\psi)$. É importante salientar que $D(\xi,\psi) = [0,\infty)$ se $\xi \geq 0$. Podemos agora derivar (3.33) em relação aos parâmetros e obter as equações de log-verossimilhança, as quais podem ser resolvidas numericamente. Os estimadores $(\hat{\xi},\hat{\psi})$ possuem as boas propriedades dos EMV quando $\xi > -\frac{1}{2}$.

A estimação de ξ é importante devido ao fato de ser $1/\xi$ o índice de cauda da distribuição F, o qual, além de medir o peso da cauda, também determina o número de momentos finitos de F.

Vale notar que, para a maioria dos estimadores, existe a questão da sensibilidade das estimativas quanto à escolha do limiar. Para a escolha do limiar iremos examinar o histograma dos excessos, observando o seu decaimento, o qual deve ser estritamente decrescente.

Para acessar a qualidade dos ajustes iremos aplicar o teste GOF, examinar gráficos tipo PP-Plot e QQ-Plot. Pode-se também testar a hipótese nula H_0: $\xi = 0$ através do teste da razão de verossimilhanças, buscando-se um modelo mais simples.

3.3 Medidas de risco

Medir risco é uma prática comum nas instituições financeiras. Estes números obtidos são utilizados para auxiliar a tomada de decisão, podendo, muitas vezes, envolver grandes quantias de dinheiro, e podem ser o ponto de partida para o cálculo de reservas financeiras para cobrir possíveis perdas. Caso o cenário desenhado seja muito conservador, superestimando assim o risco, haverá uma perda no lucro, pois uma parte significativa de capital será colocada separada para cobrir eventuais perdas. Já, caso o risco seja subestimado, esse valor colocado à parte será constantemente ultrapassado, perdendo sua função e gerando impactos financeiros não previstos para a instituição financeira.

Medir o risco não condicional de um ativo ou uma carteira é basicamente estimar a distribuição de probabilidade F, $F(x) = P(r_t \leq x)$. Até recentemente, modelos para os cálculos destes riscos consideravam que os retornos eram normalmente distribuídos, devido à fácil implementação da premissa, porém estudos empíricos comprovaram que distribuição de perdas e ganhos de ações ou carteiras possuem caudas mais pesadas que as previstas pela distribuição Normal.

A medida de risco mais utilizada é o Valor em Risco, VaR_α, onde α é a probabilidade associada à medida. De maneira informal, o VaR_α pode ser definido como um valor limite de perda tal que a probabilidade de que uma perda da carteira em um determinado

horizonte de tempo exceda este valor é α. De maneira mais formal, o VaR_α é o menor número x tal que a probabilidade que o retorno exceda x não é maior que α:

$$\text{VaR}_\alpha = \inf\{x \in \Re : P(r_t > x) \leq 1 - \alpha\} = \inf\{x \in \Re : F(x) \geq \alpha\} \tag{3.34}$$

onde a probabilidade $P(\cdot)$ pode ser condicional ou não condicional. Pode-se também definir o risco na cauda direita:

$$\text{VaR}_\alpha = \sup\{x \in \Re : F(x) \leq 1 - \alpha\}. \tag{3.35}$$

Sob a ótica estatística, o VaR é um quantil de uma distribuição. A função quantil fornece o q-quantil, r_q, da distribuição F de r_t:

$$r_q = \inf\{x \in \Re : F(x) \geq q\} = F^{-1}(q)\ . \tag{3.36}$$

Desta forma, para o cálculo do VaR_α de um ativo precisamos calcular o $F^{-1}(q)$, sendo $q = \alpha$ se na cauda esquerda ou $q = (1 - \alpha)$ na cauda direita da distribuição.

O risco de uma carteira, quando este é medido pelo VaR, pode ser maior que a soma dos riscos individuais de cada componente. Isto significa que, gerenciar o risco de uma carteira através do VaR pode não estimular a diversificação. Este tem sido um ponto de crítica relacionado ao VaR.

3.3.1 Medidas de risco não condicionais

Diversos modos de se estimar a distribuição não condicional F levam a diferentes valores do VaR. A seguir daremos os métodos que iremos aplicar para o cálculo do VaR não condicional e da Perda Média (*Expected Shortfall*). Essas medidas refletem riscos de longo prazo. São cruciais para vários modelos, como na teoria de Markowitz para carteiras eficientes ou modelos teóricos para apreçamento de ativos. Ressaltamos que as medidas de risco condicionais serão obtidas a partir dos modelos condicionais que serão vistos na seção 3.4.

(i) VaR empírico

É a abordagem não-paramétrica para o cálculo do VaR. O VaR_α empírico é o $(1 - \alpha)$ quantil da distribuição empírica dos dados, definida em 3.23

$$\text{VaR}_\alpha = \widehat{F_T^{-1}}(1 - \alpha)\ . \tag{3.37}$$

Esta abordagem supõe que a distribuição preditiva dos retornos é igual à da amostra. Esse procedimento distingue as caudas mas fornece estimativas ruins para α pequeno (menor que 0.05) e T pequeno.

(ii) VaR baseado no modelo Normal

Para este caso, assumimos ser F a distribuição Normal com média μ e variância σ^2, $r_t \sim N(\mu, \sigma^2)$. O VaR_α (definido para a cauda direita, ganhos) é

$$\text{VaR}_\alpha = \bar{r} + z_\alpha \; S \tag{3.38}$$

onde z_α é o quantil de probabilidade de excedência α de uma Normal padrão, e $\bar{r}$ e S^2 os EMV de μ e σ^2.

(iii) VaR baseado no modelo t-Student

Assumimos ser a distribuição F dos dados a t-Student .com ν graus de liberdade. O quantil Q_α calculado pela maioria dos pacotes é baseado numa distribuição t_v com $\mu = 0$, $\sigma = 1$ que tem variância igual a $\frac{\nu}{\nu-2}$. Assim, se quisermos o quantil associado à uma distribuição com variância 1, a qual denotaremos por t^*_ν, devemos dividir Q_α por $\sqrt{\nu/(\nu-2)}$. Ou seja,

$$\begin{aligned}
\alpha = P(t_\nu > Q_\alpha) &= P\left(\frac{t_\nu}{\sqrt{\nu/(\nu-2)}} > \frac{Q_\alpha}{\sqrt{\nu/(\nu-2)}}\right) \\
&= P\left(t^*_\nu > \frac{Q_\alpha}{\sqrt{\nu/(\nu-2)}}\right) \\
&= P\left(t^*_\nu > Q^*_\alpha\right) \quad , \; \nu > 2.
\end{aligned}$$

O VaR_α (ganhos) é dado por

$$\text{VaR}_\alpha = \widehat{\mu} + Q^*_\alpha \; \widehat{\sigma} \tag{3.39}$$

onde $\widehat{\mu}$ e $\widehat{\sigma}$ podem ser quaisquer estimadores para μ e σ, podendo ser $\bar{r}$ e S, ou os estimadores de máxima verossimilhança da distribuição t_v. Neste trabalho usaremos os estimadores de máxima verossimilhança.

(iv) VaR baseado no modelo t-Student assimétrico

A função probabilidade densidade da AST (*asymmetric Student-t*) é dada por

$$f_{AST}(y;\delta,\nu_1,\nu_2) = \begin{cases} \frac{\delta}{\delta^*} K(\nu_1)[1 + \frac{1}{\nu_1}(\frac{y}{2\delta^*})^2]^{-\frac{\nu_1+1}{2}}, & \text{se} \quad y \leq 0 \\ \frac{1-\delta}{1-\delta^*} K(\nu_2)[1 + \frac{1}{\nu_2}(\frac{y}{2(1-\delta^*)})^2]^{-\frac{\nu_2+1}{2}}, & \text{se} \quad y > 0 \; . \end{cases} \tag{3.40}$$

onde $\delta \in (0,1)$ é o parâmetro de assimetria, $\nu_1 > 0$ e $\nu_2 > 0$ são os parâmetros da cauda esquerda e direita respectivamente, $K(\nu) = \frac{\Gamma((\nu+1)/2)}{[\sqrt{\pi\nu}\Gamma(\nu/2)]}$ e α^* é definido como

$$\delta^* = \frac{\delta K(\nu_1)}{[\delta K(\nu_1) + (1-\delta)K(\nu_2)]}. \tag{3.41}$$

A f.d.a. e a função quantil da AST são dadas por

$$F_{AST}(y) = 2\delta F_t(\frac{y \wedge 0}{2\delta^*}); \nu_1) + 2(1-\delta)[F_t(\frac{y \vee 0}{2(1-\delta^*)}; \nu_2) - \frac{1}{2}] \tag{3.42}$$

e

$$F^{-1}_{AST}(p) = 2\delta^* F_t^{-1}(\frac{p \wedge \delta}{2\delta}); \nu_1) + 2(1-\delta^*)[F_t^{-1}(\frac{p \vee \delta + 1 - 2\delta}{2(1-\delta)}; \nu_2) \tag{3.43}$$

onde δ^* foi definido em 3.41.

O VaR_α (ganhos) da AST é então

$$\text{VaR}_{AST}(\alpha) \equiv F^{-1}_{AST}(1-\alpha)$$

e

$$\text{VaR}_\alpha = \widehat{\mu} + \text{VaR}_{AST}(\alpha) * \widehat{\sigma}.$$

(v) *VaR baseado no modelo GPD*

O VaR_α é estimado a partir da expressão (3.29). Estimamos $\bar{F}(u)$ empiricamente usando $\frac{N_u}{T}$,onde N_u é o número de r_t's que ultrapassaram o limiar u, ou seja, o número de excedentes, e T é o tamanho da série.

Sendo $u + y = \text{VaR}_\alpha$, temos

$$\bar{F}(\text{VaR}_\alpha) = \alpha = \bar{P}_{\xi,\psi}(y)\ p^*\ , \tag{3.44}$$

onde $p^* = \frac{N_u}{T}$. Calculamos, então, o quantil y de $\bar{P}_{\xi,\psi}$ tal que $\bar{P}_{\xi,\psi}(y) = \frac{\alpha}{p^*}$. Logo,

$$y = P^{-1}_{\xi,\psi}\left(1 - \frac{\alpha}{p^*}\right),$$

e portanto temos

$$\text{VaR}_\alpha = u + P^{-1}_{\xi,\psi}\left(1 - \frac{\alpha}{p^*}\right),$$

onde as estimativas de (ψ, ξ) serão obtidas por máxima verossimilhança.

(vi) *Expected Shortfall*

Pelo fato do VaR não tratar da magnitude das perdas as quais se refere, algumas outras medidas de risco foram propostas para poder quantificar essa magnitude, como por exemplo o *Expected Shortfall* ou Perda Média, em português. Para um α entre 0 e 1, a Perda Média de risco α no dia t, denotada por $\bar{S}_{t,\alpha}$ é o valor médio da perda além de um certo limite, no nosso caso é o VaR_α, definida como:

$$\bar{S}_{t,\alpha} = E[r_{t+1} | r_{t+1} > \text{VaR}_{t,\alpha}]. \tag{3.45}$$

Assim, a Perda Média é o valor esperado da distribuição condicional dos excessos , isto é, da GPD. Portanto pode também ser estimado usando $\frac{\psi}{1-\xi}$ se $\xi > 0$.

3.3.2 Teste de Kupiec

O teste de cobertura mais famoso é o de Kupiec (1995), baseado no modelo binomial onde são comparados os números de violações esperadas e observadas. A hipótese nula é de que a probabilidade α ($\alpha = P(r_t > \text{VaR}_\alpha)$ ou $\alpha = P(r_t < \text{VaR}_\alpha)$) está corretamente especificada, ou seja, H_0: $p = \alpha$, onde p é a verdadeira probabilidade de sucesso. A probabilidade de se observar v violações em T tentativas, onde $0 \leq v \leq T$, sob H_0 e de acordo com a distribuição binomial, é dada por

$$\binom{T}{v}(1-\alpha)^{T-v}\alpha^v. \tag{3.46}$$

A estatística teste é baseada na razão das log-verossimilhanças e tem distribuição assintótica chi-quadrado com 1 grau de liberdade (ver detalhes em Kupiec (1995)).

3.4 Modelagem Condicional

3.4.1 Modelagem AR(F)IMA

A evolução temporal da média condicional de uma série pode ser muitas vezes descrita através de processos (integrados) autorregressivos e de média móvel, ARIMA(p, d, q). Os modelos ARIMA (popularizados por Box, G. E. P., Jenkins, G.M. e Reinsel, G. (1994)) tem como casos especiais os modelos AR(p), MA(q) e ARMA(p, q).

Considere o processo $\{p_t\}$, onde p_t representa o logaritmo do preço P_t de um ativo ou carteira no dia (ou qualquer unidade de tempo) t. O processo $\{p_t\}$ segue um modelo ARIMA(p, d, q), d inteiro, se $\Delta^d p_t \equiv (1-B)^d p_t = r_t$ seguir um ARMA(p, q), isto é,

$$r_t = \phi_0 + \phi_1 r_{t-1} + \cdots + \phi_p r_{t-p} + a_t - \theta_1 a_{t-1} - \cdots \ \theta_q a_{t-q}, \tag{3.47}$$

onde $\phi_0 = \mu(1 - \phi_1 - \cdots \phi_p)$, e onde $a_t \sim \text{RB}(0, \sigma_a^2)$ (onde RB significa Ruído Branco). Supondo $\mu = 0$, temos $\Phi(B)\Delta^d p_t = \Theta(B)a_t$, onde B é o operador retroativo. A diferenciação Δ^d é necessária para estacionarizar a série. Se após d diferenças a série resultante for estacionária dizemos que a série original $\{p_t\}$ é integrada de ordem d, uma série I(d), e a série final, $\{r_t\}$ é uma série I(0). Em finanças, geralmente basta uma diferenciação, isto é, $d = 1$ para séries de preços diários. Existem várias estatísticas para se testar estacionariedade como por exemplo o teste KPSS (Kwiatkowski, D., Phillips, P. C. B., Schmidt, P. e Shin, Y. (1992)) ou o teste ADF (Dickey, D. A. e Fuller, W. A. (1979)).

3.4.1.1 Processos Autorregressivos AR(p)

Um processo autorregressivo de ordem p assume que

$$r_t = \phi_0 + \phi_1 r_{t-1} + \cdots + \phi_p r_{t-p} + a_t,$$

onde $\{a_t\}$ é uma série tipo ruído branco com média zero e variância constante, $a_t \sim RB(0, \sigma_a^2)$.

Processos AR(1)
Consideraremos o caso particular p = 1, $r_t = \phi_0 + \phi_1 r_{t-1} + a_t$, e calcularemos as esperanças e variâncias condicionais e não condicionais.

$$E[r_t|r_{t-1}] = \phi_0 + \phi_1 r_{t-1} \quad e \quad var(r_t|r_{t-1}) = \sigma_a^2.$$

A esperança não condicional pode ser calculada a partir de

$$E[r_t] = E[E[r_t|r_{t-1}]] = E[\phi_0 + \phi_1 r_{t-1}] = \phi_0 + \phi_1 E[r_{t-1}],$$

e como o processo é estacionário, $E[r_t] = E[r_{t-1}]$, obtemos

$$\mu \equiv E[r_t] = \frac{\phi_0}{1-\phi_1}.$$

Pode-se então notar que:

1. $\phi_1 \neq 1$ para μ existir;
2. μ será zero se e somente se (sss) $\phi_0 = 0$.

Para achar a variância não condicional de r_t pode-se usar a fórmula

$$var(r_t) = E[var(r_t|r_{t-1}, \cdots)] + var(E[r_t|r_{t-1}, \cdots]),$$

ou, equivalentemente, a partir de

$$r_t - \mu = \phi_1(r_{t-1} - \mu) + a_t,$$

obter

$$var(r_t - \mu) = var(r_t) = \phi_1^2 var(r_{t-1}) + \sigma_a^2,$$

já que a_t e a_{t-1} são não correlacionados. Como, por estacionariedade, $var(r_{t-1}) = var(r_t)$, temos

$$\gamma_0 \equiv var(r_t) = \frac{\sigma_a^2}{1-\phi_1^2},$$

desde que $\phi_1^2 < 1$. Assim, um AR(1) fracamente estacionário tem $|\phi_1| < 1$. Por outro lado, pode-se mostrar que $|\phi_1| < 1$ implica que o AR(1) é fracamente estacionário.

Assim, escrevendo r_t como uma combinação linear de um número infinito de inovações, e sabendo que $-1 < \phi_1 < +1$, podemos provar que $E[r_t] < \infty$ e $var(r_t) < \infty$, sendo $\gamma_0 = var(\sum_{j=0}^{\infty} \phi_1^j a_{t-j}) = \sigma_a^2 \sum_{j=0}^{\infty} \phi_1^{2j} = \frac{\sigma_a^2}{1-\phi_1^2}$. Além disto, usando a desigualdade de Cauchy-Schwartz podemos mostrar que as autocovariâncias são finitas. Em resumo, um AR(1) é fracamente estacionário se e somente se $|\phi_1| < 1$.

