

FUNDAÇÃO GETULIO VARGAS  
ESCOLA DE ADMINISTRAÇÃO DE EMPRESAS DE SÃO PAULO  
PROGRAMA DE GRADUAÇÃO EM ADMINISTRAÇÃO DE EMPRESAS

**PIBIC – Programa Institucional de Bolsas de Iniciação Científica**  
ESTUDO DOS FATORES DE SUCESSO DE VALORIZAÇÃO DE UMA  
CRIPTOMOEDA

ALUNO: FILIPE LINHARES AMANCIO DE OLIVEIRA

ORIENTADOR: PROFESSOR JULIO FIGUEIREDO

AGOSTO DE 2018

Aos meus maiores exemplos de vida e perseverança, meus pais Jefferson e Ceíça que sempre me apoiaram durante minha jornada acadêmica.

Aos meus avós paternos e maternos, pela existência de meus pais, pois sem eles este trabalho e muitos dos meus sonhos não se realizariam.

## **AGRADECIMENTOS**

Ao Curso de Administração de Empresas da Fundação Getúlio Vargas, seu corpo docente, direção e administração que oportunizaram a janela pela qual hoje vislumbro um horizonte superior.

Ao meu professor, orientador e amigo Professor Júlio Figueiredo pelo suporte, orientação, apoio, paciência e confiança durante toda a elaboração deste trabalho.

Ao colega graduando e pesquisador Yan Kaled pela convivência e colaboração neste trabalho.

A todos que direta ou indiretamente fizeram parte da minha formação.

## Sumário

I.	Apresentação .....	5
I.	Moeda .....	5
1.	O conceito de Moeda .....	5
2.	A moeda ao longo da História .....	6
3.	As Funções da Moeda .....	6
II.	Criptomoedas.....	7
1.	Introdução .....	7
2.	O Conceito de Criptomoeda.....	8
3.	O Processo de Criação de uma Criptomoeda.....	9
4.	O Processo de Emissão e Certificação de uma Criptomoeda .....	10
	A Mineração .....	10
	Proof-of-Work (PoW).....	10
	Proof-of-Stake (PoS).....	12
	O Blockchain .....	14
	ICO – Initial Coin Offering .....	14
	Smart Contracts – Contratos Inteligentes .....	14
	Fork.....	16
III.	Os Principais Mercados de Troca .....	16
1.	Bitfinex .....	17
2.	Binance .....	17
3.	Bittrex.....	17
4.	Bithumb.....	17
IV.	A Principais Criptomoedas .....	17
	Bitcoin (BTC) .....	17
	Ethereum (ETH).....	17
	Ripple (XRP).....	18
	Dogecoin (DOGE).....	20
V.	Percurso Metodológico da Pesquisa.....	22
	Análise de Conteúdo .....	22
	Passos Metodológicos.....	23
	Análise Dos Dados Obtidos.....	28
VI.	Conclusões.....	28
	Bibliografia .....	30

## I. Apresentação

O objetivo foi entender e relatar quais são as interações necessárias no ambiente econômico financeiro das Criptomoedas que possibilitam a sua valorização baseando-se nas teorias econômicas de valorização das chamadas moedas comuns dentro do escopo e cronograma propostos previamente.

Atividade	Meses											
	1	2	3	4	5	6	7	8	9	10	11	12
a) Pesquisas Bibliográficas sobre Criptomoedas	█	█	█	█	█	█	█	█	█	█		
b) Pesquisas Específicas Relativas à Ripple			█	█	█	█	█	█				
c) Pesquisas específicas a outras altcoins de rápida difusão					█	█	█	█				
d) Estudo comparativo dos resultados obtidos entre as Criptomoedas							█	█	█			
f) Elaboração do relatório final										█	█	█

# Revisão Teórica

## I. Moeda

### 1. O conceito de Moeda

De acordo com o dicionário Houaiss da Língua Portuguesa, Moeda é:

1. *peça de metal cunhada por instituição governamental que representa o valor do objeto trocado por ela;*
2. *meio pelo qual são feitas as transações comerciais;*
3. *dinheiro*

(Houaiss, 2015)

O termo dinheiro para a economia, que difere do uso diário da palavra. No dia-a-dia as pessoas se referem ao dinheiro quando querem falar de renda ou de riqueza, enquanto na economia, o termo dinheiro se refere especificamente aos ativos que são aceitos como meio de pagamento, ou seja, a moeda. Historicamente as formas de dinheiro tem mudado desde contas e conchas até a era da prata e do ouro, em algumas ocasiões como prisões até cigarros são utilizados como moeda de troca. Nos tempos atuais, a forma mais comum de dinheiro são as moedas e o papel moeda.(Abel, Bernanke e Croushore, 2013)

Para que algo possa ser considerado uma moeda este deve desempenhar algumas funções, são estas funcionar como meio de troca, ser denominador comum de valor e servir como reserva de valor. (“Moeda :: Política Monetária”, [s.d.]) Essas Funções serão melhor estudadas em tópico a seguir.

Assim, a moeda compõe tudo aquilo que é aceito como meio de realizar transações, pagando por bens e serviços e quitando obrigações, tais como as moedas físicas e notas que são emitidas pelos governos para circular na economia.

## 2. A moeda ao longo da História

De acordo com a historiadora e arqueóloga Maria Beatriz Florenzano, existem dois momentos diferentes que devem ser ressaltados nos primórdios da cunhagem das moedas: o primeiro, aquele em que a moeda foi criada na Ásia Menor e o segundo, a sua subsequente adoção e difusão entre as cidades gregas do continente. (Florenzano, 2001)

Em meados do século V a.C., o historiador Heródoto registra: “Os lídios foram os primeiros entre os homens, até onde vai o nosso conhecimento, a cunhar e a usar moedas de ouro e prata, e também foram os primeiros a vender mercadorias a varejo.” (Idem, 2001)

## 3. As Funções da Moeda

Desde os primórdios quase todas as sociedades tem utilizado dinheiro. Este sempre teve três papéis essenciais na economia e que devem ser verdadeiros para que algo possa ser caracterizado como dinheiro. São eles:

### a) Meio de Troca

Em uma economia onde o dinheiro não é utilizado, toda troca é realizada por meio da troca de um bem ou serviço por outros bens ou serviços. O escambo no entanto é um método ineficiente de se realizar trocas pois encontrar alguém que esteja disposto a trocar um bem que você deseja por um que você possui é algo difícil e demorado. Como um exemplo, em uma economia de escambo, se o autor desse relatório desejasse ir para uma festa ele teria que primeiramente encontrar um evento que estivesse disposto a permitir sua entrada em troca do conhecimento aqui contido sobre criptomoedas, algo que não deve ser fácil de se conseguir. (Abel, Bernanke e Croushore, 2013; Wonnacott, 1995)

Em uma economia onde há dinheiro em utilização, tal esforço de “caçar” um parceiro de troca não se vê necessário. Nessa economia, o autor deste poderia primeiramente conseguir uma bolsa com um órgão público que permitisse a realização de um estudo sobre os fatores de sucesso de valorização de uma criptomoeda e, com o dinheiro adquirido na bolsa, satisfazer sua vontade de ir à uma festa. Ao funcionar como meio de troca, o dinheiro permite que as pessoas realizem trocas de maneira mais eficiente em termos de tempo e esforço. (Abel, Bernanke e Croushore, 2013; Wonnacott, 1995)

### b) Unidade de medida

Nas transações realizadas em nosso dia-a-dia precisamos de algo que possa nos dizer quantos pães um padeiro deve vender para que possa comprar uma televisão por exemplo. Para tal, a moeda deve agir como um padrão comum de valores, nos fornecendo a informação que tanto a televisão quanto X pães franceses valem

Y unidades de tal moeda. Ou seja, um pessoa com uma televisão, X pães ou Y moedas possuem a mesma quantidade de riqueza. (Abel, Bernanke e Croushore, 2013; Wonnacott, 1995)

c) Reserva de valor

Deve ser possível para o dono de uma quantia de dinheiro guardá-lo pro qualquer período de tempo, assim mantendo um valor por uma quantia específica de tempo e possibilitando que este seja utilizado no futuro. (Abel, Bernanke e Croushore, 2013; Wonnacott, 1995)

## II. Criptomoedas

### 1. Introdução

Nossa sociedade atual gira em torno do dinheiro;

*“Money is power, freedom, a cushion, the root of all evil, the sum of blessings.”(Sandburg, 2000)*

A cada dia que passa as criptomoedas se tornam cada vez mais uma realidade no dia-a-dia das empresas e das pessoas. No ano de 1983, um criptógrafo de nome David Chaum começava o que poderia ser o início da procura e desenvolvimento de uma criptomoeda com o DigiCash, uma moeda que introduziu o conceito de “Blind Signature Technology”, tecnologia que permitia o anonimato e a privacidade para usuários que conduziam transações online. Em 2008, Satoshi Nakamoto concretizou a ideia de uma moeda virtual criptografada e sem as instituições financeiras, ideia previamente introduzida por Dai Wei como “b-money”(Dai, 1998), que hoje são necessárias para realizar a validação e o processamento das transações financeiras. Entra a Bitcoin, uma versão “peer-to-peer” de uma moeda virtual trocada entre duas partes sem o auxílio de uma instituição financeira (Nakamoto, 2008). A solução elaborada que possibilita a eficiência e o funcionamento da moeda sem tais instituições é o mecanismo chamado de “proof-of-work”, que é baseado em chaves de códigos (“hashes”), em uma estrutura conhecida como Blockchain.

Desde a criação e efetiva implementação da Bitcoin (a criptomoeda mais conhecida) por Satoshi Nakamoto em 2009, diversas novas criptomoedas têm sido criadas, as chamadas “Altcoins”. Pode-se observar na Figura abaixo uma lista com a principais criptomoedas em circulação nos dias de hoje ordenadas por Market Cap.

