FACULDADES INTEGRADAS DE CARATINGA

CIÊNCIA DA COMPUTAÇÃO

NICOLAS AUGUSTO ALVES DO VALE

**ESTUDO ANALÍTICO DESCRITIVO SOBRE ASPECTOS ESTRUTURAIS E DE PERSPECTIVA RELACIONADOS À CRIPTOMOEDAS**

**Caratinga - MG**

**2017**

**NICOLAS AUGUSTO ALVES DO VALE**

**ESTUDO ANALÍTICO DESCRITIVO SOBRE ASPECTOS ESTRUTURAIS E DE PERSPECTIVA RELACIONADOS À CRIPTOMOEDAS**

Trabalho de conclusão de curso de Ciências da Computação apresentado à Faculdades Integradas de Caratinga, como parte das exigências da disciplina de TCC, sob orientação do Professor Vagner Aquino Zeferino.

**Caratinga - MG**

**2017**

**NICOLAS AUGUSTO ALVES DO VALE**

**ESTUDO ANALÍTICO DESCRITIVO SOBRE ASPECTOS ESTRUTURAIS E DE PERSPECTIVA RELACIONADOS À CRIPTOMOEDAS**

Trabalho de conclusão de curso de Ciências da Computação apresentado à Faculdades Integradas de Caratinga, como parte das exigências da disciplina de TCC, sob a orientação do Professor Vagner Aquino Zeferino.

Aprovada em: \_\_\_/ \_\_\_/ \_\_\_\_.

Banca Examinadora:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Profª:

Examinador FIC

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Profª:

Examinador FIC

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Prof.:

Examinador FIC

Orientador

**Caratinga-MG**

**2017**

**AGRADECIMENTOS**

À minha família, principalmente meus pais, que me deram todo o suporte necessário para meu desenvolvimento pessoal e intelectual. À todos aqueles que dedicaram seu tempo para ler meu texto e sugerir correções. Aos professores que me disponibilizaram dicas e práticas de escrita que serão de grande serventia para todo meu futuro acadêmico. À todos aqueles que acreditaram no meu potencial e sempre deram apoio nos momentos de dificuldade.

**RESUMO**

O campo do estudo criptomoedas e ativos digitais em geral é muito recente. Trata-se de uma área com muito alcance de pesquisa. As criptomoedas, com destaque no Bitcoin, revolucionaram o modo como a tecnologia de informação encara as transferências digitais, criando uma fórmula inovadora, extremamente eficiente e justa de lidar com trocas monetárias. Muitas empresas surgiram para alimentar este novo mercado, que hoje é a fonte de renda de milhares de pessoas ao redor do mundo. É um paradigma que reduz custos a um nível extremo e é lucrativo para aqueles que desejam investir. O objetivo deste trabalho é analisar os aspectos desses modelos relacionados à sua segurança, volatilidade e escalabilidade, apresentando as propostas de melhoria, as vulnerabilidades e atualizações que esses sistemas agregam.

**Palavras-chave:** descentralização, blockchain, escalabilidade, bitcoin, altcoins, volatilidade.

**ABSTRACT**

The field of study of cryptocurrencies and digital assets in general is very recent. It is an area with a lot of research scope. Crypto-currencies, especially in Bitcoin, have revolutionized the way the information technology faces digital transfers. They have created an innovative, extremely efficient and fair system for dealing with monetary exchanges. Many companies have come up to feed this new market, which today is the source of income for thousands of people around the world. It is a paradigm that reduces costs to an extreme low level and is still profitable for those who wish to invest. The objective of this work is to analyze the aspects of these models related to their security, volatility and scalability, presenting the improvement proposals, the vulnerabilities and the updates that these systems promote.

Keywords: decentralization, blockchain, scalability, bitcoin, altcoins, volatility.

**SUMÁRIO**

**1. INTRODUÇÃO...................................................................................................................12**

**2. REFERENCIAL TEÓRICO..............................................................................................14**

* 1. **Redes p2p...........................................................................................................................14**
  2. **Criptomoedas: Bitcoin e Blockchain...............................................................................15**
  3. **Árvore de Merkle..............................................................................................................20**
  4. **Modelo GARCH................................................................................................................21**
  5. **Proof-of-Work vs. Proof-of-Stake...................................................................................21**
  6. **Moeda Fiduciária………………………………………………………………………..22**

**3. METODOLOGIA...............................................................................................................24**

**4. VOLATILIDADE E LIQUIDEZ.......................................................................................28**

**4.1 Halving...............................................................................................................................29**

**4.2. Influência da China..........................................................................................................33**

**4.3 O cenário das altcoins.......................................................................................................36**

* 1. **Considerações Finais.........................................................................................................41**

**5. SEGURANÇA E CONFIABILIDADE.............................................................................43**

**5.1 Questões de Validade e Lastreio......................................................................................43**

**5.2. Legabilidade e Reconhecimento.....................................................................................44**

**5.3. Histórico de vulnerabilidades do Bitcoin.......................................................................45**

**5.4. Anonimidade....................................................................................................................46**

**5.5. Descrição de Ataques.......................................................................................................48**

**5.6. Considerações Finais........................................................................................................52**

**6. ESCALABILIDADE...........................................................................................................53**

* 1. **Ramificações da corrente (Forks) ...................................................................................55**
  2. **Lightning Network............................................................................................................58**
  3. **Raiden Network.................................................................................................................59**
  4. **Fee Market.........................................................................................................................61**
  5. **Segregated Witness (Segwit) ...........................................................................................62**
  6. **Considerações Finais.........................................................................................................63**

**7. CONCLUSÃO.....................................................................................................................65**

**8. REFERÊNCIAS BIBLIOGRÁFICAS..............................................................................67**

**LISTA DE FIGURAS**

Figura 1 - Representação da Blockchain do Bitcoin.................................................................16

Figura 2 - Representação de um Árvore de Merkle..................................................................21

Figura 3 – Representação do sistema CoinJoin........................................................................46

Figura 4 – Representação de um ataque de Delay....................................................................48

Figura 5 – Raiden Network.......................................................................................................57

Figura 6 – Raiden Network: Representação dos Nodos...........................................................58

**LISTA DE GRÁFICOS**

Gráfico 1 – Inflação do Bitcoin.................................................................................................28

Gráfico 2 – Cotação Yuan Chinês x Bitcoin.............................................................................33

Gráfico 3 – Demonstração da Lei de Metcalfe.........................................................................34

Gráfico 4 – Cotação do Ethereum.............................................................................................35

Gráfico 5 – Cotação Litecoin....................................................................................................36

Gráfico 6 – Cotação Ripple.......................................................................................................37

Gráfico 7 – Cotação Dash.........................................................................................................38

Gráfico 8 – Forks na Blockchain..............................................................................................54

Gráfico 9 – Comparativo do tamanho da blockchain com e sem as assinaturas digitais..........61

**LISTA DE TABELAS**

Tabela 1 - Parâmetros de um bloco do sistema Bitcoin............................................................16

Tabela 2 - Cabeçalho de um bloco do sistema Bitcoin.............................................................17

Tabela 3 - Parâmetros de uma transação no sistema Bitcoin....................................................17

Tabela 4 - Parâmetros de entrada numa transação do sistema Bitcoin.....................................18

Tabela 5 - Parâmetros de saída de uma transação do sistema Bitcoin......................................18

Tabela 6 – Probabilidade de sucesso em tentativas de ataque à rede Darkcoin........................50

**LISTA DE SIGLAS**

**BGP**: Border Gateway Protocol; Protocolo de Roteamento de Sistemas Autônomos;

**HYIP**: High-Yeld Investment Program (Programa de Investimento de Alto Rendimento);

**P2P**: Redes ponto-a-ponto;

**PoW**: Prova de Trabalho ou Prova de Esforço;

**PoS**: Prova de Participação;

**SMPT:** Simple Mail Transfer Protocol (Protocolo de transferência de correio simples)

1. **INTRODUÇÃO**

A área de moedas digitais é muito nova no mercado de TI, boa parte dos estudos envolvendo esse tema partem para o âmbito econômico e financeiro, ignorando o funcionamento e a evolução do software ao qual o sistema se estabelece. Na internet circula desinformação, desconfiança do público a respeito da segurança dos modelos, e, há uma relativa falta de estudos que abordem os aspectos dos sistemas de criptomoedas baseados em blockchain no geral.

A finalidade deste estudo é agregar uma série de informações pertinentes às criptomoedas. A história nos ensina que a melhor maneira de entender o presente e resolver os problemas decorridos é analizando o passado, portanto, o ponto referencial será o Bitcoin, a primeira criptomoeda lançada, que hoje se vê em um estado de vulnerabilidade perante problemas de escalabilidade e as inovações trazidas pelos seus sucessores. Além da Bitcoin, serão abordadas outras moedas que funcionam por meio metodologias estruturais diferentes, como Ethreum e a Dash. Serão revisados os caminhos pelos quais se deu a evolução dessa área e o que podemos aproveitar disso, bem como pressupor as tendências futuras desse segmento.

O campo de estudo deste projeto serão as redes descentralizadas, que também são conhecidas por redes p2p (ponto a ponto). Resumidamente, são sistemas virtuais que dependem da participação direta dos usuários para sua manutenção, pois não há um servidor central que realiza um processamento em nuvem e faz gerenciamento à alocação de memória em um banco de dados próprio.

Vão ser abordados: os tópicos relacionados a volatilidade das criptomoedas, mostrando estudos acerca do cálculo de oscilação da cotação de seus valores no mercado e fatores de influência.

A questão da segurança e da confiabilidade dos sistemas baseados em blockchain também estará catalogada. Neste tópico serão apresentados casos de vulnerabilidades e as táticas para prevenir invasões e quebrar a segurança dos usuários. Além dos métodos para se promover a anonimidade na rede.

Em uma outra seção haverá o enfoque no problema da escalabilidade do sistema do Bitcoin, apresentando os tipos de soluções que existem para atualizar e propor melhorias em sistemas descentralizados de criptomoedas. Também serão apresentadas os dois paradigmas de funcionamento das redes (Proof-of-Work e Proof-of-Stake).

Por final, esse trabalho também buscará abordar como os aspectos, econômicos e geopolíticos influenciam a área de mineração e a valorização de moedas digitais. Haverá um destaque para a exploração das tendências dos modelos de redes p2p na internet, apresentando outros sistemas que funcionam utilizando o paradigma, e como o aumento do poder computacional progressivo (Lei de Moore), está abrindo oportunidades para o surgimento de novos serviços que utilizam sistemas de blockchain.

Em países que têm enfrentado crises econômicas inflacionárias graves, como a Argentina, o Bitcoin foi a alternativa encontrada pelo mercado como uma moeda mais viável de negociar e armazenar valor em moeda.

Atualmente, já estão sendo desenvolvidos sistemas de armazenamento em nuvem e de cartório descentralizados tendo como ferramenta base a blockchain. Como alguns autores já apontaram, o mundo caminha para uma grande revolução p2p onipresente em todos setores de comunicação.

Ainda há muito o que estudar para encontrar soluções para um dos problemas que mais atrapalham a adesão às criptomoedas, que é a alta volatilidade. Em um futuro hipotético em que as taxas de oscilação sejam semelhantes às das moedas fiat mais estáveis, a utilização de carteiras virtuais provavelmente seria preferível, por serem livres do domínio estatal, mais econômicas, e seguras que os bancos convencionais.

É de grande importância o incentivo ao estudo dessa área, para promover o desenvolvimento de novas tecnologias que auxiliem na sofisticação dos modelos atuais. Dessa forma poderá ser fortalecido um senso de competitividade entre as diferentes ferramentas, algo que todos mercados deveriam expandir.

**2.** **REFERENCIAL TEÓRICO**

**2.1. Redes P2P**

As redes p2p (peer-to-peer) funcionam por meio de pares de computadores, que se comunicam entre si e estão interligados em uma estrutura descentralizada, ora se comportando como servidor, ora como cliente. Como apontado por (GONZALEZ, 2008), um par é uma entidade capaz de realizar algum trabalho útil e de comunicar os resultados desse trabalho à outra entidade da rede, seja direta ou indiretamente.

Existem três razões principais pelas quais esse modelo é atrativo. O primeiro deles é a alta escalabilidade, haja vista que as redes p2p conseguem se estabelecer com eficiência em pequenos e grandes grupos de participantes. O segundo é a resistência a ataques do tipo negação de serviço, pelo fato de estarem desvinculadas de um ponto central. E o terceiro é a liberdade dos participantes de entrarem e sair da rede sem ter uma entidade externa controlando suas transações (BARCELLOS; GASPARY).

A vantagem de uma arquitetura de rede descentralizada é que ela é bem mais difícil de ser interrompida, pois não existe mais um ponto de falha. Porém a busca neste tipo de rede é muito lenta e não é garantido que a consulta terá algum resultado, porque o arquivo desejado pode estar a uma distância muito grande para ser alcançado.(SCREMIN et al., [20??], p. 5)

Um dos problemas dessa arquitetura é a dificuldade para saber e que nó da rede um dado está agregado. Segundo (MADRUGA et al., [20??]) “Como os nós entram e saem do sistema constantemente, dados podem migrar de um nó para outro, de modo que a localização dos mesmos se torna um desafio importante”.

O NAPSTER (1999) foi o primeiro modelo de rede p2p a se popularizar mundialmente na internet. É tido por muitos como o precursor da era da pirataria na internet, tendo em vista que ele era utilizado para compartilhamento de mídias ".mp3", posteriormente sendo derrubado por órgãos governamentais. O NAPSTER era de uma arquitetura mista que possuía uma central de compartilhamento de dados. Como aponta (MADRUGA et al., [20??]) o sistema “Era genial, rápido, mas também fácil de frear. Sem o servidor, o Napster não existia, e a justiça norte-americana conseguiu fechá-lo por infringir a lei de direitos autorais”.

Em 2002 surgiu o BitTorrent que hoje é utilizado amplamente ao redor do mundo para transmissão de arquivos de diversos formatos. No BitTorrent, como foi apresentado por (FILHO, 2011), o conteúdo a ser compartilhado é dividido em várias partes que interagem com os peers. Estes se dividem em dois grupos: os seeds (aqueles que possuem uma cópia completa do arquivo e fazem o upload para outros usuários) e os leechers, que são os usuários que estão recebendo a transmissão dos seeders e realizando o upload de partes que ele já possui para outros leechers. A alta popularidade do BitTorrent e outras plataformas do tipo atraíram uma grande massa de compartilhamento de produtos piratas, o que ocasionou uma série de problemas com direitos autorais por partes de produtores de conteúdo artístico, porém a estrutura descentralizada dificultou o rastreamento em larga escala, como a banda Metallica tentou ao processar o Napster, por causas relacionados à propriedade intelectual também. Por outro lado, outras organizações adotaram o protocolo para compartilhamento original dos seus produtos na rede, como é exemplo da Blizzard (desenvolvedora de jogos online) e a Amazon (empresa de e-commerce).

Segundo (FILHO, 2011), “em um sistema P2P, os nodos estabelecem ligações lógicas e interagem através das mesmas, formando uma ‘rede de sobreposição’ ou *overlay* no nível de aplicação”. Desta forma, eles podem ser classificados quanto a organização do overlay: estruturado ou não estruturado, sendo que naqueles não-estruturados há um procedimento de aplicação em que as ligações entre os nodos ocorrem arbitrariamente conforme a expansão da rede, e esta configuração sempre teve vulnerabilidades relacionadas a escalabilidade. Nos overlays estruturados há um protocolo de combinar ids para os nodos, criando associações concisas entre os objetos, podendo agregar funções criptográficas para assegurar uma conexão segura e mapear a rede com mais rigor.

**2.2. Criptomoedas: Bitcoin e Blockchain**

O conceito de criptomoeda foi utilizado pela primeira vez em 1998 pelo usuário Wei Dan em uma lista de fórum, na qual ele sugeriu uma nova forma de moeda livre de um poder centralizador que utilizasse a criptografia para o controle das transações e da obtenção de novas unidades (CALVETTE, 2015).

No início de 2009, Satoshi Nakamoto desenvolveu um modelo de moeda virtual que utiliza um sistema p2p aliado a uma plataforma de blockchain. A blockchain é um arquivo público disponível online que armazena todas transações de Bitcoins já efetuadas desde o seu surgimento. Essas transações são organizadas em blocos que são processados em intervalos de 10 minutos em média, armazenando as movimentações entre as carteiras virtuais (virtual wallets) no período. Cada usuário da rede possui uma cópia desse arquivo, que é adquirida automaticamente no momento em que o usuário adere a rede (SWAN, 2015).

A blockchain é uma inovação popularizada pelo Bitcoin, se baseia em um mecanismo de documentação das transações que ocorrem dentro da rede, sendo validadas por todos os nós participantes. Dessa forma, sem intermediários e controle externo, é possível fazer auditoria do percurso dos tokens (unidades de moeda identificados por chave criptográfica privada). Esta ferramenta dá abertura para a criação de sistemas de contratos inteligentes, aproveitando o caráter consensual de uma escritura catalogada numa cadeia de blocos descentralizada. O software que roda a aplicação estabelece um algoritmo baseado em prova de trabalho, que exige alta carga de recursos computacionais para validação dos dados de cada bloco, sendo que ao final da consumação de cada segmento, todos participantes da tarefa recebem uma recompensa em tokens. A imagem a seguir é uma representação do funcionamento da blockchain:

Figura 1 - Representação da Blockchain do Bitcoin



Fonte: (LEWIS, 2015)

Como mostra o diagrama, os blocos são encadeados e preenchidos com dados referentes às transações sendo que no final é anexado um comando de recompensa.