As expressões para os ρ_k são

$$\rho_0 = 1 \qquad \rho_k = \phi_1^k \qquad k \geq 0.$$

A f.a.c. de um AR(1) decai exponencialmente à taxa ϕ_1 e com valor inicial $\rho_0 = 1$.

A estimação do modelo AR(1) é em geral feita por máxima verossimilhança condicional.

3.4.1.2 Processos ARFIMA(p, d, q)

Como já foi observado anteriormente, séries de retornos financeiros são em geral I(0) e os preços em geral I(1). A f.a.c. de uma série I(1) decai lentamente, e pode-se mostrar que para *lag* k fixo, $\widehat{\rho}_k \uparrow 1$ quando T tende a infinito. Por outro lado, como também já falado, a f.a.c. de uma série I(0) decai exponencialmente para zero a medida que o *lag* aumenta e assim, observações separadas no tempo por um *lag* grande podem ser consideradas independentes. Entretanto, existem algumas séries para as quais a f.a.c. decai lentamente para zero numa taxa polinomial quando o *lag* aumenta. Tais processos são chamados de *memória longa*. Se $r_t = (1-B)^d p_t$, e d não é inteiro, r_t é dita ser fracionalmente integrada. Neste caso, a série primeira diferença da série p_t, mesmo se mostrando estacionária, diversas vezes exibe uma correlação não nula entre observações distantes.

Este fenômeno é conhecido em Hidrologia, onde é observada a "persistência" nos níveis dos rios, conhecido como efeito "Hurst". Memória longa na média condicional de um processo também tem sido observada em dados vindo de outras áreas tais como metereologia, astronomia, economia, veja Beran (1994). Como será que as criptomoedas se comportarão em relação à memória longa? Iremos investigar este tópico no Capítulo 4.

Um dos processos apresentando esta característica é o processo autorregressivo-média móvel fracionalmente diferenciado ARFIMA(p, d, q) que modela a presença de memória longa na média condicional da série (além da memória curta) e pode ser considerado uma extensão do modelo ARIMA. Modelos para memória longa na média foram introduzidos por Granger, C.W.J. e Joyeux, R. (1980) e Hosking, J.R.M. (1981), a partir do trabalho de Hurst, H.E. (1951). Desta forma, um modelo ARFIMA incorpora o comportamento de memória longa ao introduzir a possibilidade de d ser fracionário. Pode ser escrito como

$$\Phi(B)(1-B)^d r_t = \Theta(B)a_t, \;\; d \in \Re, \tag{3.48}$$

onde, como antes, os polinômios $\Phi(B)$ e $\Theta(B)$ possuem ordens p e q, respectivamente. O processo $\{a_t\}_{t\in Z}$ é um ruído branco com média zero e variância finita σ_a^2. O termo $(1-B)^d$ é a expansão em séries binomiais dada por $(1-B)^d = 1 - dB + \frac{d(d-1)B^2}{2!} - \frac{d(d-1)(d-2)B^3}{3!} + \cdots$ (veja propriedades em Diebold, F.X. e Rudebusch, G.D. (1989) ou Hosking, J.R.M. (1981)).

Considere o processo ARFIMA$(0, d, 0)$ que incorpora o comportamento de memória longa ao introduzir a possibilidade de d ser fracionário:

$$(1-B)^d r_t = a_t \quad -0.5 < d < 0.5 \ ,$$

um *ruído branco fracionário* (RBF) análogo no tempo discreto do movimento browniano fracionário. Naturalmente que para $d = 0$, r_t é um ruído branco e sua f.a.c. é zero para k = 1,2,3 $\cdots$. Notemos que para $d = 1$, r_t seria um *passeio aleatório* (um AR(1) com raiz unitária) e portanto sua f.a.c. ficaria próxima de 1 para todos os *lags*. Para valores fracionários de d a f.a.c. diminui hiperbolicamente a zero, isto é, $\rho_k = \Gamma k^{2d-1}$, onde Γ é a função Gama. Quando $d \geq 0.5$ a variância de r_t é infinita, e o processo é não estacionário, mas não chega a ser um "não estacionário" como um I(1). Para d entre 0 e 0,5 o processo é dito ser de memória longa porque para k grande, ρ_k ainda é significativamente diferente de zero.

A necessidade de se fazer ou não uma diferenciação poderia ser testada utilizando-se algum teste de raiz unitária. Esses testes, entretanto, possuem potência (probabilidade de rejeitar a hipótese nula quando a mesma é falsa) ainda menor contra alternativas fracionárias. O melhor é aplicar testes específicos para detectar a existência de d fracionário.

A quantidade mais utilizada para testar a presença de memória longa é a razão entre o $r$ange e o desvio padrão, $\frac{R}{S}$, originalmente proposta em Mandelbrot, B.B. (1969a) e Mandelbrot, B.B. (1969b), no contexto da economia. Esta quantidade é estimada com a estatística RS.

A hipótese nula a ser testada é "H_0 : Não existe memória longa". Porém a estatística RS é sensível à presença de dependência de memória curta, k pequeno. Isso significa que, a presença de ρ_k significativo, para k pequeno, muda a distribuição de RS sob a hipótese nula, e pode levar a conclusões erradas. Lo, A. (1991) propôs a estatística RS modificada que incorpora a presença de correlação de memória curta.

A estimação de d pode ser feita por vários métodos, inclusive alguns baseados na densidade espectral, sendo os mais conhecidos aqueles baseados no modelo de regressão, os estimadores semi-paramétricos clássicos e robustos (veja Mendes, B.V.M.e Lopes, S.R.C. (2006)). Neste trabalho usaremos os estimadores de máxima verossimilhança para os modelos ARFIMA.

3.4.2 Modelos para a volatilidade condicional

A volatilidade tem uma função extremamente importante na alocação de ativos, apreçamento de opções, administração do risco, técnicas de *hedging* e política monetária. Muito da área de pesquisa de uma instituição financeira é voltada para a modelagem e previsão de volatilidade de ativos financeiros. Dentro da área de administração de riscos, a volatilidade condicional tem papel importante pois permite calcular medidas de risco condicionais, em particular o VaR de uma certa posição condicional à situação corrente da economia.

A forma mais simples de se medir a volatilidade **não condicional** de um conjunto de dados é através do desvio padrão amostral S, onde S é a raíz quadrada da equação 3.10, às vezes chamado de volatilidade histórica. Apesar de poder ser calculado para qualquer distribuição, somente sob a suposição de normalidade a distribuição de S^2 (vide 3.10) é conhecida analiticamente. Nos outros casos, a distribuição de S^2 pode ser obtida por simulação. Dada uma série de retornos, S pode ser calculado utilizando-se as últimas N observações (janela de tamanho N) e deslocar esta janela ao longo do tempo. Notemos que sob normalidade das observações, S^2 é um estimador não viciado de σ^2, mas S não o é de σ.

A estimativa da volatilidade de retornos financeiros se torna mais precisa quando se usa modelos que atribuem peso maior às informações mais recentes. Podemos notar que a prática consagrou a palavra *v*olatilidade para descrever a variância condicional σ_t^2 de uma variável. Para se estimar a volatilidade condicional um modelo deve ser assumido.

Mesmo não podendo ser medida diretamente, a volatilidade de retornos financeiros possui algumas características (fatos estilizados) como:

1. Aparecer em grupos de maior ou menor volatilidade, ou seja, *clusters* de volatilidade;

2. Evoluir continuamente no tempo, sendo considerada estacionária;

3. Reagir diferentemente a valores positivos ou negativos da série de retornos;

4. Apresentar persistência alta e reversão para a média;

5. Ser também parcialmente explicada por variáveis exógenas.

A ideia primária que permeia o estudo da volatilidade é a de que séries (estacionárias) de retornos financeiros $\{r_t\}$ são, em geral, *n*ão autocorrelacionadas mas são *d*ependentes.

Considerando o conjunto I_{t-1} de informações passadas até o tempo $t-1$, a esperança condicional $\mu_t = E[r_t|\mathcal{I}_{t-1}]$ pode ser especificada, conforme visto anteriormente, por um modelo ARFIMA(p, d, q). Nada impede que a equação para a média condicional inclua também algumas variáveis explicativas através do modelo de regressão com erros tipo série temporal. A volatilidade é dada por $\sigma_t^2 \equiv var(r_t|\mathcal{I}_{t-1})$. A média não condicional é $\mu \equiv E[r_t] = E[E[r_t \mid I_{t-1}]]$. A variância não condicional é $\sigma^2 \equiv \gamma_0 \equiv var(r_t) = E[(r_t - \mu)^2]$. *N*esta seção referente a volatilidade, a distribuição *condicional* de r_t será denotada por F e a distribuição não condicional de $\frac{r_t-\mu}{\sigma}$ será representada por H.

O fato estilizado 1 sobre a volatilidade significa que choques correntes na volatilidade afetam volatilidades futuras. Em outras palavras, a volatilidade é *p*ersistente. Assim, um bom modelo de volatilidade deve ser capaz de capturar este fato.

Considere agora que a previsão $\sigma^2_{t+k|t}$ seja dada pela função de perda quadrática, isto é,

$$\sigma^2_{t+k|t} \equiv E[(r_{t+k} - \mu_{t+k})^2 \mid \mathcal{I}_t],$$

que significa que a previsão da volatilidade k passos a frente depende do conjunto de informações disponíveis no tempo t, em particular do retorno no tempo t. A volatilidade é dita persistente se o retorno hoje, r_t, tem grande efeito na previsão da variância condicional vários passos a frente.

A propriedade de reversão para a média da volatilidade indica que deve existir um nível *normal* de volatilidade ao qual a mesma retornaria depois de um período de alta ou baixa volatilidade. É importante notar que este nível médio pode não ser constante ao longo do tempo e também depender do ambiente econômico.

Outras variáveis podem conter informações importantes para a série da volatilidade. Isto é razoável já que preços de ativos sofrem influências dos mercados tanto na esfera local quanto na esfera global. Há na literatura diversos trabalhos propondo várias séries diferentes a serem consideradas como explicativas, inclusive séries de medidas de variância realizada (veja em Accioly, V.B. e Mendes, B.V.M. (2015)). Além de séries econômicas e financeiras, fatos isolados podem ser influenciadores na volatilidade, como por exemplo resultados macro-econômicos, dia da semana, entre outros.

Por fim, não há uma boa saída para a questão da avaliação da qualidade de uma previsão da volatilidade, já que ela não é observável. Vários autores apenas dividem cada retorno pela previsão um passo a frente do seu desvio padrão e testam se o quadrado desta série ainda seria previsível. Outro método utilizado é o de se ajustar um modelo de regressão linear simples onde a variável dependente seria a série de retornos ao quadrado e a variável explicativa a variância condicional um passo a frente. É necessário testar se o intercepto é zero e se a inclinação é um. Este método permite a comparação de diversos modelos de previsão da volatilidade. Entretanto, este método *n*ão é recomendado devido ao fato de que a série dos quadrados dos retornos ser heteroscedástica, implicando em estimativas não eficientes dos coeficientes da regressão. Soma-se a isso o fato que, r_t^2 como um estimador da variância tem uma grande variabilidade, o que implicará em um

coeficiente de explicação R^2 da regressão muito pequeno. Alternativamente, podemos substituir os retornos ao quadrado por alguma medida de variância realizada.

3.4.2.1 Modelos GARCH

Séries de retornos financeiros apresentam diversas formas de dinâmicas lineares e não-lineares, a mais forte sendo a dependência de sua variabilidade instantânea no seu próprio passado. Por conta dessas e outras características bastante conhecidas de séries financeiras, Engle, R.F. (1982) introduziu os modelos autorregressivos condicionalmente heteroscedásticos (ARCH), cujo objetivo é modelar os *clusters* de volatilidade destas séries. Esses modelos foram generalizados por Bollerslev, T. (1986) que introduziu os modelos generalizados autorregressivos condicionalmente heteroscedásticos (GARCH).

Entre as várias abordagens para a modelagem da volatilidade, aquela através de modelos da família GARCH é sem dúvida a mais popular, isto provavelmente devido à flexibilidade desses modelos, facilidade de estimação e pela sua capacidade de reproduzir alguns fatos estilizados apresentados pela maioria destas séries, incluindo o excesso de curtose na distribuição não condicional dos dados e heteroscedasticidade condicional que dão origem aos *c*lusters de volatilidade. Após o artigo de Engle de 1982 diversos outros se seguiram com aplicações e extensões.

Modelo ARCH(m)

O modelo ARCH(m) pode ser escrito como

$$r_t = \mu_t + \sigma_t \varepsilon_t, \quad \sigma_t^2 = \alpha_0 + \alpha_1 r_{t-1}^2 + \ldots + \alpha_m r_{t-m}^2,$$

onde $\{\varepsilon_t\}$ é uma sequência de v.a.'s i.i.d. com média zero e variância 1, isto é, $\varepsilon_t \sim$ i.i.d. $F(0,1)$, $\alpha_0 > 0$ e $\alpha_i \geq 0$ para $i = 1, \ldots, m$. A soma dos parâmetros α_i, $\sum_{i=1}^{m} \alpha_i$, mede a persistência e deve ser menor que um para assegurar que a variância não condicional de r_t seja finita. Na prática, em geral supomos F sendo a distribuição Normal ou t-student com ν graus de liberdade ($t(\nu)$). Podemos observar que pela definição, valores grandes de $\mid r_t \mid$ tendem a ser seguidos por outros valores grandes. Mesmo assumindo F como sendo a distribuição Normal pode-se mostrar que r_t tem excesso de curtose positivo, isto é, a distribuição não condicional dos retornos tem caudas pesadas. Este fato também explica os pontos extremos e a não normalidade de r_t.

Consideraremos agora o processo ARCH(1): $r_t = \sigma_t \varepsilon_t$, $\sigma_t^2 = \alpha_0 + \alpha_1 r_{t-1}^2$, $\varepsilon_t \sim$ i.i.d. $F(0,1)$, onde supomos (por simplicidade) $\mu_t = 0$, ou que μ_t já tenha sido estimada através de algum modelo condicional para a média, como por exemplo, algum modelo da classe ARFIMA(p,d,q). A média não condicional deste processo é $E[r_t] = E[E[r_t \mid I_{t-1}]] = 0$. A variância não condicional é $var(r_t) = E[r_t^2] = E[E[r_t^2 \mid I_{t-1}]] = E[\sigma_t^2] = \alpha_0 + \alpha_1 E[r_{t-1}^2]$. Sendo o processo estacionário de segunda ordem obtemos

$$\gamma_0 \equiv \sigma^2 \equiv var(r_t) = \frac{\alpha_0}{1 - \alpha_1},$$

e como a variância deve ser limitada, positiva, devemos ter $0 \leq \alpha_1 < 1$. Devemos também obter as covariâncias, $cov(r_t, r_{t+k}) = E[r_t r_{t+k}] = E[E[r_t r_{t+k} \mid I_{t+k-1}]] = E[r_t E[r_{t+k} \mid I_{t+k-1}]] = 0$. Isto é

$$\gamma_k \equiv cov(r_t, r_{t+k}) = 0 \quad \text{para } k \geq 1,$$

e portanto temos um processo de v.a.´s não correlacionadas, com média zero, e variância $\frac{\alpha_0}{1-\alpha_1}$ constante, um ruído branco. Por fim, assumindo F como a distribuição Normal, é possível obter o quarto momento. Sabendo que $E[r_t^4 \mid I_{t-1}] = E[\sigma_t^4\varepsilon_t^4 \mid I_{t-1}] = 3E[\sigma_t^4 \mid I_{t-1}] = 3E[(\alpha_0 + \alpha_1 r_{t-1}^2)^2 \mid I_{t-1}]$, temos $E[r_t^4] = 3(\alpha_0^2 + 2\alpha_0\alpha_1 var(r_{t-1}) + \alpha_1^2 E[r_{t-1}^4])$, e como o processo é estacionário

$$E[r_t^4] = \frac{3\alpha_0^2(1+\alpha_1)}{(1-\alpha_1)(1-3\alpha_1^2)}.$$

Logo, para que o momento de quarta ordem seja finito e positivo devemos ter $(1-3\alpha_1^2) > 0$, ou seja, $0 \leq \alpha_1^2 < \frac{1}{3}$. O coeficiente de curtose do processo ARCH(1) é então

$$C = \frac{E[r_t^4]}{(var(r_t))^2} = \cdots = 3\frac{1-\alpha_1^2}{1-3\alpha_1^2} > 3,$$

mesmo tendo inovações Normais.

Pode-se mostrar que um ARCH(1) corresponde a um AR(1) para os quadrados dos retornos. Para isto basta tomar $r_t^2 - \sigma_t^2$ e equacionar

$$r_t^2 - (\alpha_0 + \alpha_1 r_{t-1}^2) = \sigma_t^2\varepsilon_t^2 - \sigma_t^2 = \sigma_t^2(\varepsilon_t^2 - 1)$$

isto é

$$r_t^2 = \sigma_t^2(\varepsilon_t^2 - 1) + (\alpha_0 + \alpha_1 r_{t-1}^2)$$

e obtemos o AR(1)

$$r_t^2 = \alpha_0 + \alpha_1 r_{t-1}^2 + \vartheta_t$$

onde $\vartheta_t = \sigma_t^2(\varepsilon_t^2 - 1)$, ou ϑ_t é a v.a. $\sigma_t^2(\chi_1^2 - 1)$. Portanto $\{\vartheta_t\}$ é uma sequência de v.a.´s não correlacionadas com média zero, mas com variância não constante. A f.a.c. de r_t^2 decai como a de um AR(1) com $\rho_k(r_t^2) = \alpha_1^k$.