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	 Bitcoin	\$137.726.149.359	\$8249.02	\$3.915.350.000	16.696.062 BTC	1.03%	
2	 Ethereum	\$36.691.698.720	\$382.61	\$947.749.000	95.898.431 ETH	4.77%	
3	 Bitcoin Cash	\$24.645.281.959	\$1465.46	\$2.695.240.000	16.817.438 BCH	23.08%	
4	 Ripple	\$9.306.798.591	\$0.240966	\$194.737.000	38.622.870.411 XRP *	2.45%	
5	 Dash	\$4.373.744.732	\$567.64	\$381.721.000	7.705.098 DASH	10.11%	
6	 Litecoin	\$3.879.973.056	\$71.92	\$170.521.000	53.951.908 LTC	2.02%	
7	 IOTA	\$2.508.473.269	\$0.902481	\$67.239.200	2.779.530.283 MIOTA *	-1.97%	
8	 Monero	\$2.484.603.072	\$161.46	\$196.894.000	15.388.065 XMR	10.71%	
9	 NEO	\$2.334.293.000	\$35.91	\$73.624.100	65.000.000 NEO *	-0.21%	
10	 NEM	\$1.829.367.000	\$0.203263	\$7.470.810	8.999.999.999 XEM *	-0.80%	
11	 Ethereum Classic	\$1.756.127.355	\$17.97	\$108.756.000	97.708.651 ETC	-0.02%	
12	 Qtum	\$1.032.038.953	\$14.01	\$102.688.000	73.681.280 QTUM *	-0.88%	

Figura 1

Dentre todas estas moedas apresentas uma de interesse é a Ripple. O interesse se deve ao fato de que, diferentemente da maior parte das criptomoedas disponíveis no mercado, a plataforma criada pela Ripple para realizar transações internacionais com custos reduzidos possui o apoio de Instituições Financeiras de grande importância no mundo, como American Express e o Banco Santander. (Browne, 2017)

## 2. O Conceito de Criptomoeda

As criptomoedas são um meio de troca que se utiliza de uma tecnologia de criptografia, mais conhecida como Blockchain, para assegurar e validar todas as suas transações. A primeira criptomoeda descentralizada a ter um amplo sucesso foi a Bitcoin (BTC) tornando-se, portanto, a mais conhecida e disseminada no mundo hoje em dia. (Tapscott e Tapscott, 2016)

Em seu Paper, Satoshi Nakamoto discorre brevemente a respeito da Bitcoin:

*“A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution.”(Nakamoto, 2008)*

Apesar de a Bitcoin ter sido criada por Satoshi Nakamoto em 2008 em seu paper, a ideia de uma moeda virtual criptografada vem de 10 anos antes em 1998 quando Wei

Dai coloca em seu website um texto de nome “b-money” toda a estrutura sob a qual as criptomoedas seriam criadas. Na época em que Wei Dai idealizou o suposto “b-money” ele não possuía nem o conhecimento nem as ferramentas necessárias para levar a ideia para frente, portanto ficou apenas como ideia. (Dai, 1998)

As criptomoedas, possuem uma quantidade pré-determinada de moedas que serão emitidas durante sua vida útil, o programa da Bitcoin por exemplo pré-determina que 240 milhões de moedas serão “mineradas” ou emitidas até 2040. O conceito de mineração envolve os cálculos que são feitos pelos computadores dos mineradores para resolver uma equação matemática, “selando” por meio de uma criptografia o último bloco criado pela comunidade. Blocos são criados de 10 em 10 minutos.

Cada criptomoeda possui seu próprio código que determina todos os protocolos relacionados a moeda. A partir do momento que um usuário cria uma transação, ou seja, uma transferência de valor entre carteiras de criptomoeda, a mesma é incluída no blockchain. A partir desse blockchain as carteiras conseguem calcular seu saldo disponível com base nas transações que se passaram. Para finalizar o processo da adição de uma transação ao blockchain é preciso que o bloco no qual a transação foi incluída seja minerado por diferentes computadores que tem como propósito a mineração desses blocos. (“Como o Bitcoin funciona?”, [s.d.]

As criptomoedas representam para muitos em sua comunidade um sinônimo de liberdade e esperança. Elas permitem que minorias que muitas vezes não possuem acesso à uma conta própria no banco pois não lhe são permitidas possam ter sua própria independência, como é o caso da Afegã Parisa Ahmadi, que vive tal realidade em um país que não permite que as mulheres da família lidem com seu próprio dinheiro. Ahmadi, uma das melhores de sua turma, começou sua jornada com as criptomoedas em uma classe oferecida em sua escola sobre o uso da internet e de mídias sociais que paga as alunas com criptomoedas pelo sucesso na classe. Com as criptomoedas que adquiriu desde então, Ahmadi já conseguiu comprar seu próprio laptop. (Vigna e Casey, 2015)

### 3. O Processo de Criação de uma Criptomoeda

É possível imaginar um processo complicado para a criação de uma Criptomoeda, algo que demandasse diversas horas de programação computacional e trabalho duro, porém, com o avanço da tecnologia e o surgimento diário de novos tokens, a parte difícil deixa de ser a criação da mesma, mas sim sua manutenção, convencimento de um público específico de que há futuro para sua Criptomoeda e a criação de um incentivo para que as pessoas usem a sua criptomoeda e não a do “vizinho” que está em alta no momento. Há inclusive websites que permitem a fácil criação de uma nova criptomoeda se assim for desejado.

Um bom exemplo de uma criptomoeda que foi criada como uma brincadeira e que depois teve seu valor desintegrado devido à uma má gestão da criptomoeda é a DogeCoin, descrita na seção “As Principais Criptomoedas”.

Algumas moedas podem surgir de maneiras não convencionais como o Fork e o ICO, dos quais descrevemos adiante.

O processo padrão para a criação de uma criptomoeda é extremamente minudenciado, incluindo as linhas de programação e seus detalhes, no Estudo da implementação de plataformas de criptomoedas em ambientes compartilhados e distribuídos: Criando a GvCoin por Yan Kaled (2018), o qual recomendamos como leitura complementar para um entendimento brando da criação de uma Criptomoeda desde o início.

#### 4. O Processo de Emissão e Certificação de uma Criptomoeda

##### A Mineração

É um processo computacional com dois propósitos principais, confirmar transações de uma maneira confiável quando uma certa quantidade de poder computacional é empregada ao bloco minerado e lançar novas moedas contidas em cada bloco no mercado.(Mining?, 2017)

O processo de mineração é aquele pelo qual as transações são verificadas e depois adicionadas ao “livro de registro” conhecido como blockchain.

A comunidade de uma determinada criptomoeda tem um objetivo primariamente monetário ao minerá-las, pois uma vez que o bloco é resolvido a mineração gera prêmios para aqueles que o fazem, permitindo o crescimento e a manutenção de sua comunidade.

Na figura 3 pode-se observar um fluxo que detalha o processo da Mineração.

##### Proof-of-Work (PoW)

As minerações de algumas criptomoedas, como o Bitcoin, são baseadas em um sistema de loteria, onde os mineradores são remunerados quando o sistema utilizado por eles ou o pool no qual ele está inserido resolve um bloco ao gerar randomicamente um conjunto de caracteres que resolve um problema matemático. A partir do momento em que alguém encontra a solução para o problema, aquele bloco é trancado e as pessoas que possuem a chave conseguem ver que o problema foi realmente resolvido, pois ele só tem uma solução.

A prova de trabalho é então um meio pelo qual alguém pode provar que empregou um esforço computacional na mineração de um bloco.

# Como funciona uma transação de Bitcoin

Bob, um vendedor online, decide que irá aceitar bitcoins como pagamento. Alice, uma compradora, possui Bitcoins e quer comprar algo de Bob

## CARTEIRAS E ENDEREÇOS

Bob e Alice possuem carteiras de Bitcoin em seus computadores

Carteiras são arquivos que fornecem acesso à diversos endereços de Bitcoin

Um endereço é uma sequência composta por letras e números como: THULMwZEPMEPECH43BeKIL1ybLCwRfDpN

## CRIANDO UM NOVO ENDEREÇO

Bob cria um novo endereço de Bitcoin para que Alice envie seu pagamento.

## SUBMETENDO UM PAGAMENTO

Alice diz ao seu cliente de Bitcoin que ela deseja enviar o valor referente à compra para o endereço de Bob.

Chave Privada  
Chave Pública

## Criptografia de chave pública 101

Quando Bob cria um novo endereço, o que ele está realmente fazendo é gerando um "par de chaves criptográficas" compostas de uma chave privada e uma chave pública. Se você assinar uma mensagem com sua chave privada (que apenas você sabe), ela pode ser verificada utilizando a chave pública correspondente (que todos sabem). O novo endereço de Bitcoin de Bob representa uma única chave pública, e a chave privada correspondente fica guardada em sua carteira. A chave pública permite que qualquer pessoa verifique a autenticidade da mensagem assinada.



A Carteira de Alice possui uma chave para cada um de seus endereços. O cliente de Bitcoin de Alice usa a chave pública com a chave privada do endereço de onde ela está transferindo Bitcoins. Qualquer um na rede pode agora usar a chave pública para verificar que a solidificação da transação está realmente vindo do real dono da conta.

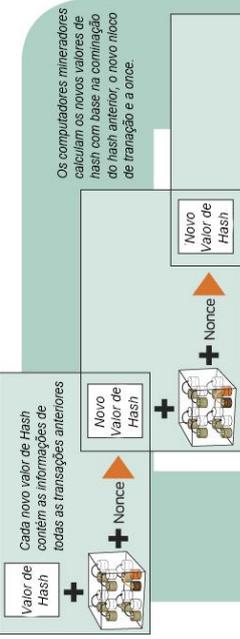
É tentador imaginar os endereços como contas de banco, mas eles funcionam de maneira um pouco diferente. Os usuários de Bitcoin podem criar quantos endereços desejarem, são na realidade encorajados a fazê-lo a cada transação realizada a fim de aumentar a privacidade. Portanto, se ninguém souber quais endereços são da Alice, sua anonimidade permanece protegida.



Gary, Garth e Grem são mineiros de Bitcoin. Seus computadores agrupam as transações dos últimos 10 minutos em um novo "bloco de Transação". Os computadores dos mineiros são configurados para calcular funções de hash gráficas.

## TRANSAÇÃO VERIFICADA

Conforme passa o tempo, a transação entre Alice e Bob vai se enterrando em blocos de transações mais recentes. Para que qualquer um modifique os detalhes, ele teria que refazer o trabalho feito pelo Gary - pois qualquer modificação requer um nonce vencedor novo - e então refazer todo o trabalho dos mineiros subsequentes. Tal feito é praticamente impossível!



