UNIVERSIDADE FEDERAL DO PARANÁ

LUIS FILIPE GOLD COELHO DE ALMEIDA DOS REIS

CRIPTOMOEDAS: UMA ANÁLISE SE AS CRIPTOMOEDAS SÃO O FUTURO DO DINHEIRO

CURITIBA

2017

LUIS FILIPE GOLD COELHO DE ALMEIDA DOS REIS

CRIPTOMOEDAS: UMA ANÁLISE SE AS CRIPTOMOEDAS SÃO O FUTURO DO DINHEIRO

Monografia apresentada ao Curso de Ciências Econômicas, Setor de Ciências Sociais Aplicadas, Universidade Federal do Paraná, como requisito parcial à obtenção do grau de Bacharel em Ciências Econômicas.

Orientador: Prof. José Guilherme Silva Vieira

CURITIBA

2017

TERMO DE APROVAÇÃO

LUIS FILIPE GOLD COELHO DE ALMEIDA DOS REIS

CRIPTOMOEDAS: UMA ANÁLISE SE AS CRIPTOMOEDAS SÃO O FUTURO DO DINHEIRO

Monografia apresentada ao Curso de Ciências Econômicas, Setor de Ciências Sociais Aplicadas, Universidade Federal do Paraná, como requisito parcial à obtenção do grau de Bacharel em Ciências Econômicas.

Orientador: Prof. José Guilherme Silva Vieira
Departamento de Economia, UFPR.

Prof. Dayani Aquino
Departamento de Economia, UFPR.

Prof. Wladmir Fonseca
Departamento de Economia, UFPR.

Curitiba, 6 de Dezembro de 2017.

RESUMO

Essa monografia tem como objetivo entender se as criptomoedas serão o modelo monetário principal no futuro. Essas criptomoedas são atualmente um dos assuntos mais comentados na internet muito devido a sua valorização o que traz muita atenção para entender qual será o futuro da mesma.

Para averiguar o futuro das criptomoedas será utilizado o modelo de pesquisa qualitativo além da analogia histórica.

Foi possível notar como resultado dessa pesquisa que as criptomoedas possuem as características necessárias para se tornarem a moeda do futuro, mas que não é possível determinar se isso ocorrerá devido alguns desafios nas quais a mesma deve superar para ser efetivamente consolidada como meio dinheiro.

Apesar de não ser possível concluir com 100% de assertividade o futuro das cripotmoedas o trabalho apresentou quais informações e quais movimentos devem ser observados para compreender se elas serão ou não o principal meio de pagamento.

Palavras-chave: Criptomoeda, Moeda, Blockchain,Bitcoin

ABSTRACT

This monography aims to understand if the crypto-coins will be the mainstream monetary model in the future. These criptocurrency are currently one of the most talked about subjects on the internet much due to its appreciation which brings much attention to understand what will be the future of it. To investigate the future of the crypto-coins will be used the qualitative research model in addition to the historical analogy. It was noted that as a result of this research, crypto-coins have the necessary characteristics to become the currency of the future, but it is not possible to determine if this will occur due to some challenges in which it must overcome to be effectively consolidated as the mainstream payment sistem. Although it is not possible to conclude with a 100% assertiveness of the future of the crypto-currencies, the work presented what information and what movements should be observed to understand if they will be the main means of payment or not.

Key-words: Cryptocurrency, Currency, Blockchain, Bitcoin

SUMÁRIO

1. INTRODUÇÃO

1.1. Contexto e problema

O tema criptomoedas vem sendo discutido com grande freqüência pelas mídias atuais, principalmente pelo fato da valorização acentuada e constante de uma criptomoeda em específico chamada Bitcoin. O objetivo desse trabalho não é de verificar aspectos referentes a valorização da moeda em si, mas sim entender se as criptomoedas tem o necessario para serem o dinheiro no longo prazo e se estamos vivendo agora uma fase de transição como foi do padrão ouro para o padrão atual de moeda fiduciária. Ou se elas são apenas uma moda passageira.

Para buscar identificar qual o futuro das criptomoedas serão considerados inicialmente quais são os conceitos de moeda e uma breve história da mesma, seguida por uma explicação de o que é uma criptomoeda e uma breve história. Através de uma análise entre o que consiste uma moeda e uma criptomoeda será verificado se ela pode ou não subsituir a moeda atual da economia.

Concluindo o trabalho com uma averiguaçao sobre quais são os principais determinantes para o futuro da criptomoeda e quais os princicpais desafios da mesma.

2. MOEDA E SUA HISTÓRIA

As transações mercantis podem ser realizadas de forma direta - também conhecida como escambo - ou de forma indireta, através do uso da moeda.