De maneira análoga pode-se mostrar que um modelo ARCH(m) corresponde a um AR(m) para os quadrados dos retornos.

$$r_t^2 = \alpha_0 + \alpha_1 r_{t-1}^2 + \ldots + \alpha_m r_{t-m}^2 + \vartheta_t,$$

onde $\{\vartheta_t\}$ é um ruído branco, o que irá justificar o teste abaixo e o uso da f.a.c.p. como ferramenta exploratória.

Para o ajuste de um modelo da família (G)ARCH(m) a uma série de retornos financeiros, pode-se iniciar examinando a f.a.c.p. amostral da série $\{r_t^2\}$. Esta inspeção nos dará uma proposta inicial para a ordem m. Pode-se também efetuar o teste Multiplicadores de Lagrange (M.L.) proposto por Engle (1982) cuja a hipótese nula é $H_0 : \alpha_1 = \alpha_2 = \ldots = \alpha_m = 0$. Este teste considera a regressão linear $r_t^2 = \alpha_0 + \alpha_1 r_{t-1}^2 + \ldots + \alpha_m r_{t-m}^2 + e_t$, $t = 1, \ldots, T$, e ajusta o modelo por mínimos quadrados ordinários. A hipótese nula é rejeitada para valores grandes da estatística teste e significa que "existe efeito ARCH". É válido lembrar que o retorno ao quadrado é um estimador viciado para a variância (superestima) e não é eficiente, não sendo portanto uma boa proxy para avaliar a performance da volatilidade GARCH estimada, mas serve para especificar as dependências lineares de r_t^2 em $r_{t-1}^2, \ldots, r_{t-m}^2$, o que justifica o uso da f.a.c.p.

A estimação dos modelos GARCH é geralmente feita pelo método da máxima verossimilhança, e assim é preciso especificar a densidade f das inovações. Os *pseudo* estimadores

de máxima verossimilhança são aqueles obtidos a partir da suposição de normalidade das inovações quando de fato elas seguiriam uma outra distribuição. Bollerslev, T. e Wooldridge, J.M. (1992) mostraram que os *pseudo* EMV dos parâmetros do modelo são consistentes. Entretanto, os estimadores da variância desses estimadores não são consistentes se a suposição de normalidade é violada.

A distribuição $t(\nu)$ é uma opção melhor e está em geral implementada nos pacotes usuais. Neste caso a inovação padrão com média zero e variância um é obtida dividindo-se a v.a. $t(\nu)$ por seu desvio padrão $\sqrt{\frac{\nu}{\nu-2}}$.

Todos os passos sugeridos para o ajuste de um modelo AR(p) devem ser aqui repetidos. Eles são, nesta ordem, identificação da ordem do modelo utilizando testes e as f.a.c. e f.a.c.p. amostrais, estimação do modelo escolhido, testes de significância das estimativas dos parâmetros, análise dos resíduos padronizados $\frac{r_t}{\sigma_t}$, ou de $\frac{r_t-\mu_t}{\sigma_t}$ se a média condicional for estimada conjuntamente, e uma possível reformulação do modelo. O critério de Akaike pode ser usado para decidir entre modelos. A verificação feita nos resíduos pode incluir um teste KS, um QQ-Plot, aplicação do teste de M.L. nos resíduos, aplicação do teste de Ljung-Box nos resíduos e resíduos ao quadrado e o exame da f.a.c. e f.a.c.p. dos mesmos. É interessante ver o gráfico no tempo da volatilidade estimada, tentando identificar crises, e também examinar no tempo o gráfico dos resíduos padronizados, observando que os *c*lusters de volatilidade desapareceram mas que os pontos extremos ainda estão lá. Isto nos motiva a usar modelos da TVE para estimar com precisão as caudas da distribuição desses resíduos padronizados para, por exemplo, usar no cálculo de medidas de risco. É válido também notar que uma estimação com o uso de uma distribuição com caudas pesadas irá implicar em variâncias condicionais *n*ão infladas (ou menos infladas), o que pode destacar ainda mais os pontos atípicos.

As previsões da volatilidade são obtidas recursivamente como nos modelos AR(p). Seja a origem h das previsões. A previsão 2-passos-a-frente é estimada a partir da previsão 1-passo-a-frente $\widehat{\sigma_h^2}(1)$

$$\widehat{\sigma_h^2}(2) = \widehat{\alpha_0} + \widehat{\alpha_1}\widehat{\sigma_h^2}(1) + \widehat{\alpha_2} r_h^2 + \ldots + \widehat{\alpha_m} r_{h-m+2}^2,$$

e portanto a previsão l passos a frente é estimada como

$$\widehat{\sigma_h^2}(l) = \widehat{\alpha_0} + \sum_{j=1}^{m} \widehat{\alpha_j}\widehat{\sigma_h^2}(l-j),$$

onde $\widehat{\sigma_h^2}(l-j) = r_{h+l-j}^2$ se $l - j \leq 0$.

Alguns autores apontam algumas deficiências do modelo ARCH:

1. Choques positivos e negativos têm o mesmo efeito na volatilidade;
2. Algumas restrições complicadas para os α_i's;
3. Fornecem apenas uma fórmula para descrever o mecanismo gerador dos *clusters* de volatilidade, não dando nenhuma "pista"ou indicação das causas de tal comportamento;
4. Grande sensibilidade à observações atípicas, isto é, grandes choques que poderiam ser "*outliers*"causam super-previsão de σ_t.

Diversas das extensões que se seguiram foram concebidas com a ideia de corrigir essas falhas.

Modelo GARCH(m, s)

O modelo *Generalized autoregressive conditionally heteroskedastic* GARCH, proposto por Bollerslev, T. (1986), Bollerslev, T. (1987) expressa de maneira mais parcimoniosa a estrutura de dependência da variância condicional, já que é fato comprovado empiricamente que um ARCH(m) não ajusta bem séries de retornos financeiros a menos que m seja grande. Nesse modelo, a variância condicional, além de depender dos quadrados dos retornos passados como no modelo ARCH, depende também das próprias variâncias condicionais passadas.

Se $\{r_t\}$ segue um modelo GARCH(m, s), então $r_t = \sqrt{\sigma_t^2}\varepsilon_t$ e

$$\sigma_t^2 = \alpha_0 + \alpha_1 r_{t-1}^2 + \cdots + \alpha_m r_{t-m}^2 + \beta_1 \sigma_{t-1}^2 + \beta_2 \sigma_{t-2}^2 + \cdots + \beta_s \sigma_{t-s}^2, \tag{3.49}$$

com $\varepsilon_t \sim$ i.i.d.$F(0, 1)$, $\alpha_0 > 0$, $\alpha_i \geq 0$, $i = 1, \cdots, m$, $\beta_i \geq 0$, $i = 1, \cdots, s$, e onde a *persistência* $\sum_{j=1}^{q}(\alpha_j + \beta_j)$ deve ser menor que 1 para que a variância não condicional, $\gamma_0 = \sigma^2 = \frac{\alpha_0}{1-\sum \alpha_i + \sum \beta_j}$, seja finita, $q = \max(m, s)$. Na prática, novamente, supomos F sendo a distribuição Normal, $t(\nu)$ ou t-assimétrica.

Da mesma forma como foi feito nos modelos ARCH, podemos escrever o GARCH como um ARMA(q, s) nos quadrados dos retornos, r_t^2.

A estimação dos modelos GARCH(m, s) segue os mesmos passos vistos para o ARCH(m), devendo começar com a determinação das ordens m e s. Para isto pode-se examinar a f.a.c.p. amostral (da série ao quadrado) e também aplicar o teste de M.L. para detectar efeito ARCH. É indiferente se usar os retornos ou os retornos filtrados (resíduos) por um modelo ARFIMA(p, d, q), já que o interesse é no segundo momento. É possível também aplicar o teste de Ljung-Box na série ao quadrado.

O segundo passo é a estimação do modelo. Uma abordagem usual é superparametrizar e ir aos poucos retirando os coeficientes não significativos do modelo e utilizando o critério AIC para decidir entre os modelos (desde que os modelos competidores contenham todas as estimativas dos parâmetros significativas). Como no caso ARCH, geralmente o método de estimação utilizado é o de máxima verossimilhança. No caso dos erros seguirem a distribuição $t_(\nu)$, os graus de liberdade devem também ser estimados. A escolha de uma distribuição F com caudas pesadas sempre melhora o ajuste e reduz o número de parâmetros.

Por fim, temos que examinar os resíduos do melhor modelo ajustado. Os choques padronizados $\{\widehat{\varepsilon}_t\}$ devem ser i.i.d.$F(0, 1)$. Pode-se usar os testes de Ljung-Box, de assimetria, de curtose e também examinar os QQ-Plots, e as f.a.c. e f.a.c.p. Se alguma suposição não se verificar, devemos voltar ao primeiro passo e procurar por um modelo melhor. Somente após todas essas verificações pode-se seguir com as estimativas das previsões do modelo. Além disto, é interessante observar o gráfico das volatilidades *in-sample*.

Modelo GARCH$(1, 1)$

O modelo mais simples nesta família é o GARCH(1,1). A atração dessa especificação mora no fato de ser um modelo parcimonioso que geralmente explica muito bem a dinâmica da volatilidade de retornos financeiros.

Vários artigos já mostraram empiricamente que geralmente basta um modelo GARCH$(1,1)$ para capturar a dinâmica da volatilidade da série de retornos financeiros. Será que este fato também será observado para as criptomoedas? Iremos responder a essa pergunta no Capítulo 4.

Supondo normalidade para as inovações, temos que para o GARCH$(1,1)$ a curtose C é

$$C(r_t) = \frac{E[r_t^4]}{(E[r_t^2])^2} = \frac{3(1-(\alpha_1+\beta_1)^2)}{1-(\alpha_1+\beta_1)^2-2\alpha_1^2} > 3.$$

Um processo GARCH$(1,1)$ tem portanto caudas mais pesadas que a Normal mesmo quando as inovações são Normais.

Pode-se calcular a expressão da *forward persistence*, ou simplesmente persistência, para o GARCH(1,1). Primeiro, notando que $\gamma_0 = \frac{\alpha_0}{(1-\alpha_1-\beta_1)}$, temos $\alpha_0 = (1-\alpha_1-\beta_1)\gamma_0$. Temos então que

$$\sigma_t^2 - \gamma_0 = \alpha_1(r_{t-1}^2 - \gamma_0) + \beta_1(\sigma_{t-1}^2 - \gamma_0)$$

Sendo $\varepsilon_t \equiv i.i.d.(0,1)$ temos que $E[r_t^2 \mid \mathcal{I}_{t-1}] = E[\sigma_t^2\varepsilon_t^2 \mid \mathcal{I}_{t-1}] = \sigma_t^2$. Podemos mostrar que

$$E[r_{t+k}^2 \mid \mathcal{I}_t] = \sigma_{t+k}^2.$$

Assim, para $k \geq 2$

$$E[(\sigma_{t+k}^2 - \gamma_0) \mid \mathcal{I}_t] = (\alpha_1+\beta_1)E[(\sigma_{t+k-1}^2 - \gamma_0) \mid \mathcal{I}_t].$$

Após algumas iterações chegamos a

$$\sigma_{t+k|t}^2 = \gamma_0 + (\alpha_1+\beta_1)^{k-1}(\alpha_0 + \alpha_1 r_t^2 + \beta_1\sigma_t^2 - \gamma_0)$$

e assim

$$\theta_{t+k|t} = \alpha_1(\alpha_1+\beta_1)^{k-1}.$$

De acordo com Engle e Patton (2001) θ é a *forward persistence* e também um número adimensional. Para muitos modelos de volatilidade, θ declina geometricamente, mas pode ser importante até um ano no futuro.

Pode-se obter também a persistência acumulada

$$\phi_{t+k|t} = \frac{1}{k}(\theta_{t+k|t} + \theta_{t+k-1|t} + \cdots + \theta_{t+1|t})$$

que para o GARCH(1,1) é

$$\phi_{t+k|t} = \frac{1}{k}\alpha_1\frac{1-(\alpha_1+\beta_1)^k}{1-\alpha_1-\beta_1}.$$

A meia vida da volatilidade é

$$k = \frac{\log((\alpha_1+\beta_1)/2)}{\log(\alpha_1+\beta_1)},$$

já que $\mid \gamma_0+(\alpha_1+\beta_1)^{k-1}(\sigma^2_{t+1}-\gamma_0)-\gamma_0 \mid = 0.5 \mid \sigma^2_{t+1}-\gamma_0 \mid$ o que implica em $(\alpha_1+\beta_1)^{k-1} = 0.5(\alpha_1+\beta_1)$.

Modelo GARCH(m,s) com *leverage*

Os modelos GARCH padrão assumem que os termos de erro positivo e negativo têm um efeito simétrico na volatilidade. Em outras palavras, boas e más notícias têm o mesmo efeito sobre a volatilidade desse modelo. Na prática, essa suposição é frequentemente violada, em particular pelo retorno das ações, na medida em que a volatilidade aumenta mais após notícias ruins do que depois de boas notícias de mesma magnitude. Este chamado *leverage effect* aparece pela primeira vez em Black (1976), que observou que uma queda no valor da empresa causará um retorno negativo sobre sua ação e normalmente aumentará o *leverage* da ação. Esse aumento no índice de endividamento certamente significará um aumento na volatilidade da ação. Grandes mudanças seguem as grandes mudanças e pequenas mudanças seguem as pequenas mudanças no mercado de ações. Choques negativos têm um efeito muito maior sobre os preços das ações do que choques positivos da mesma magnitude. O choque negativo tem um impacto duradouro, fazendo com que o mercado de ações demore muito tempo para recuperar o nível de pré-choque, após apenas alguns dias de colisão. Isso mostra que a distribuição simétrica ou distribuição normal nem sempre é uma suposição realista. Mais tarde, modelos GARCH, levando em consideração essa assimetria no impacto da volatilidade para notícias boas e ruins, foram criados. Diversos autores começaram a estudar a assimetria na volatilidade para as reações do mercado, como por exemplo Hsieh (1989), Akgirary *et al* (1991). Nelson (1991) introduziu o modelo *Exponential GARCH* (EGARCH) para retornos no mercado de ações americano. A correlação negativa entre os choques e o retorno é uma característica saliente do mercado de ações. O sinal e a magnitude dos choques têm efeitos assimétricos nos retornos. Portanto, Glosten, Jagannathan e Runkle (1993) introduziram o GARCH com diferentes efeitos de choques negativos e positivos, levando em conta o fenômeno de *leverage*, conhecido como GJR GARCH (Ali, G. 2013). Pode ser escrito como

$$\sigma^2_t = w + \alpha r^2_{t-1} + \gamma r^2_{t-1} d_{t-1} + \beta \sigma^2_{t-1}$$

onde $d_t = 1$ se $r_t < 0$, e zero caso contrário, para captar o efeito das notícias negativas. Se $\gamma \neq 0$ existe assimetria da informação, sendo que se γ estatisticamente maior que zero, significa que as notícias ruins tem efeito maior que as boas. No caso geral temos

$$\sigma^2_t = (\omega + \sum_{j=1}^{m}(X_j v_{jt}) + \sum_{j=1}^{q}(\alpha_j \varepsilon^2_{t-j} + \gamma_j I_{t-j} \varepsilon^2_{t-j}) + \sum_{j=1}^{p}(\beta_j \sigma^2_{t-j})$$

onde γ_j representa o termo *"leverage"*.

A persistência do modelo é dada por

$$\sum_{j=1}^{q} \alpha_j + \sum_{j=1}^{p} \beta_j + \sum_{j=1}^{q} \gamma_j \kappa,$$

onde κ é o valor esperado dos resíduos padronizados z_t abaixo de zero,

$$\kappa = \int_{[-\infty,0]} f(z,0,1,...)dz$$

onde f é a densidade condicional padronizada podendo possuir parâmetros adicionais de escala e forma. No caso de distribuições simétricas, o valor de κ é 0,5. (Fonte: PDF pacote rugarch).

Modelo FIGARCH(m, D, s)

A teoria por detrás dos processos ARFIMA foi também estendida para os modelos de volatilidade. Introduzidos primeiramente por Baillie, R. T., Bollerslev, T. e Mikkelsen, H. O. (1996), e Bollerslev, T. e Mikkelsen, H. O. (1996), a criação dos modelos *Fractionally Integrated Generalized Autoregressive Conditionally Heteroskedastic* (FIGARCH) se deu pelo fato de que a função de autocorrelação dos quadrados dos retornos, ou do seu valor absoluto, decai lentamente mesmo quando a série não possui correlação serial, diferente de modelos como GARCH onde choques decaem numa taxa exponencial ou como IGARCH (*integrated* GARCH) onde choques persistem para sempre.