A tabela apresentada a seguir apresenta com mais definição os parâmetros de um bloco na blockchain do Bitcoin:

Tabela 1 - Parâmetros de um bloco do sistema Bitcoin

|  |  |  |
| --- | --- | --- |
| **Campo** | **Descrição** | **Tamanho** |
| Número Mágico (identificador) | Sempre 0xD9B4BEF9 | 4 bytes |
| Tamanho do bloco | Número de bytes até o fim do bloco | 4 bytes |
| Cabeçalho | 6 outros campos, descritos a seguir | 80 bytes |
| Contador de transações | Inteiro positivo | 1-9 bytes |
| Transações | Uma coleção não-vazia de transações | Variável |

Fonte: (MACEDO, 2014)

O cabeçalho é composto por:

Tabela 2 - Cabeçalho de um bloco do sistema Bitcoin

|  |  |  |
| --- | --- | --- |
| **Campo** | **Descrição** | **Tamanho** |
| Versão | Versão do bloco | 4 bytes |
| Hash do bloco anterior | Hash de 256 bits do cabeçalho do bloco anterior | 32 bytes |
| Hash da raiz de Merkle | Hash de 256 bits baseado em todas as transações | 32 bytes |
| Timestamp | Segundos desde a Era Unix (1 de janeiro de 1970) | 4 bytes |
| Alvo | Número alvo para o valor do hash | 4 bytes |
| Nonce | Número de 32 bits | 4 bytes |

Fonte: (MACEDO, 2014)

A tabela abaixo apresenta os campos pertinentes às transações:

Tabela 3 - Parâmetros de uma transação no sistema Bitcoin

|  |  |  |
| --- | --- | --- |
| **Campo** | **Descrição** | **Tamanho** |
| Versão | Versão do bloco | 4 bytes |
| Contador de entradas | Inteiro positivo | 1-9 bytes |
| Entradas | Coleção de entradas | Variável |
| Contador de saídas | Inteiro positivo | 1-9 bytes |
| Saídas | Coleção de saídas | Variável |
| Expiração | Se diferente de zero e menor que 0xFFFFFFFF, número do bloco ou timestamp que expira a transação. | 4 bytes |

Fonte: (MACEDO, 2014)

Uma entrada possui a estrutura mostrada na tabela a seguir:

Tabela 4 - Parâmetros de entrada numa transação do sistema Bitcoin

|  |  |  |
| --- | --- | --- |
| **Campo** | **Descrição** | **Tamanho** |
| Hash da transação anterior | Hash duplo SHA-256 de uma transação anterior | 32 bytes |
| Índice de saída | Índice do registro de saída a ser utilizado da transação dada | 4 bytes |
| Tamanho do script | Tamanho do script do registro | 1-9 bytes |
| Script | Script para esta entrada | Variável |
| Número de sequência | normalmente 0xFFFFFFFF, irrelevante se a expiração for igual a zero | 4 bytes |

Fonte: (MACEDO, 2014)

Os campos da saída são representados a seguir:

Tabela 5 - Parâmetros de saída de uma transação do sistema Bitcoin

|  |  |  |
| --- | --- | --- |
| **Campo** | **Descrição** | **Tamanho** |
| Valor | Valor, em satoshis[[1]](#footnote-1), a ser transferido | 8 bytes |
| Tamanho do Script | Tamanho do script do registro | 1-9 bytes |
| Script | Script para esta entrada | Variável |

Fonte: (MACEDO, 2014)

Satoshi Nakamoto (2009) definiu uma moeda digital como uma cadeia de assinaturas digitais, na qual cada usuário possui seus tokens atrelados a uma chave privada e utiliza-se de uma chave pública para realizar transferências para outros. Essas transferências serão validadas agregando seus dados à cadeia de blocos citada. Ele ainda fez uma inferência de que dada a Lei de Moore, os computadores poderão acompanhar o desenvolvimento da rede conforme a dificuldade para o processamento dos blocos aumente.

A alta confiabilidade desse sistema se dá pelo fato de que sua integridade não pode ser alterada por um usuário pelo benefício próprio, já que todos outros nodos da rede possuem o arquivo original que será consultado a cada nova transação.

Uma outra abordagem para explicar o ponto vantajoso da utilização da blockchain foi apresentada por (COSTA, 2014), destacando que para alterar as informações contidas em um bloco é necessário o processamento recursivo de todos os outros da cadeia, pois cada bloco está interligado com os anteriores, o que funciona como um mecanismo de proteção, visto que obriga o malfeitor a gastar processamento computacional e muita energia para resolver todos os blocos da extensa cadeia principal, para que possa fraudar as informações do bloco, tornando mais vantajoso para os mal intencionados utilizar seus recursos para adquirir moedas ao minerar os lotes honestamente.

Como foi exposto por (KING; NADAL, 2012), o Bitcoin se estabelece num algoritmo à prova de trabalho, ou seja, é dependente do consumo de energia do minerador que irá quebrar a criptografia entorno dos blocos. Dessa forma, ao passo que a recompensa da mineração diminui, a taxa da expansão monetária diminui e eventualmente o mercado irá se mobilizar para encontrar alguma forma de compensar o gasto computacional da mineração.

Para contornar esses problemas, surgiram novas propostas para implantação de moedas com outras configurações de gerenciamento, as Altcoins. O Litecoin por exemplo, foi lançado em 2011 e uma de suas diferenças em relação ao Bitcoin é a alteração do tempo de atualização de blocos, que é em torno de 2 minutos. Dessa forma, as transações são efetuadas mais rapidamente e o retorno ao minerador também é mais ágil.

Além disso, a rede prevê a diminuição da recompensa de tempos em tempos, para que seja atingido o limite de 21 milhões de unidades de bitcoins após mais de cem anos decorridos desde o primeiro bloco (NAKAMOTO, 2008). O grande entrave dessa construção é a possibilidade de que em um futuro próximo os gastos com mineração serão muito superiores às recompensas, obrigando os mineradores a cobrarem taxas de transação maiores, correndo um certo risco de inviabilizar o sistema ou sua adoção em massa.

Após a popularização surgiram outros sistemas de criptomoedas, que são denominadas pelo termo *altcoins* (“moedas alternativas”). Como aponta (POELSTRA, 2016). uma das diferenças mais comuns que se nota nestas moedas em comparação com o Bitcoin é o aumento da frequência de blocos, devido a um mal entendimento sobre o propósito e significado das confirmações de transações, o que aumenta as chances de ramificações de suas estruturas de blockchain, tendendo a rede à centralização e fragilizando sua estrutura. Se a taxa de atualização dos blocos é muito alta, o tempo para confirmação e validação das transações pode ser insuficiente, o que afeta o desempenho do sistema. Aproximadamente 99% das altcoins são negociadas em bitcoins, apenas algumas delas como Litecoin são negociadas em moedas fiduciárias. Enquanto o tempo de processamento de cada bloco no bitcoin é de 10 minutos, no Litecoin e no Dash este foi reduzido para 2,5 minutos (AMADORI, 2015). Entre outras alterações apresentadas por (POELSTRA, 2016), destaca-se a adoção de múltiplos algoritmos de criptografia para mineração dos blocos, e a utilização de um novo modelo de funcionamento que dispensa a prova de trabalho (Proof of Work) da blockchain convencional, adotando um paradigma baseado em prova de participação (Proof of Stake).

Todas essas diferentes tecnologias de aplicação de moedas virtuais permitiram a criação de um novo mercado, a geração de um senso competitivo entre as moedas e seus investidores, em busca de um modelo ideal sustentável de dinheiro.

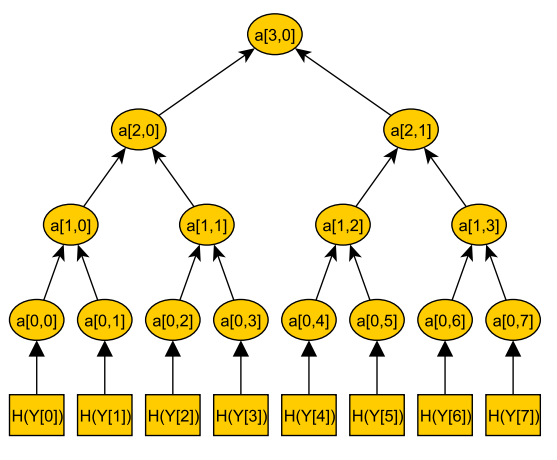
**2.3. Árvore de Merkle**

Segundo (MACEDO, 2014), “uma árvore de Merkle é uma estrutura onde as folhas sao os dados a serem processados e os nós são os valores de hash de seus filhos. Desta forma, a raiz da árvore é um valor de hash de todos os dados presentes na árvore”.

Em sistemas distribuídos, busca-se a utilização de algoritmos de hash seguros para verificar a integridade do conteúdo. A segurança resguardada pelo algoritmo permite que os sistemas recuperem o conteúdo de hosts completamente não confiáveis ​​com apenas uma pequena quantidade de metadados confiáveis. (EDEROV, 2003)

Destaca-se que muitos sistemas modernos de entrega de conteúdo peer-to-peer empregam "hashes de bloco" de tamanho fixo para fornecer um nível mais fino de granularidade em sua verificação de integridade. Além disso é necessário um estabelecimento de confiança entre os nodos para evitar fraudes, por meio da criação de uma forma de incentivo de boa conduta dentro do sistema. A imagem a seguir representa uma Árvore de Merkle com 8 nós folhas:

Figura 2 - Representação de um Árvore de Merkle



Fonte: (BECKER, 2008)

O hash do nó raiz por si só apresenta o mesmo comportamento que os hashes de arquivos completos fazem. Se o hash da raiz for recuperado de uma fonte confiável, ele pode ser usado para verificar a integridade de todo o conteúdo. E ainda mais importante, o hash de raiz pode ser combinado com um pequeno número de outros hashes para verificar a integridade de qualquer um dos segmentos de arquivo. (EDEROV, 2003)

**2.4. Modelo GARCH**

O modelo GARCH é uma técnica para cálculo de volatilidade econômica que se configura como uma generalização do modelo ARCH. Segundo (FURRIEL, 2011), esse método pertence à classe dos modelos heterocedásticos e tem grande influência e adesão em análises de séries temporais financeiras que apresentam alta volatilidade.

* 1. **Proof-of-work vs. Proof-of-Stake**

De acordo com (POELSTRA, 2014), a metodologia Proof-of-Stake, que está sendo aplicada em modelos recentes de moedas virtuais e se dá por meio de um consenso sobre os valores das carteiras de cada usuário que participa da rede. Nesse meio, cada usuário possui a capacidade de mineração de moedas proporcional à sua riqueza em moedas, eliminando assim a necessidade de gastar fortunas em eletricidade e equipamento quebrando a criptografia dos blocos (Proof of Work).

A prova de participação, como também é chamada, veio como uma alternativa ao modelo de prova de trabalho. Nessa implementação, o nó que vai participar da geração do bloco tem que provar a posse de uma certa quantia de moedas para que seja aceito na rede. Gerar blocos envolve enviar moedas para si próprio, como uma forma de provar a sua posse. (VASIN, 2014)

Por meio da prova de participação, os detentores de moeda podem bloquear sua moeda por algum tempo, validando a participação (“stake”) que é criptograficamente verificável. Logo, para ampliar e preservar o consenso, em vez de anexar uma prova de trabalho, cada participante digitalmente assina a extensão. Por razões de praticidade, tipicamente uma pequena seleção aleatória de partes interessadas é escolhido para cada uma destas extensões, e apenas uma maioria da seleção é necessária para fornecer a validação final. As partes interessadas escolhidas recebem uma recompensa e, depois de algum tempo, conseguem desbloquear sua participação se assim o desejarem. (POELSTRA, 2014)

**2.6. Moeda Fiduciária**

Destacado por (AMATO, 2004), o conceito de moeda fiduciária remonta a ideia de uma unidade monetária que não possui quase nenhum valor intrínseco, valendo-se pela confiança (do latim Fiducia) daqueles que a utilizam. Sendo a moeda o maior elemento de comunicação em massa, os países devem dedicar esforços para gerenciar, personalizar e garantir a integridade e a segurança dos seus sistemas monetários. Para isso, se utilizam de alguns elementos de segurança, como marcas d’agua e de hologramas, desenhos de fundo, tintas especiais, entre outras artimanhas que complexibilizam a tarefa de falsificar cédulas. Portanto, eventualmente os bancos centrais recolhem moedas gastas ou defeituosas substituindo-as por outras.

Sendo o dinheiro utilizando como meio de troca para negociação de bens e serviços numa sociedade, é necessário atentar para a oferta monetária deste sistema. Segundo (ROTHBARD, 1963), o volume de moeda numa econômia sempre se equipará ao valor dos bens atrelados a ela. Portanto tem-se que uma redução da oferta monetária irá aumentar a capacidade de cada unidade monetária de cumprir sua função.

Por outro lado, não importa qual seja a oferta monetária. Uma determinada quantidade de dinheiro será tão boa quanto qualquer outra quantidade. O livre mercado simplesmente se ajustará alterando o poder de compra, ou a efetividade, da unidade de ouro. Não há nenhuma necessidade de se interferir no mercado com o intuito de alterar a oferta monetária determinada pelo livre mercado.(ROTHBARD, 1963)

**3. METODOLOGIA**

Para a realização deste trabalho, o enfoque será a pesquisa bibliográfica. Trata-se de uma área na qual não é viável aplicar métricas de análise de software convencionais para utilizar como parâmetros de resultados. Quando o assunto é sistemas de criptomoedas, realizar testes de desempenho em computadores pessoais seria um desafio incalculável, e seus resultados seriam os menos confiáveis, dado à característica intrinsecamente oscilante destes modelos. Em moedas digitais, o bom desempenho do sistema depende entre outros fatores externos, o exclusivo engajamento e organização daqueles que mantém a rede. O modo de operação dos modelos (em suas respectivas categorias) é muito similar uns aos outras, o que não demanda profundas diferenças no código fonte, por exemplo. Os pontos críticos da infraestrutura estão difundidos pela rede, de maneira que é o hardware do usuários que influenciará mais na execução da tarefa de mineração.

Portanto, essa pesquisa terá abrangência analítica e descritiva, com base em aspectos comuns a todos sistemas desse tipo (redes descentralizadas de criptomoedas). Pode-se destacar características mais específicas como: paradigma de aplicação da blockchain, controle de emissão de novas unidades, tempo de atualização dos blocos, propostas de escalabilidade, além estrutura de gerenciamento da rede. Com base nesses aspectos, será feito um tratamento dos dados compilados pela pesquisa bibliográfica, a partir da apresentação dessas informações relacionadas a imposição de determinados pontos que configuram uma rede de criptomoeda, sendo aqui apresentados: volatilidade e liquidez, segurança e confiabilidade, além de escalabilidade.

Grande parte da pesquisa científica voltada para o campo das moedas digitais atenta no âmbito econômico e administrativo. Buscando entender por exemplo: os fatores que elevam o valor das criptomoedas, como se dá essa elevação, qual o nível dos riscos que os investidores tomam ao aplicar capital no sistema e também rotular papéis para esse novo paradigma. Existe um apelo por parte desses autores para o questionamento a respeito de questões jurídicas e regulamentares, algo que também será abordado nesta monografia.

Como referência bibliográfica para entender o funcionamento da blockchain, será utilizado como base o livro de Melanie Swan, intitulado Blockchain, a blueprint for a new economy. Em muitos dos trabalhos de pesquisa voltados para o campo de criptomoedas e ativos digitais, vê-se a construção de um paralelo entre moedas fiduciárias e criptomoedas. De fato, essa abordagem também estará presente neste projeto, porém de uma maneira mais prática e imparcial, para destacar como o advento dessa nova tecnologia altera definições e especificidades comuns às moedas fiat.

Desta obra, serão utilizados uma variedade de informações relacionadas a aplicações menos populares da blockchain, sendo uma das grandes propostas dessa pesquisa é explorar todas possibilidades visíveis à realidade atual para este paradigma. Entendendo a influência que determinadas metodologias de organização faz.

Por mais que a proposta deste trabalho não seja voltado para questões puramente econômicas, como já citado anteriormente. Há muito do que se aproveitar das referências daqueles que se propuseram a tomar esse rumo de pesquisa. A análise aprofundada do fenômeno da deflação nos sistemas de criptomoedas, que está relacionado com um dos tópicos do trabalho (volatilidade), exterioriza características desses sistemas que promovem direta ou indiretamente tais tendências. Ainda mais se considerar que uma pesquisa voltada para essa ocorrência também envolve de maneira abrangente, as conjecturas do sistema que atraem a recente alta de investimentos, abarcando então neste ponto o aspecto da confiabilidade

Os gráficos disponibilizados por organizações que fornecem sistema de câmbio em criptomoedas também serão de grande serventia para construção desse material. A partir deles será possível desenvolver paralelos que determinem relações entre oscilações de valorização e liquidez com a iminência da aplicação de renovações para resolver o problema da escalabilidade como o Segwit no caso do Bitcoin ou mesmo a própria oscilação do mercado internacional..