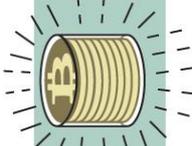
Cada novo valor de Hash contém as informações de todas as transações anteriores. Os computadores mineiros calculam os novos valores de hash com base na combinação do hash anterior, o novo bloco de transação e a nonce.

## Hash criptografadas

Funções de Hash criptografadas transformam um conjunto de dados em uma corda alfanumérica com um comprimento fixo, chamado de valor de hash. Mesmo pequenas mudanças nos dados originais alteram drasticamente o valor de hash resultante. Além disso, é essencialmente impossível prever quais dados criaram um valor de hash específico.

The root of all evil (56 more characters)  
The root of all evil  
The root of all evil

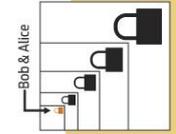
Nonces Para criar diferentes valores de Hash dos mesmos valores, a Bitcoin usa "nonces". Um nonce é apenas um número randômico que é adicionada aos dados antes do hashing. A Mudança do Nonce resulta em diversos valores de hash completamente diferentes.



Cada bloco inclui uma transação de criação de moedas que paga 50 bitcoins para o mineiro vencedor - nesse caso o Gary. Um novo endereço é criado na carteira de Gary contendo as novas criptomoedas.



Os mineiros não conseguem prever qual nonce criará um valor de hash com o número requerido de zeros iniciais. Portanto, eles são forçados a gerar quantos hashes com diferentes nonces forem necessários até que um funcione.



## Proof-of-Stake (PoS)

Como vimos acima, a Bitcoin utiliza o modelo de verificação chamado de “proof-of-work”, ou prova de trabalho. Contudo, alguns desenvolvedores vêm criando criptomoedas que utilizam uma forma de verificação diferente e mais eficiente, chamada “proof-of-stake” que, no lugar de distribuir o prêmio pela resolução do bloco baseando-se na capacidade de processamento utilizada (“Hashes”), distribui a recompensa pela mineração proporcionalmente com base na quantidade monetária que um minerador possui, além de somente permitir que usuários com uma quantidade específica de participação (“stake”) na moeda participem do processo. Esse método reduz significativamente a energia dispendida para operar as moedas que nele se baseiam. (Antonopoulos, 2017; Barski e Wilmer, 2014)

O conceito de proof-of-stake foi provavelmente introduzido pela primeira vez em um fórum de discussão sobre Bitcoin em 2011 (QuantumMechanic, 2011) onde um usuário coloca como ideia a utilização da quantidade de criptomoedas que o usuário possui “depositada” no sistema para definir qual o usuário que deve aprovar a próxima transação. Para o usuário, a fidedignidade da aceitação das transações ocorreria pois os usuários com maior posição em termos de posse e, conseqüentemente, as pessoas com maior interesse na confiabilidade do sistema, teriam uma maior chance de aprovar as transações. Os validadores do sistema não são escolhidos de maneira completamente randômica, sendo necessário que depositem uma quantidade da moeda no sistema para que se tornem validadores.

Como exemplo prático, imaginemos que a pessoa A deposite 100 unidades monetárias no sistema enquanto a pessoa B deposita 1000 unidades monetárias. No exemplo proposto, a chance de B ser escolhido para validar a próxima transação é 10x a chance de A uma vez que o valor depositado por B é 10x o valor depositado por A. O sistema, portanto, escolhe quem será o próximo a validar a transação com base na quantidade de patrimônio possuído pelos validadores em relação ao total de valor de mercado daquela moeda. (James Ray, 2018; “What is Proof of Stake?”, 2018)

Há quem descredite esse sistema por oferecer uma possibilidade de fraude caso alguém do sistema seja dono de 51% do valor daquela criptomoeda. A realidade é um pouco diferente e apresenta um desafio para que isso aconteça com as criptomoedas mais utilizadas, como a Ethereum por exemplo, uma vez que o valor de mercado delas é muito alto, é muito difícil que uma pessoa seja capaz de controlar 51% do valor de mercado da criptomoeda. (QuantumMechanic, 2011; Ramzan, [s.d.]; Simply Explained - Savjee, 2018)

O infográfico apresentado à seguir retirado e traduzido do “Lisk Academy” ilustra bem o funcionamento do Proof-of-Stake (“What is Proof of Stake?”, 2018):

# Proof of Stake

No **Proof of Stake**, cada validador deve possuir uma quantidade do sistema e deve "trancar" essa quantidade para poder ser selecionado.

**1**

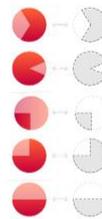
Qualquer um que tenha alguma posição da criptomoeda pode se tornar um validador, algumas vezes o valor de depósito deve ficar "trancado"



**2**

A chance de um validador ser escolhido para resolver um bloco é com base na quantidade do valor depositado por ele daquela criptomoeda.

Por exemplo, se você é dono de 1% do valor de mercado da criptomoeda, você poderia resolver 1% de todas as transações



**3**

O protocolo PoS vai randomicamente assinalar o direito de criar um bloco entre os diversos validadores selecionados de acordo com o valor depositado por eles

O validador escolhido é bonificado com uma parte ou toda a taxa de transação.

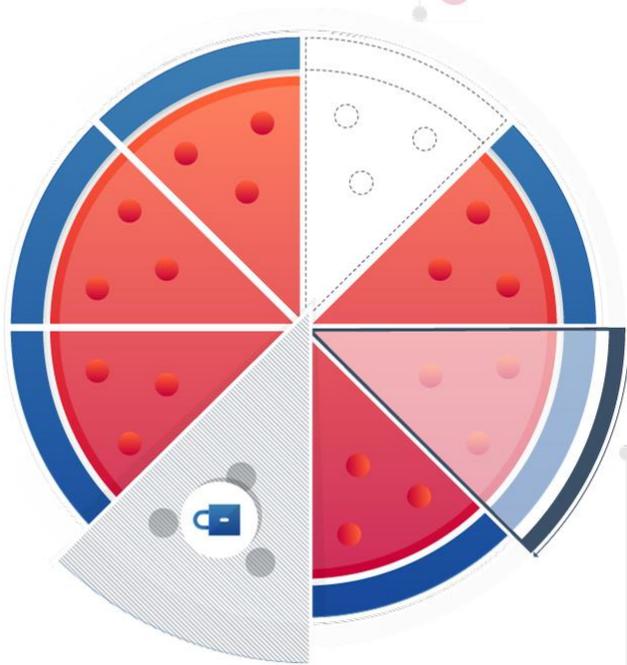


Figura 2 – Infográfico de Proof of Stake Traduzido por: Filipe Oliveira

## O Blockchain

O blockchain é um livro digital de registro de transações econômicas incorruptível que pode ser programado não apenas para registrar tais transações, mas praticamente tudo que possua um valor. (Tapscott e Tapscott, 2016)

Nesse livro de registro, comumente chamado de “Ledger”, é possível verificar todas as transações que já foram realizadas no passado, permitindo a validação de todas elas tendo em vista que todos na rede possuem tal registro.

Ao permitir a distribuição de informações digitais sem que as mesmas sejam copiadas, a tecnologia do blockchain tem revolucionado o nosso presente. Originalmente criado para server as criptomoedas, hoje a comunidade tecnológica não para de encontrar novos usos que expandem cada vez mais o potencial do blockchain.

Pode-se observar um exemplo do processo de validação de uma transação por meio do blockchain na Imagem na página seguinte traduzida do website PC World. (Alex Wawro, 2013)

## ICO – Initial Coin Offering

As criptomoedas existentes hoje e as que vierem a ser criadas tem iniciado seu processo de entrada no mercado por meio dos ICO's (Oferta Inicial de Moeda – *Initial Coin Offering*), um processo parecido com o IPO (Initial public offering) das ações na bolsa de valores ou com os processos de “crowdfunding”. Os criadores da criptomoeda tentam atrair investimentos de terceiros por meio da apresentação da ideia da criptomoeda a ser desenvolvida em forma de um “white paper”. (“How does an ICO work”, 2017)

Os desenvolvedores podem tanto determinam um número total de moedas que serão vendidas e distribuídas inicialmente durante o ICO, que costuma durar por um período de uma semana, e colocar um valor fechado para cada uma das moedas vendidas ou eles podem abrir o ICO sem determinar um valor para cada token, e ao final do ICO, o valor da moeda dependerá do valor arrecadado, ou seja, quanto maior o valor total arrecadado, maior será o valor individual de cada token. (“How does an ICO work”, 2017)

## Smart Contracts – Contratos Inteligentes

Os contratos inteligentes são muito similares aos contratos comuns utilizados pela nossa sociedade. Nos contratos normais temos duas partes que desejam realizar um acordo e o fazem por meio de uma terceira parte na qual as duas primeiras partes confiam.

Como exemplo usaremos a plataforma de “*crowdfunding*” Kickstarter onde temos as empresas tentando conseguir investimento da comunidade e uma comunidade de pessoas procurando projetos para investir seu dinheiro. Por fim temos o Kickstarter

em si, que tem como papel garantir que, caso um projeto seja completamente financiado, o dinheiro chegue às mãos da empresa procurando investimento e, caso o projeto não atinja a meta que o dinheiro volte aos investidores. Todas as partes estão conectadas por um contrato e tudo é centralizado pelo Kickstarter, que precisa ter a confiança de ambas as partes de que o dinheiro seguirá o caminho correto dependendo do resultado do financiamento.

Para o caso acima é necessário que todas as partes confiem no centralizador, o Kickstarter no caso, o que pode gerar custos adicionais para todas as partes participantes do sistema.