Consideremos a formulação dos modelos GARCH, $r_t = \sigma_t \varepsilon_t$, onde ε_t é uma sequência i.i.d. com média zero e varância um, e seja $\mathcal{F}_{t-1}$ a sigma-álgebra de eventos gerada pelas informações passadas. Para um processo FIGARCH a variância de $r_t \mid \mathcal{F}_{t-1}$ é dada por

$$\sigma_t^2 \;=\; \omega\,(1-\beta(B))^{-1} + \lambda(B) r_t^2,$$

onde

$$\lambda(B) = \sum_{k=0}^{\infty} \lambda_k B^k = 1 - (1-\beta(B))^{-1}\phi(B)(1-B)^D, \tag{3.50}$$

onde $\phi(B) = 1 - \alpha(B) - \beta(B))$, onde $\omega > 0$ é uma constante real, $\alpha(B) = \sum_{i=1}^{m} \alpha_i B^i$ e $\beta(B) = \sum_{j=1}^{s} \beta_j B^j$. A expansão binomial em B é dada por

$$(1-B)^D \;=\; 1 + \sum_{k=1}^{\infty} \frac{\Gamma(k-D)}{\Gamma(k+1)\Gamma(-D)} B^k = 1 - D \sum_{k=1}^{\infty} \frac{\Gamma(k-D)}{\Gamma(k+1)\Gamma(1-D)} B^k.$$

Em um processo FIGARCH(m, D, s) os parâmetros devem satisfazer restrições bem difíceis para garantir que a variância seja sempre positiva. Por exemplo, para um FIGARCH$(1, D, 1)$, além da condição $\omega > 0$, tem que ter $\beta_1 - d \leq \pi_1 \leq \frac{2-d}{3}$; e $d(\pi_1 - \frac{1-d}{2}) \leq \beta_1(d + \alpha_1)$, onde $\pi_1 = \alpha_1 + \beta_1$ (Wilkins, 2004). Vale comentar que o FIGARCH$(1, d, 1)$ equivale a um GARCH(1,1), quando $d = 0$ e a um IGARCH(1,1) quando $d = 1$. De acordo com os resultados de Nelson (1990) e Bougerol e Picard (1992), o modelo FIGARCH (1, d, 0) é estritamente estacionário para $0 < \mathrm{d} < 1$.

Autores têm apontado fraquezas do modelo FIGARCH. Por exemplo, Davidson, J. (2004) provou que a persistência nos choques na volatilidade de um processo FIGARCH diminui quando o parâmetro de memória longa aumenta. Ruiz e Pérez (2003) mostraram que o modelo proposto por Hwang (2001) tem problemas de identificabilidade. A estimação do modelo para ordens maiores também apresenta problemas de convergência. Há várias propostas de variações de modelos. Por exemplo, Hwang (2001) propôs estender o modelo de memória longa FIGARCH de Baillie *et al.* (1996) para também representar o efeito *leverage*. O modelo FIEGARCH (processos EGARCH com memória longa, que

considera o log da volatilidade) é computacionalmente mais estável e produz melhores estimativas.

Os modelos EGARCH (m, s) e GARCH-M (m, s) (GARCH-in-Mean) são bastante utilizados e muito interessantes mas como não foram apropriados para as séries de retornos analisadas (veja Capítulo 4) não são revistas aqui. Como distribuições condicionais iremos utilizar a t-student, Normal (por conta do Euro) e t-student assimétrica.

A Tabela 3.1 servirá de base para o próximo capítulo quando iremos ajustar os modelos condicionais. A função dela é guiar o leitor no que concerne ao modelo que está sendo discutido.

Tabela 3.1: *Significado das nomenclaturas a serem utilizadas para os modelos condicionais no Capítulo 4.*

Notação	Especificação do modelo
M1	ARFIMA(p, d, q)-GARCH (m, s) sem *leverage*, distribuição t
M2	ARFIMA(p, d, q)-GARCH (m, s) sem *leverage*, distribuição t-assimétrica
M3	ARFIMA(p, d, q)-GARCH (m, s) sem *leverage*, distribuição Normal
M4	ARFIMA(p, d, q)-GARCH (m, s) com *leverage*, distribuição t
M5	ARFIMA(p, d, q)-GARCH (m, s) com *leverage*, distribuição t-assimétrica
M6	ARFIMA(p, d, q)-GARCH (m, s) com *leverage*, distribuição Normal
M7	ARFIMA(p, d, q)-FIGARCH (m, s), distribuição t
M8	ARFIMA(p, d, q)-FIGARCH (m, s), distribuição t-assimétrica
M9	ARFIMA(p, d, q)-FIGARCH (m, s), distribuição Normal

Vale lembrar que a t-assimétrica usada pelo R no ajuste dos modelos GARCH é pelo método de *Skewed Distributions by Inverse Scale Factors* (veja seção 2.3.4 do pacote rugarch) onde δ é o parâmetro de assimetria e ν representa o número de graus de liberdade.

É importante salientar que o modelo GPD foi ajustado às caudas dos resíduos padronizados obtidos do ajuste do modelo condicional.

Capítulo 4

Análises Empíricas

Serão analisadas as séries de preços (e retornos) diários das criptomoedas Bitcoin, Ethereum, Ripple, Litecoin e Stellar, além da série do Euro. Os dados utilizados são da base de dados BNC2 da Quandl. É calculado um índice global de preços para cada criptomoeda a cada 5 minutos. Isso é baseado em dados agregados de todas as trocas negociadas em cada criptomoeda por qualquer outra forma de moeda. Para cada mercado de moeda, uma média ponderada do volume é obtida a partir do preço mais recente informado de cada troca. Para derivar o índice, cada valor é convertido para dólares norte-americanos usando as taxas de conversão *fiat* internacionais e uma média ponderada do volume geral calculada com base no volume total de cada mercado. Para o Euro, os dados foram retirados do Banco Central Europeu (BCE) através da base Quandl. A data de começo das séries é 8 de agosto de 2015 e o término da análise é 9 de dezembro de 2018. Isso representa para as criptomoedas 1219 observações, ao passo que para o Euro são 855 observações. A data de começo foi escolhida pelo fato do Ethereum constar na base a partir desta data. As criptomoedas foram escolhidas de acordo com a posição na capitalização de mercado no ranking do site *CoinMarketCap* em 9 de dezembro de 2018. Vale notar que Bitcoin Cash e EOS foram omitidas da análise pois só começaram a ser negociadas em 2017. As cinco criptomoedas escolhidas correspondem, na época do começo da análise, a uma capitalização de mercado de 78% aproximadamente do mercado total de criptomoedas.

Todas as análises estatísticas foram realizadas com o auxílio do *software* R.

4.1 Fatos Estilizados

Aplicando a metodologia dada no Capítulo 3, iremos agora verificar se há para as séries a presença dos 12 fatos estilizados usualmente verificados para ações e índices. O primeiro fato estilizado analisado, que diz que as séries de retornos são estacionárias, foi confirmado. O teste KPSS aceitou a hipótese nula para Ethereum, Stellar e Euro ao n.s. de 5%, e para as restantes ao n.s. de 1%. Já para os preços o teste recusou a hipótese nula para a 1%. A Figura 4.1 ilustra o comportamento das séries temporais de preços e retornos para as seis séries analisadas.

O segundo fato estilizado a ser verificado é se as séries de retornos apresentam média próxima de zero. A Tabela 4.1 fornece várias estatísticas básicas das séries de retornos.

A tabela fornece o Limite Inferior (LCL) e o Limite Superior (UCL) do intervalo de confiança de 95% para a verdadeira média dos retornos. Para o Ethereum, como não há

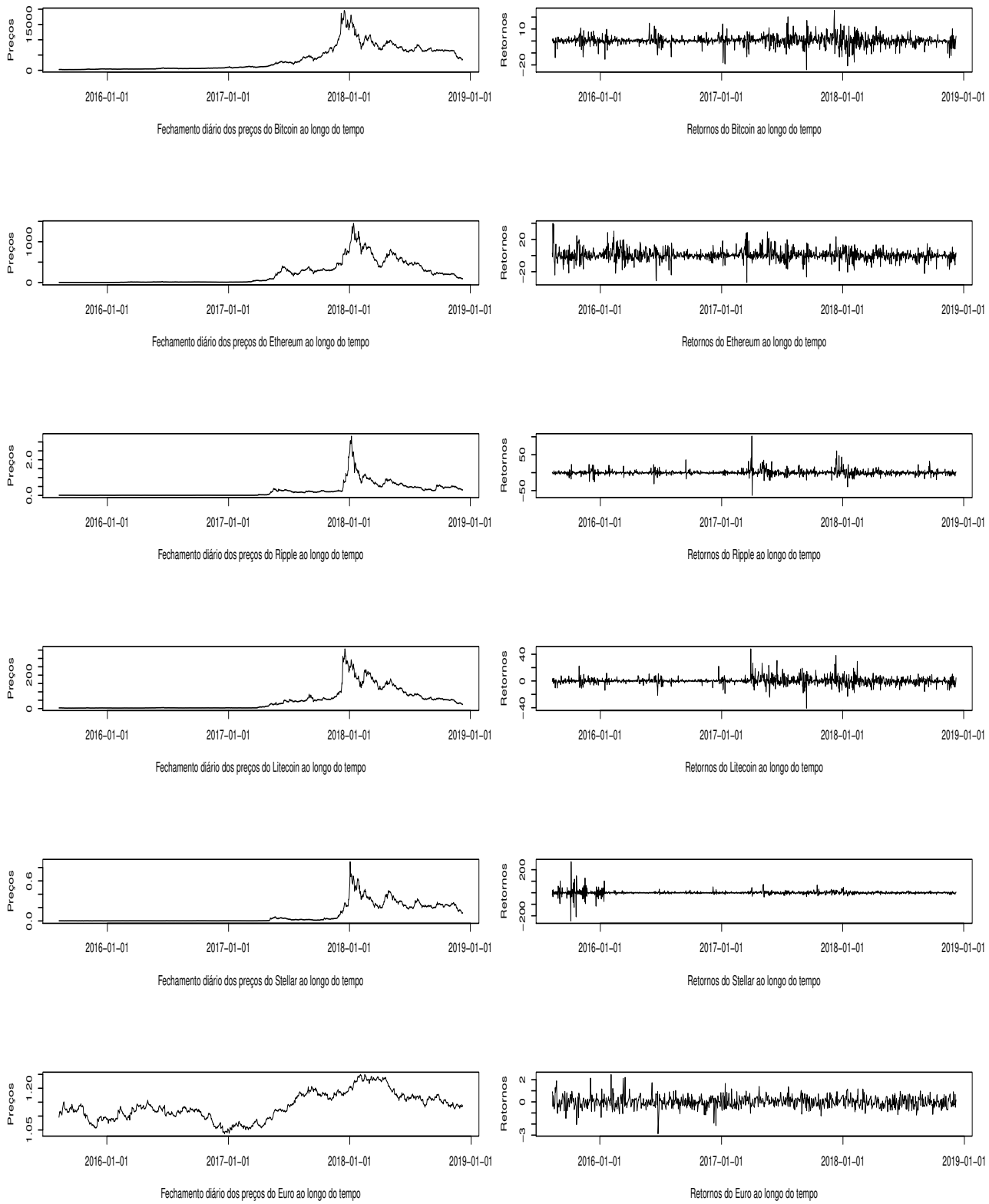

Figura 4.1: Séries temporais dos preços e retornos das séries analisadas

Tabela 4.1: *: Estatísticas básicas para as séries de retornos.*

	Bitcoin	Ethereum	Ripple	Litecoin	Stellar	Euro
Mediana	0.262	-0.086	-0.335	-0.056	-0.365	-0.009
Média amostral	0.216	0.403*	0.294	0.154	0.324	0.004
LCL	-0.016	0.015	-0.156	-0.166	-0.798	-0.031
UCL	0.448	0.790	0.745	0.475	1.447	0.039
DP	4.129	6.900	8.018	5.711	19.973	0.521
$\widehat{A}$	-0.293**	0.433**	2.456**	1.079**	0.028	0.093
$\widehat{C^*}$	5.626**	4.501**	31.052**	12.390**	63.558**	2.934**
Máximo	25.494	39.946	101.976	47.968	269.140	2.466
2º maior valor	20.209	38.644	60.570	38.207	146.345	2.208
3º maior valor	18.114	30.171	47.423	36.975	127.368	2.142
Mínimo	-23.974	-33.353	-63.158	-40.603	-244.649	-2.877
2º menor valor	-20.729	-31.150	-39.498	-24.237	-208.818	-2.137
3º menor valor	-19.142	-28.892	-31.201	-22.949	-126.096	-2.045

Convenções utilizadas na tabela: DP: desvio padrão amostral; $\widehat{A}$: coeficiente de assimetria amostral; $\widehat{C^*}$: excesso de curtose amostral (valor que excede 3). * e ** significam, respectivamente, rejeição de H_0 a 5% e 1%.

a inclusão do valor zero no intervalo, pode-se concluir que $\mu > 0$. Para as outras séries, o fato estilizado é verificado. Entretanto, para o Ethereum, o teste t aceita hipótese nula de $\mu = 0$ para o n.s. de 1% (p-valor = 0,0419).

O terceiro fato estilizado a ser verificado é se as séries de retornos apresentam distribuição (não condicional) simétrica. Para a Stellar e o Euro o teste de assimetria aceitou com p-valor de 0,6919 e 0,2676 respectivamente. Para as outras séries a hipótese nula foi rejeitada com p-valores menores que 0,000029.

O quarto fato estilizado afirma que as séries de retornos diários apresentam distribuição (não condicional) não Normal. O teste Jarque-Bera rejeita fortemente a hipótese nula, com todos os p-valores menores que 0,00000000000000022.

O quinto fato estilizado a ser verificado é se as séries de retornos apresentam excesso de curtose positivo (caudas pesadas). Para todas as séries estudadas o p-valor encontrado para o teste explicado no Capítulo 3 foi zero, recusando a hipótese nula.

O sexto fato estilizado é se as séries de retornos apresentam caudas com pesos diferentes. Para todas as séries analisadas, as estimativas pontuais de ξ (parâmetro de forma da distribuição de Pareto, veja Capítulo 3) para as caudas direita e esquerda são bem diferentes, o que indicaria caudas com pesos diferentes. Entretanto os erros padrões dessas estimativas são grandes, o que faz com que haja interseção entre os 95% intervalos de confiança construídos para ξ das caudas esquerda e direita, conforme mostra a Tabela 4.2.

O sétimo fato estilizado afirma que as séries de retornos financeiros apresentam alguns pontos bem mais extremos que a maioria. Ao se observar o lado direito da Figura 4.1 que traz as séries de retornos para as seis séries analisadas, podemos verificar visualmente que há alguns pontos bem mais extremos que outros. Além disso, para ilustrar, para cada série de retornos tomamos os três maiores valores absolutos e calculamos quantos desvios-padrão cada valor extremo representava. A Tabela 4.3 fornece esses valores. Observamos que, por exemplo, um extremo igual a 4,834 vezes o desvio-padrão amostral (menor valor do Ethereum) corresponde a um quantil de probabilidade acumulada de 99,99991% em uma distribuição Normal, indicando que há pontos bem mais extremos que a grande maioria dos retornos.

Tabela 4.2: *: Estimativa (erro padrão) e 95% intervalo de confiança para o parâmetro de forma ξ para as criptomoedas. Última coluna indica se há superposição dos intervalos de confiança para as caudas esquerda e direita.*

Criptomoedas	Cauda direita		Cauda esquerda		Superposição
	$\widehat{\xi}$ (e.p.)	95% I.C.	$\widehat{\xi}$ (e.p.)	95% I.C.	dos intervalos
Bitcoin	0.217 (0.102)	[0.018 , 0.417]	0.026 (0.081)	[-0.132 , 0.184]	✓
Ethereum	0.004 (0.082)	[-0.156 , 0.164]	0.035 (0.088)	[-0.137 , 0.207]	✓
Ripple	0.400 (0.122)	[0.161 , 0.639]	0.254 (0.105)	[0.048 , 0.459]	✓
Litecoin	0.280 (0.118)	[0.048 , 0.512]	0.124 (0.096)	[-0.065 , 0.313]	✓
Stellar	0.610 (0.118)	[0.379 , 0.840]	0.636 (0.121)	[0.400 , 0.873]	✓
Euro	0.171 (0.123)	[-0.071 , 0.412]	0.215 (0.120)	[-0.020 , 0.451]	✓

Tabela 4.3: *: Maiores valores absolutos expressos em termos dos desvios-padrão das séries de retornos*

	Bitcoin	Ethereum	Ripple	Litecoin	Stellar	Euro
DP	4.129	6.900	8.018	5.711	19.973	0.521
Maior valor absoluto (#DP)	25.494 (6.174)	39.496 (5.789)	101.976 (12.718)	47.968 (8.399)	269.140 (13.475)	2.877 (5.526)
Segundo maior valor absoluto (#DP)	23.974 (5.806)	38.644 (5.601)	63.158 (7.877)	40.603 (7.110)	244.649 (12.249)	2.466 (4.737)
Terceiro maior valor absoluto (#DP)	20.729 (5.020)	33.353 (4.834)	60.570 (7.554)	38.207 (6.690)	208.818 (10.455)	2.208 (4.241)

O oitavo fato estilizado a ser verificado é se as séries apresentam clusters de volatilidade (heteroscedasticidade condicional). Ao se observar o lado direito da figura 4.1, podemos verificar visualmente que há conglomerados de baixa e alta volatilidade nas séries de retornos. Este fato estilizado é confirmado na seção 4.4 através de ajuste dos modelos GARCH. Esses ajustes GARCH também comprovam o nono fato estilizado que afirma que as séries de retornos apresentam alguma forma de não-linearidade.