Para análises de liquidez e oscilação da moeda virtual mais popular, o portal Bitcoin, que poderíamos denominá-lo oficial, é uma fonte de vários artigos e notificações oficiais a respeito de alterações no sistema, e entendimento da blockchain que a Bitcoin utiliza.

A respeito das altcoins, academicamente falando, no geral elas são bastante generalizadas em citações. Como sendo um segmento compacto concorrente ao Bitcoin. Muito se questiona sobre a valorização destas e o possível estabelecimento de um senso de confiabilidade ímpar tal qual o Bitcoin conquistou, a ponto de serem tratadas tanto como commodities quanto moedas no sentido mais difundido do termo (para transações cotidianas entre indivíduos e empresas).

É importante ressaltar que um dos pilares primários desta pesquisa é o desmembramento dessas altcoins, não para análises isoladas, e sim para estudar as conjecturas intrínsecas a todas moedas digitais. No momento da redação desse texto já foram identificados milhares de diferentes criptomoedas. É intuitivo dizer que muitas delas compartilham caracteristicas idênticas diferindo entre si apenas o nome. Na fase a qual essa área enfrenta, as limitações de possibilidades para aplicação da blockchain induzem a adoção de um padrão quase único de operação. Se tratando de softwares de outras denominações, que permitem uma variabilidade incalculável. Dessa forma, é válido dizer que não seria proveitoso desenvolver um estudo que busque entender as configurações das criptomoedas focando em exemplares específicos.

A pesquisa também terá uma abrangência para estudar os aspectos relacionados à segurança dos modelos de criptomoedas e as decisões tomadas pelos stakeholders para solucionar problemas de anonimidade e riscos de ataques externos. É importante ressaltar a necessidade de desenvolver sistemas seguros, ainda mais quando se trata de um mercado em que estão em jogo bilhões de dólares. Esta monografia apresentará alguns tipos de ataques aos quais as redes de criptomoedas estão suscetíveis, além de mostrar um breve histórico de acontecimentos desastrosos perpetrados pela falta de segurança, principalmente no início da popularização das ferramentas.

O outro parâmetro de análise da pesquisa é o tempo de atualização e tamanho limite dos blocos e a influência que a determinação desses valores causa. Como o Bitcoin foi a moeda pioneira, é natural que ele sempre seja um ponto de referência para qualquer análise desenvolvida sobre esse tema. Em seu caso, há uma série de desdobramentos da pesquisa que surgem para complementar o estudo das modalidades de funcionamento de criptomoedas. Trata-se do Segregated Witness, popularmente abreviado para SegWit, que é uma proposta de atualização do cliente padrão denominado Bitcoin Core para aumentar a escalabilidade do sistema atual. A sua procedência vem de um desafio comum a todas criptomoedas cuja expectativa de propagação é superada, o tamanho do bloco. Tomando o padrão de limite de 1 Megabyte por bloco na blockchain, Satoshi Nakamoto (criador do Bitcoin) esperou que o volume de transações não excederia tal limite. O que tornou um pesadelo para toda a rede recentemente, pois o acúmulo de transações para um mesmo bloco tem se tornado de tal insuficiência que inevitavelmente levará a rede a um colapso.

Na presente pesquisa será feito um levantamento dos dados referentes às atualizações concorrentes para ultrapassar este obstáculo. Buscando entender o funcionamento e todos aspectos críticos dessas tomadas de decisões. Isso veio a se tornar um alvo de debate intenso na comunidade de mineradores, investidores e entusiastas, o que acarretou no surgimento de novas hipóteses articuladas por especialistas, muitos deles envolvidos no processo de desenvolvimento da atualização das plataformas, que também estarão em voga na sessão de resultados desta monografia. Essa partição envolverá a análise aprofundada dos modelos de *softfork* e *hardfork* e as propostas do Segwit e Lightning Network, entre outros. Que apontará especificidades técnicas de implementação de propostas de soft e hard-fork na rede do Bitcoin.

A questão do limite e ritmo de emissão de novas unidades de criptomoedas também configura como sendo uma das faces da pesquisa. De fato, não se pode ignorar as consequências que esse parâmetro pode performar. O Bitcoin determinou uma configuração que promove um processo denominado “halvening”, que determina que a cada 210 mil blocos minerados (o que leva cerca de 4 anos), essa recompensa de mineração diminua pela metade. O que instituiu uma curva bastante significativa de ritmo de mineração, de forma que a última das 21 milhões de unidades de bitcoins será minerada em 2140. Certamente esses números foram escolhidos por intermédio de cálculos do próprio processo de desenvolvimento. O Litecoin por exemplo, quadruplicou esse número para 84 milhões, que serão minerados em blocos de dois minutos e meio, contra os 10 minutos em que o Bitcoin está configurado.

Posteriormente também serão apresentados e documentados as implementações de masternodes, um outro arranjo organizacional que visa acelerar o processo de valorização de altcoins seguindo uma metodologia alternativa à tomada pelo bitcoin ao dificultar o processo de mineração. Nesse caso, há um grupo separado no sistema de mineradores que concentram uma fatia significativa de moedas para si, forçando uma deflação no valor das unidades restantes. A tomada dessa medida pela Piecoin elevou de maneira surpreendente o valor de cotação da moeda. Porém já pode-se associar série de fatores ao sucesso ou não desta manobra.

**4. VOLATILIDADE E LIQUIDEZ**

A volatilidade é um fator intrínseco às moedas e ativos de mercado no geral. Em uma economia dinâmica uma série de eventos pode influenciar diretamente na valorização e desvalorização dos produtos e serviços, portanto nenhum bem possui valor fixo ad eternum. Segundo (FURRIEL, 2011), “os instrumentos financeiros possuem geralmente comportamentos dinâmicos diferentes ao longo do tempo”. No que diz respeito ao cenário das criptomoedas, essas oscilações são muito intensas se comparadas ao modelo fiduciário, e os parâmetros que as promovem são de certa forma difíceis de mensurar, dado ao caráter descentralizado e anônimo destes sistemas. “A correta previsão da volatilidade é importante não só no esboço de estratégias ótimas de hedge com derivativos, como também permite captar momentos de grande incerteza no mercado”. (MORAIS; PORTUGAL, 1999)

A Escola Austríaca de Economia sempre denunciou as práticas irresponsáveis de emissão desregulada de moedas fiduciárias. Destaca-se como um grande fator que gera inflação a prática da reserva fracionada praticada pelos bancos sob resguardo dos governos que, aliados à emissão desequilibrada de novas unidades e a forte influência Keynesiana (abolição de lastro e alta oferta de crédito) do cenário mundial contemporâneo, que geram uma expansão disforme da base monetária, que eventualmente acarreta em colapsos econômicos como o de 1929.

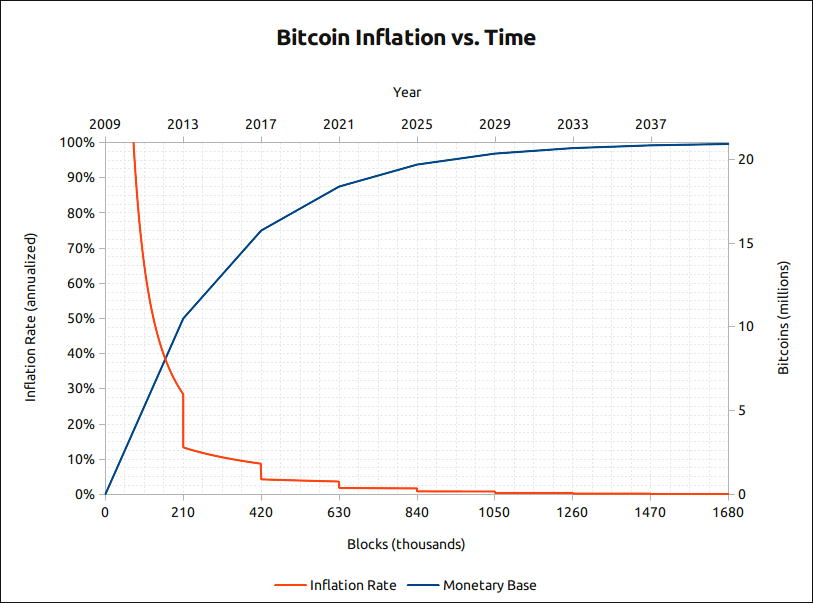
Esta foi a análise de Murray Rothbard ao falar sobre os males da intervenção estatal no setor monetário. “Fica claro que o atual arranjo monetário está longe de ser estável e seguro. Desde o estouro da última crise, o sistema monetário tornou-se ainda mais sujeito às arbitrariedades dos banqueiros centrais”(ROTHBARD, 1963). Essa emissão de moedas pode ser bem instável e imprevisível por parte dos investidores e especuladores, uma pequena variação em centavos do dólar é bastante significativa para um país como o Brasil que tem commodities cotadas nessa moeda. Em compensação, a liquidez de uma moeda como o dólar é algo de proporção global, portanto é mais difícil haver um grande desequilíbrio nesse sentido em comparação à moedas restritas à sociedades pequenas, nas quais muitas vezes há uma adoção paralela de uma moeda mais estável, como no caso de Cuba por exemplo.

**4.1 *Halving***

As moedas virtuais, como anteriormente repetido, não possuem um órgão centralizador que tome o controle de sua emissão. Nelas há um ritmo pré-estabelecido da expansão do crédito. No início do Bitcoin, a recompensa para cada bloco (atualizado em intervalos de cerca de 10 minutos), era de 50 bitcoins, desde então a cada ciclo de 4 anos (nos quais 210 mil blocos são minerados), esse número se divide pela metade. Para esse processo damos o nome de halving. Sendo assim, em 2012 a recompensa por bloco minerado passou a ser 25 bitcoins, para 12,5 em 2016 e assim sucessivamente. (NAKAMOTO, 2008)

O halving do bitcoin gera uma curva bastante acentuada na perspectiva de geração de novas unidades. É estimado que até 2040 cerca de 99% dos bitcoins já tenham sido minerados. De forma que os restantes 1% sejam disponibilizados após os próximos 80 a 100 anos seguintes. O gráfico a seguir[[2]](#footnote-2) apresenta o ritmo da expansão da base monetária do Bitcoin:

Gráfico 1 – Inflação do Bitcoin



Fonte: (Bitcoin Wiki)

Considerando o limite de bitcoins na rede de 21 milhões de unidades, vem a tona o questionamento sobre a possibilidade do valor da moeda se tornar tão alto que se dificulte a representação numérica do valor de produtos muito baratos. Isso é algo recorrente não só ao bitcoin, mas a todas criptomoedas, que nesse sentido seguem padrões semelhantes. Atualmente o bitcoin suporta uma divisão em até oito casas decimais, porém esse limite pode se estender conforme for a demanda da rede no futuro. Dessa forma, o problema se reduz apenas ao fator social das negociações, para a representação de números com muitas casas após a vírgula em etiquetas ou anúncios de lojas por exemplo.

A criptomoeda Dash (Digital Cash), apresenta um ritmo de emissão que diminui 7,1% ao ano, com um teto de 22 milhões de unidades emitidas, a recompensa por mineração dos blocos é dinâmica e o sistema de governança do sistema reserva 10% dessas unidades para fundos de pesquisa e marketing da empresa. O sistema que garante a flutuação do valor em Dash de recompensa para cada bloco é projetado para garantir que a rede nunca caia para níveis menores que 79 Gigahashes[[3]](#footnote-3) de mineração por segundo. Caso essa taxa esteja abaixo desse parâmetro, a recompensa por bloco é aumentada da mesma forma acontece o oposto se a frequência aumente bastante. (DUFFIELD et al. 2014)

Um fator agravante para esse problema do alto valor da unidade é a natural diminuição progressiva da disponibilidade de moedas no mercado por fatores externos como os usuários que por descuido ou razão de falecimento, citado por (ULRICH, 2014) como um desafio de segurança, já que nesses casos os usuários envolvidos perdem suas carteiras virtuais e as moedas aos quais a carteira estava atrelada tornam-se inutilizáveis. Essas adversidades as moedas fiduciárias não enfrentam pois os governos não definem limites intransigíveis a emissão de novas moedas. Porém há casos de desastres de grandes proporções em que há uma perda de dinheiro físico considerável que gera um impacto significativo nesse sentido. Em sua trágica viagem inaugural, o navio RMS Titanic transportava um alto volume de cargas de alto valor, desde cofres, veículos, joias, e muito dinheiro de propriedade dos empresários e imigrantes abordo. O naufrágio impactou diretamente a economia da época, assim como o atentado ao World Trade Center em Nova York. A imersão das criptomoedas no contexto virtual da internet não exclui a possibilidade de uma tragédia impelir um desajuste negativo na estrutura dos seus sistemas.

Segundo (ULRICH, 2014) a mineração nas criptomoedas adiciona um fator mercadológico que promove uma alocação responsável de recursos e uma metodologia de tomada de decisões mais prudente e responsável. Existe um incentivo por parte desses investidores para manter a rede estável e próspera, para que seja economicamente vantajoso manter a prática da mineração. Eles se beneficiam da deflação e do aumento da popularidade que gera um efeito cíclico de bom funcionamento do sistema: a moeda ganha liquidez, valoriza, ganha confiabilidade e assim adquire mais popularidade.

Esse fator de incentivo é pouco presente em moedas fiduciárias. Os governos não tem pudor para promover impressão desregulada de dinheiro. Muitas das vezes os bancos centrais tem todos os incentivos para tal, seja para o estabelecimento de acordos comerciais com grandes corporações, financiamento de campanhas políticas, guerras ou investimentos superfaturados. Todo esse descaso econômico por parte da classe política aliada aos grandes banqueiros, foi um grande fator de agravamento de grandes crises econômicas na história.

A emissão desregulada de crédito sem dúvidas sempre foi um fator preponderante nos eventos de inflação sistemática e crashing financeiros ao redor do mundo. É a grande razão pela qual as moedas fiduciárias fatalmente sempre tenderão a perder o valor com o tempo. O exemplo mais próximo dessa realidade é o real brasileiro. Na ocasião de seu lançamento, a cotação estava se equiparando ao dólar americano, e com o passar do tempo, o brasileiro teve seu poder de compra dilacerado pela inflação. Uma das causas primárias do aumento de preços é a dependência de produtos e matéria prima importados por parte da indústria nacional. Além disso, com a moeda mais fraca, a exportação de alimentos se torna mais barata para o bolso do mercado externo e assim, a oferta dentro do domínio brasileiro fica deficitária.

O segundo problema da desvalorização cambial a qual deve-se atentar é a inevitável diminuição dos índices de investimento no mercado ao qual a moeda circula. Se a moeda está em um estado de fragilidade, com a constante recessão econômica, a certeza de retorno é menor, principalmente em investimentos de longo prazo, os quais demandam um gasto maior.

O economista de escola austríaca Friedrich Hayek defendia uma filosofia de concorrência de mercado monetário difuso em todos níveis de organização política, de maneira que as pessoas tenham liberdade de utilizar a moeda que preferirem. Dessa forma elas teriam uma proteção primária contra oscilações, e os órgãos que gerenciam a expansão monetária nesse mercado teriam todos incentivos para controlar a inflação, já que os consumidores agora podem optar por outra moeda se assim for vantajoso.

No Bitcoin, a volatilidade sempre foi um fator de insegurança para quem é leigo a respeito da ferramenta. De fato, golpes online estão sendo difundidos sob os mais diversos disfarces. Nos primórdios da rede, a moeda circulava entre os entusiastas que na ocasião impuseram seus esforços para tornar o bitcoin popular e funcional em fóruns pela internet. Um caso, que talvez se configure como a primeira comercialização pública utilizando uma criptomoeda, teve início através de um post do usuário laszlo, no fórum Bitcoin Talk em maio de 2010. Ele procurava alguém que lhe vendesse 2 pizzas por 10 mil bitcoins. Na ocasião, houve um usuário que levantou a possibilidade destas pizzas valerem milhões de dólares no futuro e outro chegou a desejá-lo boa sorte em tentar ganhar pizzas grátis. Lazlo teve sucesso em sua negociação (Fonte: https://bitcointalk.org/index.php?topic=137.0). Em homenagem a esse dia a comunidade lançou o “*Bitcoin Pizza Day*”, bem como uma conta no twitter (bitcoin\_pizza) que atualiza diariamente o valor dessas pizzas em dólares.

A volatilidade é sem dúvidas uma real desvantagem da utilização de uma criptomoeda, principalmente quando falamos do bitcoin. Por mais que as transações tenham um extremo baixo custo operacional, que independe da distância que as partes envolvidas estão um do outro. As casas de câmbio de moedas fiduciárias corroem o orçamento dos turistas que fazem viagem para o exterior, principalmente nos casos em que o itinerário passa por países que usam diferentes moedas, e cada recorrência a uma casa de câmbio demanda uma taxa em cima da negociação anterior. Esse problema, assim como outros relacionados a transações financeiras entre países é facilmente contornado pela utilização de moedas digitais.

No primeiro dia de operação do bitcoin foram mineradas as primeiras 50 unidades pelo criador Satoshi Nakamoto[[4]](#footnote-4) e posteriormente com a sua popularização na internet surgiu a atualmente descontinuada Mt. Gox, a primeira casa de câmbio da moeda. Foi apenas em 2011 que o bitcoin começou a se tornar de considerável importância mercadológica e ganhar espaço da mídia e dos economistas *mainstream*.