Imaginemos agora a mesma situação sem um regulador central, onde o papel dele é realizado por um contrato inteligente automático. O contrato teria como regra a possibilidade de financiamento de um projeto e dependendo do resultado realizaria uma ação, conforme observado na figura 4 abaixo:

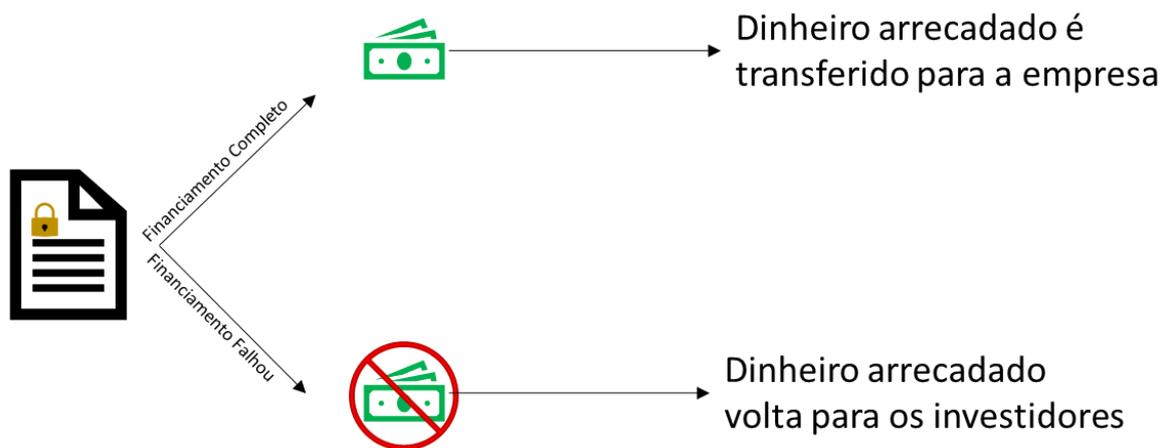


Figura 4 - Exemplo de Smart Contract

O contrato entende que quando um projeto não recebe o financiamento esperado ele retorna o dinheiro aos investidores e quando ocorre o oposto o dinheiro é liberado e transferido para a empresa buscando o financiamento. Agora a confiabilidade dos contratos inteligentes provém de seu armazenamento em um blockchain, onde herda duas propriedades de grande importância, ser imutável e distribuído. A imutabilidade significa que uma vez que o contrato é criado ele não pode mais ser modificado. Ser distribuído significa que os outputs do seu contrato são validados por todos os participantes do sistema, ou seja, uma única pessoa não poderia sozinha alterar as regras do contrato para que o dinheiro fosse liberado erroneamente pois o resto do sistema marcaria tal transação como inválida.

Portanto, um contrato inteligente é, em sua essência, um software que grava as regras de um contrato e, automaticamente o verifica para executar, quando necessário, os termos acordados. (Simply Explained - Savjee, 2017)

## Fork

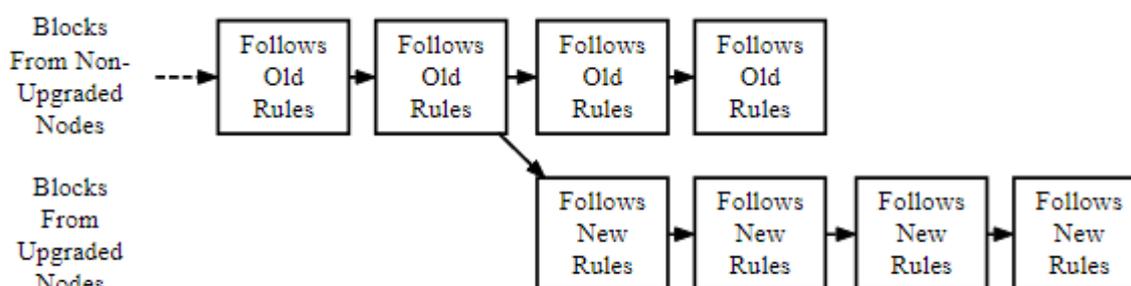
Acima definimos que as Criptomoedas são um meio de troca que se utiliza de uma tecnologia de criptografia para assegurar e validar todas as suas transações. Definimos também que para que tais transações sejam asseguradas e validadas é necessário que blocos de dados sejam minerados. Os mineradores, a fim exercer sua funcionalidade dentro desse ecossistema, utilizam softwares que permitem a comunicação entre seus hardwares e o sistema responsável pela geração dos blocos.

Diversas vezes, os desenvolvedores de uma criptomoeda decidem por realizar mudanças no código da criptomoeda que acabam gerando incompatibilidades entre as versões nova e antiga, isso leva ao chamado “hard fork”. (“Cryptocurrency”, 2014)

Há também uma segunda ocorrência que pode também levar ao “fork”, esse chamado de “acidental fork” ocorre quando os usuários acabam, devido a diferentes versões utilizadas do software acima mencionado, gerando dois livros de registros (“ledger”) diferentes, um da versão antiga e um da nova, quando isso ocorre o desenvolvedor da moeda pode escolher tentar resolver os problemas gerados e fundir os dois registros ou optar pelo “fork”. (“Cryptocurrency”, 2014)

O “fork” é importante pois pode ser implementado a fim de corrigir riscos de segurança que foram encontrados na versão antiga do software, adicionar funcionalidades à criptomoeda ou reverter transações caso algo como um Hack tenha ocorrido como foi o caso do Hack à DAO (Decentralized Autonomous Organization) no Blockchain da Ethereum. Nesse último caso, ao invés de criar uma nova moeda, as transações referentes à DAO foram “rebobinadas” para que os milhões de dólares que haviam desaparecido voltassem, e invalidando as que estavam na carteira do hacker. (CFA, 2016)

Sumarizando, o “fork” é uma mudança radical feita no protocolo que leva os usuários da versão antiga e da versão nova a seguirem dois caminhos distintos como observado abaixo:



A Hard Fork: Non-Upgraded Nodes Reject The New Rules, Diverging The Chain

(CFA, 2016)

## III. Os Principais Mercados de Troca

Podemos citar centenas de mercados de troca das Criptomoedas e suas diferenças mas vamos, no entanto, focar nos quatro principais mercados de troca em ordem de grandeza de volume nas últimas 24 horas do dia 26/12/17 de acordo com o website “Cryptocurrency Market Capitalization” que juntos representam aproximadamente 34.07% das transações (“CoinMarketCap”, 2017).

1. Bitfinex
2. Binance
3. Bittrex
4. Bithumb

## IV. A Principais Criptomoedas

O conceito utilizado para escolher as principais moedas a serem pesquisadas e estudadas para uma futura comparação com a moeda em estudo e seus diferentes padrões de valorização foi em ordem de grandeza de capitalização de mercado (“*Market Cap*”) de acordo com o website “Cryptocurrency Market Capitalization” (“CoinMarketCap”, 2017).

### Bitcoin (BTC)

A principal e mais difundida criptomoeda presente no mercado nos dias de hoje, possivelmente por ter sido a primeira a ser efetivamente utilizada em massa sem instituições financeiras, seguindo a ideia previamente apresentada por Dai Wei como “b-money”(Dai, 1998).

O Bitcoin teve sua primeira aparição em 2008 quando sua primeira moeda foi minerada por Satoshi Nakamoto, o criador do paper responsável pela criptomoeda.

### Ethereum (ETH)

Enquanto o Bitcoin vem atraindo os olhares e a atenção de traders e investidores, o blockchain ether da Ethereum foi designado com algumas características adicionais para apelar para o mundo corporativo. Tal apelo, aliado ao apoio de empresas como o JPMorgan Chase & Co, a Microsoft Corporation e a Intel Corporation, leva muitos a preverem que em 2018 o valor de mercado da Ethereum ultrapassará o da Bitcoin.

A Ethereum é uma Plataforma descentralizada que é capaz de rodar contratos inteligentes. Seu token, o Ether, é atualmente minerado por meio de um protocolo “Proof-of-Work”, mas está destinado a ser alterado para o protocolo “Proof-of-Stake”.

O paper da Ethereum foi publicado em 2013 por um jovem programador russo de nome Vitalik Buterin. No início de 2014, a empresa suíça “Ethereum Switzerland GmbH” desenvolve o primeiro projeto de software Ethereum, o que leva ao lançamento de seu ICO em 20 de julho de 2014 até 2 de setembro de 2014, um total de 42 dias, onde BTC 31.5 mil (USD 18.4 milhões na época) foram coletados,

tornando este o 2º ICO mais bem-sucedido da história. (“Ethereum (ETH) price, charts, market cap, and other metrics | CoinMarketCap”, 2017; “Ethereum Project”, 2017; “How does an ICO work”, 2017; October 18, Blockchain e Fintech, 2017)

A principal diferença entre a Ethereum e o Bitcoin é a sua capacidade de transacionar não apenas Criptomoeda, mas também os chamados contratos inteligentes e a denominada Máquina Virtual Ethereum (“*Ethereum Virtual Machine*”).(Marr, 2018)

## Ripple (XRP)

O nome “Ripple” pode ser utilizado tanto para a criptomoeda quanto para a rede de pagamentos na qual a moeda é amplamente trocada.

No caso, o modelo de negócios principal da empresa gira em torno da plataforma de pagamentos baseada em blockchain que já está em utilização por mais de 100 das maiores instituições financeiras do mundo, entre elas o Citibank, a American Express, o Santander e o Bank of America Meryll Lynch. (Browne, 2017; “rippletnet\_brochure.pdf”, [s.d.]) Esse ambiente chamado “RippleNet” permite que as instituições financeiras ao redor do mundo realizem transações financeiras intercontinentais com baixo custo e de maneira extremamente rápida.

*“RippleNet is a decentralized global network of banks and payment providers using Ripple’s distributed financial technology, which provides real-time messaging, clearing and settlement of financial transactions.”*

Os benefícios citados para as empresas que se juntarem a esse ambiente são oportunidades de novas rendas, uma diminuição dos custos totais, uma uniformização na experiência e um framework legal padronizado.

Por meio da disponibilização de produtos de pagamentos e serviços sob demanda e em tempo real, oferecidos ao varejo e aos clientes corporativos, a plataforma de pagamentos da Ripple diz aumentar as oportunidades de geração de receitas para as instituições financeiras que fizerem parte do “RippleNet”. (“rippletnet\_brochure.pdf”, [s.d.])

A diminuição dos custos totais é possível devido a um processamento mais eficiente das transações individuais além de uma liquidez menor necessária ao enviar pagamentos globalmente. (“rippletnet\_brochure.pdf”, [s.d.])

Ao utilizar a plataforma de pagamentos da Ripple, que disponibiliza a todos os participantes uma série de regras, processamento de mensagens e tecnologia padronizada, é possível uniformizar a experiência dos usuários finais com serviços de pagamentos consistentes. (“rippletnet\_brochure.pdf”, [s.d.])

Especialistas acreditam existirem cinco principais motivos para a rápida e difundida valorização da moeda em questão. Primeiramente devido à um inevitável aumento no volume de troca de altcoins e na constante entrada de novos investidores nesse mercado.