O décimo fato estilizado diz que os retornos em geral não apresentam autocorrelação significativa na média, mas quando ela existe é pequena e apenas para os primeiros *lags*. O décimo primeiro afirma que as séries apresentam autocorrelação nos retornos ao quadrado significativa para vários *lags*. São todas positivas e podem decair lentamente. A inspeção visual da f.a.c. amostral e o teste de Ljung-Box utilizados para essas verificações comprovam os fatos, embora a f.a.c. dos quadrados dos retornos não seja tão marcante como no caso de índices e ações. Em todos os casos, foram observadas autocorrelações significativas nos quadrados dos retornos. Para o Euro, ao n.s. de 1% não é significativo, porém para um n.s. de 5% é significativo. A Figura 4.2 apresenta a f.a.c. amostral sem o *lag* zero para os retornos (esquerda) e para os retornos ao quadrado (direita) para a Ripple.

Por exemplo, a Figura 4.2 ilustra a f.a.c. amostral para os retornos (à esquerda), e para os quadrados dos retornos (à direita) no caso da Ripple. O teste de Ljung-Box neste caso rejeitou a hipótese nula com p-valor igual a 0 e m = 5 para os retornos e também rejeitou no caso dos quadrados dos retornos com p-valor igual a 0. Para a Stellar ocorreu o mesmo que para o Ripple, rejeitando a hipótese nula tanto para os retornos quanto para os retornos ao quadrado. Para o Euro, a hipótese nula para os retornos foi aceita, porém para os retornos dos quadrados obtivemos um p-valor de 0.033, ou seja, aceitando para

um n.s. de 1% porém rejeitando para um n.s. de 5%. Para as outras séries, a hipótese nula foi aceita para os retornos mas rejeitada para os retornos ao quadrado, conforme o esperado.

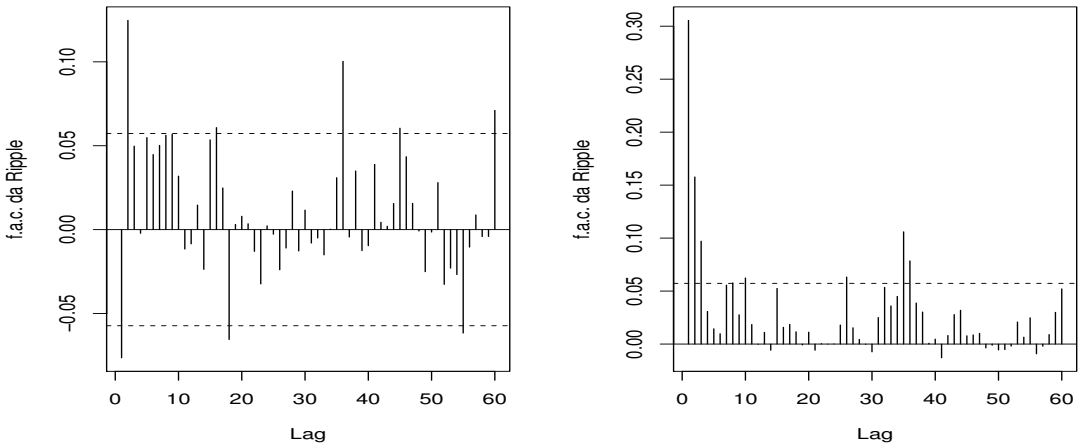

Figura 4.2: f.a.c. amostral das séries de retornos e retornos ao quadrado do Ripple

O décimo segundo fato estilizado afirma que as séries de retornos apresentam memória longa na média e na volatilidade (decaimento lento da f.a.c. amostral). Ao ajustarmos os modelos condicionais ARFIMA e FIGARCH (Capítulo 4), foi verificado que Bitcoin, Ethereum, Litecoin e Euro possuem memória longa na volatilidade e na média. Já para Ripple e Stellar, verificou-se que há memória longa na volatilidade, mas não na média.

A Tabela 4.4 resume os achados para os doze fatos estilizados.

Tabela 4.4: *Resumo dos doze fatos estilizados para as séries de retornos das criptomoedas e do Euro. O símbolo ✓representa a verificação do fato e ✗a não verificação. F representa a distribuição não condicional dos retornos.*

	Criptomoedas					
Fatos estilizados	Bitcoin	Ethereum	Ripple	Litecoin	Stellar	Euro
1. Séries são estacionárias.	✓	✓	✓	✓	✓	✓
2. Média amostral próxima de zero	✓	✗	✓	✓	✓	✓
3. F aproximadamente simétrica	✗	✗	✗	✗	✓	✓
4. F não é a distribuição Normal	✓	✓	✓	✓	✓	✓
5. Excesso de curtose positivo	✓	✓	✓	✓	✓	✓
6. Caudas com pesos diferentes	✗	✗	✗	✗	✗	✗
7. Apresentam pontos extremos	✓	✓	✓	✓	✓	✓
8. Apresentam *clusters* de volatilidade	✓	✓	✓	✓	✓	✓
9. Apresentam alguma forma de não-linearidade	✓	✓	✓	✓	✓	✓
10. Retornos não autocorrelacionados	✓	✓	✗	✓	✗	✓
11. Retornos ao quadrado são autocorrelacionados	✓	✓	✓	✓	✓	✓
12. Memória longa na média	✗	✓	✗	✗	✓	✗
13. Memória longa na volatilidade	✗	✗	✗	✗	✗	✗

O décimo segundo fato estilizado foi separado em dois: um sendo memória longa na média e o outro sendo memória longa na volatilidade. Os resultados apresentados são provenientes dos ajustes dos modelos condicionais.

Vale ressaltar também que a presença de clusters de volatilidade pode ser formalmente testada pelo teste ARCH. Neste teste, o p-valor encontrado foi zero para todas as

criptomoedas mas não para o Euro, que teve p-valor = 0.13.

4.2 Ajustes não condicionais

O primeiro passo no cálculo do risco não condicional é o ajuste da melhor distribuição para cada série de retornos.

Para identificar o melhor ajuste para cada moeda foram escolhidas, além da distribuição Normal, as distribuições t-student e a t-ZG. Outras especificações para a t-assimétrica foram também testadas. A distribuição t-ZG foi escolhida devido à sua potencialidade de fornecer um bom ajuste já que possui cinco parâmetros. A Figura 4.3 evidencia o ajuste ruim da distribuição Normal para as séries de retornos do Bitcoin e Ethereum, onde a linha vermelha é a curva Normal superposta ao respectivo histograma. Na Figura 4.4 podemos observar o ajuste da distribuição t-Student e o Q-Q plot deste ajuste para os retornos do Bitcoin e Ethereum.

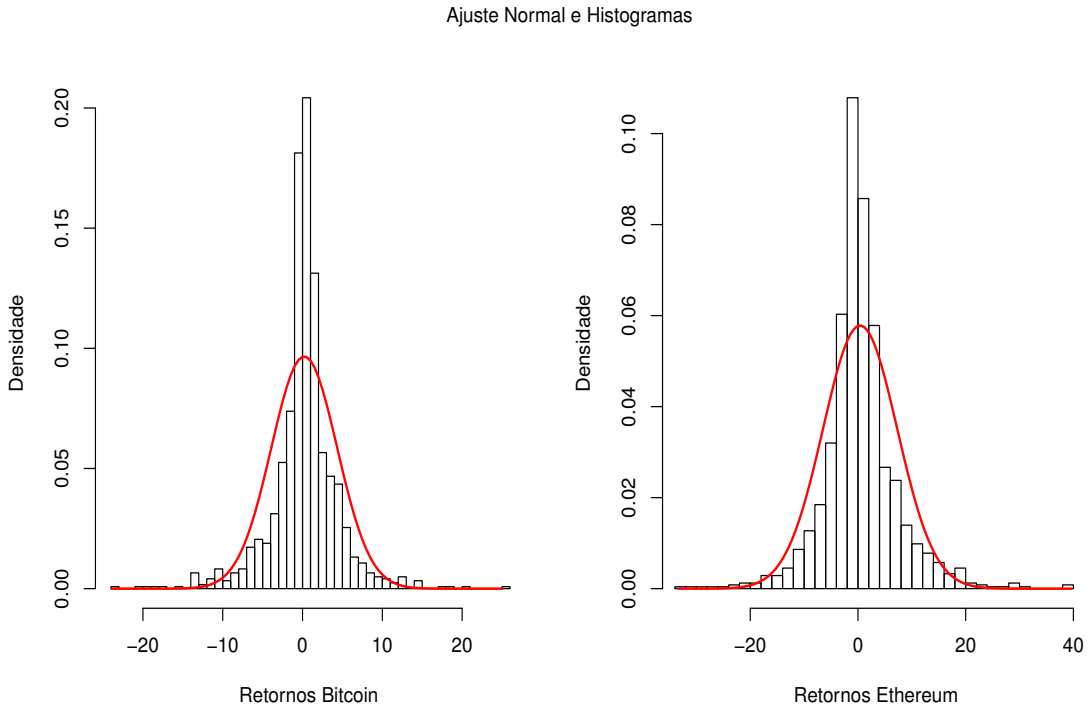

Figura 4.3: Histograma dos retornos do Bitcoin e Ethereum e o ajuste da curva Normal.

Para testar a qualidade dos ajustes foi aplicado o teste de Kolmogorov-Smirnov (teste GOF). A Tabela 4.5 resume o resultado dos testes para a identificação da distribuição subjacente dos retornos.

Como esperado, a distribuição Normal não fornece um bom ajuste, com exceção do Euro. Assim como para a distribuição t-assimétrica, a distribuição t-simétrica foi também rejeitada pelo teste GOF para todas as moedas. A única exceção foi o Euro na distribuição t-simétrica, que o teste GOF aceita a 1% (p-valor $= 0.0212$). Investigando um pouco melhor vimos que essa falta de ajuste ocorria exatamente para a parte central da distribuição (veja Figura 4.5 para o caso do Ethereum e Litecoin).

Nesta procura pelo melhor modelo não condicional para os retornos das séries, uma outra opção é focar apenas nas caudas, já que é nesta região que se calculam as medidas de

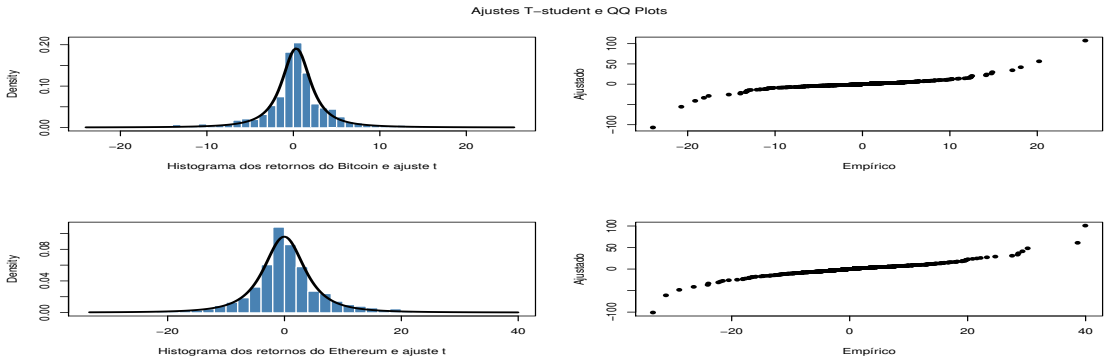

Figura 4.4: Distribuição t-Student ajustada aos retornos para Bitcoin e Ethereum e os Q-Q plots correspondentes.

Tabela 4.5: *Resultado do teste GOF para os ajustes não condicionais.*

Distribuição	Bitcoin	Ethereum	Ripple	Litecoin	Stellar	Euro
t-assimétrica de Zhu & Galbraith	✗	✗	✗	✗	✗	✗
t-Student simétrica	✗	✗	✗	✗	✗	✓
Normal	✗	✗	✗	✗	✗	✓
GPD (Limiar direito)	✓	✓	✓	✓	✓	✓
GPD (Limiar esquerdo)	✓	✓	✓	✓	✓	✓

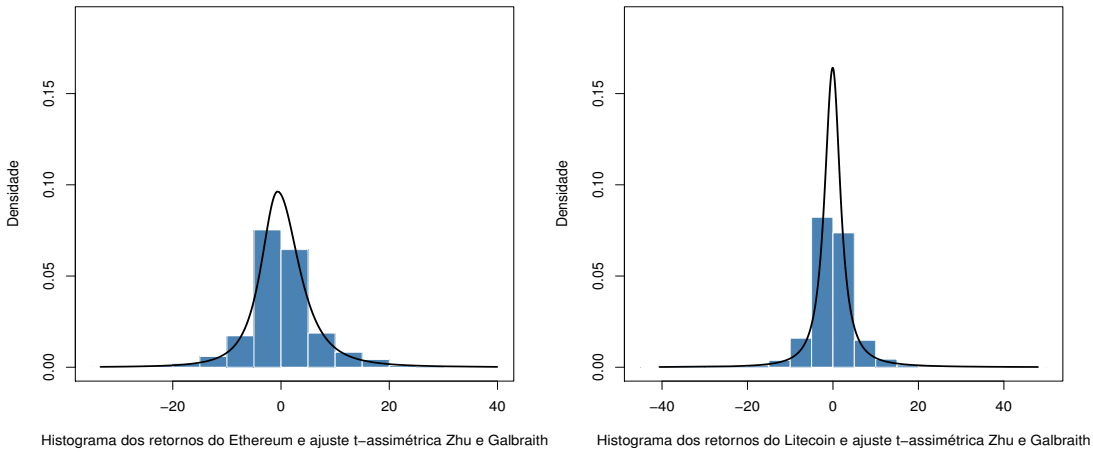

Figura 4.5: Histograma dos retornos de Ethereum e Litecoin e o ajuste da curva t-ZG.

risco. Conforme explicamos no capítulo 3, para acessar a forma das caudas da distribuição dos retornos das criptomoedas iremos ajustar o modelo GPD nos excessos além de um limiar alto. As estimativas dos parâmetros da GPD para as séries de retornos analisadas

estão na Tabela 4.6. Todas as estimativas do parâmetro de forma ξ são positivas indicando caudas pesadas (Pareto). Os limiares foram escolhidos como aqueles resultando no melhor ajuste possível, ajuste confirmado pelo teste GOF.

Tabela 4.6: *: Estimativas dos parâmetros (u, ψ, ξ) da GPD para séries de retornos das criptomoedas. A tabela também fornece o percentual (%) de observações na cauda definindo o limiar u.*

Criptomoedas	Bitcoin	Ethereum	Ripple	Litecoin	Stellar	Euro
u cauda direita (%)	3.709 (14%)	6.709 (13%)	4.950 (14%)	5.666 (10%)	6.651 (17%)	0.638 (10%)
ψ cauda direita	2.214	5.837	4.995	4.027	6.698	0.261
ξ cauda direita	0.217	0.004	0.400	0.280	0.610	0.171
u cauda esquerda (%)	2.200 (17%)	5.175 (13%)	5.110 (13%)	4.960 (11%)	6.888 (15%)	0.5845 (11%)
ψ cauda esquerda	3.598	4.908	3.776	3.640	5.760	0.221
ξ cauda esquerda	0.026	0.035	0.254	0.124	0.636	0.215

4.3 Medidas de risco não condicionais

4.3.1 Medidas de risco *in-sample* (amostra completa)

Em primeiro lugar usaremos a amostra completa com 1219 observações para o cálculo do VaR e análise de sua performance. Para todas as criptomoedas foi calculado o VaR_α, $\alpha = 1\%$ e 5%, para as caudas esquerda e direita utilizando os procedimentos histórico, Normal, t-student, t-ZG e GPD (melhor ajuste nas caudas). O VaR Normal foi incluído apenas por ser um procedimento simples e popular. O VaR histórico pela sua facilidade de cálculo. Os valores obtidos estão na Tabela 4.7. Observamos que o VaR histórico e o baseado na modelagem GPD apresentam valores bem próximos para todos os α's de todas as séries. É interessante observar também que, em geral, o VaR t-student e o VaR t-ZG superestimam o risco pois, por exemplo, vemos que o VaR 1% e 5% estão além dos mínimos e máximos, porém na t-ZG essa superestimação é muito mais acentuada. O teste de aderência indicou que a t-simétrica ajusta bem a parte central dos dados e mal nas caudas. Ao contrário, t-ZG ajusta mal a parte central dos dados e melhor nas caudas. Por isto, a decisão de qual melhor estimativa do VaR a ser usada será dada pela verificação da performance do VaR. Qual das estimativas falha um número de vezes mais próximo do percentual de vezes (risco) que ela é esperada falhar? A resposta será dada pelo teste de Kupiec. Esta análise será feita *in-sample* e *out-of-sample*.