A partir da popularização do bitcoin, a alta volatilidade fortificou a tendência da utilização dele como commodity virtual ao invés de um intermediário entre trocas comum. Afinal, tendo a moeda um caráter predominantemente especulativo, deixá-la sob custódia pode custar caro. Com o surgimento das altcoins essa corrente se firmou ainda mais. Um dos obstáculos que (YERMARK, 2013) afirmou acerca da volatilidade do bitcoin é a necessidade dos lojistas terem de adaptar constantemente o preço dos produtos, algo que não se aplica mais, pois há inúmeros softwares que dispõem o serviço de carteira virtual e podem fazer essas conversões automaticamente no momento da transação. Por outro lado, como (CERMAK, 2017) citou, o fato de que as transações não tenham efetividade instantânea, por conta do tempo para processamento dos blocos cria um outro problema na ocasião da volatilidade ser expressivamente alta, de forma que após a confirmação de uma negociação o valor transferido não corresponde mais à cotação atual da moeda. Essas suposições se tornaram realidade conforme o bitcoin exclusivamente passou a sofrer problemas de escalabilidade, a serem citados em outro capítulo, em que o tempo para efetivação das transações saiu dos esperados 10 minutos, que é o tempo que o bloco demora para ser registrado, para horas e até dias.

Pelo fato da moeda ser de caráter predominantemente deflacionário, dado o ritmo decrescente de sua adição à rede, é racional dizer que há uma tendência para que no mercado não haja uma taxa de circulação muito alta, pois isso se configura um estímulo natural para a poupança. Alguns diriam que isso é uma desvantagem, porém é importante ressaltar que o acúmulo de capital em uma sociedade é de suma importância para a alocação racional dos recursos conforme a perspectiva de investimentos dos indivíduos. É necessário poupar antes de investir, e naturalmente aqueles que não tem capacidade ou possibilidade de fazê-lo dificilmente terão êxito nos seus planos de carreira ou financeiros em geral. Portanto o acúmulo ordenado de capital é algo a se almejar em uma sociedade.

Segundo (COSTA, 2015) a volatilidade do bitcoin é alta pois seu volume ainda é baixo se comparado às moedas fiduciárias convencionais. De fato, conforme a base de mercado da moeda se expande, os esforços para criar oscilações se tornam maiores. Se uma moeda circula somente dentro de uma cidade por exemplo, é mais esperado que a sua volatilidade seja alta. Paralelamente a isso, o bitcoin e todas as altcoins vivem um momento de início de suas operações. Um outro ponto de vista a ser destacado é que o fato de que as criptomoedas em geral não passam pelo crivo das políticas governamentais de emissão, tendo sua liquidez guiada pelo próprio mercado.

**4.2. Influência da China**

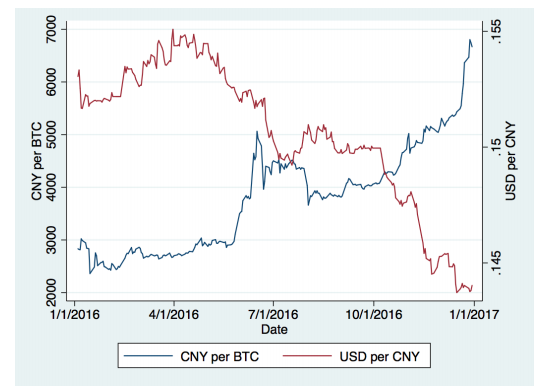
A China tem grande participação no ramo da mineração de criptomoedas, com casas de câmbio altamente ativas, principalmente quando se trata de bitcoins. Um traço secundário, muitas vezes estereotipado, da cultura chinesa moderna é a tendência a tomada de investimentos de grande risco e inclusive existe lá uma grande disseminação da prática de jogos de apostas por exemplo. Portanto é de se esperar que o mercado chinês abrace a ideia de especulação de moedas descentralizadas.

Outro incentivo para o surgimento de mineradoras na China é o baixo custo de manutenção do hardware dos processadores e também de gastos com energia elétrica, que viabilizam uma migração em massa de outras empresas que realizam esse serviço em países vizinhos para lá.

Em 2016 o valor do bitcoin sofreu um inchaço repentino de 130%, atribuido por (CERMAK, 2017) à hiperinflação na Venezuela, desvalorização monetária na Índia, a saida do Reino Unido da União Europeia (BREXIT). Estes eventos geram um grande fluxo de negociação de bitcoins por pessoas em busca de alguma forma de estabilidade financeira.

Além disso, a moeda chinesa (yuan - CNY) entrou em queda no período entre 2016 e 2017, devido ao quadro atual de emissão desregulada de crédito que gerou uma bolha imobiliária o qual os analistas mais pessimistas estão a dizer que irá gerar um colapso econômico de alta proporção. Com essa alta influência no mercado de bitcoins,(CERMAK, 2017) constatou que é possível perceber uma relação inversa de proporção de preços entre o dólar americano e o yuan chinês pela perspectiva do Bitcoin. O gráfico a seguir mostra a variação entre o yuan e o Bitcoin entre 2016 e 2017:

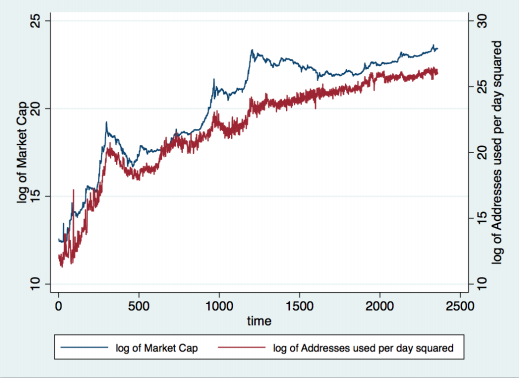
Gráfico 2 – Cotação Yuan Chinês x Bitcoin



Fonte:(CERMAK, 2017)

Em seu estudo, ele também concluiu que o Bitcoin parece obedecer a lei de Metcalfe, que apesar de ser originalmente voltada para as máquinas de FAX, pode ser aplicada num contexto de redes de ativos digitais. Ela diz que em um cenário amplo, o valor de uma rede é proporcional ao quadrado do número de usuários conectados ao sistema. Ele conseguiu correlacionar os dados de valor de mercado do bitcoin com o registro de usuários da rede por dia elevado ao quadrado, e o resultado foi bastante semelhante.

Gráfico 3 – Demonstração da Lei de Metcalfe



Fonte:(CERMAK, 2017)

Como o gráfico apresentou, a linha que representa o valor de mercado do bitcoin (linha azul) acompanha de maneira bem próxima a taxa que representa o número de usuários diários do sistema por dia elevados à segunda potência (linha vermelha).

A análise da volatilidade do bitcoin é bastante semelhante se for passada para outros ativos digitais. Como eles não possuem uma limitação territorial, se comportando como moedas globais livres de fronteiras, a metodologia de cálculo da volatilidade não deve ser a mesma que a das moedas fiduciárias que são restringidas a nível nacional. Assim, (CERMAK, 2017) atentou para estudar a participação das principais moedas em que são feitas as negociações na rede do bitcoin. Como esperado, a China foi a vencedora na disputa com o yuan, seguida do euro e do iene japonês. A metodologia utilizada foi o método GARCH de regressão e a sua conclusão foi de que a tendência de centralização do bitcoin torna a sua volatilidade suscetível ao mercado chinês, e para que ela seja verdadeiramente descentralizada não pode estar com uma disparidade tão grande de concentração de mercado como o que vemos atualmente. É certo dizer que eventos intervencionistas do governo irão influenciar diretamente a volatilidade de criptomoedas conforme a proporção de volume ao qual ela transita. No início de 2017 a China bloqueou a retirada de bitcoins dos usuários locais sob a justificativa de tentar evitar fuga de capital, uma semana após a decisão, o valor do ativo caiu em cerca de 30% e voltou a subir depois de um tempo.

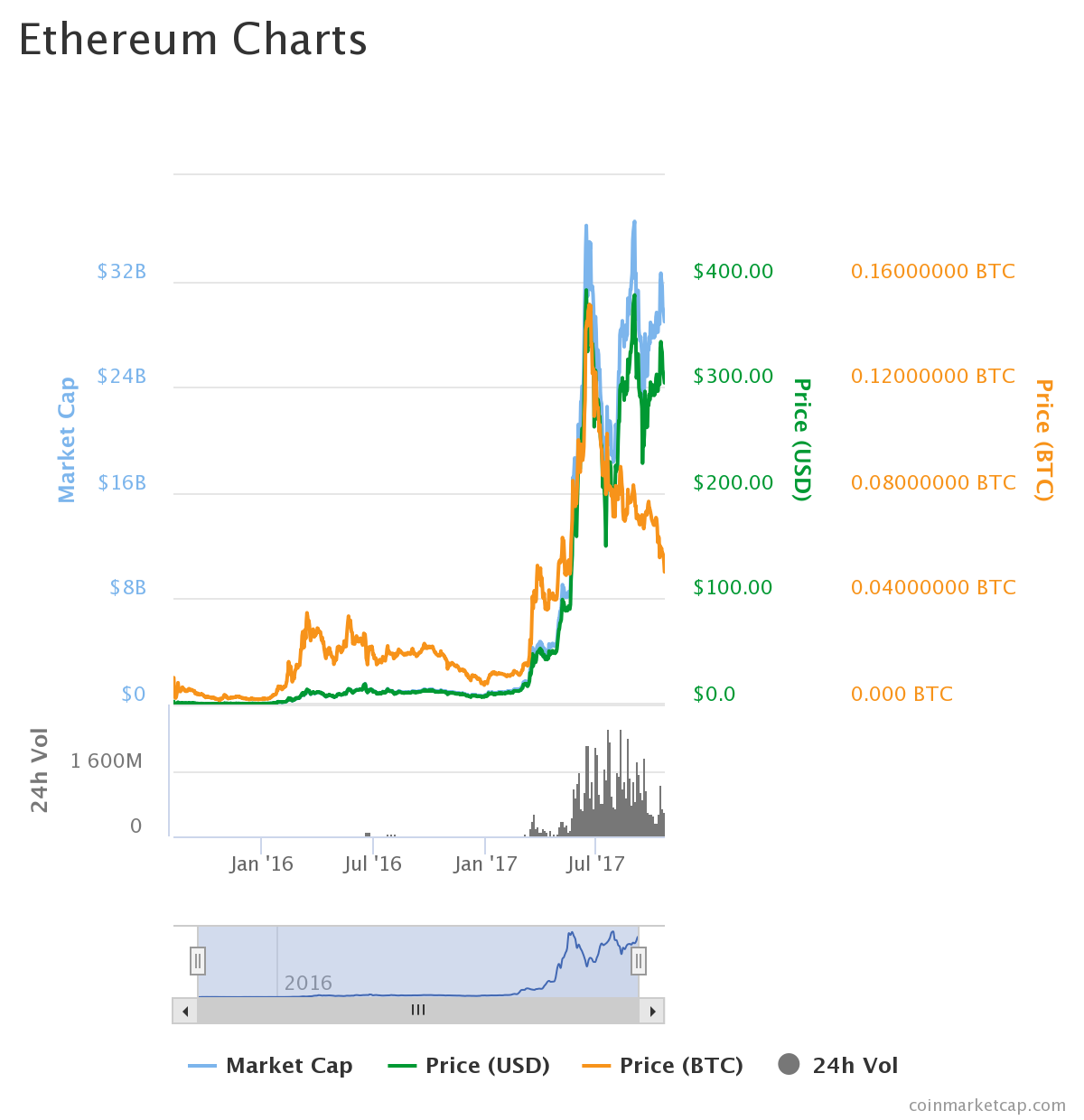
Apesar do bitcoin ter sofrido momentos de pico especulativo em 2013 e agora recentemente em 2017, a sua volatilidade tem diminuído com o passar do tempo e se seguir o ritmo atual a moeda deve alcançar um nível de estabilidade próximo ao de moedas fiat entre 2019 e 2020. Nesse cenário ela poderá satisfazer os critérios de viabilidade de utilização de uma moeda e assim passar a ter uma adoção em massa da sociedade.

Em sua pesquisa sobre a volatilidade do Bitcoin comparado a moedas fiduciárias de grande circulação, (BARBOSA, 2016) utilizando o método I-GARCH chegou a conclusão que: o. “A série analisada do Bitcoin apresentou seu indicador choque (lambda) cerca de quatro vezes maior do que a carteira e cerca de 2.2 vezes maior que a moeda Real, a mais volátil das moedas analisadas da carteira”.

**4.3. O cenário das altcoins**

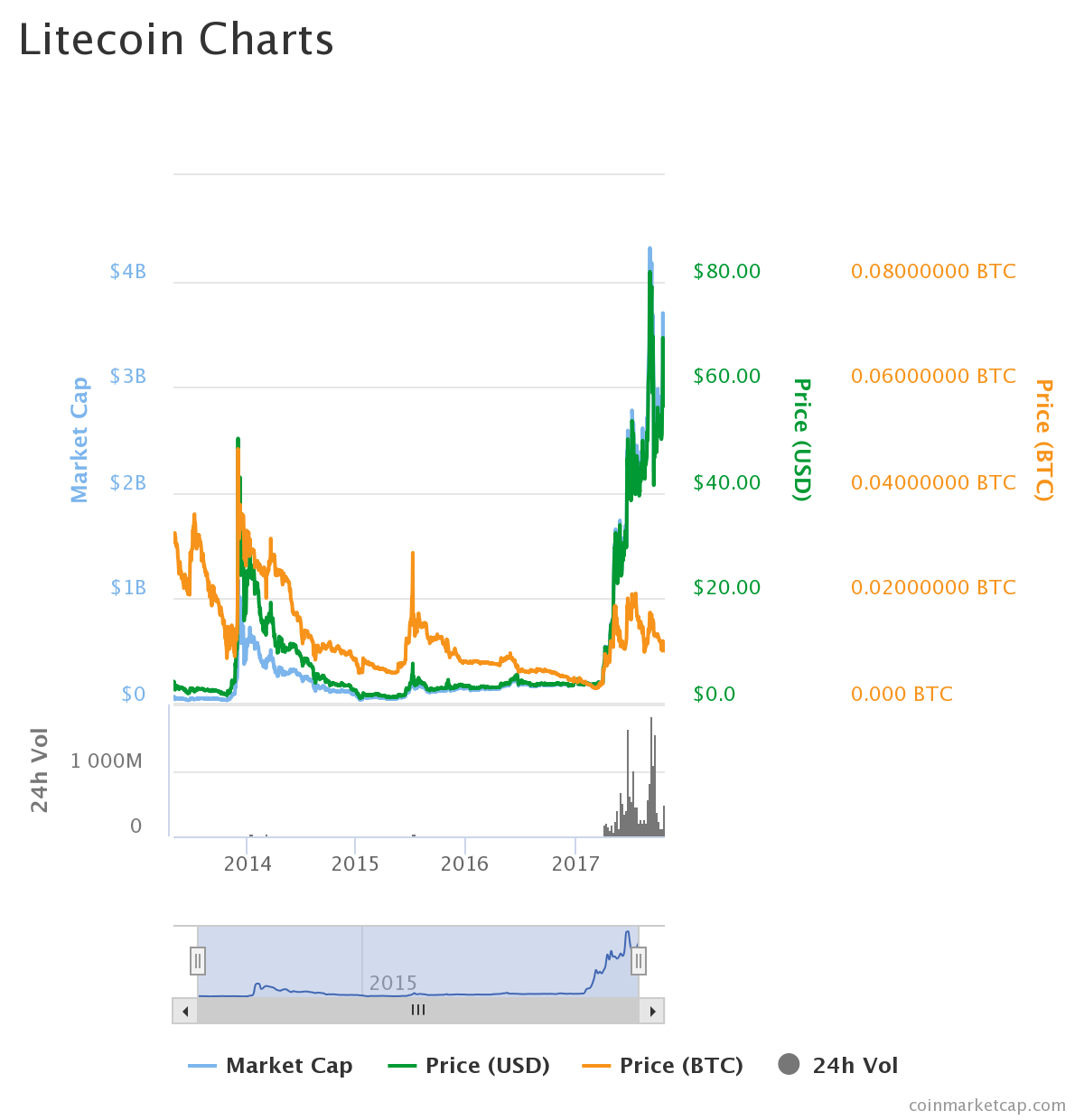
O ano de 2017 trouxe muito alvoroço no mercado de criptomoedas. Principalmente se tratando do bitcoin, que bateu o recorde de cotação no período de agosto, chegando a valores na casa dos 16 mil reais. O início dessa alta chamou atenção até da grande mídia, o que causou um fenômeno de atração de novos usuários na rede, que alimentaram o *hype* comprando mais bitcoins. Essa mesma tendência foi percebida nas principais altcoins, como mostram os gráficos a seguir:

Gráfico 4 – Cotação do Ethereum



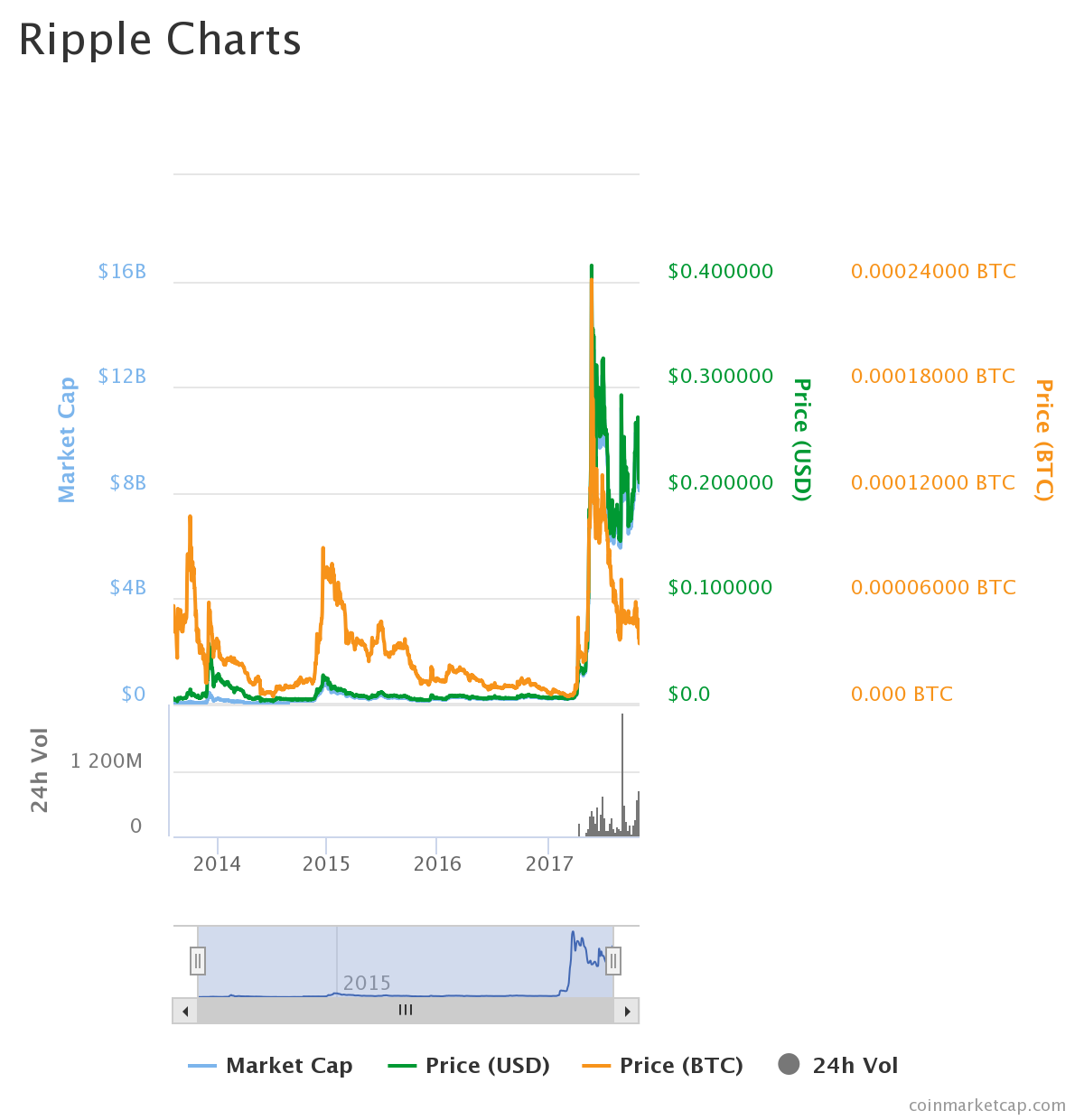
Fonte: Coinmarketcap

Gráfico 5 – Cotação Litecoin



Fonte: Coinmarketcap

Gráfico 6 – Cotação Ripple



Fonte: Coinmarketcap

Gráfico 7 – Cotação Dash



Fonte: Coinmarketcap

Os exemplos apresentados acima estão no topo da lista de criptomoedas com maior valor de mercado da atualidade. Uma delas que não está presente é o Bitcoin Cash, uma variação do Bitcoin que surgiu no meio do ano de 2017 num processo chamado de *forking* para resolver problemas de escalabilidade, portanto ainda não possui dados sólidos para análise à longo prazo. Essa questão será discutida mais à frente.

É fácil notar como as grandes variações de cotação do Bitcoin acompanham oscilações nas altcoins em diferentes níveis proporcionais. É possível chegar a conclusão que os mercados de moedas digitais são bem paralelos. De fato, é muito comum que as moedas alternativas sejam comercializadas utilizando o Bitcoin, assim como muitos dos seus mineradores trabalham constantemente aplicando seus lucros nele.

Dentro da comunidade engajada na comercialização de criptomoedas aplicam-se técnicas para maximizar lucros a partir de uma rotatividade que segue no ritmo da oscilação do valor de mercado dos ativos digitais. Dessa forma, um investidor em Litecoin por exemplo, pode vender tokens em uma fase de estabilidade para tentar investir em uma outra alternativa que está ganhando valorização.

O Ripple é um exemplo interessante de funciona diferente dos demais, pois é uma rede que se comporta mais como um sistema de pagamento utilizando um token intermediário do que uma moeda tradicional simplesmente. O seu limite de mercado é de 100 bilhões de unidades, sendo que atualmente cerca de 38 bilhões estão em circulação e 55 bilhões estão guardados em uma carteira protegida da empresa para serem liberados posteriormente (SCHWARTZ, 2014).

**4.4. Considerações Finais**

O fator volatilidade em criptomoedas é talvez o ponto que mais atrai o público em geral. Para uma grande parcela dos usuários, ferramentas como o Bitcoin tem apenas função especulativa, de maneira que suas buscas por informação técnica e especialização na área tem aplicações restritas à intencionalidade de lucrar comprando na baixa cotação e vendendo na alta. Esta realidade é utilizada como argumento pelos críticos para desqualificar os ativos digitais como meios válidos e eficientes de armazenar riqueza e realizar transações diretas sem intermediários ou órgãos centralizadores. Nota-se uma tendência forte nestas análises para uma visão estatista, intervencionista e monopolista exacerbada, por meio de um clamor por regulação e reconhecimento desnecessário por parte de órgãos políticos de esfera nacional, perpetrando a mentalidade Anticapitalista que Ludwig Von Mises sempre discorreu.

Os ativos digitais atuam como uma alternativa revolucionária ao status quo, trazendo uma nova perspectiva de manuseabilidade de recursos cambiais. Considerando-se um cenário econômico no qual uma grande parte das pessoas é dependente das jurisdições burocráticas e algumas vezes abusiva dos bancos, as criptomoedas suprem de maneira ímpar a expectativa de quem deseja armazenar dinheiro em segurança. Porém o problema da alta volatilidade torna esta tarefa um tanto quanto perigosa para desinformados e pessoas que consideram esta uma forma de investimento com alguma garantia de lucro a priori.

**5. SEGURANÇA E CONFIABILIDADE**

No mercado, as questões relacionadas a segurança deve sempre estar sob prioridade por parte de todos os lados atuantes. As criptomoedas surgiram com o propósito de oferecer um serviço que garante um altíssimo nível de resistência à fraudes. A ideia de Satoshi Nakamoto é em última instância bem simples de compreender e de um nível de solidez nunca vista antes em propostas revolucionárias relacionadas ao mundo virtual. É um paradigma que pode servir para uma série de outros serviços na busca da descentralização do poder nos sistemas. Esta é uma perspectiva importante que demorou para ser explorada. Através do paradigma do *blockchain* é possível criar sistemas eleitorais, de contratos inteligentes, de assinatura digital e muitos outros.

**5.1. Questões de Validade e Lastreio**

O primeiro questionamento do leigo no assunto é a respeito da segurança. As pessoas tendem a não confiar à primeira vista em mecanismos mirabolantes, como é a ideia de uma moeda virtual que ninguém controla e todos podem utilizar sem grandes requisitos. É possível que a desconfiança nas criptomoedas já tenha assustado muitos aspirantes na área de investimentos, assim como estimulou muitos veículos de notícia a espalharem informações negativas ora bastante coerentes e dignas de destaque, ora infundadas ou falaciosas. A seguir serão apresentadas algumas delas.

Uma recorrência nas críticas a respeito do Bitcoin em especial, é de que esta é uma moeda que não possui valor intrínseco, recorrendo ao argumento secundário a este de que a falta de lastro da moeda é um ponto negativo. Para responder a este questionamento, (ULRICH, 2014) apresentou a praxeologia como uma prerrogativa para explicar como que o valor das coisas está muito relacionado à utilidade que elas têm, portanto é algo subjetivo. Logo, o valor do bitcoin e de criptomoedas no geral, é atrelado não à propriedades físicas e químicas tangíveis, mas sim à complexidade do sistema ao qual ele está inserido que o permite ser um intermediário de trocas que atende aos atributos que valorizam uma moeda, que são: escassez, portabilidade, fungibilidade e divisibilidade.

Segundo (ULRICH, 2014), “lastro não é uma necessidade teórica de uma moeda, apenas uma tecnicalidade empírica cujo principal serviço foi o de servir como restrição às práticas imprudentes de banqueiros e às investidas inflacionistas do estado”. Na história, o ouro foi por muito tempo o padrão monetário nas negociações e com o tempo os bancos se modernizaram e passaram a adotar uma espécie de comprovante que substituía o ouro em aplicações corriqueiras no mercado. Dessa forma, dizia-se que o papel-moeda era lastreado em ouro, pois ele servia como um “vale-ouro” que representava exatamente o valor armazenado em cofre neste padrão. Posteriormente, os governos ao redor do mundo passaram a quebrar essa ligação entre o ouro e o papel e as moedas passaram a ser de curso forçado, na qual o governo faz um *enforcement* de sua utilização através de sua legislação.

**5.2. Legabilidade e Reconhecimento**

Os céticos ao mercado de criptomoedas alertam a sua falta de legabilidade e reconhecimento por parte de autoridades governamentais, apontando isso como uma possível fragilidade desse setor, já que na ocasião dos governos tentarem regular ou proibir o comércio, afetaria de maneira extremamente incisiva o mercado de ativos digitais como um todo, por mais que as moedas digitais ofereçam alto nível de anonimidade (algumas mais que outras, como será mostrado mais a frente).

Se o comércio delas passar a ser do nicho do mercado negro, haveria uma alta distorção na questão da cotação e isso inviabilizaria uma adoção em larga escala. Atualmente percebe-se mais um viés voltado para a regulamentação invés de proibição, o que não deixa de ser impactante, pois na iminência do estabelecimento de uma política regulatória para as criptomoedas, é esperado a uma adaptação no sistema tributário na intenção de englobar esse campo. Nesse caso, os custos de operação numa empresa voltada para o desenvolvimento desse setor seriam maiores, causando assim impactos negativos à respeito do crescimento do mercado e o alcance de novos clientes.

Parte desse temor acerca de uma intervenção governamental proibitiva parte do fato de que as criptomoedas podem ser utilizadas para evasão e sonegação fiscal de maneira bem mais discreta (devido ao seu caráter anônimo) do que outras formas de armazenamento de valor convencionais. Além disso, o início da popularização do Bitcoin provém da sua ampla disseminação no mercado negro na *deep web*, tendo sido utilizado como intermediário em comercializações do site “Silk Road”, uma espécie de loja virtual que permitia a venda de drogas, armas e outros produtos contrabandeados. O fechamento do site e a prisão do seu idealizador, o agorista libertário Ross Ulbricht em 2013, deixou de certa forma como herança, uma visão pessimista a respeito dos Bitcoins.

Segundo (ALBERTS; FRY, [201?]), Bitcoin não parece estar dentro da ampla definição de "contrato de investimento". Quando é realizada uma venda de Bitcoin é não há um contrato de investimento porque uma compra da Bitcoin não é um investimento em uma empresa comum e porque os compradores não devem esperar receber lucros de sua compra com base nos esforços do vendedor. O ecossistema de moeda virtual de rápido desenvolvimento envolve uma grande variedade de transações que poderiam envolver a venda de títulos dependendo de como estas transações são estruturadas, incluindo a captação de recursos para empresas Bitcoin e para moedas virtuais alternativas. Como resultado, podemos esperar que a indústria de moedas virtuais continue a gerar novas questões de direito (regulamentais) nos próximos anos conforme se modelarem as relações do público com tais ferramentas.

**5.3. Histórico de vulnerabilidades do Bitcoin**

Antes da sua primeira hipervalorização no final desse mesmo ano, o Bitcoin já tinha uma reputação deveras negativa por conta de outras falhas que ele apresentou no passado. Num site considerado a enciclopédia da moeda, estão catalogadas mais de 25 falhas e vulnerabilidades que o sistema enfrentou em sua trajetória. Cada bug recebe uma identificação que é armazenada em um banco de dados para consulta pública ( Disponível em: https://en.bitcoin.it/wiki/Common\_Vulnerabilities\_and\_Exposures).

Em julho de 2010, foram descobertas duas falhas no manuseio dos scripts de transações, o que permitiu que usuários mal intencionados pudessem gastar moedas que não possuíam.

No dia 15 de agosto de 2010, foi descoberto que o bloco da ordem 74638 continha uma transação que criou mais de 184 bilhões de bitcoin de uma hora pra outra. Pouco tempo depois o sistema foi atualizado e estabilizado na altura do bloco 74691, através de uma bifurcação na rede que criou um log distinto que invalidou a transação fraudulenta.

Em 2011 foi detectado um malware do tipo cavalo de Troia intitulado Infostealer.coinbit circulando pela internet que captura as carteiras das vítimas hospedeiras do script que utilizam o sistema operacional Windows. Ele envia as informações da carteira para o beneficiário através do servidor de SMTP smtp.wp.pl.

Muito do risco das criptomoedas em geral está atrelado a falta de fiscalização por parte de usuários que aderem a casas de câmbio não confiáveis. Nos primórdios do Bitcoin surgiu a Mt. Gox que sofreu uma invasão hacker em seus sistemas e acabou decretando falência em 2014, desaparecendo com cerca de 744.408 moedas de seus clientes, o que equivalia a cerca de quase 3 milhões de dólares. Também há um histórico de construção de esquemas de pirâmide financeira sob um eufemismo ilusório do tipo “marketing multinível” que cativam curiosos desinformados em busca de enriquecimento rápido à baixo custo.

Além disso, os usuários que não tem backups seguros de suas carteiras estão altamente suscetíveis a perderem suas posses em moedas digitais. O ideal seria guardar as chaves de autenticação em sistemas de armazenamento em nuvem distintos além de um backup de segurança físico em papel por exemplo. Vale ressaltar a desvantagem de que após perdida, uma carteira não pode ser recuperada de nenhuma forma por intermédio da rede. Atualmente no mercado existem as *hardware-wallets,* dispositivos eletrônicos semelhantes aos *flash drives* comuns que prometem assegurar as chaves criptográficas das carteiras do proprietário, assegurando ataques online ou de *keyloggers*.

Com a popularização das criptomoedas os esquemas de HYIPs, conseguiram encontrar um novo nicho de mercado. Nas moedas digitais esses sistemas se baseiam em negociações entre clientes que investem uma certa quantia para custear uma aplicação de mineração e ter retornos em curto período de tempo. A credibilidade das empresas que fornecem esse tipo de serviço é bem questionável, basta utilizar uma lógica simples: se eles têm capacidade para lucrar em escala com a mineração em nuvem, é questionável os motivos pelos quais eles iriam repartir esse lucro com investidores de baixo capital que só tornam mais complexa a logística do esquema.

**5.4. Anonimidade**

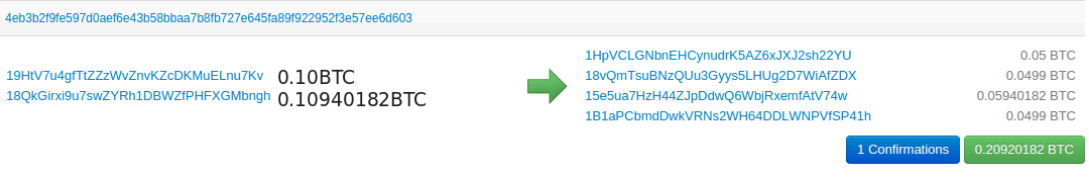
Por mais que o Bitcoin não exija dados pessoais para cadastro, seus usuários não estão completamente anônimos na rede. A *blockchain* é de acesso público, estando disponível em <https://blockchain.info>. Qualquer um pode rastrear as movimentações das moedas entre as carteiras até o momento de suas concepções através da mineração. Esse aspecto pode abrir brechas para a espionagem, da mesma forma que clientes de banco se sentiriam menos seguros se suas transações fossem públicas, ainda que sem a presença suas respectivas informações cadastrais. Vale ressaltar que não é uma tarefa impossível encontrar o vínculo entre uma identidade pessoal e uma carteira dentro do sistema da *blockchain*. Na internet todos usuários deixam rastros de suas movimentações e grande parte dos envolvidos na comercialização de moedas digitais são adeptos às casas de câmbio, que armazenam informações pessoais dos clientes. Para assegurar a sua anonimidade, um usuário deve recorrer à pseudônimos e criptografia na sua conexão através da utilização de navegadores como o Tor, que proporciona conexão anônima à internet.