Nos primórdios, as relações comercias eram baseadas no escambo de mercadorias, onde havia a troca de produtos entre os indivíduos.

Deveria existir uma dupla coincidência de desejos, isto é, o ofertante de uma mercadoria deveria achar um demandante que fosse simultaneamente ofertante do produto desejado, para que a transação comercial pudesse acontecer.

Esse sistema começou a apresentar falhas a partir do momento em que o volume das trocas se ampliou, sendo, desta forma, necessário a utilização de um meio de trocas que facilitasse as transações. Assim surge o primeiro modelo de moeda, a chamada moeda mercadoria na qual uma determinada comunidade concordava em atribuir a uma mercadoria um valor de troca facilitando as relações comerciais.

Diversas mercadorias já foram utilizadas como moeda ao longo da história, sendo algumas delas, conchas, sal, açúcar, ouro entre outros. Segundo Radford (1945) durante a segunda guerra mundial era possível identificar a volta desse modelo moeda mercadoria, sendo utilizados cigarros para a compra de comida, vestimentas, remédios entre outros.

Tais moedas mercadoria podem ser identificadas e atribuídas sua criação com base na peculiaridade de cada região e conforme as trocas se ampliavam e a sociedade se desenvolvia as moedas mercadoria também eram alertadas conjuntamente.

A atribuição dos metais como moeda pode ainda ser considerado uma forma de moeda mercadoria devido a presença intrínseca de valor de uso, mas com o aumento no volume o transporte de grandes quantidades de moeda metálica se tornou um desafio.

Para solucionar tal dificuldade foi criado o primeiro papel moeda baseado na ideia da fidúcia, ou seja, confiança da pessoa na qual havia emitido tal papel que garantia ao portador do mesmo a retirada do montante declarado no papel em moedas metálicas.

É possível observar tal moeda apesar de ser uma moeda em papel ela ainda possuía seu lastro em metal não sendo uma alteração significativa na moeda em si

mas apenas na forma como ela era transacionada, que agora por se tratar de papel fiduciário possibilitou aos seus portadores carregarem grandes volumes monetários sem grandes esforços comparado com a moeda metálica.

Com o tempo os emissores dessa moeda fiduciária identificaram que os detentores de metais não costumavam sacar todo o metal no qual eles haviam depositado, e sendo assim, o emissor de papel moeda tinha uma margem para emitir mais papel moeda que a quantidade real de metais no qual ele detinha em seu cofre, criando uma moeda que não tinha seu lastro de um para um com o metal e aumentando a quantidade de papel moeda em circulação (Rossetti, 2005).

Com o desenvolvimento desse processo temos as moedas emitidas por um banco central sem ter seu lastro em metais, mas sim na fidúcia de cada governo, e com o desenvolvimento da sociedade, entramos na era digital onde os bancos responsáveis por armazenar as moedas passam a utilizar computadores que facilitam as trocas, permitindo que valores monetários sejam transacionados entre agentes econômicos apenas por ordens eletrônicas e não necessariamente tendo a sua moeda física sendo deslocada (a chamada moeda virtual) (Rossetti, 2005).

Essa moeda apesar de ser uma moeda digital, ainda possui o seu lastro na moeda emitida por determinado país e, apesar de ser transacionada *online* ela é apenas uma representação dessa moeda física em uma forma digital.

Segundo (Paiva 2008) as moedas possuem três características sendo elas I. Meio de troca, instrumento intermediário de aceitação geral. II. Unidade de conta, permite a contabilização dos agregados econômicos numa unidade só e III. Reserva de valor, a moeda deve ter seu poder de aquisição preservada, sendo um meio de acumulação de riqueza.

Para Marx (1977) a moeda é uma representação material da riqueza social, cujo valor de troca se torna independente das particularidades dos valores de uso.

Segundo Keynes (1936) a moeda é uma medida que passa segurança para os agentes econômicos de forma que estes consigam enfrentar o futuro, quanto da existência de incertezas. Segundo o autor, existiriam três motivos pelos quais os agentes econômicos demandam moeda: o motivo transacional, por precaução e para especulação.

Para o monetarista Milton Friedman (1997), a moeda é vista como um ativo como outro qualquer e concorre por uma posição na carteira dos agentes econômicos. Além disso, segundo o autor, a demanda por moeda possui uma relação estável com a renda nominal, portanto, a oferta de moeda afetará apenas o nível geral de preços, hipótese similar a que chegaram os clássicos sobre o papel desempenhado pela moeda na economia. Nas palavras de Friedman (1997):

> "Para as famílias a moeda é um ativo como outro qualquer que fornece algum serviço útil; enquanto que para uma firma a moeda é como um bem de capital, uma fonte de serviços produtivos" (Friedman, 1977, p. 235).