Para acessar a performance dos VaR's da Tabela 4.7 calculamos o número de violações *in-sample*, comparamos o número de violações esperadas e efetuamos o teste de Kupiec. O número de violações e o resultado do teste de Kupiec são dados na Tabela 4.8. Notamos que, utilizada toda a amostra, o teste de Kupiec não rejeita a hipótese nula para a GPD, rejeita onze vezes para a t-Student, todas as vezes (24 vezes) para a t-assimétrica e doze vezes para a Normal para todas as séries. Apesar do teste GOF ter rejeitado a distribuição Normal, o VaR_α Normal ainda foi aceito pelo teste de Kupiec em algumas situações para todas as séries. Importante notar que todas as rejeições sob normalidade para 1% e 99% foram devidas à subestimação do risco, já para 5% e 95% foi devido a superestimação. Já as rejeições do teste de Kupiec para a t-student sempre foram devidas à superestimação

Tabela 4.7: *: Estimativas do VaR_α através das abordagens histórica, Normal, t-student, t-assimétrica de Zhu e Galbraith e GPD utilizando toda a amostra.*

		α - cauda esquerda		α - cauda direita	
Criptomoedas	VaR	1%	5%	5%	1%
Bitcoin	Histórico	-13.06%	-6.66%	6.10%	12.31%
	Normal	-9.39%	-6.58%	7.01%	9.82%
	t-student	-12.02%	-7.56%	7.99%	12.46%
	t-assimétrica	-54.12%	-17.64%	16.96%	40.56%
	GPD	-12.78%	-6.67%	6.25%	11.59%
Ethereum	Histórico	-17.98%	-9.77%	12.69%	20.04%
	Normal	-15.65%	-10.95%	11.75%	16.45%
	t-student	-19.47%	-12.39%	13.19%	20.27%
	t-assimétrica	-55.61%	-24.31%	32.85%	72.37%
	GPD	-18.33%	-9.93%	12.28%	21.74%
Ripple	Histórico	-18.09%	-9.24%	11.49%	29.24%
	Normal	-18.36%	-12.89%	13.48%	18.95%
	t-student	-24.16%	-15.04%	15.62%	24.74%
	t-assimétrica	-63.45%	-24.60%	32.24%	103.77%
	GPD	-18.74%	-9.18%	11.29%	28.29%
Litecoin	Histórico	-13.98%	-8.13%	8.48%	19.05%
	Normal	-13.13%	-9.24%	9.55%	13.44%
	t-student	-17.11%	-10.71%	11.02%	17.42%
	t-assimétrica	-60.80%	-21.50%	24.31%	80.43%
	GPD	-15.08%	-7.94%	8.71%	18.63%
Stellar	Histórico	-51.42%	-15.41%	19.51%	59.83%
	Normal	-46.14%	-32.53%	33.18%	46.79%
	t-student	-62.80%	-38.61%	39.25%	63.45%
	t-assimétrica	-152.36%	-45.71%	57.41%	193.90%
	GPD	-48.41%	-16.00%	18.82%	57.42%
Euro	Histórico	-1.18%	-0.78%	0.84%	1.31%
	Normal	-1.21%	-0.85%	0.86%	1.22%
	t-student	-1.38%	-0.92%	0.93%	1.39%
	t-assimétrica	-3.28%	-2.00%	2.29%	3.70%
	GPD	-1.27%	-0.77%	0.83%	1.37%

do VaR para as devidas rejeições. Para a *t*-assimétrica, que rejeitou para todos os VaR's, isso foi devido à superestimação do risco.

A partir dos cálculos realizados tanto do VaR como da PE para toda a amostra para as distribuições (histórica, Normal, *t*-Student, *t*-ZG e GPD) foi possível calcular, para ambas as caudas e a partir dos melhores ajustes, o impacto financeiro (em USD) causado para o risco de 1% em T+1, onde T é o último dia da série. Vamos supor por simplicidade que o preço da criptomoeda neste dia, P_t, equivalha a 100 USD. No dia seguinte, qual poderia ser a variação de preço ao risco de 1% para o caso da GPD, por exemplo? Sendo hoje o retorno dado por r_T este valor em risco de 1% seria o $\text{VaR}_{1\%}$ (cauda esquerda ou direita).

Na cauda direita:

$$\log \text{P}_{T+1} = 4.605 + 0.11586$$
$$\log \text{P}_{T+1} = 4.7210$$
$$\text{P}_{T+1} = 112.28 USD$$

Na cauda esquerda:

Tabela 4.8: *: Número de violações na amostra completa (in-sample).*

Número de violações do VaR na amostra completa														
α	Esperado Criptomoedas	Esperado Euro	Bitcoin				Ethereum				Ripple			
			N	t	t-ZG	GPD	N	t	t-ZG	GPD	N	t	t-ZG	GPD
1% (esquerda)	12.19	8.55	33	16	0	14	22	10	0	11	12	5	0	12
5% (esquerda)	60.95	42.75	65	47	4	60	53	36	4	59	34	22	5	64
5%(direita)	60.95	42.75	49	36	4	58	68	54	2	63	47	41	8	65
1%(direita)	12.19	8.55	23	9	0	16	30	12	0	10	30	16	0	14
α	Esperado Criptomoedas	Esperado Euro	Litecoin				Stellar				Euro			
			N	t	t-ZG	GPD	N	t	t-ZG	GPD	N	t	t-ZG	GPD
1% (esquerda)	12.19	8.55	21	8	0	12	16	9	2	15	8	7	0	7
5% (esquerda)	60.95	42.75	43	29	3	66	25	17	16	57	28	20	3	45
5%(direita)	60.95	42.75	50	36	8	61	29	28	14	63	37	28	1	44
1%(direita)	12.19	8.55	25	17	0	14	19	10	1	14	10	8	0	8

Teste de Kupiec												
α	Bitcoin				Ethereum				Ripple			
	N	t	t-ZG	GPD	N	t	t-ZG	GPD	N	t	t-ZG	GPD
1% (esquerda)	✗	✓	✗	✓	✗	✓	✗	✓	✓	✗	✗	✓
5% (esquerda)	✓	✓	✗	✓	✓	✗	✗	✓	✗	✗	✗	✓
5% (direita)	✓	✗	✗	✓	✓	✓	✗	✓	✓	✗	✗	✓
1% (direita)	✗	✓	✗	✓	✗	✓	✗	✓	✗	✓	✗	✓
α	Litecoin				Stellar				Euro			
	N	t	t-ZG	GPD	N	t	t-ZG	GPD	N	t	t-ZG	GPD
1% (esquerda)	✗	✓	✗	✓	✓	✓	✗	✓	✓	✓	✗	✓
5% (esquerda)	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✓
5% (direita)	✓	✗	✗	✓	✗	✗	✗	✓	✓	✗	✗	✓
1% (direita)	✗	✓	✗	✓	✓	✓	✗	✓	✓	✓	✗	✓

Notação na tabela: N representa a distribuição Normal, t a t-simétrica, t-ZG a t-assimétrica de Zhu e Galbraith, ✓significa que H_0 foi aceita e ✗significa que H_0 foi rejeitada

$$\log \mathrm{P}_{T+1} = 4.605 - 0.12779$$

$$\log \mathrm{P}_{T+1} = 4.47737$$

$$\mathrm{P}_{T+1} = 88.002 USD$$

Tabela 4.9 nos mostra as melhores estimativas das medidas de risco para cada uma das criptomoedas e a Tabela 4.10 os preços em T+1 baseados nos melhores ajustes para o VaR, baseados na GPD.

Tabela 4.9: *Melhores estimativas (GPD) do VaR e PE.*

	VaR				PE			
	α - cauda esquerda		α - cauda direita		α - cauda esquerda		α - cauda direita	
Criptomoedas	1%	5%	5%	1%	1%	5%	5%	1%
Bitcoin	-12.78%	-6.67%	6.25%	11.59%	-15.85%	-10.63%	9.99%	14.80%
Ethereum	-18.33%	-9.93%	12.28%	21.74%	-24.82%	-15.30%	18.00%	29.28%
Ripple	-18.74%	-9.18%	11.29%	28.29%	-27.33%	-15.37%	22.19%	42.00%
Litecoin	-15.08%	-7.94%	8.71%	18.63%	-20.70%	-12.14%	15.31%	27.75%
Stellar	-48.41%	-16.00%	18.82%	57.42%	-95.35%	-43.35%	45.72%	100.03%
Euro	-1.27%	-0.77%	0.83%	1.37%	-1.90%	-1.08%	1.16%	1.95%

Logo, para o Bitcoin, por exemplo, existe um risco de 1% para que o preço amanhã 12,28% maior que o de hoje.

Tabela 4.10: *Previsões um passo a frente dos preços baseados no VaR vencedor (GPD) ao risco de 1%.*

Criptomoedas	Valor em Risco de 1% (na cauda esquerda) em $t+1$ expresso em termos do preço (em USD)	Preço hoje (t) (em USD)	Valor em Risco de 1% (na cauda direita) em $t+1$ expresso em termos do preço (em USD)
Bitcoin	88.00	100.00	112.28
Ethereum	83.25	100.00	124.29
Ripple	82.91	100.00	132.70
Litecoin	86.00	100.00	120.48
Stellar	61.62	100.00	177.56
Euro	98.74	100.00	101.38

4.3.2 Medidas de risco *out-of-sample* (fora da amostra)

Em segundo lugar, para testar a performance das medidas fora da amostra aplicamos um procedimento de janelas móveis (*rolling windows*). O tamanho da janela de estimação foi fixado em dois anos (730 observações) para as criptomoedas e aproximadamente um ano e meio para o Euro (530 observações). Para cada janela os modelos não condicionais (Normal, t-student, t-ZG e GPD) foram estimados e uma estimativa do VaR_α obtida para o dia seguinte. Em seguida uma nova observação era incorporada à amostra de estimação e a observação mais antiga eliminada da mesma. O processo resultou em 489 estimativas fora da amostra para as criptomoedas e 325 estimativas fora da amostra para o Euro.

Para acessar a performance das previsões fora da amostra foi novamente aplicado o teste de Kupiec. O número de violações na amostra de verificação o resultado do teste de Kupiec estão na Tabela 4.11. Notamos que o teste de Kupiec rejeita a hipótese nula sete vezes para a GPD, doze vezes para a t-student, todas as vezes (24 vezes) para a t-assimétrica e treze vezes para a Normal para todas as criptomoedas e o Euro *out-of-sample*. A GPD foi rejeitada pelo teste de Kupiec para o Bitcoin e Litecoin para $\alpha = 5\%$ enquanto que para essa mesmas criptomoedas a t-student foi aceita para todos os α's, performando melhor. Para o Ethereum, GPD e t-student aceitam para os mesmos α's (1% e 5%). Para a Ripple, enquanto a GPD aceita para todos os α's, a t-student só aceita para $\alpha = 99\%$. Para a Stellar, enquanto a GPD rejeita apenas para $\alpha = 1\%$, a t-student só aceita para $\alpha = 99\%$. Por fim, para o Euro a GPD aceita para $\alpha = 1\%$ e $\alpha = 5\%$ enquanto que a t-student rejeita para todos os α's. A Figura 4.6 ilustra a performance do VaR *out-of-sample* para o caso do Ripple.

A Tabela 4.12 resume todas as informações sobre os ajustes não condicionais. Foram estabelecidos critérios para definirmos qual a melhor distribuição para cada série. Onde a distribuição performou bem, foi contabilizado um ponto para a mesma. Vale notar que, para o aceite do teste GOF há GPD para ambas as caudas a serem consideradas. Só foi considerado um ponto para a GPD caso a performance de ambas as caudas fosse boa. Onde consta "Histórico"na tabela significa que não houve uma boa performance de nenhum ajuste naquele critério analisado, sendo sugerido assim observar a distribuição histórica. Pode-se observar que a GPD, de uma forma geral, possui a melhor performance para todas as séries dentre as distribuições não-condicionais utilizadas.

Aceite teste GOF para ajuste de uma distribuição e melhor performance *in-sample* de modelo não-condicional servem para investimentos a longo prazo, por exemplo, 3, 5, 10 anos. Melhor performance VaR *out-of-sample* de modelo não-condicional para investi-

Tabela 4.11: *: Número de violações fora da amostra (out-of-sample).*

Número de violações do VaR fora da amostra														
α	Esperado Criptomoedas	Esperado Euro	Bitcoin				Ethereum				Ripple			
			N	t	t-ZG	GPD	N	t	t-ZG	GPD	N	t	t-ZG	GPD
1% (esquerda)	4.89	3.25	19	7	0	7	8	3	0	4	3	1	0	3
5% (esquerda)	24.45	16.25	36	29	3	39	25	18	1	31	15	7	2	32
5%(direita)	24.45	16.25	27	19	3	34	1	8	0	8	18	13	4	22
1%(direita)	4.89	3.25	12	6	0	6	1	1	0	1	12	5	0	4
α	Esperado Criptomoedas	Esperado Euro	Litecoin				Stellar				Euro			
			N	t	t-ZG	GPD	N	t	t-ZG	GPD	N	t	t-ZG	GPD
1% (esquerda)	4.89	3.25	9	3	0	6	1	1	0	1	4	0	0	1
5% (esquerda)	24.45	16.25	23	17	3	37	8	3	0	26	12	6	0	26
5%(direita)	24.45	16.25	25	17	3	25	10	6	1	21	9	8	0	9
1%(direita)	4.89	3.25	12	7	0	6	4	3	0	2	0	0	0	0

Teste de Kupiec												
α	Bitcoin				Ethereum				Ripple			
	N	t	t-ZG	GPD	N	t	t-ZG	GPD	N	t	t-ZG	GPD
1% (esquerda)	✗	✓	✗	✓	✓	✓	✗	✓	✓	✗	✗	✓
5% (esquerda)	✗	✓	✗	✗	✓	✓	✗	✓	✗	✗	✗	✓
5% (direita)	✓	✓	✗	✓	✗	✗	✗	✗	✓	✗	✗	✓
1% (direita)	✗	✓	✗	✓	✗	✗	✗	✗	✗	✓	✗	✓
α	Litecoin				Stellar				Euro			
	N	t	t-ZG	GPD	N	t	t-ZG	GPD	N	t	t-ZG	GPD
1% (esquerda)	✓	✓	✗	✓	✗	✗	✗	✗	✓	✗	✗	✓
5% (esquerda)	✓	✓	✗	✗	✗	✗	✗	✓	✓	✗	✗	✓
5% (direita)	✓	✓	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗
1% (direita)	✗	✓	✗	✓	✓	✓	✗	✓	✗	✗	✗	✗

Notação na tabela: N representa a distribuição Normal, t a t-simétrica, t-ZG a t-assimétrica de Zhu e Galbraith, ✓significa que H_0 foi aceita e ✗significa que H_0 foi rejeitada

Tabela 4.12: *: Melhores performances dos ajustes em cada série*

Critérios	Bitcoin	Ethereum	Ripple	Litecoin	Stellar	Euro
Distribuição NC aceita pelo teste GOF	GPDe GPDd	GPDe GPDd	GPDe GPDd	GPDe GPDd	GPDe GPDd	N, t, GPDe, GPDd
VaR NC *in-sample* 1%	t, GPD	t, GPD	N, GPD	t, GPD	N, t, GPD	N, t, GPD
VaR NC *in-sample* 5%	N, t, GPD	N, GPD	GPD	GPD	GPD	GPD
VaR NC *in-sample* 95%	N, GPD	N, t, GPD	N, GPD	N, GPD	GPD	N, GPD
VaR NC *in-sample* 99%	t, GPD	t, GPD	t, GPD	t, GPD	N, t, GPD	N, t, GPD
VaR NC *out-of-sample* 1%	t, GPD	N, t, GPD	N, GPD	N, t, GPD	Histórico	N, GPD
VaR NC *out-of-sample* 5%	t	N, t, GPD	GPD	N, t	GPD	N, GPD
VaR NC *out-of-sample* 95%	N, t, GPD	Histórico	N, GPD	N, t, GPD	GPD	Histórico
VaR NC *out-of-sample* 99%	t, GPD	Histórico	t, GPD	t, GPD	N, t, GPD	Histórico
Número de boas performances geral						
Normal	3	4	4	4	3	6
t-Student	7	5	2	6	3	3
t-assimétrica	0	0	0	0	0	0
GPD	8	7	9	8	8	7
Histórico	0	2	0	0	1	2

Notação na tabela: NC representa não-condicional, N a distribuição Normal, t a t-simétrica, t-ZG a t-assimétrica de Zhu e Galbraith, GPDe significa GPD ajuste cauda esquerda e GPDd significa GPD ajuste cauda direita

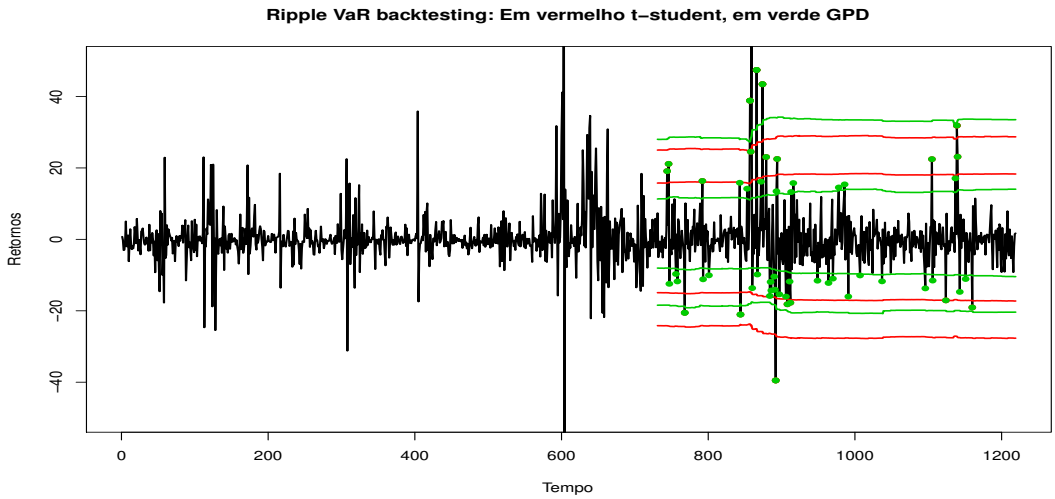

Figura 4.6: Performace do VaR *out-of-sample* para a t-simétrica e GPD para o Ripple

mentos de médio prazo (6 meses a 2 anos). Melhor performance *out-of-sample* de modelo condicional serve para investimentos com acompanhamento diário ou semanal (*"frequent trading"*). Veja Tabela 4.21 ao final da seção de ajustes condicionais. Por exemplo, negociando com o Ethereum, em um investimento de longo prazo, e tendo como medida de risco 5% (cauda esquerda) sugerimos utilizar o ajuste da GPD. Outro exemplo seria para investimentos de médio prazo com o Bitcoin, por exemplo, e tendo como medida de risco 5% (cauda esquerda) sugerimos utilizar o ajuste da t-simétrica.