Para contornar este e outros problemas, o Dash possui um sistema no qual uma parte dos seus mineradores é responsável por fazer um tipo de embaralhamento virtual das informações relacionadas às transações, tornando-as tecnicamente irrastreáveis. As moedas transacionadas são divididas em frações que dificulta o rastreio. Os Masternodes são um grupo especial dentro da rede do Dash, pois estes recebem 45% da recompensa da mineração dos blocos. Para se tornar um Masternode é necessário ter posse de 1000 unidades da moeda Dash que ficarão travadas, mas não apenas isso. Há um preço para receber essa regalia: os licenciados devem ter um IP dedicado à conexão ininterrupta com a rede, não sendo tolerado mais que 1 hora de ausência (DUFFIELD; DIAZ, 2015). Eles também estabeleceram um sistema intitulado *proof-of-service* (prova de serviço), nos quais a rede confirma a presença e a fidedignidade dos Masternodes em torno de 6 vezes ao dia. Essa é uma maneira que eles encontraram de centralizar a ação deste setor, aumentando drasticamente os requisitos para um ataque externo. Outras criptomoedas também podem aplicar um sistema análogo a este, requisitos de unidades de moeda coniventes com a cotação e o ritmo de crescimento da rede.

Após a implementação desse sistema, logo surgiram o que a comunidade chama de *pool* de Masternodes, em que usuários que não possuem o requisito de 1000 Dash na carteira se agrupam para conseguir entrar no seleto grupo, dividindo os lucros entre si. É uma prática que tem seus riscos já que há casos em que os contratos para essa associação são meramente implícitos ou algum envolvido pode conseguir falsificar a própria identidade e calotear o resto do grupo.

O Coinjoin é uma diretriz proposta por gmaxwell para incrementar a anonimidade nas transações no Bitcoin, a qual é aplicada uma metodologia que conecta duas ou mais partes que desejam realizar uma transação para apenas um destinatário e retira a correlação entre elas. Dessa forma, o rastreamento dos dados individuais de cada uma das transferências se torna uma tarefa mais complexa, pois o processo os deixou implícitos.

Figura 3 – Representação do sistema CoinJoin



Fonte: (Duffield; Dias, 2015)

Neste exemplo, o Coinjoin foi utilizado com uma transação com dois usuários. Cada um dos valores a ser negociado foi divido em outras duas partes, que somadas ao valor da taxa para efetuar a transação na rede remontam aos dois valores iniciais do lado esquerdo da imagem. (DUFFIELD; DIAZ, 2015) Destacaram que o nível de dificuldade para o rastreamento aumenta exponencialmente conforme se adicionam mais participantes nesse embaralhamento.

**5.5. Descrição de ataques**

O “ataque 51%”, como é amplamente conhecido na comunidade de criptomoedas, é uma singularidade que ocorre numa projeção em que um dos usuários da rede p2p possui domínio de mais da metade do poder de processamento do sistema. Dessa forma, assim como no mercado de ações, onde quem detém a maior parte das ações de uma empresa possui controle sobre muitas decisões estratégicas (por ter a maioria de votos), abrangendo assim seu domínio sobre o restante dos acionistas. Nas criptomoedas esse cenário também é previsto. Se um nodo possui todo esse poder de processamento ele tem o poder de validar as transações de maneira completamente arbitrária, desestabilizando todo o sistema.

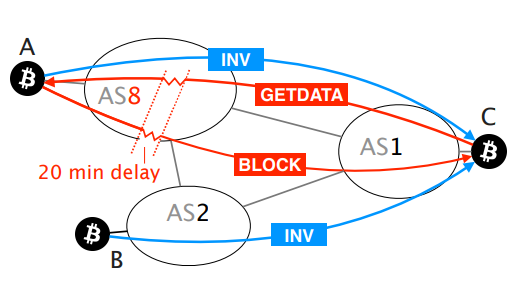
Os mecanismos para performar ataques do tipo DOS (Denial of Service, ou Negação de Serviço) em uma rede descentralizada devem ser bastante persistentes, e exigem um alto nível de investimento para tal, como no caso dos ataques à rede Etherium, em que tentava-se congestionar o sistema para tornar a rede mais lenta. Um usuário mal intencionado pode tentar um ataque de negação de serviço acumulando várias requisições de transações para si próprio na rede para tentar desestabilizá-la, porém para cada uma dessas transferências há uma taxa que se paga para efetivá-la. Na versão original do Bitcoin o limite de tamanho de cada bloco é de 1 Mb, o que restringe bastante a amplitude desse ataque. É válido dizer que os incentivos para tais invasões não costumam ser a busca por lucratividade, já que os invasores precisam aplicar muitos recursos com o objetivo de fragilizar o sistema aos quais ele deseja compensar em rentabilidade.

(ZOHAH et. al., 2017) Apresentaram uma lista de ataques possíveis na rede do Bitcoin. Vale destacar alguns deles:

Ataques de particionamento: nessa modalidade, o objetivo é desconectar um grupo de nós na rede, impedindo eles de atuarem. Eles descrevem um ataque desse tipo por meio de uma fraude no protocolo BGP (Border Gateway Protocol), que controla o roteamento de pacotes na internet. Um vácuo de tráfego poderia desconectar grande parte da rede, tornando-a mais fragilizada e suscetível ao “ataque dos 51%”.

Ataque de Delay (atraso): consiste em atrasar o contato dos nodos ao ritmo de propagação da corrente de blocos, tornando a rede suscetíveis à fraudes de gasto duplo.

Figura 4 – Representação de um ataque de Delay



Fonte: Aviv Zohah et al. (2017).[[5]](#footnote-5)

(FRANCO, 2014) destacou outros tipos de ataque que serão apresentados a frente:

O *Race Attack* descrito por Franco, ocorre quando um fornecedor aceita o pagamento de uma transferência não confirmada por meio da verificação de apenas alguns nodos da rede. O invasor pode enviar uma transação para aqueles nodos próximos ao fornecedor e um log de transação diferente para o restante da rede, como uma máscara. O sistema do Bitcoin possui um dispositivo interno chamado de *mempool,* que é uma redução do termo *Memory Pool*. Ocorre que quando uma nova transação está para ser efetivada, ela é verificada por toda a cadeia de nodos disponível no momento, que realizará uma validação e transporte dos dados da transação para este repositório de memória, para ser incluído no próximo bloco da corrente dinamicamente. Segundo (FRANCO, 2014), para se proteger desse ataque o fornecedor deveria esperar que esta transação esteja catalogada em pelo menos um bloco, já que um evento de gasto duplo de uma transação é bem improvável se a porção majoritária dos nodos já tenham uma transação válida em sua *mempool*. Ele destacou ainda o perigo de se salvar todas as transações incluindo as conflitantes de forma deliberada, pois isso poderia ser extensivamente utilizado em um ataque em que o invasor congestiona a rede com várias cópias ilegítimas da mesma transação.

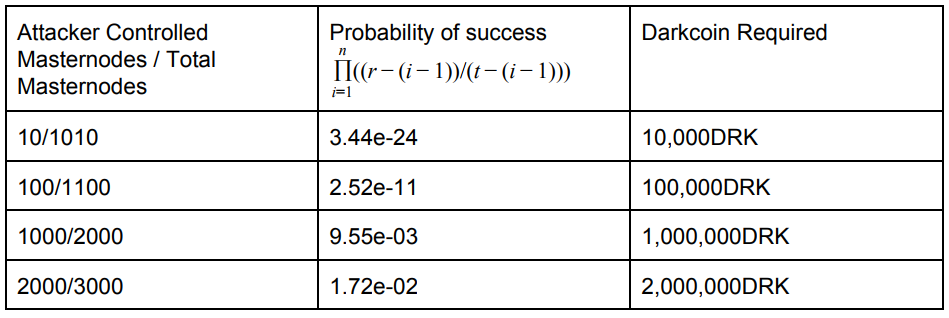
O ataque de Finney, apontado por (FRANCO 2014) recebe o nome de seu descobridor. Nessa estratégia, o atacante minera um bloco que possui uma transação para si próprio porém não transmite este bloco e envia as mesmas moedas para outro usuário, que confirma a transação porém nessa hora ele efetua a transmissão do bloco que possui a transferência cujo destinatário é ele mesmo, sobrescrevendo a operação na qual as moedas iriam para este segundo usuário.

Entretanto há muita chances de falha dessa implementação, já que um outro minerador pode encontrar esse bloco e impedir o golpe. Uma defesa contra essa irregularidade seria a exigência de duas confirmações por parte do beneficiário.

O Dash desenvolveu o sistema Darksend, no qual se adota o Coinjoin descrito acima. Quando um usuário deseja realizar um envio de moedas para outro na rede são selecionados aleatoriamente os Masternodes que irão efetivar o embaralhamento da transferência, isso diminui as chances de um suposto espião coincidir com a vítima que ele deseja explorar. Em todo caso, para reduzir ainda mais os riscos nessas situações, esse sistema também tem um dispositivo que retransmite os dados de um grupo de outros usuários que desejam efetuar operações para outro *Masternode*. Ao receber esses dados, se este for um elemento mal intencionado na comunidade, não oferecerá risco para as vítimas, pois as informações relacionadas às transações foram misturadas.

A probabilidade de se conseguir efetuar um ataque depende da quantidade de nodos sobre o domínio de quem deseja fazê-lo. De acordo com (DUFFIELD et al., 2014), com o custo de 1000 Darkcoins para se associar ao grupo, é muito caro o investimento para ter chances razoáveis de ser eleito em uma determinada demanda de trocas pelo sistema de transações travadas e fraudá-la. Para ter a probabilidade de 1,72% de ser escolhido para um bloco específico, é necessário controlar dois terços da rede de *Masternodes*. Esse tal golpista deveria adquirir controle de 2000 *Masternodes*. Como mostra a tabela a seguir[[6]](#footnote-6):

Tabela 6 – Probabilidade de sucesso em tentativas de ataque à rede Darkcoin



Fonte: (Duffield et al., 2014);

O Monero, que surgiu em 2014 possui um sistema denominado *ring signature* o qual as transações são confirmadas sem revelar os dados dos envolvidos.

A moeda Zcash, trouxe mais uma inovação nesse sentido. Em seu sistema as informações das negociações não são sequer divulgadas, ficando por conta da própria rede a tarefa de criptografar esses dados. Em sua *blockchain* as únicas informações disponíveis para rastreio são relacionadas ao horário das transações.

A rentabilidade da atividade mineradora no Bitcoin em CPUs comuns se tornou ineficiente em um curto período de tempo. Os mineradores logo perceberam que os lucros que eles acumulavam eram menores que os gastos com energia elétrica e eventualmente com manutenção de seus equipamentos. Logo, o aparato técnico de hardware teve que ser ampliado, popularizando o que a comunidade chama de “Rig de mineração”, que são máquinas mais arrojadas, com múltiplos processadores, conectadas a sistemas de refrigeração sincronizados, que funcionam dia e noite na tarefa de validar a blockchain. Atualmente, a concorrência na mineração do Bitcoin chegou a um nível tão alto que até mesmo com todo esse investimento em processamento, nem sempre é viável arriscar nessa moeda. Em consequência disso, os proprietários dos Rigs passaram a se dedicar às Altcoins, conforme a oscilação dos valores da cotação destes ativos e a equalização dos seus gastos de manutenção.

A consequência dessa tendência foi uma crescente centralização da rede do Bitcoin para as mãos dos grandes investidores, uma considerável parte desse pacote vem da China, como já citado anteriormente, onde muitas vezes, secretamente, se instalam salões equipados com máquinas do tipo ASIC (sigla para circuitos integrados para aplicação específica).

Essa centralização da rede é vista de uma maneira pessimista. Afinal a filosofia intencional da ideia do Bitcoin foi oferecer o máximo de descentralização. Conforme o poder da rede ganha acúmulo nas mãos de poucos, torna-se mais fácil que esses destruam o caráter democrático do sistema, impondo seus interesses com mais rigor em detrimento dos outros. Para tentar evitar ou pelo menos prorrogar esse processo em seu sistema, o Dash utiliza o modelo criptográfico citado por (DUFFIELD; DIAZ, 2015) pelo nome de “x11”, que de acordo com eles permitem que variantes de sistemas mineradores atuem com algum nível de viabilidade.

A confiabilidade de uma rede de criptomoedas está intimamente relacionada aos esforços da rede em controlar o gasto duplo, o que em muitos dos casos implica na metodologia *Proof-of-Work* (prova de esforço), na qual a criptografia atua como um inibidor de um ataque que busca tirar a validez das transações. A ideia proposta pelos idealizadores da Darkcoin (precursora do Dash), foi ter um segmento pessoal responsável para realizar uma vigilância dentro da rede, impedindo essas fraudes. Em outro aspecto desse modelo também seria agregado a possibilidade de bloquear transações com determinados atributos reconhecidos como não aceitáveis.

**5.6. Considerações Finais**

O paradigma das criptomoedas é muito recente e ainda não se solidificou de forma abrangente todas as nuances de brechas de segurança que elas podem apresentar. É esperado que no início do desenvolvimento de uma nova tecnologia surjam falhas mais ingênuas que serão contornadas de forma pontual em ocasiões futuras. Essa é a realidade que vivemos hoje pela ótica da evolução dos sistemas web por exemplo. No início da expansão digital, a circulação de dados pessoais e de caráter sigiloso das organizações e governos mundo afora pela internet foi um chamativo para indivíduos mal intencionados em busca de capturar tais informações e utilizar para o benefício próprio. Com o passar dos anos a questão da segurança foi vista com mais seriedade e as práticas de implementação de sistemas de defesa foram se modernizando, e hoje de maneira análoga, esse cenário se repete com os ativos digitais.

A respeito da confiabilidade dos modelos, as opiniões se dividem e muitas vezes se levantam controvérsias variadas. A abstração da ideia de um sistema descentralizado que se autorregula, sendo potencialmente seguro contra invasões externas é de difícil sintetização para uma grande parte das pessoas. Tem-se uma abertura para mais uma analogia, desta vez remontando o início da popularização dos cartões de crédito, que na ocasião causou grande desconfiança popular.

Em contrapartida, ainda é muito cedo para tomar conclusões definitivas sobre o quão seguro são as redes de criptomoedas e até que ponto elas serão de acesso viável. Vale ressaltar que novas modalidades de ataque podem surgir, e a centralização da rede pode ser um indicador de risco para o que o futuro trará para este mercado.

**6. ESCALABILIDADE**

A abrangência do Bitcoin entre 2009 e o início de 2010 era bem restrita. O sistema criado por Satoshi Nakamoto tinha pouca relevância fora do meio de divulgação onde foi idealizado. Era difícil imaginar que um dia a mineração das moedas criaria um novo ramo mercadológico que agregaria tanto acúmulo de capital quanto o que se vê hoje. Todo software necessita de reparos, atualizações e correções de irregularidades que surgem conforme sua popularização e exploração por parte de seus usuários. Assim ocorre com sistemas operacionais, jogos, aplicativos de *streaming* e outros. É de se esperar que essa realidade não seria diferente com as redes de criptomoedas.

A epistemologia da escalabilidade pode ser estudada sob a ótica de quase todos aspectos de um software. O foco principal da tarefa de promover um desenvolvimento equilibrado e próspero de uma criptomoeda é estabelecer uma adaptatividade na progressão do volume de transações sem congestionar o sistema, acomodando a oscilação de nodos adjuntos na rede.

Por ser a primeira e mais popular moeda digital, o Bitcoin também foi pioneiro em enfrentar problemas de escalabilidade, com o grande avanço das exchanges e das altcoins que ampliaram a malha de fluxo monetário. A configuração padrão do Bitcoin Core prevê um limite de 1 Mb no tamanho de cada bloco minerado. Esse aspecto é abordado por (RODRIGUES 2016), que apontou o limite suportável cerca de 7 transações por segundo na rede do Bitcoin. Esse número é muito baixo numa perspectiva de adoção à nível global, considerando ainda a análise de Rodrigues de que, tendo uma única transação o peso de 250 bytes, e a frequência de atualização dos blocos flutuando em torno de 10 minutos. Utilizando uma perspectiva em que cada transação demanda 300 bytes, em um caso onde o tamanho do bloco é ilimitado, se o volume de transações no Bitcoin for equivalente ao dos cartões de crédito Visa (47 mil por segundo), cada bloco teria cerca de 8 gigabytes, totalizando 400 terabytes por ano (POON; DRYJA, 2015). Conforme se acumulam as solicitações de transferência que não encaixam no bloco mais próximo, cria-se uma espécie de fila de espera resguardada.

Em 2017 que essa situação chegou a um ponto insustentável, com a rede enfrentando um problema sério de escalabilidade. As negociações que antes demoravam minutos para se efetivarem passaram a demandar várias horas. Os mineradores passaram a dar prioridade àquelas cujo valor de taxa eram maiores, flagelando as microtransações, e causando um fluxo natural de aumento das taxa para realizar transferências, baseando-se na lei de oferta e demanda. As soluções para o problema já vinham sendo discutidas anteriormente, com a responsabilidade e cautela para preservar os valores que conservam a filosofia primordial de descentralização, segurança e baixo custo.

Em uma análise rasa é dedutível a tomada de uma decisão que aumente esse tamanho limite do pacote dos blocos para um valor com uma boa folga, de maneira a abarcar por um longo período todas as transferências pendentes no tempo mais rápido possível (ocupando o bloco mais próximo). Entretanto essa decisão se implica em um cenário desagradável, visto que todos os nodos da rede possuem sua cópia da blockchain, que cresce progressivamente e no momento da escrita desse texto já ultrapassou a marca dos 130 Gb de memória. Dado o nível de desenvolvimento computacional de armazenamento atual essa taxa não é preocupante, porém na ocasião do tamanho do bloco passar a ser mais alto, esse número seria elevado exponencialmente em pouco tempo.