Verifica-se que todos os modelos monetários apresentados até o momento sempre possuíram tais características e que aparentemente o *Bitcoin* tem apresentado todas as características acima mencionadas.

3. CRIPTOMOEDAS

3.1 Definição

Para melhor compreensão e possibilidade de analisar se o futuro dos meios de pagamento realmente é a criptomoeda, é preciso definir em primeiro lugar o que é uma criptomoeda e o que a faz diferente das demais moedas conhecidas até o momento.

Atualmente quando acessamos o banco através de nossos celulares ou computadores para transferir dinheiro para alguém, estamos utilizando uma moeda digital afinal naquele momento o que podemos ver é somente o montante que aparece em nossa tela ser alterado. Porém esse valor está ligado a um dinheiro emitido e controlado pelo governo. O dinheiro virtual como é o caso do bitcoin também é um dinheiro digital, porém sua única existência advém da internet em si não possuindo um governo emitindo e controlando o mesmo.

A ideia da criptomeoda diferente do que muitos imaginam foi primeiramente descrita em 1998 em um artigo publicado por Wei Dai no grupo de internet chamado *Cypherpunks* (Bitcoin.org, 2015).

Os *Cypherpunks* eram um grupo de programadores nos anos 90 que tinham grande preocupação com a privacidade e para tanto utilizavam da criptografia para conseguirem tal anonimato. O termo criptografia vem do grego (*Kryptós Graphién*) que significa escrita escondida, no caso a criptografia utilizada pelos *Cypherpunks* era uma forma de enviar informações através da internet onde somente o destinatário da mensagem obtivesse a formula que a tornasse legível e compreensível, permitindo assim a privacidade que o grupo tanto prezava. (Assange, 2012)

No artigo onde Wei Dai (1998) descreve pela primeira vez o que é uma criptomoeda, ele se mostra muito interessado na possibilidade de criar uma moeda na qual o governo não teria a capacidade de identificar a origem ou seu destino, possibilitando um anonimato para seus usuários e uma independência do governo.

Essa preocupação que Wei Dai(1998) tinha com o anonimato das transações vem devido toda e qualquer transação financeira realizada na internet pode ser rastreada pelo governo, algo que um pagamento em espécie não ocorre, por exemplo um indivíduo ao sacar um determinado montante de valor em espécie no banco fica registrado essa saída monetária para aquela pessoa. Porém, se ao sair do banco ele comprar um refrigerante com o dinheiro em uma lanchonete o governo não consegue rastrear que ele comprou esse refrigerante ou que o dono da lanchonete recebeu tal valor a não ser que o mesmo declare.

Sendo assim a criptomoeda volta a oferecer esse anonimato para os indivíduos, mas outro fator de até maior relevância é que ao contrário do exemplo supracitado toda a operação realizada pelo indivíduo que sacou o dinheiro e pagou ao dono da lanchonete, mesmo que de forma anônima, foi realizada utilizando um meio de pagamento (dinheiro) impresso e controlado pelo banco central do país em questão.

No caso das criptomoedas elas não são nem sequer impressas, mas sim definidas pelo seu programador que escolhe sua quantidade e como ela será gerada. Não tendo assim qualquer ligação com o governo, algo similar com o que ocorre durante um evento como um show onde o responsável pelo evento cria uma ficha que é aceita durante o show para comprar alimentos e bebidas não tendo ela ligação alguma com o governo.

> Estou fascinado com a Crypto-anarquia de Tim May. Diferente das comunidades tradicionalmente associadas com a palavra anarquia, a criptoanarquia o governo não é temporariamente destruído mas sim permanentemente proibido e desnecessário. É uma comunidade onde a ameaça de violência é impotente porque a violência é impossível, e ela é impossível devido seus participantes não serem linkados com o seu verdadeiro nome ou sua verdadeira localização.
> (Wei Dai, 1998)

Neste artigo, portanto, Wei Dai (1998) descreve a ideia inicial de criptomoeda como uma possibilidade de transferir uma quantidade de moedas para um outro individuo utilizando um mecanismo de criptografia para encobrir o seu rastro, tornando este sistema mais seguro do que os meios tradicionais de transação.