4.4 Ajustes condicionais

Para a seleção do melhor modelo condicional para a média e para a volatilidade, iremos adotar a abordagem que especifica um modelo completo ARFIMA(p,d,q)-FIEGARCH(m,d,s) e após o seu ajuste vai simplificando o mesmo a partir da eliminação dos parâmetros (ou ordens) cujas estimativas forem não significativas. Quando necessário iremos aplicar o critério AIC para a escolha do melhor modelo. Mostraremos em detalhe todos os passos desta abordagem para o caso da criptomoeda Bitcoin. Para as outras daremos apenas a solução final.

O primeiro passo é verificar se existe memória longa na média, ajustando apenas um modelo ARFIMA(p,d,q). Isto é necessario porque a função do R utilizada não ajustava simultaneamente os modelos para a média e volatilidade com memória longa. Foram testadas todas as combinações das ordens p e q variando de 0 a 3.

Para o Bitcoin o melhor modelo para a média foi um ARFIMA(0,d,0) com $\widehat{d} = 0.0134$ não significativo ($p - valor = 0.5494$). De fato, o Bitcoin não apresenta memória longa na média. Para Ethereum, Ripple, Litecoin, Stellar e Euro os melhores modelos foram ARFIRMA (0,d,0), ARFIRMA (0,d,0), ARFIRMA (0,d,0), ARFIRMA (0,d,1) e ARFIRMA (0,d,0) com $\widehat{d}$ iguais a 0.0623, 0.0197, 0.0297, 0.1317 e -0.0369 respectivamente. Para Ethereum e Stellar as estimativas de $\widehat{d}$ foram significativas ($p - valor = 0.0056$ e $p - valor = 0.0000$ respectivamente), apresentando assim memória longa na média. Já para Ripple, Litecoin e Euro, as estimativas de $\widehat{d}$ não foram significativas ($p - valor = 0.3803$, $p - valor = 0.1858$ e $p - valor = 0.1688$), não apresentando memória longa na média.

A próxima etapa é ajustar um modelo com memória para a volatilidade. Para Bitcoin, Ripple, Litecoin e Euro utilizamos as séries originais. Já para Ethereum e Stellar utilizamos a série de resíduos do ajuste ARFIMA encontrada no passo anterior. Ajustamos então um modelo FIGARCH(m,d,s) para as criptomoedas. Conforme visto no Capítulo 3, em um processo FIGARCH(m, d, s) os parâmetros devem satisfazer restrições bem difíceis para garantir que a variância seja sempre positiva. Por exemplo, para um FIGARCH$(1, d, 1)$, além da condição $\omega > 0$, tem que ter $\beta_1 - d \leq \pi_1 \leq \frac{2-d}{3}$; e $d(\pi_1 - \frac{1-d}{2}) \leq \beta_1(d + \alpha_1)$, onde $\pi_1 = \alpha_1 + \beta_1$, além de $0 <$ d < 1. Foram ajustados os modelos FIGARCH(1,d,1) para o Bitcoin, FIGARCH(1,d,1) para o Ethereum, FIGARCH(1,d,1) para o Ripple, FIGARCH(1,d,1) para o Litecoin, FIGARCH(1,d,1) para a Stellar e FIGARCH(1,d,1) e FIGARCH(1,d,2) para o Euro. Para Euro FIGARCH(1,d,2) o $\widehat{d}$ não foi significativo ($p - valor = 0.1223$). Para os modelos restantes, a restrição $\beta_1 - d \leq \pi_1 \leq \frac{2-d}{3}$ não foi respeitada, π_1 foi sempre maior que $\frac{2-d}{3}$. Portanto não há memória longa na volatilidade para nenhuma série aqui estudada.

O próximo passo é ajustar o modelo sem memória longa na volatilidade. No caso do Bitcoin, o modelo completo ARFIMA(p,d,q)-FIGARCH(m,d,s) reduziu-se a um ARMA(0,d,0)-GARCH(1,1) com distribuição condicional t, modelo M1, na Tabela 3.1 do Capítulo 3. As estimativas de todos os parâmetros são estatisticamente significativas, e o teste de Ljung-Box aceita a hipótese nula para os resíduos (para um n.s. de 1%) e os quadrados dos resíduos. Na Tabela 4.13 damos as estimativas por máxima verossimilhança dos parâmetros desse modelo, seus erros padrões robustos e o $p - valor$ do teste t.

Para o Ethereum, o modelo completo ARFIMA(p,d,q)-FIGARCH(m,d,s) reduziu-se a um ARMA(0,d,0)-GARCH(1,1) com distribuição condicional t-simétrica, modelo

Tabela 4.13: *Estimativas dos parâmetros, erros padrões e p-valor do teste t para o Bitcoin, com parâmetro* $\nu = 3.5$.

ARMA(0,*d*,0)-GARCH(1,1): Modelo M1			
Parâmetros	Estimativa	Erro padrão robusto	p-valor do teste t
ω	0.1413	0.0874	0.1117
α_1	0.1602	0.0259	0.0000
β_1	0.8388	0.0279	0.0000

M1, onde o teste de Ljung-Box aceita a hipótese nula para os resíduos e os quadrados dos resíduos. Na Tabela 4.14 damos as estimativas por máxima verossimilhança dos parâmetros desses modelos, seus erros padrões robustos e o p-valor do teste t.

Tabela 4.14: *Estimativas dos parâmetros, erros padrões, estatística t e p-valor do teste t para o Ethereum, com parâmetro* $\nu = 3.8$.

ARMA(0,*d*,0)-GARCH(1,1): Modelo M1			
Parâmetros	Estimativa	Erro padrão robusto	p-valor do teste t
μ	-0.3423	0.1087	0.0016
ω	2.4726	0.9242	0.0075
α_1	0.2798	0.0473	0.0000
β_1	0.7192	0.0422	0.0000

Para o Ripple, o modelo completo ARFIMA(p,d,q)-FIGARCH(m,d,s) reduziu-se a um ARMA(0,d,0)-GARCH(1,1) com distribuição condicional t-simétrica, modelo M1, onde o teste de Ljung-Box aceita a hipótese nula para os resíduos e os quadrados dos resíduos. Na Tabela 4.15 damos as estimativas por máxima verossimilhança dos parâmetros desses modelos, seus erros padrões robustos e o p-valor do teste t.

Tabela 4.15: *Estimativas dos parâmetros, erros padrões e p-valor do teste t para o Ripple, com parâmetro* $\nu = 3.7$.

ARMA(0,*d*,0)-GARCH(1,1): Modelo M1			
Parâmetros	Estimativa	Erro padrão robusto	p-valor do teste t
μ	-0.3009	0.0781	0.0001
ω	2.4601	1.8986	0.1951
α_1	0.4227	0.164	0.0099
β_1	0.5763	0.1672	0.0006

Para o Litecoin, o modelo completo ARFIMA(p,d,q)-FIGARCH(m,d,s) reduziu-se a um ARMA(0,d,0)-GARCH(1,1) com distribuição condicional t-simétrica, modelo M1, onde o teste de Ljung-Box aceita a hipótese nula para os resíduos e os quadrados dos resíduos. Na Tabela 4.16 damos as estimativas por máxima verossimilhança dos parâmetros desses modelos, seus erros padrões robustos e o p-valor do teste t.

Para a Stellar, o nosso modelo completo ARFIMA(p,d,q)-FIGARCH(m,d,s) reduziu-se a um ARMA(0,d,0)-GARCH(1,1) com distribuição condicional t-simétrica, modelo M1, onde o teste de Ljung-Box não aceita a hipótese nula para os resíduos mas aceita para os

Tabela 4.16: *Estimativas dos parâmetros, erros padrões e p-valor do teste t para o Litecoin, com parâmetro* $\nu = 3.0$.

ARMA(0,*d*,0)-GARCH(1,1): Modelo M1			
Parâmetros	Estimativa	Erro padrão robusto	p-valor do teste t
ω	0.1148	0.0883	0.1935
α_1	0.1309	0.0267	0.0000
β_1	0.8681	0.0339	0.0000

quadrados dos resíduos. O motivo pela qual estamos utilizando o modelo ARMA(0,*d*,0)-GARCH(1,1) é pelo fato do modelo ARMA(1,*d*,0)-GARCH(1,1) não estar rodando quando tentamos realizar o processo de *Rolling Windows* no R. Na Tabela 4.17 damos as estimativas por máxima verossimilhança dos parâmetros desses modelos, seus erros padrões robustos e o p-valor do teste t.

Tabela 4.17: *Estimativas dos parâmetros, erros padrões, estatística t e p-valor do teste t para a Stellar, com parâmetro* $\nu = 7$.

ARMA(0,*d*,0)-GARCH(1,1): Modelo M1			
Parâmetros	Estimativa	Erro padrão robusto	p-valor do teste t
μ	-0.3964	0.1203	0.0010
ω	4.4741	2.4398	0.0667
α_1	0.4607	0.0922	0.0000
β_1	0.5382	0.0925	0.0000

Por fim, para o Euro, o nosso modelo completo ARFIMA(p,d,q)-FIGARCH(m,d,s) reduziu-se a um ARMA(0,*d*,0)-GARCH(1,2) com distribuição condicional Normal, modelo M3, onde o teste de Ljung-Box aceita a hipótese nula para os resíduos e os quadrados dos resíduos. Na Tabela 4.18 damos as estimativas por máxima verossimilhança dos parâmetros desses modelos, seus erros padrões robustos e o p-valor do teste t.

Tabela 4.18: *Estimativas dos parâmetros, erros padrões, estatística t e p-valor do teste t para o Euro.*

ARMA(0,*d*,0)-GARCH(1,2): Modelo M3			
Parâmetros	Estimativa	Erro padrão robusto	p-valor do teste t
ω	0.0003	0.0007	0.6461
α_1	0.0056	0.0035	0.1081
β_1	0.7658	0.0001	0.0000
β_2	0.2266	0.0003	0.0000

A Tabela 4.19 compila todas as estimativas para os parâmetros em uma única tabela.

Foi realizada uma comparação entre a média amostral das séries originais de retornos com a média amostral das séries após a retirada do efeito da memória longa para Ethereum e Stellar. A Tabela 4.20 consolida essa comparação.

Vemos acima que a média amostral da série original de retornos é positiva, relativamente grande e estatisticamente diferente de zero para o Ethereum e estatisticamente

Tabela 4.19: *Estimativas dos parâmetros dos modelos de volatilidade para todas as séries de criptomoedas analisadas e Euro.*

Séries	Parâmetros						
	μ	$\widehat{d}$	ω	α_1	β_1	β_2	ν
Bitcoin	-	0.0134	0.1413	0.1602	0.8388	-	3.5
Ethereum	-0.3423	0.0623	2.4726	0.2798	0.7192	-	3.8
Ripple	-0.3009	0.0197	2.4601	0.4227	0.5763	-	3.7
Litecoin	-	0.0297	0.1148	0.1309	0.8681	-	3.1
Stellar	-0.3964	0.1317	4.4741	0.4607	0.5382	-	7.0
Euro	-	-0.0369	0.0003	0.0056	0.7658	0.2266	-

Tabela 4.20: *: Comparação entre a média amostral da série original de retornos e a média amostral da série de retornos sem o efeito da memória longa, seus respectivos erros padrões e 95% intervalo de confiança para Ethereum e Stellar. Última coluna indica se são estatisticamente igual a zero.*

Criptomoedas	Série original			Série sem memória longa		
	Média dos retornos (e.p.)	95% I.C.	Estatisticamente igual a zero?	Média dos retornos (e.p.)	95% I.C.	Estatisticamente igual a zero?
Ethereum	0.4025 (0.1976)	[0.0151 , 0.7898]	✗	-0.0262 (0.1969)	[-0.4121 , 0.3596]	✓
Stellar	0.3241 (0.5720)	[-0.7970 , 1.4454]	✓	-0.0161 (0.6039)	[-1.1998 , 1.1675]	✓

igual a zero para a Stellar. Quando retiramos o efeito da memória longa, a média dos retornos é praticamente zero (sendo negativa em ambas as séries de retorno), onde na verdade as duas são estatisticamente iguais a zero. Existe então a possibilidade de sermos levados a pensar que o retorno esperado para Ethereum e Stellar é acima de zero, o que não é verdade, tendo sido esta crença devida à memória longa.

Assim como feito para os modelos não condicionais, para testar a performance das medidas de risco condicionais fora da amostra aplicamos o mesmo procedimento de janelas móveis. O tamanho da janela de estimação foi fixado em dois anos (730 observações) e aproximadamente um ano e meio para o Euro (530 observações) para cada janela os modelos condicionais das séries e foram estimados para as respectivas criptomoedas e uma estimativa do VaR_α obtida para o dia seguinte. Em seguida uma nova observação era incorporada à amostra de estimação e a observação mais antiga eliminada da mesma. O processo resultou em 489 estimativas fora da amostra para as criptomoedas e 325 estimativas fora da amostra para o Euro.

Para acessar a performance das previsões fora da amostra foi aplicado o teste de Kupiec. O número de violações na amostra de verificação e o resultado do teste de Kupiec para os modelos com e sem GPD estão na Tabela 4.21.

É interessante observar que os modelos sem GPD obtiveram melhor desempenho para Ethereum e Euro, ao passo que para Ripple e Litecoin os modelos com GPD obtiveram melhor desempenho. Já para Bitcoin e Stellar o desempenho foi igual no Teste de Kupiec. Foi ajustada a GPD com a intenção de se conseguir um melhor ajuste nas caudas das distribuições. Conforme requerido pela TVE, é importante que os resíduos padronizados não mais apresentem conglomerados de volatilidade e dependência temporal para o ajuste

Tabela 4.21: *: Número de violações fora da amostra (out-of-sample) e teste de Kupiec.*

Número de violações do VaR fora da amostra													
α	Esperado	Bitcoin		Ethereum		Ripple		Litecoin		Stellar		Euro	
		M1	M1 GPD	M1	M1 GPD	M1	M1 GPD	M1	M1 GPD	M1	M1 GPD	M3	M3 GPD
1%	4.89	8	8	11	11	8	9	9	8	10	11	4	2
5%	24.45	39	33	33	35	34	35	47	40	29	32	13	20
95%	24.45	29	15	22	13	37	25	36	24	32	20	16	13
99%	4.89	5	3	3	2	11	7	9	2	6	3	3	0
Teste de Kupiec													
α		Bitcoin		Ethereum		Ripple		Litecoin		Stellar		Euro	
		M1	M1 GPD	M1	M1 GPD	M1	M1 GPD	M1	M1 GPD	M1	M1 GPD	M3	M3 GPD
1%		✓	✓	✗	✗	✓	✓	✓	✓	✗	✗	✓	✓
5%		✗	✓	✓	✗	✓	✗	✗	✗	✓	✓	✓	✓
95%		✓	✗	✓	✗	✗	✓	✗	✓	✓	✓	✓	✓
99%		✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗

Notação na tabela: ✓significa que H_0 foi aceita e ✗significa que H_0 foi rejeitada

da GPD.