O grande obstáculo para a execução de alterações tão agressivas no sistema é aplicável à todas criptomoedas. É o fato das redes serem descentralizadas. Como não há um controle solidificado que toma as decisões, as modificações precisam estar sob a concepção de um consenso generalizado entre os usuários. Logo, as redes de criptomoedas apresentam um aspecto bastante justo e competitivo nesse sentido: a propagação se dá por meio da utilização do software que possui mais adeptos e por assim se infere que tenha maior segurança e estabilidade.

**6.1. Ramificações da corrente (*Forks*)**

No âmbito das atualizações do software responsável por consumar as movimentações dos tokens na rede, existe o paradigma dos *forks*. Um *fork* (garfo em inglês) é uma bifurcação de todo o desenvolvimento da cadeia gerada pelas transferências. No Bitcoin e em outras criptomoedas, os responsáveis pela da arquitetura e expansão do programa que roda a aplicação, fazem parte de uma equipe formada em grande número por profissionais financiados por empresas relacionadas à mineração ou institutos de pesquisa, além de profissionais voluntários. O software do Bitcoin é versionado e estabelecido pela plataforma do GitHub, por onde é possível ter acesso ao código-fonte.

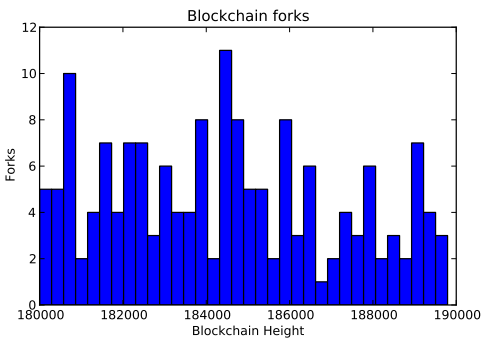
Existem duas categorias de fork:

Os *softforks* são aqueles em que há certa compatibilidade unilateral entre os dois programas, de forma que há a aprovação confirmada da cronologia que precede a bifurcação. Nesse caso, as regras predefinidas não sofreram uma alteração grave.

Um *hardfork* acorre quando a alteração é mais incisiva e os dois programas desenvolvem suas respectivas blockchains de maneira incompatível, se comportando como moedas diferentes. Essa é uma conjuntura severamente evitada pelos desenvolvedores, pois causa um grande impacto de instabilidade na cotação da moeda e na sua percepção pública em geral. Eventualmente uma das partes pode ficar fragilizada e outra ganhar maior porção de adeptos e as bifurcações podem originar outros desdobramentos da cadeia.(DECKER; CHRISTIAN, 2016)

Existem *forks* que surgem naturalmente, a partir de um setor da mineração que resolve decriptar um bloco diferente do restante da rede, e em cima desse novo segmento eles podem continuar a construir a *blockchain* em paralelo aos outros, até que eventualmente o consenso na rede instaura em apenas uma direção. O gráfico a seguir[[7]](#footnote-7) apresenta os casos de *fork* na rede de acordo com altura da *blockchain*.

Gráfico 8 – Forks na Blockchain



Fonte: (DECKER; CHRISTIAN, 2016)

Na análise de (Decker; Christian, 2016), houveram 169 forks da blockchain do Bitcoin no intervalo de 10000 blocos, categorizando uma taxa de proporção de 1,69%.

Existe mais de uma variável que pode estimular uma bifurcação sistemática na rede, (FRANCO 2016) destacou os diferentes tipos de gargalos que podem ser encontrados:

Poder computacional: o volume dos dados relacionado às transações deve ser compatível com a capacidade dos nodos de processá-los de acordo com a complexidade do algoritmo de criptografia.

Rede: com uma largura de banda de 10 Mbits/s é possível gerenciar um fluxo de 2500 transações por segundo. Quanto mais eficiente as máquinas poderem desempenhar essa tarefa, mais estabilidade tem a rede.

Armazenamento: Tendo as transações uma média de 0.5 kB de peso, a manutenção da memória pode passar por mudanças conforme se aumenta o fluxo de transferências. No exemplo de (FRANCO, 2016), num fluxo de 1 Mb por segundo no sistema, são acumulados 30 Terabytes por ano, o que causa um impacto nos requisitos de memória RAM das máquinas que processam as transações, visto que de 2009 até 2017 a blockchain ainda nem chegou à marca de 200 Gb.

Segundo (RODRIGUES,2016), existem quatro versões principais do software do Bitcoin, sendo elas:

- Bitcoin Core: esse é o programa que deriva da primeira implementação original designada por Satoshi Nakamoto, ele agrega uma cópia completa da *blockchain*.

- Bitcoin XT: surgiu de uma série de propostas de escalabilidade por Mike Hearn e Gavin Andresen, sendo uma delas aumentar progressivamente o tamanho de cada bloco. Essa versão foi entrando em declínio até perder bastante visibilidade perante outras.

- Bitcoin Classic: é uma implementação que remove o limite de 1 Mb por bloco. Segundo (RODRIGUES,2016) e o site oficial do software[[8]](#footnote-8), esse cliente auxilia no estabelecimento de um sistema de governança dentro da rede, além de ser compatível com outras versões como Core e Unlimited.

- Bitcoin Unlimited: é uma aplicação mais voltada para a livre iniciativa entre os envolvidos. Nesse caso não é necessariamente um hard-fork. Os usuários podem optar pela configuração de execução mais adequada aos seus anseios. É uma proposta bastante escalável e compatível com o conceito de Consenso Emergente

O site <https://coin.dance/nodes> lista outras versões do bitcoin em execução, com suas respectivas quantidades de nodos e informações adicionais. Algumas delas foram descontinuadas pela pouca aceitação e baixo engajamento dos participantes.

**6.2. Lightning Network**

A Lightning Network é uma proposta para solucionar o problema de escalabilidade no Bitcoin e no Litecoin, sendo aplicável em outros sistemas de criptomoedas também. Trata-se de um modelo que permite um volume muito maior de transações na rede a um baixo custo operacional.

Com o problema latente da escalabilidade, os responsáveis pela validação das transferências dentro da rede passam a dar prioridade àquelas de maior volume, que agregam um “fee”(taxa para validar a transação) mais alto. Dessa forma as microtransações ficam insustentáveis, já que o valor que se paga para acrescentá-las no bloco ficam altos, bem como a validação se dá apenas muitos blocos posteriormente.

Resumidamente, o funcionamento da Lightning Network se dá por meio de transações sendo efetuadas por fora da blockchain, por meio de um canal bidirecional, que não demanda validação coletiva, o resultado dessas transações é enviado para a cadeia de blocos oficial posteriormente, o que acaba reduzindo para um nível muito menor o tráfego de dados na rede principal em que a cadeia de blocos é escrita.

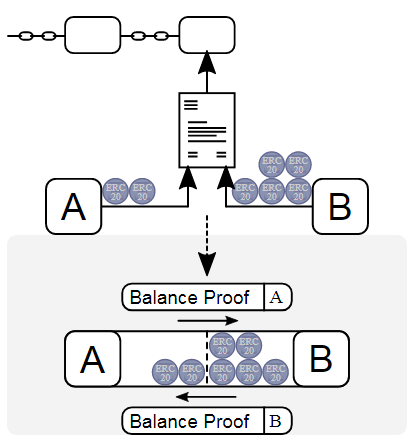
A analogia metafórica utilizada por (POON; DRYJA, 2016) para compreender a lógica por trás dessa metodologia foi a expressão de um questionamento externo: “Se uma árvore cai na floresta porém ninguém está por perto para ouvi-la, nesse caso fez-se algum som?”. A intenção era realizar uma análise acerca de eventos não observados, sendo possível destacar um paralelo com o estabelecimento de consenso em redes de criptomoedas: se dois participantes estão envolvidos em transações diárias recorrentes, não é necessário que o resto da rede tome algum tipo de responsabilidade coletiva a respeito disto. Dessa forma, o livro razão que toma nota do histórico de permutações entre as carteiras fica mais leve, dinâmico e simplista.

É ressaltado pelo axioma que se todas partes concordam que a árvore caiu às 14:45, então é essa afirmação é tida como verdade. Os canais de microtransações possibilitam uma interação de confiança direta entre duas partes, que realizam trocas monetárias entre si para que então após um determinado período, o saldo destas negociações seja então atualizado dentro da blockchain. Entretanto,sem o envolvimento de criptografia, surgem problemas de segurança para aplicar esta técnica em carteiras de moedas digitais. Se uma das partes não concorda com a hora de queda da tal árvore se torna uma disputa da palavra de um contra a do outro (POON; DRYJA, 2016).

**6.3. Raiden Network**

A Raiden Network é uma aplicação análoga à Lightning Network do Bitcoin, tendo sido desenvolvida para o sistema Etherium. Seu funcionamento se dá por meio de contratos inteligentes utilizando assinatura digital que possibilita a execução de transferências travadas chamadas de balance proofs (Raiden Network).

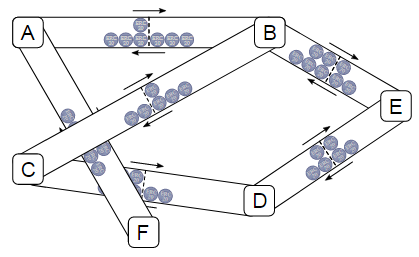
Figura 5 – Raiden Network



Fonte: Raiden Network[[9]](#footnote-9)

Como mostrado na figura, a Raiden Network permite a realização de transações entre A e B segregadas da cadeia principal, desde que elas não excedam os limites monetários das carteiras. A inovação trazida por esse modelo é que por meio dele não se faz necessário que ambas partes estejam conectadas diretamente na rede, basta que haja uma rota que faça a conexão entre as duas partes envolvidas em uma negociação, já o sistema cria uma rede de canais em que os nodos se conectam entre si, como mostra a figura a seguir:

Figura 6 – Raiden Network – Representação dos Nodos



Fonte: Raiden Network

Já que a maioria das movimentações nessa modalidade são feitas fora da cadeia de blocos principal, existe um nível mais alto de privacidade na sua utilização. Muitos dos dados relacionados aos canais paralelos é de difícil rastreio até a atualização na cadeia principal. A proteção de dados pessoais também é assegurado pela rede para evitar ataques.

Uma das desvantagens desse sistema é a necessidade do travamento de uma determinada quantidade de tokens para permutação. Isso é necessário para evitar fraudes, evitar que um participante fique em débito e dificultar a ação de quem deseja aplicar golpes. Para participar de um canal de transferência é preciso garantir uma quantia que ficará presa por contrato. Esse ponto pode ser, em algum nível, um fator dificultante para a adoção em massa da plataforma. Além disso, por mais que os gastos de recursos sejam menores, a rede não é livre de taxas, tendo dois tipos de taxas que são pagas pelos participantes, sendo uma delas voltada para o suporte para serviços de monitoramento da rede para otimização e outra dedicada para o equilíbrio e o mantimento dos canais de pagamento dentro da grade.

Uma solução para resolver o problema de escalabilidade chama-se Sharding, e foi descrita na Etherium wiki disponível na plataforma GitHub. Seu funcionamento é baseado em uma segregação da cadeia única em que se desenvolvem os blocos para formar um agrupamento de vários segmentos desse tipo (Shards) funcionando concorrentemente, conservados por um protocolo designado para preservar certas garantias e propriedades entre eles que promovam a consistência da rede. Dessa forma, as transações dentro da rede são direcionadas para o shard referente a ela, de maneira que o desenvolvimento da corrente de blocos seja segmentado paralelamente entre estes shards. Para promover a conexão entre dois shards, a proposta também envolve a criação de um protocolo de transferência de mensagens por meio de uma plataforma de distribuição compartilhada sob impedimento de modificações por parte de outros integrantes.

A proposta do Sharding é talvez uma das menos viáveis para se resolver o problema da escalabilidade de qualquer criptomoeda, já que o modelo atual é a implementação que permite a centralização dos blocos, que acarretará no consenso coletivo dos usuários que irão validar todas as transações individualmente. Essa segregação dificulta o estabelecimento dessa prova de confiança, abrindo espaço para um ataque de um usuário com relativo alto poder computacional capaz de ruir o sistema, considerando o fato de que agora ele não necessita de concorrer com a decisão de todos os nodos participantes da rede, mas apenas os do shard em que este é atuante.

**6.4. Fee Market**

Esta é uma proposta levantada por Peter R. Rizun, que tem como foco o desenvolvimento de um mercado livre de taxas de transação (origem do nome Fee Market). Para Rizun, esta é uma maneira mais eficiente de resolver o problema do tamanho do bloco, ao invés de um número fixo definido pelo protocolo.

Existe uma logística por trás da mineração dos blocos que determina a lucratividade desse papel dentro da rede, como foi pontuado por (RODRIGUES, 2015): “Ao minerar um bloco, o minerador tem uma recompensa esperada que depende do bloco (emissão de novas unidades de moeda + taxas de transação) e do custo computacional para encontrar o nonce que satisfaz o hash de acordo com a dificuldade (target) atual”. Porém, como mostra a análise de Rodrigues, há uma chance de um bloco se tornar órfão ao ser propagado pela rede, sendo ignorado pelos outros nodos e este aspecto está relacionado com a agilidade para essa propagação do bloco. Se mineradores perdem blocos (tornando-os órfãos) há um prejuízo com gastos de recursos computacionais. A equação do lucro apresentada por Rizun foi adaptada por Rodrigues na seguinte declaração:

Lucro = (recompensa+ fees) × hashPowerminerador / hashPowerRede ×(1−ℙórfão)

“O minerador então tem que escolher da sua lista de transações disponíveis (mempool) aquelas tais que maximizem o seu lucro e minimizam seu prejuízo”, (RODRIGUES, 2015). De acordo com Rizun, a chance de perda de um bloco (tornando-o órfão) deve ser baixa se o tempo de propagação dele é curto e alta se o tempo de propagação for maior.

A fórmula da probabilidade dessa perda de bloco (ℙ) é dada por:

ℙórfão = 1 - e.- t /t [[10]](#footnote-10)

A convicção da proposta de Rizun é de que uma ordem mercadológica por parte dos responsáveis pela mineração dos blocos seguindo padrões de oferta e demanda podem controlar de maneira mais eficaz as falhas pertinentes à orfandade de blocos.

Um minerador, querendo maximizar seu lucro, não arrisca criar um bloco demasiadamente grande. Ao criar tal bloco, ele está correndo o risco de perder todo seu trabalho, pois o bloco pode se tornar órfão. Logo, o minerador vai buscar por um limite sadio que maximize seu lucro. (RODRIGUES, 2015)

**6.5. Segregated Witness (Segwit)**

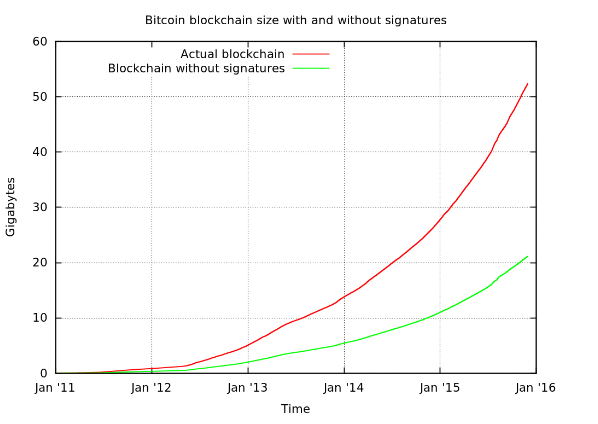
O Segwit é uma sugestão de atualização para sistemas baseados em blockchain para resolver o problema da escalabilidade e descomplexificar a performance e o desempenho dessas ferramentas.

O contexto da proposta do Segwit emerge da forma como se tornam efetivas as transações dentro dessas redes, o foco do projeto foi de ser implementado para o Bitcoin, que é maior das redes de criptomoedas. Todas transferências de tokens dentro de uma aplicação desse tipo necessitam de inputs, sendo um deles a assinatura digital que integra a negociação com seus participantes. Esses inputs geram outputs que compõem o arquivo encadeado denominado *blockchain* que documenta esses dados que são validados a partir do consenso dos mineradores que ratificam as transações (WUILLE, 2015).

A indagação que o Segwit levanta concerne a real necessidade da presença desta assinatura dentro da cadeia de blocos. A existência dessas instâncias dentro de cada uma das transferências causa um peso muito grande de dados a longo prazo no tamanho do arquivo da blockchain e atualmente não é possível rejeitar a assinatura de uma transação, pois isso invalidaria sua aceitação dentro do seu respectivo bloco. A ação do Segwit é estabelecer uma segregação dessa assinatura de dentro dos blocos, dessa forma há uma melhoria no que tange os requisitos de memória de um full-node para armazenar esses dados. A efetivação dessa nova diretriz estava prevista para o dia 15 de novembro de 2017, o que acabou sendo suspendido e deve permanecer sob debate dentro da comunidade.

O gráfico a seguir[[11]](#footnote-11) mostra a diferença do ritmo de crescimento da blockchain do Bitcoin com a presença das assinaturas dentro dos blocos em comparação com o ritmo de crescimento sem as assinaturas:

Gráfico 9 – Comparativo do tamanho da blockchain com e sem as assinaturas digitais



Fonte: (WUILLE, 2015)

Como mostra o gráfico, a ausência da assinatura das transações nos blocos a longo prazo causaria um impacto positivo à respeito do gerenciamento do espaço que elas ocupam nas máquinas que rodam o software.