Em segundo lugar, vem as parcerias e a mídia envolvida por trás da Ripple. Por ser composta por um time de finanças, tecnologia e veteranos de Fintechs, a Ripple vem

demonstrando um entendimento claro da importância que as parcerias e a atração de novos consumidores têm para o desenvolvimento de companhias emergentes de tecnologia. (Damiani, 2017)

Há também uma grande importância atribuída ao papel da Ásia nesse cenário visto que mais da metade, mais precisamente 59.65%, das trocas realizadas nos últimos três meses foram realizadas na moeda chinesa, o Yuan Renminbi (CNY), como observado no Gráfico 1 abaixo. (Damiani, 2017; Rapoza, 2017; “XRP Charts”, [s.d.]

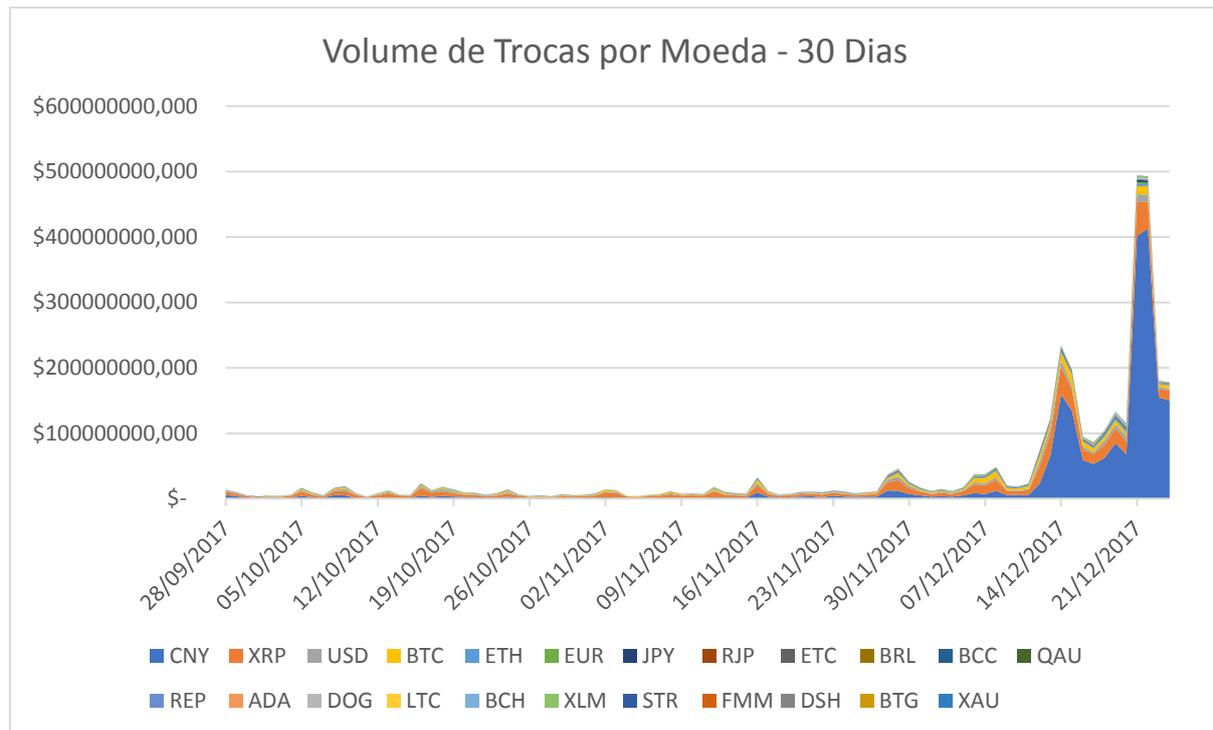


Gráfico 1

O quarto motivo seria devido a uma especulação em torno da entrada da Ripple no portfólio de criptomoedas oferecidas pela Coinbase, uma corretora de massa citada anteriormente. (Damiani, 2017)

Por último, muitas das transações de troca hoje são realizadas puramente em base de especulação, o que não é algo errado per se, o que permite que diversas altcoins com ideias inovadoras floresçam antes mesmo de se tornarem operacionais. Entretanto, isso também significa que tais moedas são apoiadas exclusivamente por suas ideias e pela fé de seu público em seu potencial, uma posição um tanto quanto perigosa em um mercado tão volátil. A criptomoeda Ripple no entanto, por ser um produto pronto, por se posicionar como uma solução para as principais instituições financeiras do mundo e por possuir alta velocidade e baixos custos de transação, tornando-se apelativa para os consumidores em geral, são características que tornam a Ripple uma moeda muito mais forte em relação às outras altcoins disponíveis, como pode-se observar na tabela a seguir. (Damiani, 2017)

	<b>Velocidade</b> <i>por transação</i>	<b>Custo</b> <i>por transação</i>	<b>Escalabilidade</b> <i>transações por segundo</i>
 XRP	3.3 segundos	USD 0.00	1,500.00 TPS
 BTC	45 minutos	USD 1.88	16.00 TPS
 ETH	4.49 minutos	USD 0.46	16.00 TPS
 BCC	60 minutos	USD 0.21	24.00 TPS
 DASH	15 minutos	USD 0.39	10.00 TPS
 LTC	12 minutos	USD 0.12	56.00 TPS

Tabela 1 - Características operacionais comparativas de criptomoedas – Filipe Oliveira

## Dogecoin (DOGE)

A DogeCoin começou em 2013 como uma brincadeira de um Australiano especialista em marketing e branding e de um programador de Portland, Oregon que combinaram os dois maiores fenômenos de 2013, a BitCoin e o “meme” do Doge (Wile, 2013). O resultado foi a criação da DogeCoin, a 11ª criptomoeda em termos de Market Cap. Essa moeda teve uma rápida ascensão em 2014 quando a moeda estava “na moda”.

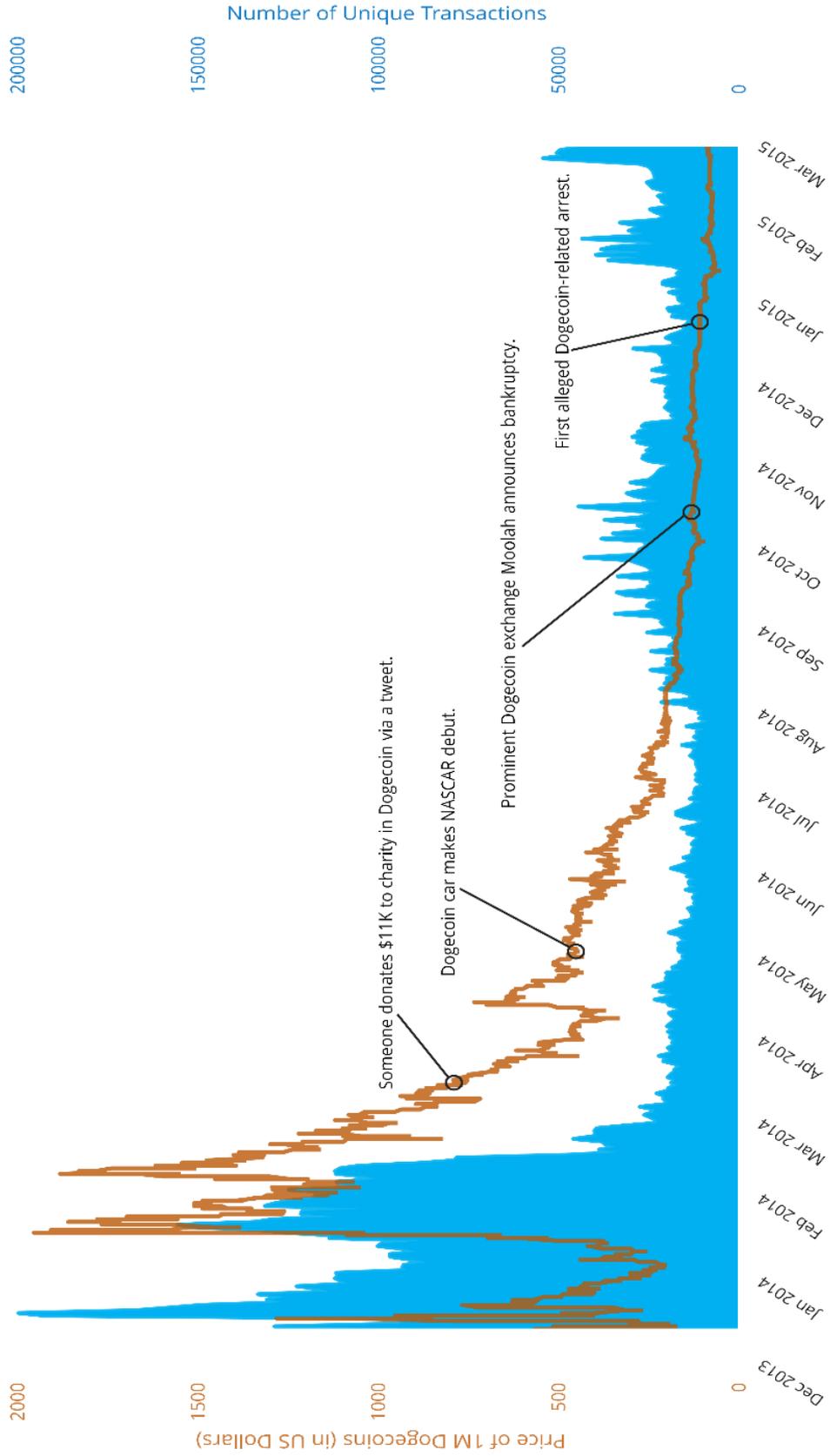
Na Figura 5 a seguir podemos observar alguns marcos históricos da DogeCoin e sua rápida valorização.

Essa criptomoeda em particular é muito utilizada por usuários do “reddit”, um site de mídia social onde usuários podem votar tanto positivamente como negativamente nas publicações de outros usuários, em suas transações. Desde o início de sua utilização a DogeCoin é muito utilizada por ser considerada uma criptomoeda de fácil acesso, por ser “barata” pode ser utilizada como gorjeta nos posts do “reddit”.

Por ter sido uma criptomoeda criada como uma suposta brincadeira, ela é muitas vezes citada como a moeda divertida (the fun currency). A Dogecoin Foundation, uma instituição voltada para realizar projetos beneficentes com a Dogecoin, realizou alguns projetos graças à comunidade dos “Shibes”, termo usado para denominar as pessoas adeptas à altcoin.