A seguir, foram calculados a Perda Média condicional. A Tabela 4.22 apresenta essas informações.

Tabela 4.22: *: Perda Média condicional.*

Perda Média							
α	Bitcoin		Ethereum		Ripple		
	M1	M1 GPD	M1	M1 GPD	M1	M1 GPD	
1%	-13.68%	-13.68%	-17.33%	-17.33%	-17.45%	-16.80%	
5%	-9.59%	-9.95%	-12.63%	-12.46%	-12.23%	-12.20%	
95%	8.72%	10.96%	10.23%	12.75%	16.34%	19.85%	
99%	15.30%	14.09%	11.85%	11.38%	25.96%	27.52%	
α	Litecoin		Stellar		Euro		
	M1	M1 GPD	M1	M1 GPD	M3	M3 GPD	
1%	-17.26%	-17.72%	-17.89%	-17.95%	-1.18%	-1.23%	
5%	-10.99%	-11.36%	-14.79%	-15.02%	-0.96%	-0.88%	
95%	12.86%	15.26%	18.23%	18.72%	0.92%	0.96%	
99%	20.03%	20.49%	26.49%	40.69%	1.16%	NA	

Notação na tabela: NA significa *not available*. Pelo fato de não ter violado nenhuma vez, não sabemos qual será a PE.

Um dado interessante desta tabela é o fato de $\alpha = 1\%$ para a cauda direita do Ethereum para o modelo com apresentar um valor menor que o $\alpha = 5\%$ para a cauda direita para a mesma moeda. Isso ocorre em função de haver apenas 2 violações para o $\alpha = 1\%$ na cauda direita fora da amostra em um período de menor volatilidade da série. A Figura 4.7 ilustra este acontecimento.

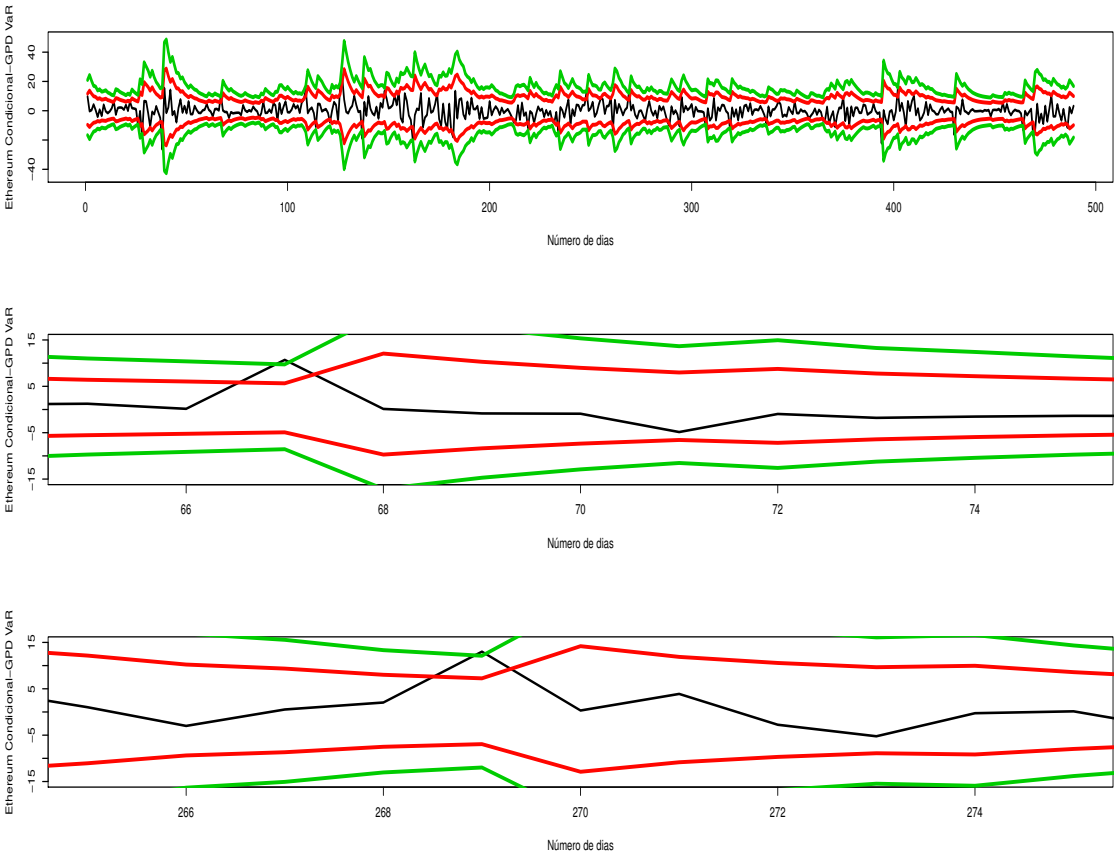

Figura 4.7: Ethereum: VaR Condicional GPD

Capítulo 5

Conclusões

Nesta dissertação analisamos o comportamento da série de retornos do Euro e das cinco mais importantes criptomoedas no momento, que são Bitcoin, Ethereum, Ripple, Litecoin e Stellar. Juntas, estas criptomoedas são atualmente responsáveis por mais de 70% da capitalização de todo o mercado de criptomoedas.

Utilizando amostras de aproximadamente três anos e meio para as criptomoedas de dados diários e dois anos e meio para o Euro de dados em dias úteis prcuramos entender o comportamento das séries através de análises exploratórias e ajustes de modelos estatísticos. Vários resultados interessantes, a maioria esperados, foram observados. Por exemplo, os famosos fatos estilizados comprovados para ações e índices são também verificados para essas séries. Para os ajustes não condicionais, vimos que o teste GOF rejeita a t-assimétrica de Zhu e Galbraith para todas as séries. Para a Normal e t-student o teste GOF aceita apenas para o Euro e para a GPD, tanto cauda esquerda como direita, o teste GOF aceita para todas as séries. Já para as medidas de risco não condicionais, a GPD forneceu a melhor performance, tanto *in-sample* quanto *out-of-sample* de acordo com o Teste de Kupiec. Já para os ajustes condicionais, o melhor modelo para a volatilidade foi o GARCH (1,1) (com exceção do Euro), novamente reproduzindo resultados conhecidos para ações e carteiras. Para a performance das previsões fora da amostra, os modelos sem GPD obtiveram melhor desempenho para Ethereum e Euro, ao passo que para Ripple e Litecoin os modelos com GPD obtiveram melhor desempenho. Já para Bitcoin e Stellar o desempenho foi igual no Teste de Kupiec. Tanto para os modelos condicionais como para os não condicionais, foi fornecida a Perda Média Esperada para os melhores modelos. Para áreas como administração do risco e investimentos, essa informação é de grande importância para o apoio a tomada de decisão. Para pesquisas futuras sugerimos, além de analisar outros criptomoedas, a utilização de outras modelos.

Referências Bibliográficas

[1] Armknecht F., Karame G.O., Mandal A., Youssef F. e Zenner E. Ripple: Overview and Outlook. In: Conti M., Schunter M., Askoxylakis I. (eds) Trust and Trustworthy Computing. Trust 2015. Lecture Notes in Computer Science, vol 9229. Springer, Cham, 2015. Disponível em https://www.researchgate.net/publication/281631024_Ripple_Overview_and_Outlook.

[2] Bickel, P.J. e Doksum, K.A. *Mathematical statistics: basic ideas and selected topics*, Holden-Day, 1977.

[3] Bickel, P.J. e Doksum, K.A. *Mathematical statistics: basic ideas and selected topics*. Prentice Hall, 2001.

[4] Bitcoin.org. Disponível em https://bitcoin.org/en/faq#who-created-bitcoin.

[5] Bitcoinblockhalf. Disponível em https://www.bitcoinblockhalf.com/.

[6] Blockchain.info. Disponível em https://blockchain.info/charts/n-transactions?timespan=all.

[7] Blockchain.info. Disponível em https://blockchain.info/pools?timespan=4days.

[8] Blockgeeks.com. Disponível em https://blockgeeks.com/guides/blockchain-scalability/.

[9] Blockgeeks.com. Disponível em https://blockgeeks.com/guides/cryptocurrency-wallet-guide/.

[10] Blockgeeks.com. Disponível em https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/.

[11] Blockgeeks.com. Disponível em https://blockgeeks.com/guides/smart-contracts/.

[12] Bloomberg. Disponível em https://www.bloomberg.com/features/2017-the-ether-thief/.

[13] Bollerslev, T. Generalized Autoregressive Conditional Heteroskedasticity. *Journal of Econometrics*, 31: 307-327, 1986.

[14] Buterin, V. A next generation smart contract decentralized application platform, 2013.

[15] Chan, S., Chu, J., Nadarajah, S. e Osterrieder, J. A Statistical Analysis of Cryptocurrencies. *Journal of Risk Financial Management*, 10, 17; doi:10.3390/jrfm10040017.

[16] Chan, S., Chu, J., Nadarajah, S. e Osterrieder, J. GARCH Modelling of Cryptocurrencies. *Journal of Risk Financial Management*, 10, 12; doi:10.3390/jrfm10020012.

[17] Chartered Online. Disponível em http://www.charteredonline.in/2017/02/bitcoins-india-mining-exchange-buy.html.

[18] Chartered Online. Disponível em https://99bitcoins.com/wp-content/uploads/2017/02/ledger-nano-s-review.png.

[19] Chohan, U.W. The Double Spending Problem and Cryptocurrencies. *SSRN Electronic Journal*, 2017. Disponível em SSRN: https://ssrn.com/abstract=3090174 ou http://dx.doi.org/10.2139/ssrn.3090174.

[20] Coin Market Cap. Disponível em https://coinmarketcap.com/.

[21] Coin Market Cap. Disponível em https://coinmarketcap.com/charts/dominance-percentage.

[22] Coindesk. Disponível em https://www.coindesk.com/information/will-ethereum-scale/.

[23] Coinsutra.com. Disponível em https://coinsutra.com/ethereum-blockchain-vs-bitcoins-blockchain/.

[24] Cointelegraph.com. Disponível em https://cointelegraph.com/explained/ico-explained.

[25] Cointelegraph.com. Disponível em https://cointelegraph.com/explained/smart-contracts-explained.

[26] Croman, K., Decker, C., Eyal, I., Gencer, A.E., Juels, A., Kosba, A., Miller, A., Saxena, P., Shi, E., Sirer, E.G., Song. D., Wattenhofer, R. On Scaling Decentralized Blockchains. *Financial Cryptography and Data Security: FC 2016 International Workshops, BITCOIN, VOTING, and WAHC, Christ Church, Barbados, February 26, 2016, Revised Selected Papers*,106-125, 2016. Disponível em https://www.tik.ee.ethz.ch/file/74bc987e6ab4a8478c04950616612f69/main.pdf.

[27] de Haan, L. Slow variation and characterization of domains of attraction. *Statistical Extremes and Applications*, 131:31-48, 1984.

[28] Etherscan.io. Disponível em https://etherscan.io/chart/gaslimit.

[29] Etherscan.io. Disponível em https://etherscan.io/chart/gasprice.

[30] Gervais, A., Karame, G.O., Capkun, V. e Capkun, S. Is Bitcoin a decentralized currency? *IEEE Security and Privacy Magazine*, 12(3):54-60, 2014. Disponível em https://eprint.iacr.org/2013/829.pdf.

[31] Github.com. Disponível em https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ.

[32] Guo, T. e Antulov-Fantulin, N. An experimental study of Bitcoin fluctuation using machine learning methods. *Association for Computing Machinery*, Article 4.

[33] Hosking, J. R. M. e Wallis, J. R. Parameter and quantile estimation for the generalized pareto disitribution. *Technometrics*, 29(3):339-349, 1987.

[34] Invest in Blockchain. Disponível em https://www.investinblockchain.com/lightning-network-bitcoin-scaling/.

[35] Invest in Blockchain. Disponível em https://www.investinblockchain.com/stellar-lumens-vs-ripple/.

[36] Investopedia. Disponível em https://www.investopedia.com/articles/investing/042015/bitcoin-vs-litecoin-whats-difference.asp.

[37] Katsiampa, P. Volatility estimation for Bitcoin: A comparison of GARCH models. *Economics Letters*, vol. 158, issue C, 3-6, 2017.

[38] Kupiec, P. H. Techniques for verifying the accuracy of risk measurement models. Finance and Economics Discussion Series 95-24, Board of Governors of the Federal Reserve System (U.S.), 1995.

[39] Litecoinblockhalf. Disponível em https://www.litecoinblockhalf.com/.

[40] Liu, R., Shao, Z., Wei, G. e Wang, W. GARCH Model With Fat-Tailed Distributions and Bitcoin Exchange Rate Returns. *Journal of Accounting, Business and Finance Research*, Vol. 1, No. 1, pp. 71-75.

[41] Ljung, G.M. e Box, G.E.P. On a measure of a lack of fit in time series models. *Biometrika*, 65(2):297-303, 1978.

[42] Mazières, D. The Stellar Consensus Protocol:A Federated Model for Internet-level Consensus, 2016.

[43] Medium. Disponível em https://blog.unocoin.com/bitcoins-segwit-explained-5dc6b0afcb08.

[44] Medium. Disponível em https://medium.com/@karthik.seshu/cryptocurrency-proof-of-work-vs-proof-of-stake-e1eee1420b10.

[45] Medium. Disponível em https://medium.com/FolusoOgunlana/cracking-the-ethereum-white-paper-e0e60c44126.

[46] Medium. Disponível em https://medium.com/lightcoin/the-differences-between-a-hard-fork-a-soft-fork-and-a-chain-split-and-what-they-mean-for-the-769273f358c9.

[47] Medium. Disponível em https://medium.com/tbis-weekly-bits/i-see-you-xrp-fcf151feb96d.

[48] Medium. Disponível em https://medium.com/verge-currency-xvg/what-is-the-wraith-protocol-bd1dfb289cda.

[49] Medium. Disponível em https://medium.com/@BLMPNetwork/whats-the-difference-between-litecoin-and-bitcoin-6e9adb92a8b8.

[50] Mendes, B.V.M. Asymmetric extreme interdependence in emerging equity markets. *Applied Stochastic Models in Business and Industry*, 21(6):483-498, 2005a. ISSN 1524-1904. doi:http://dx.doi.org/10.1002/asmb.v21:6.

[51] Mendes, B.V.M. Modelagem de risco financeiro. *Relatórios COPPEAD* 429, 2016.

[52] Multicoin Capital. Ripple ($XRP) Analysis, 2017. Disponível em https://multicoin.capital/2017/08/31/xrp2017/.

[53] Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System, 2009.

[54] Nasdaq. Disponível em https://www.nasdaq.com/article/credit-card-fraud-and-id-theft-statistics-cm520388.

[55] Pickands, J. III. *Spline and Isotonic Estimation of the Pareto Function*, volume 12, pages 285-296. Statistical Extremes and Applications Proceedings of the NATO Symposium on Extreme Values, reindel publishers co. edition, 1984.

[56] Pickands, J. III. Statistical inference using extreme order statistics. *Annals of Statistics*, 3:119-131, 1975a.

[57] Pickands, J. III. Statistical inference using extreme order statistics. *Annals of Statistics*, 3:119-131, 1975b.

[58] Ripple Labs Inc. Building Network Effects on Ripple. Disponível em https://ripple.com/files/ripple_vision.pdf.

[59] Schwartz, D., Youngs, N. e Britto, A. The Ripple Protocol Consensus Algorithm. Disponível em https://ripple.com/files/ripple_consensus_whitepaper.pdf.

[60] Smith, R. L. Estimating tails of probability distributions. *Annals of Statistics*, 15:1174-1207, 1987.

[61] The Mail Archive. Disponível em https://www.mail-archive.com/search?l=cryptography@metzdowd.com&q=from:%22Satoshi+Nakamoto%22.

[62] Tsay, R. S. *Analysis of Financial Time Series.*, Wiley Series in Probability and Statistics. Wiley-Interscience, New York, 2002.

[63] Tsay, R. S. *Analysis of Financial Time Series.*, Wiley Series in Probability and Statistics. Wiley-Interscience, New York, 2002.

[64] Visa. Disponível em https://usa.visa.com/run-your-business/small-business-tools/retail.html.

[65] WeUseCoins. Disponível em https://www.weusecoins.com/en/questions/.

[66] Wikipedia.com. Disponível em https://en.wikipedia.org/wiki/Ripple_(company).

[67] Wikipedia.com. Disponível em https://pt.wikipedia.org/wiki/Peer-to-peer.

[68] Wilkins, N., Indirect Estimation of Long Memory Volatility Models. Econometric Society 2004 Far Eastern Meetings 459, Econometric Society, 2004.

[69] Youtube.com. Disponível em https://www.youtube.com/watch?v=apdQsrwAEXE.

[70] Youtube.com. Disponível em https://www.youtube.com/watch?v=rrr_zPmEiME.

[71] Zhu, D. e Galbraith J.W. A generalized asymmetric Student-t distribution with application to financial econometrics. *Journal of Econometrics*, 157: 297-305, 2010.