**6.6. Considerações Finais**

O problema da escalabilidade sempre é recorrente em todos sistemas que não sofrem atualizações proporcionais ao seu crescimento, e essa realidade não é diferente com as criptomoedas e as soluções para melhorar a progressão saudável da rede sempre estarão sob debate. Sob a perspectiva do Bitcoin, em certas ocasiões as altcoins servem como um ambiente de teste para as tentativas de melhorar a escalabilidade. Atualmente boa parte das propostas são incisivas e tem uma pretensão explícita de concretizar melhorias à curto prazo, haja vista que o aplicação destas atualizações dependem do estabelecimento de consenso em volta dos nodos da rede e a iminência de um colapso envolve riscos de prejuízo de proporções milionárias dada ao patamar de engajamento que esse mercado tomou.

O aspecto descentralizado dos ativos digitais cria esse determinismo paradoxal, no qual todos lados querem tomar as melhores decisões porém dependem da concordância de todo o resto dos participantes, cuja falta agrava o problema já que a sua solução é prorrogada.

Para evitar melhor a escolha menos desejável, que são os hard-forks que fragilizam o sistema, o melhor dos cenários a se almejar é aquele em que o posicionamento dos participantes seja bem esclarecido e disposto abertamente para agilizar a tomada de decisões.

**7. CONCLUSÃO**

O novo paradigma levantado pelo advento das criptomoedas traçou um caminho irreversível no contexto socioeconômico mundial. Há muito o que se explorar da tecnologia da blockchain, pois todas vantagens dela partem de uma conquista inédita na área de tecnologia da informação, que é a escassez de um dado gerado por um processo descentralizado livre de fraudes. A partir desse ponto os limites de aplicação são inúmeros, já que grande parte dos problemas de segurança de dados em redes de computadores partem do cenário clássico no qual a informação é facilmente copiada e distribuida, muitas vezes ilegalmente. Uma aplicação em blockchain abre portas não apenas para aplicações monetárias de trocas entre usuários, mas também de validações de contratos descentralizados além de sistemas de votação e auditoria, haja vista que as técnicas convencionais de decretação de documentos estão suscetíveis a uma variedade maior de fraudes e irregularidades se comparado aos modelos descentralizados.

Entretanto, as limitações e os desafios para resolução de problema devem estar bem esclarecidos, visto que nenhum sistema é completamente seguro e intocável. Apesar das falhas apresentadas neste trabalho, atualmente estes sistemas estão ganhando muita aceitação e evoluindo de forma satisfatória na função de englobar mais possibilidades de aplicação.

A variedade de sistemas de criptomoedas cria um senso de concorrência saudável dentro deste novo mercado que se espande e passa por mais aprimoramentos com o passar do tempo. Tendo em vista a situação atual desta área de ativos digitais, sugere-se que uma das últimas barreiras para a adoção em massa de ferramentas descentralizadas na sociedade como um todo é a questão da alta oscilação da cotação dos valores das moedas em comparação com moedas fiduciárias, se levarmos em consideração que o acesso à internet e a smartphones (que atuam como carteiras) está em vias de atingir até as camadas menos favorecidas da sociedade.

Presume-se que, mesmo que em um futuro hipotético no qual as criptomoedas sofram algum tipo de colapso generalizado, de maneira a perder o engajamento e serem descontinuadas, ainda assim o paradigma da blockchain continuará ativo para outras formas de aplicação. Portanto é de suma importância o desenvolvimento de mais trabalhos científicos que explorem ao máximo novas perspectivas para essa área.

Também é valido dizer que essa constante evolução do mercado e da tecnologia à qual as moedas digitais estão envolvidas torna muito volátil os ciclos de manutenção de pesquisas acerca de qualquer um dos aspectos citados no trabalho. Dessa forma, é provavel que em poucos anos qualquer trabalho desse tipo se torne parcialmente ou completamente obsoleto. A possibilidade da descoberta de uma nova funcionalidade ou metodologia de aplicação de um sistema de criptomoedas é sempre latente, bem como o completo abandono de técnicas mais antigas e ineficazes.

Com esse trabalho, foi possivel perceber também uma forte imponencia e dominancia do Bitcoin perante outras criptomoedas graças ao seu pioneirismo e solidificação rápida no mercado. É deduzível que esse cenário pode mudar facilmente conforme a implementação das atualizações para resolução dos problemas de escalabilidade aqui citados.

**8. REFERENCIAS BIBLIOGRÁFICAS**

ALBERTS, Jeffrey E.; FRY, Bertrand. **IS BITCOIN A SECURITY?**. [20??]. Disponível em: <<https://www.bu.edu/jostl/files/2016/01/21.1_Alberts_Final_web.pdf>>. Acesso em: 20 ago. 2017.

AMADORI, Marco. **Alternative Cryptocurrencies a quick primer**. 2015. Disponível em:

<<http://www.science.unitn.it/~sala/events2015/Amadori_bitcoin.pdf>>.

Acesso em: 11 jul. 2017.

AMATO, Claudio P.. **A Moeda Fiduciária**. 2004. Disponível em:

<<http://www.snb.org.br/portal/boletins/pdf/54%20-%20A%20Moeda%20Fiduciária.pdf>>

Acesso em: 18 dez. 2017.

APOSTOLAKI, Maria; ZOHAH, Aviv; VANBEVER, Laurent. **Hijacking Bitcoin: Routing Attacks on Cryptocurrencies**. 2017. Disponível em:

<<https://btc-hijack.ethz.ch/files/btc_hijack.pdf>>. Acesso em: 12 out. 2017.

BARBOSA, Paulo Celso Lavinas. **Bitcoin e moedas fiat: Um estudo de volatilidade comparada.** 2016. Acesso em: 11 jun. 2017.

BARCELLOS, Marinho P. ; GASPARY, Luciano P. **Segurança em Redes P2P: Princípios, Tecnologias e Desafios.**

**Disponível em: <[https://www.lume.ufrgs.br/bitstream/handle/10183/7510/000546396](https://www.lume.ufrgs.br/bitstream/handle/10183/7510/000546396.pdf)>**

Acesso em: 23 mai. 2017.

**Bitcoin Nodes Summary.** Coin Dance. Disponível em: <<https://coin.dance/nodes>>. Acesso em: 29 out. 2017.

**Blocksize. Bitcoin Classic.** Disponível em:

**<**<https://bitcoinclassic.com/devel/Blocksize.html>**>.** Acesso em: 11 jul. 2017.

CALLADO, Arthur; SADOK, Djamel. **Colaboração na Internet e a Tecnologia Peer-to-Peer.** 2014. Acesso em: 12 out. 2017.

CALVETTE, Rafael Cintra. **BITCOIN: Um estudo sobre a moeda digital e Deflação**. 2015. Acesso em: 11 jun. 2017.

CERMAK, Vavrinec. **Can Bitcoin Become a Viable Alternative to Fiat Currencies? An empirical analysis of Bitcoin’s volatility based on a GARCH model**. 2017. Disponível em: <<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2961405>>. Acesso em: 29 ago. 2017.

**Cryptocurrency Market Capitalizations**. Coin Market Cap. Disponível em:

<<https://coinmarketcap.com/coins/>>. Acesso em: 14 set. 2017.

**Common Vulnerabilities and Exposures**. BitcoinWiki. Disponível em:

<<https://en.bitcoin.it/wiki/Common_Vulnerabilities_and_Exposures>>. Acesso em: 12 out. 2017.

COSTA, Eric Tedesco da. **Bitcoin: Análise da moeda virtual descentralizada e suas implicações**. 2015. Acesso em: 11 jun. 2017.

**CVE-2010-5139 Detail**. 2010. National Vulnerability Database. Disponível em:

<<https://nvd.nist.gov/vuln/detail/CVE-2010-5139>>. Acesso em: 12 out. 2017.

DECKER, Christian. **On the Scalability and Security of Bitcoin**. 2016. Disponível em: <<https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/114732/eth-48881-02.pdf>>. Acesso em: 23 out. 2017.

DUFFIELD, Evan; DIAZ, Daniel. **Dash: A Privacy-Centric Crypto-Currency**

2015. Disponível em: <<https://www.dash.org/wp-content/uploads/2015/04/Dash-WhitepaperV1.pdf>>. Acesso em: 25 out. 2017.

DUFFIELD, Evan; HAGAN, Kyle. **Darkcoin: Peer­to­Peer Crypto­Currency with Anonymous Blockchain Transactions and an Improved Proof­-of-­Work System**. 2014. Disponível em:

<<https://bravenewcoin.com/assets/Whitepapers/DarkcoinWhitepaper.pdf>>.

Acesso em: 25 out. 2017.

DUFFIELD, Evan;SCHINZEL, Holger; GUTIERREZ, Fernando. **Transaction Locking and Masternode Consensus: A Mechanism for Mitigating Double Spending Attacks**. 2014. Disponível em: <<https://pt.scribd.com/doc/241012134/Transaction-Locking-and-Masternode-Consensus-A-Mechanism-for-Mitigating-Double-Spending-Attacks>>.

Acesso em: 15 nov. 2017.

EDEROV, Boris. **Merkle Tree Traversal Techniques.** 2007. Disponível em:

< <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.84.9700&rep=rep1&type=pdf>>

Acesso em: 27 nov. 2017.

FILHO, Paulo C. H.. **Anatomia do BitTorrent a Ciência da Computação no Transmission**. 2013. Disponível em: <<http://bcc.ime.usp.br/tccs/2013/rec/paulo/arquivos/monografia.pdf>>.

Acesso em: 15 nov. 2017.

FRANCO, Pedro. **Understanding Bitcoin: Cryptography, engineering, and economics**. 1. ed. Wiley. 2015. Acesso em: 30 mai. 2017.

FURRIEL, Ana M. Q. Sepúlveda. **Modelos Heterocedásticos - ARCH e GARCH**. 2011. Disponível em:

<<https://repositorio-aberto.up.pt/bitstream/10216/57365/2/TeseMestradoMargaridaSepulveda.pdf>>.

Acesso em: 15 nov. 2017.

JUNIOR, Meira Vagner. **Um sistema de reputação resistente a ataques Sybil para redes overlay∗**. [20??]. Disponível em:

<<http://www.lbd.dcc.ufmg.br/colecoes/wp2p/2007/005.pdf>>

Acesso em: 12 out. 2017.

# **Infostealer.Coinbit**. Symantec. 2011. Disponível em:

<<https://www.symantec.com/security_response/writeup.jsp?docid=2011-061615-3651-99>>

Acesso em: 23 ago. 2017.

KING, Sunny; NADAL, Scott. **PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake.** 2012.

Disponível em: <<https://peercoin.net/assets/paper/peercoin-paper.pdf>>. Acesso em: 11 jun. 2017.

LEWIS, Antony. **A Gentle Introduction To Blockchain Technology**. [201?]. Disponível em:

<<https://bravenewcoin.com/assets/Reference-Papers/A-Gentle-Introduction/A-Gentle-Introduction-To-Blockchain-Technology-WEB.pdf>>. Acesso em: 18 nov. 2017.

MACEDO, Ricardo Tavares. **Pataca um sistema de promoção da descentralização da moeda através de moedas criptográficas**. 2014.

Disponível em: <<http://bcc.ime.usp.br/tccs/2014/rickmacedo/monografia.pdf>>.

Acesso em: 18 nov. 2017.

MADRUGA, Marcelo; LOEST, Sérgio; MAZIERO, Carlos; SANTIN, Altair. **Um Sistema de Arquivos Distribuído Peer-to-Peer Tolerante a Faltas usando Arquivos Transparentes**. [20??]. Disponível em:

<<http://wiki.inf.ufpr.br/maziero/lib/exe/fetch.php?media=research:2009-sbrc.pdf>>

MORAIS, I. A. C.; PORTUGAL, M. S. **Modelagem e previsão de volatilidade determinística e estocástica para a série do Ibovespa. Estudos Econômicos**. 1999.

Disponível em: < http://www8.ufrgs.br/ppge/pcientifica/1999\_03.pdf >

Acesso em: 18 nov. 2017.

NAKAMOTO, Satoshi. **Bitcoin: A Peer-to-Peer Electronic Cash System.** 2008. Online content. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 25 abr. 2017.

**Pizza for bitcoins?**. Bitcoin Forum. 2010. Disponível em: <[https://bitcointalk.org/index..php?topic=137.0](https://bitcointalk.org/index.php?topic=137.0)>. Acesso em: 24 ago. 2017.

**On sharding blockchains**. Github[/](https://bitcointalk.org/index.php?topic=137.0)Ethereum. Disponível em:

<<https://github.com/ethereum/wiki/wiki/Sharding-FAQ>>. Acesso em: 15 nov. 2017.

POELSTRA, Andrew. **A Treatise on Altcoins**. 2016. Disponível em: <<https://download.wpsoftware.net/bitcoin/alts.pdf>>. Acesso em: 15 nov. 2017.

POELSTRA, Andrew. **Distributed Consensus from Proof of Stake is Impossible**. 2014. Acesso em: 18 nov. 2017.

POON, Joseph; DRYJA, Thaddeus. **The Bitcoin Lightning Network: Scalable Off-Chain** Instant Payments. 2015. Disponível em:

<<https://lightning.network/lightning-network-paper.pdf>>. Acesso em: 28 out. 2017.

RODRIGUES, Elias Italiano. **Estudo sobre Bitcoin: escalabilidade da blockchain**. 2016. Disponível em:

<<http://elias19r.com/files/cv/tcc1-monografia_7987251.pdf?i=2>>. Acesso em: 12 out. 2017.

ROTHBARD, Murray. **What Has Government Done to Our Money?.** 1963. Disponível em:

<https://mises.org/system/tdf/What%20Has%20Government%20Done%20to%20Our%20Money\_3.pdf?file=1&type=document>

Acesso em: 28 out. 2017.

SILVA, Douglas Emanuel. **Aspectos de segurança na rede Bitcoin.** [20??]. Disponível em:

<<http://www.cdn.ueg.br/source/observatorio_inhumas/conteudoN/3322/CAP_8__CR_ASPECTOS_DE_SEGURANCA_NA_REDE_BITCOIN.pdf.pdf>>. Acesso em: 29 mai. 2017.

SWAN, Melanie. **Blockchain: Blueprint for a New Economy**. 1. ed. O’Reilly Media, Estados Unidos, 2015.

SCHWARTZ, David; YOUNGS, Noah; BRITTO, Arthur. **The Ripple Protocol Consensus Algorithm**. 2014. Disponível em: <<https://ripple.com/files/ripple_consensus_whitepaper.pdf>>. Acesso em: 15 nov. 2017.

SCREMIN, Martinez Alberto; HERRERA, Barbara Sabrina; PAIXÃO, B. C. da; TAMAKI, Daniel. **Sistemas de redes *peer to peer***. [20??]. Disponível em:

<http://www2.ic.uff.br/~otton/graduacao/informaticaI/P2P.pdf>.

Acesso em: 12 out. 2017.

VASIN, Pavel. **BlackCoin’s Proof-of-Stake Protocol v2.**. [20??]. Disponível em:

<<https://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf>>. Acesso em: 23 out. 2017.

ULRICH, Fernando. **Bitcoin: A moeda na era digital**. 1. ed. Mises Brasil. 2015.

Disponível em:

<<http://www.informatrader.com.br/datafiles/conteudo_downloads/9/Fernando-Ulrich-Bitcoin.pdf>>. Acesso em: 25 abr. 2017.

WUILLE, [Pieter](https://prezi.com/user/wvjh0ybtdzgy/). **Segregated Witness and Deploying it for Bitcoin**. 2017. Disponível em: <<https://prezi.com/lyghixkrguao/segregated-witness-and-deploying-it-for-bitcoin>>. Acesso em: 12 out. 2017.

1. Unidade de medida de valor em bitcoin. O nome foi dado em referência ao seu criador, Satoshi Nakamoto, sendo 1 satoshi = 0,00000001 BTC. [↑](#footnote-ref-1)
2. Linha vermelha: projeção da taxa de inflação

   Linha azul: base monetária da moeda [↑](#footnote-ref-2)
3. Métrica de representação da quantidade de cálculos para quebra de criptografia durante a mineração. [↑](#footnote-ref-3)
4. Bloco 0 -https://blockchain.info/pt/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f [↑](#footnote-ref-4)
5. Representação esquemática do AS8 (Sistema Autônomo) atrasa o envio dos blocos em 20 minutos para o acesso do nó C. [↑](#footnote-ref-5)
6. Primeira coluna: Masternodes controlados pelo atacante/Total de Masternodes;

   Segunda coluna: Probabilidade de sucesso. Sendo: n: comprimento da cadeia de Masternodes; t: número total de Masternodes na rede; r: número de nodos masternodes controlados pelo invasor, sendo ≥ n;

   Terceira coluna: Quantidade de Darkcoins requeridas. [↑](#footnote-ref-6)
7. Eixo vertical: número de forks

   Eixo horizontal: altura da blockchain [↑](#footnote-ref-7)
8. https://bitcoinclassic.com [↑](#footnote-ref-8)
9. Disponível em <https://raiden.network/101.html> [↑](#footnote-ref-9)
10. Sendo t: tempo de propagação do bloco e T: tempo de atualização dos blocos [↑](#footnote-ref-10)
11. Linha vermelha: crescimento da blockchain no modelo atual

    Linha verde: crescimento da blockchain com a segregação das assinaturas [↑](#footnote-ref-11)