Sua rápida valorização tem sido discutida por alguns periódicos e revistas, que mostram como a massificação dessa altcoin, incentivada por sua forte comunidade concretizada no reddit, vem cada vez mais dando destaque à criptomoeda, fazendo inclusive com que seja utilizada para compras lado-a-lado a outras moedas como o Bitcoin e a Litecoin. (“An Internet Currency Joke May Turn Serious”, 2014; Reutzel, 2014; Wile, 2013)

# The History of Dogecoin



Credit: Tika Analytics/Motherboard

Data Sources: <https://bitinfocharts.com/> and <http://www.dogepay.com/>

Figura 5 – Marcos na valorização da Dogecoin

Um dos usuários do reddit começou a doar grandes quantidades de DogeCoins para os usuários em forma de gorjeta. Depois de algum tempo, o usuário acabou criando um “fundo de investimento” para criptomoedas. Por ser um usuário famoso entre a comunidade, muitos usuários acabaram adotando a ideia e deixando seus investimentos com ele. No fim, o usuário desapareceu com o dinheiro dos usuários e de seus sócios fazendo com que muitos dos usuários parassem de usar a DogeCoin.

## V. Percurso Metodológico da Pesquisa

Este capítulo possui como objetivo o detalhamento da metodologia de pesquisa aplicada no presente estudo, determinando a abordagem geral da pesquisa, sua abordagem específica, o detalhamento dos métodos utilizados para a obtenção de dados e por fim o detalhamento do método de análise de dados utilizado.

Para esse estudo, uma abordagem geral qualitativa foi utilizada, uma vez que o acreditamos que um aprofundamento nos conhecimentos das Criptomoedas se faz necessário uma vez que esse é um campo de pesquisa pouco explorado por ser um tema relativamente novo e não haver dados ou informações suficientes disponíveis para que se possa realizar um estudo quantitativo com qualidade como se pode fazer com um estudo qualitativo.

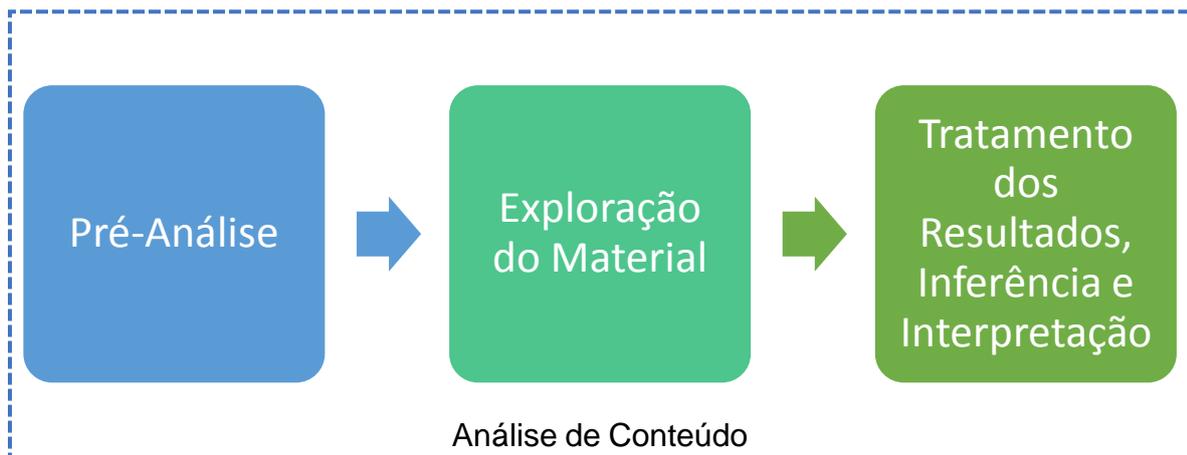
Tendo em vista o objetivo deste trabalho, a abordagem qualitativa teve caráter exploratório.

O método definido para a obtenção de dados foi o de pesquisas bibliográficas exploratórias a fim de criar uma base teórica concreta antes de iniciar as análises bibliográficas para comparar as criptomoedas acima descritas.

Utilizamo-nos da análise qualitativa de conteúdo, que é definida como uma técnica para estudar e analisar a comunicação de uma maneira objetiva, sistemática e quantitativa além de uma técnica de pesquisa para fazer inferências válidas e confiáveis de dados com relação ao seu contexto. (Collado, Sampieri e Lucio, 2006)

### Análise de Conteúdo

De acordo com Laurence Bardin, a Análise de Conteúdo tem seu processo dividido em 3 etapas, a pré-análise, a exploração do material e o tratamento dos resultados, a inferência e a interpretação, conforme mostrado a seguir:



A pré-análise se caracteriza por toda a organização e a preparação feitas antes do início da pesquisa, e tem por objetivo *operacionalizar e tornar sistemáticas as ideias iniciais* da pesquisa. (Bardin, 2011)

A Exploração do Material, de acordo com Bardin, não é nada mais do que a administração sistemática das decisões tomadas na fase de pré-análise. Durante essa fase definimos as principais categorias para a análise que foi realizada sobre cada uma das moedas.

Na fase de exploração do material, espera-se uma escolha das categorias de análise conforme o observado na fase da Pré-Análise. Bardin discorre que as categorias escolhidas devem conter fatores qualitativos enquanto são produtivas e objetivas ao tema estudado.

Por fim, a última parte se define pelo tratamento dos resultados observados na fase anterior.

Para Bardin, existem duas maneiras de se realizar o tratamento dos dados supracitado, por meio da inferência e da interpretação.

### Passos Metodológicos

Primeiramente foram definidas, com base na revisão teórica realizada, 9 categorias de análise. As mesmas podem ser encontradas abaixo na tabela 2.

As categorias de análise escolhidas foram: Número de transações por minuto; custo por transação realizada; velocidade por transação; método de validação das transações; existência de um projeto por trás do projeto e a possibilidade da utilização de “*smart contracts*”.

Com essas categorias visamos compará-los frente à rentabilidade média dos retornos diários dentro de diferentes períodos de cada uma das moedas para averiguar se essas variáveis nos possibilitam analisar o que leva a uma maior valorização de uma das criptomoedas em detrimento às demais.

Tabela de Constructos	
Tema de Pesquisa	Pontos principais observados
Número de Transações por minuto	Esta sessão consiste em analisar a eficiência de uma Criptomoeda frente às suas “competidoras” baseando-se na quantidade de transações possíveis dentro do espaço de tempo de 60 segundos.
Custo por transação realizada em USD	Esta sessão visa classificar uma Criptomoeda em relação às outras disponíveis baseando-se no custo de cada transação realizada em USD.
Velocidade por transação em segundos.	Nesta sessão analisaremos as Criptomoedas estudadas de acordo com a velocidade em segundos necessária para que cada transação se complete.
Método de validação das transações	Essa sessão visa classificar as moedas de acordo com seu método de validação de suas transações, pelo Proof-of-Work ou pelo Proof-of-Stake.
Existência de um projeto por trás da Criptomoeda.	Nessa sessão analisaremos a existência ou não de um projeto por trás da criptomoeda além da moeda em si, como um <i>crowdfunding</i> .
Possibilidade da utilização de “Smart Contracts”	Essa sessão visa analisar a possibilidade da utilização dos “ <i>Smart Contracts</i> ” no ambiente da criptomoeda em questão.
Número de mercados nos quais a criptomoeda pode ser trocada	A sessão visa quantificar o número de mercados que permite comprar ou vender a criptomoeda em questão.
Rentabilidade média nos primeiros 6 meses.	Essa sessão tem por objetivo analisar a Rentabilidade média dos retornos diários no preço de cada criptomoeda frente ao Dólar Americano (USD) durante os seus 6 primeiros meses desde a sua criação.
Rentabilidade média no primeiro ano.	Essa sessão tem por objetivo analisar a Rentabilidade média dos retornos diários no preço de cada criptomoeda frente ao Dólar Americano (USD) durante os seus 12 primeiros meses desde a sua criação.
Rentabilidade média da criação até o presente.	Essa sessão tem por objetivo analisar a Rentabilidade média dos retornos diários no preço de cada criptomoeda frente ao Dólar Americano (USD) durante toda a vida da criptomoeda desde a sua criação.

Tabela 2 – Tabela de Constructos

O próximo passo foi realizar a escolha das Criptomoedas a serem estudadas. Conforme previamente observado, as mesmas foram definidas com base em seu *Market Cap* apresentado no website “Coin Market Cap” no dia 26/12/2017.

Após feita a escolha dos objetos de estudo, cada um dos constructos foi devidamente classificado de acordo com as propriedades de cada criptomoeda a fim de entender quais levam a uma maior ou menor valorização de cada uma das mesmas.

Para realizar tal comparação as tabelas que seguem foram criadas:

<b>Tabela de Constructos</b>	<b>BTC</b>	<b>ETH</b>	<b>XRP</b>	<b>DOGE</b>
<b>Tema de Pesquisa</b>				
Número de Transações por minuto	960.00	960.00	90,000.00	1,980.00
Custo por transação realizada em USD	\$ 1.88	\$ 0.46	\$ -	\$ 0.01
Velocidade por transação em segundos	2,700.00	269.40	3.30	60.00
Método de validação das transações	PoW	PoS	Próprio	PoW
Existência de um projeto por trás da Criptomoeda.	Não	Não	Sim	Não
Possibilidade da utilização de “Smart Contracts”	Não	Sim	Não	Não
Número de mercados nos quais a criptomoeda pode ser trocada	400	400	191	284
Rentabilidade média nos primeiros 6 meses.	0.29%	1.05%	1.53%	1.71%
Rentabilidade média no primeiro ano.	0.51%	1.11%	0.51%	0.81%
Rentabilidade média da criação até o presente.	0.37%	1.07%	0.67%	0.61%

*Tabela 3 – Respostas por Criptomoeda*

<b>BTC</b>	Retorno % Médio	Desv. Pad.	<b>XRP</b>	Retorno % Médio	Desv. Pad.
183 dias	0.29%	4.41%	183 dias	1.53%	13.60%
365 dias	0.51%	6.45%	365 dias	0.51%	10.93%
1702 dias	0.37%	4.41%	1604 dias	0.67%	9.16%

<b>ETH</b>	Retorno % Médio	Desv. Pad.	<b>DOGE</b>	Retorno % Médio	Desv. Pad.
183 dias	1.05%	9.21%	183 dias	1.71%	22.12%
365 dias	1.11%	8.95%	365 dias	0.81%	16.48%
871 dias	1.07%	7.60%	1470 dias	0.61%	10.04%

*Tabela 4 – Retornos médios por criptomoeda*

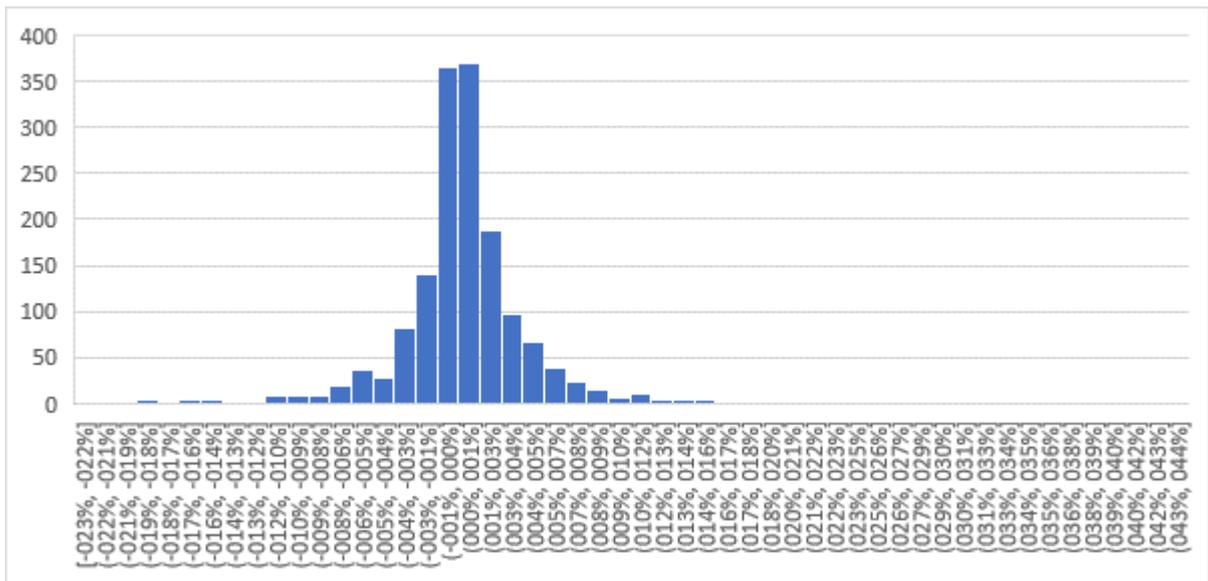


Gráfico 2 - Histograma dos Retornos Observados (BTC)

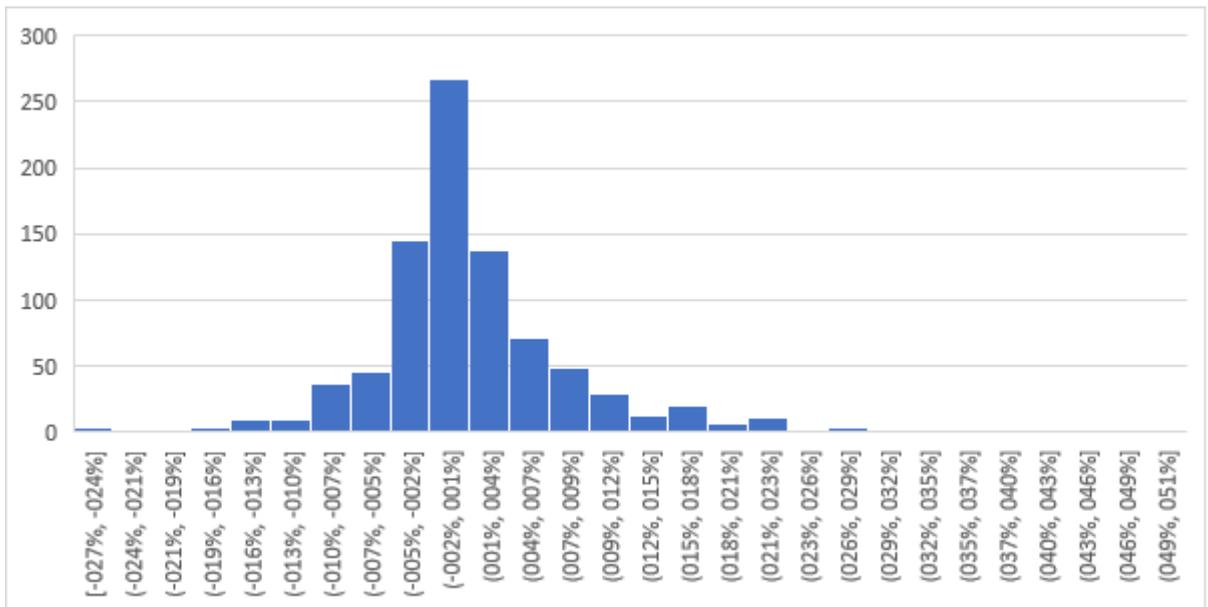


Gráfico 3 - Histograma dos Retornos Observados (ETH)

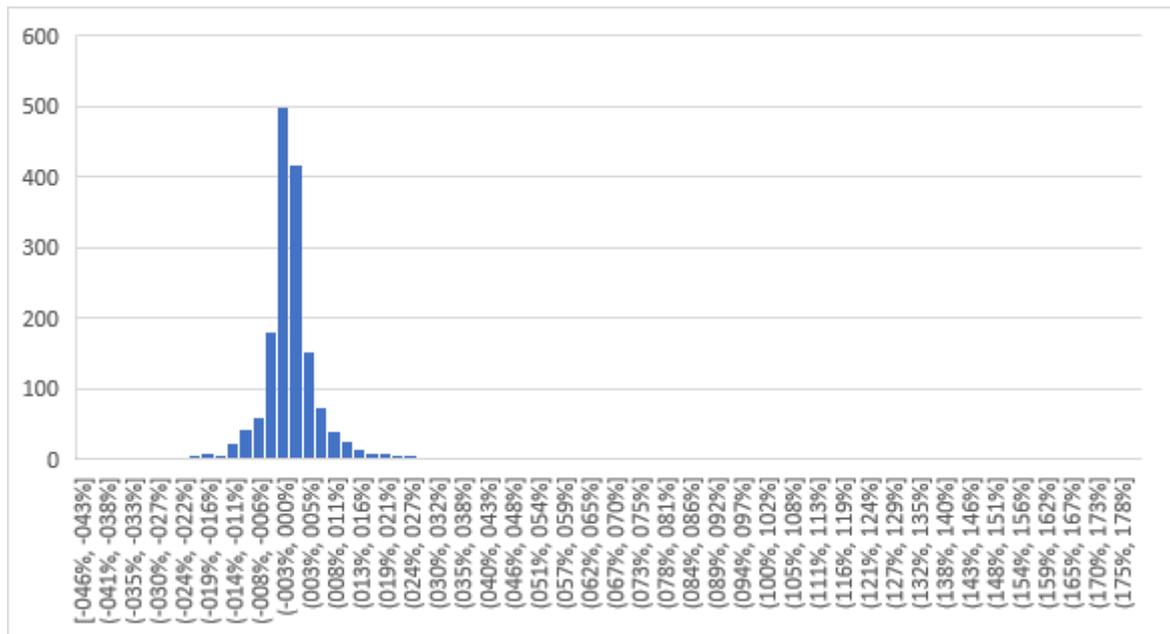


Gráfico 4 - Histograma dos Retornos Observados (XRP)

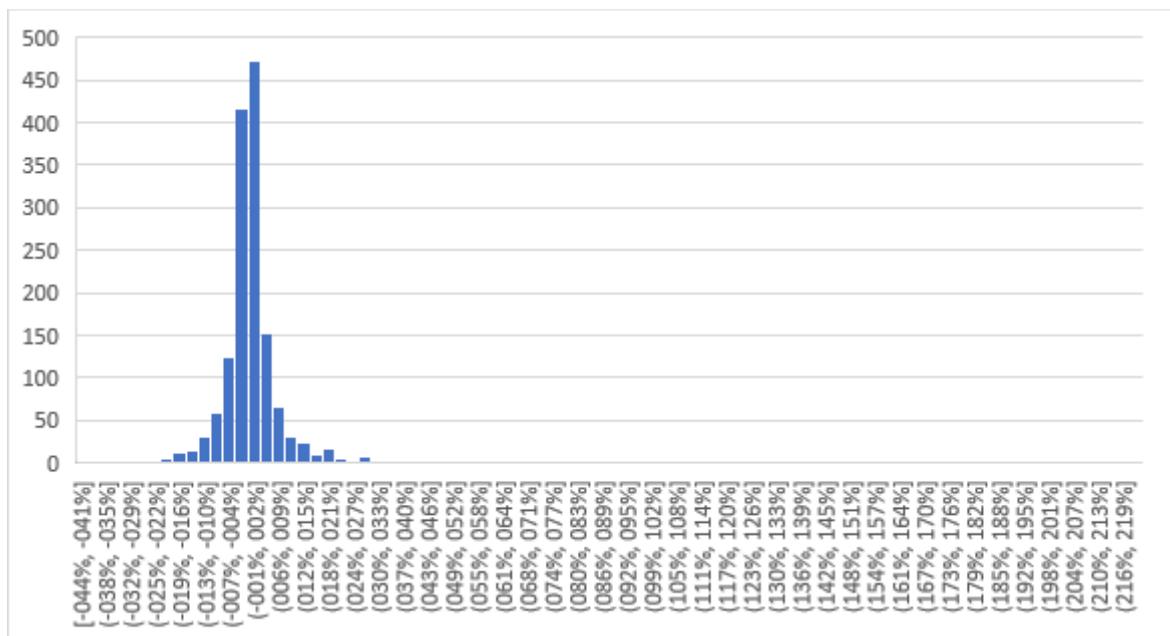


Gráfico 5 - Histograma dos Retornos Observados (DOGE)

As tabelas e gráficos acima apresentam os resultados obtidos por meio da análise do conteúdo estudado. Os histogramas representam toda a vida útil das criptomoedas até a data previamente estipulada.

## Análise Dos Dados Obtidos

É possível observarmos pela Tabela 4 acima que, entre as criptomoedas analisadas, a Bitcoin é a que possui a maior aderência à sua média de retornos com o menor desvio padrão dos retornos para os três períodos analisados, sendo teoricamente, o menos arriscado entre eles e o com menor variação de retornos. Pelo histograma da Bitcoin também é possível observarmos que ela possui uma concentração de retornos nos intervalos de -1.27% a 0.03% e de 0.03% a 1.33%. As demais criptomoedas são ainda mais voláteis, com desvios padrão chegando à 22.12% na Dogecoin por exemplo.

Os histogramas das variações de todas as criptomoedas possuem uma quantidade significativa de outliers que podem ser observados em sua maioria positivos.

Observamos também que a Ethereum foi a que manteve a rentabilidade mais alta por todo o período desde que foi criada. Acreditamos que a possibilidade de uso de Smart Contracts tenha colocado a moeda à frente das demais pois sua plataforma oferece maiores benefícios aos seus usuários. Além da possibilidade do uso dos smart contracts, a Ethereum verifica suas transações por meio do Proof-of-stake, o que pode também ter surtido efeito em uma maior rentabilidade nela. O número de mercados nos quais a moeda é utilizada pode também ter influenciado na rentabilidade superior dela.

A Ripple, apesar de possuir uma competitividade em relação à sua velocidade por transação, custo por transação realizada e número de transações possíveis por minuto, observamos uma rentabilidade média alta nos seus 6 primeiros meses, porém essa decai com o tempo.

## VI. Conclusões

Após observarmos o comportamento diário dos preços das principais criptomoedas nos principais mercados de troca durante os meses de pesquisa e diante da pesquisa bibliográfica realizada e final análise com base no método de Análise de Conteúdo verificamos características importantes desse mercado:

- a) O comportamento volátil dos ativos analisados.
- b) Indicativos de variação de preço relacionados à especulação de mercado.
- c) O aparente impacto das notícias midiáticas nos preços.
- d) As características funcionais das moedas como fator de precificação das mesmas.
- e) O volume de negociação como formador de preço.
- f) Os mercados de negociação como formador de preço.
- g) As mídias sociais e sua influência na velocidade no trânsito das informações influenciando os fatores relacionados a preço.
- h) O método de certificação de cada moeda como benefício e consequente influenciador no preço de cada moeda.

Durante nossos estudos enfrentamos dificuldades relativas à escassez de conteúdo acadêmico sobre o tema por ser ainda muito incipiente no meio acadêmico, o que, positivamente, nos levou a aprendizagens e descobertas das mais diversas sobre o tema, além de novos parâmetros que possibilitam ainda um futuro aprofundamento no tema. Esperamos que as descobertas realizadas no estudo auxiliarão todos aqueles que queriam embrenhar-se no tema futuramente.

Após estudarmos e pesquisarmos profundamente sobre o assunto nos baseando em fundamentação bibliográfica de peso e descrevendo da forma mais didática possível os termos mais usuais utilizados no ambiente das Criptomoedas, indicamos que os resultados do estudo em relação aos fatores de sucesso que levam à valorização de uma criptomoeda nos fazem crer que as características acima podem, em um estudo futuro, se provar como os principais fatores mas no presente momento os mesmos foram inconclusivos.

## Bibliografia

ABEL, A.; BERNANKE, B.; CROUSHORE, D. **Macroeconomics**. Global ed of 8th revised ed edition ed. Harlow: Pearson, 2013.

ALEX WAWRO. **7 things you need to know about Bitcoin | PCWorld**. Disponível em: <<https://www.pcworld.com/article/2033715/7-things-you-need-to-know-about-bitcoin.html>>. Acesso em: 31 ago. 2018.

An Internet Currency Joke May Turn Serious. **ISO & Agent Weekly**, v. 10, n. 15, p. 15–15, 17 abr. 2014.

ANTONOPOULOS, A. M. **Mastering Bitcoin: Programming the Open Blockchain**. 2 edition ed. Beijing Boston Farnham: O'Reilly Media, 2017.

BARDIN, L. **Análise de conteúdo**. Edição: 1 ed. [s.l.] Almedina, 2011.

BARSKI, C.; WILMER, C. **Bitcoin for the Befuddled**. 1 edition ed. San Francisco, CA: No Starch Press, 2014.

BROWNE, R. **American Express, Santander team up with Ripple on blockchain platform**. Disponível em: <<https://www.cnbc.com/2017/11/16/american-express-santander-team-up-with-ripple-on-blockchain-platform.html>>. Acesso em: 27 dez. 2017.

CFA, A. H. **Hard Fork**. Disponível em: <<https://www.investopedia.com/terms/h/hard-fork.asp>>. Acesso em: 4 jan. 2018.

COLLADO, C. F.; SAMPIERI, R. H.; LUCIO, P. B. **Metodologia de pesquisa**. 3. ed. São Paulo: McGraw-Hill, 2006.

**Como o Bitcoin funciona? - Bitcoin**. Disponível em: <[https://bitcoin.org/pt\\_BR/como-funciona](https://bitcoin.org/pt_BR/como-funciona)>. Acesso em: 30 maio. 2017.

**Cryptocurrency Market Capitalizations | CoinMarketCap**. Disponível em: <<https://coinmarketcap.com/>>. Acesso em: 27 dez. 2017.

**Cryptocurrency: What is a fork?** Disponível em: <<http://www.tech-recipes.com/rx/48517/cryptocurrency-what-is-a-fork/>>. Acesso em: 4 jan. 2018.

DAI, W. **b-money**. Disponível em: <<http://www.weidai.com/bmoney.txt>>. Acesso em: 19 maio. 2017.

DAMIANI, J. **5 Reasons Why The Ripple (XRP) Price Continues To Surge In The Face Of Crypto Market Corrections.** Disponível em: <<https://www.forbes.com/sites/jessedamiani/2017/12/22/5-reasons-why-the-ripple-price-is-going-up-so-fast-will-the-xrp-surge-continue/>>. Acesso em: 26 dez. 2017.

**Ethereum (ETH) price, charts, market cap, and other metrics | CoinMarketCap.** Disponível em: <<https://coinmarketcap.com/currencies/ethereum/>>. Acesso em: 23 nov. 2017.

**Ethereum Project.** Disponível em: <<https://www.ethereum.org/>>. Acesso em: 23 nov. 2017.

HOUAISS, A. **Pequeno Dicionário Houaiss da Língua Portuguesa.** Edição: 1ª ed. [s.l.] Moderna, 2015.

**How does an ICO work.** Disponível em: <<https://www.cryptocompare.com/coins/guides/how-does-an-ico-work/>>. Acesso em: 23 nov. 2017.

JAMES RAY. **Proof of Stake FAQs - GitHub.** [s.l.] ethereum, 2018.

MARR, B. **Blockchain: A Very Short History Of Ethereum Everyone Should Read.** Disponível em: <<https://www.forbes.com/sites/bernardmarr/2018/02/02/blockchain-a-very-short-history-of-ethereum-everyone-should-read/>>. Acesso em: 31 ago. 2018.

MINING?, W. IS B. **Everything you need to know about Bitcoin mining.** Disponível em: <<https://www.bitcoinmining.com/>>. Acesso em: 23 nov. 2017.

NAKAMOTO, S. **Bitcoin: A Peer-to-Peer Electronic Cash System,** 31 ago. 2008. Disponível em: <<https://bitcoin.org/bitcoin.pdf>>

OCTOBER 18, P. ON; BLOCKCHAIN, 2017 IN; FINTECH. **[INFOGRAPHIC] The history of Ethereum.** Disponível em: <<https://readwrite.com/2017/10/18/infographic-ethereum-history/>>. Acesso em: 23 nov. 2017.

QUANTUMMECHANIC. **Proof of stake instead of proof of work.** Disponível em: <<https://bitcointalk.org/index.php?topic=27787.0>>. Acesso em: 31 ago. 2018.

RAMZAN, Z. **Bitcoin: Proof of work,** [s.d.]. Disponível em: <<https://pt.khanacademy.org/economics-finance-domain/core-finance/money-and-banking/bitcoin/v/bitcoin-proof-of-work>>. Acesso em: 5 jan. 2018

RAPOZA, K. **Asians “Going Mad” For Ripple Coin**. Disponível em: <<https://www.forbes.com/sites/kenrapoza/2017/12/21/asians-going-mad-for-ripple-coin/>>. Acesso em: 27 dez. 2017.

REUTZEL, B. Why A Currency Based On An Internet Joke Should Be Taken Seriously. **Credit Union Journal**, v. 18, n. 14, p. 17–17, 21 abr. 2014.

**rippletnet\_brochure.pdf**, [s.d.]. Disponível em: <[https://ripple.com/files/rippletnet\\_brochure.pdf](https://ripple.com/files/rippletnet_brochure.pdf)>. Acesso em: 26 dez. 2017

SANDBURG, C. **Sandburg Range**. 1 edition ed. Place of publication not identified: Mariner Books, 2000.

SIMPLY EXPLAINED - SAVJEE. **Smart contracts - Simply Explained**, 20 nov. 2017. Disponível em: <<https://www.youtube.com/watch?v=ZE2HxTmxfrl>>. Acesso em: 31 ago. 2018

\_\_\_\_\_. **Proof-of-Stake (vs proof-of-work)**, 21 mar. 2018. Disponível em: <[https://www.youtube.com/watch?v=M3EFi\\_POhps](https://www.youtube.com/watch?v=M3EFi_POhps)>. Acesso em: 31 ago. 2018

TAPSCOTT, D.; TAPSCOTT, A. **Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World**. [s.l.] Penguin, 2016.

VIGNA, P.; CASEY, M. J. **The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order**. 1. ed. United States of America: St. Martin's Press, 2015.

**What is Proof of Stake?** Disponível em: <<https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/proof-of-stake>>. Acesso em: 31 ago. 2018.

WILE, R. **DOGECOIN: How A Thing That Started As A Joke Became The Hottest Digital Currency In The World**. Disponível em: <<http://www.businessinsider.com/what-is-dogecoin-2013-12>>. Acesso em: 18 maio. 2017.

WONNACOTT, P. **Economia**. 2 edition ed. São Paulo: Pearson, 1995.

**XRP Charts**. Disponível em: <<https://xrpcharts.ripple.com>>. Acesso em: 27 dez. 2017.