3.2. Digi Cash

Uma das primeiras formas de pagamento baseado em criptografia que podemos encontrar foi a *Digicash*, essa moeda foi criada por David Chaum em 1989. David Chaum foi o criador do *Blind Signature Technology* que tinha como objetivo além de esconder a mensagem como é a definição da palavra criptografia, mas também de esconder quem enviou e quem recebeu tal informação, no caso transação financeira com a *Digicash*. (Maulid, 2008)

A Digicash diferentemente das moedas atuais era um sistema de pagamento que necessitava de *software* para permitir que usuários saquem ou até mesmo transfiram dinheiro entre eles e era uma moeda centralizada em uma empresa. Devido sua promessa de superioridade em termos de segurança para seus usuários alguns bancos compraram o sistema entre eles o *Mark Twain Bank e o Deutsche Bank*.

Porém em 1998 a *Digicash* declarou falência após ter suas tentativas de ampliar sua base de clientes frustrada, segundo David Chaum o motivo de seu fracasso foi de que o comércio eletrônico não estava suficientemente desenvolvido na época para seu uso, tendo então em 2002 os ativos da empresa vendidos. (Greenberg, 2016)

3.3 Blockchain

Como informado no item anterior a *Digicash* diferente das criptomoedas atuais era uma moeda centralizada, nesse caso fica a dúvida sobre o que é uma moeda não centralizada e como elas funcionam.

A criptomoeda que modificou essa forma de centralizado para descentralizado foi a bitcoin com sistema chamado de *Blockchain*. (Tapscott, 2013)

A forma mais comum e usada até hoje para proteger informações na internet é de alocá-las em um determinado computador e criar sistemas de bloqueio contra a entrada de usuários não autorizados. Assim funcionam os sistemas de bancos do seu computador pessoal, empresas e até mesmo as informações que armazenamos em nuvens como *Dropbox*.

No *Blockchain* as suas informações não ficam armazenadas em apenas um computador, mas sim em um grupo de computadores que recebem suas informações criptografadas e as armazenam permitindo somente quem tem a chave obter tal informação novamente. Com esse modelo de segurança fica muito mais difícil para algum hacker entrar e modificar alguma informação como por exemplo a quantidade de moeda que você possui, isso ocorre pois ele só irá conseguir modificar a informação em um computador, mas quando ela for confrontada com os demais da rede ela não será aprovada. (Tapscott, 2013)

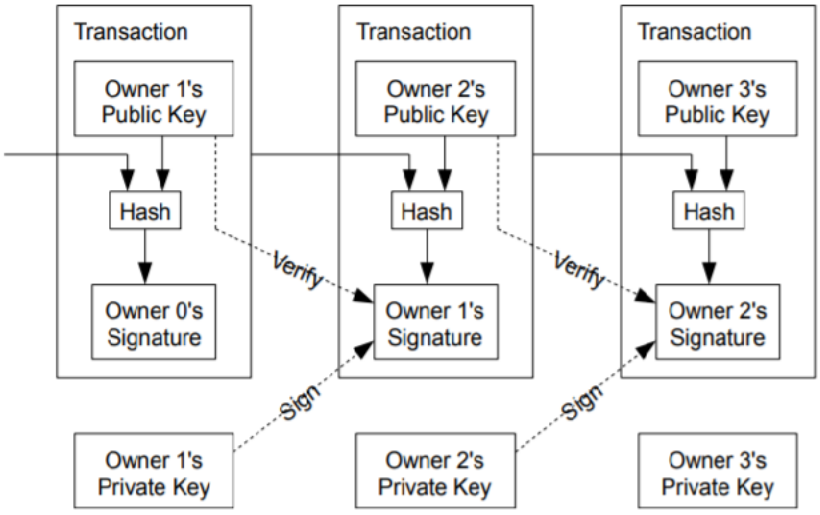

Figura 1 – Blockchain

Fonte, Bitcoin a peer-to-peer electronic cash system

Satoshi Nakamoto

Sendo assim podemos afirmar que o sistema de *blockchain* usado hoje pelas criptomoedas como *bitcoin* é considerado por muitos como mais seguro que o modelo utilizado pelos bancos comercias. Vendo isso alguns bancos atuais estão tentando

desenvolver sistemas de segurança baseados no modelo utilizado pelo *bitcoin* com algumas diferenças. (Kelly, 2017)

No caso do *blockchain* dos *bitcoins* as informações são verificadas através de mineradores anônimos em diversos lugares do mundo, já no modelo que os bancos estão buscando desenvolver é criar um sistema de *blockchain* privado onde as informações serão verificadas por uma rede de computadores privados do próprio banco. (Silva, 2016, p. 525)

3.4. Bitcoin

Quando estamos buscando analisar se as criptomoedas serão a moeda do futuro precisamos entender e verificar o que é e como começou *a Bitcoin*, a criptomoeda mais famosa e com maior valor financeiro atualmente.

O *Bitcoin* é um meio de pagamento eletrônico que possibilita aos usuários efetuar transferências instantaneamente entre si, até mesmo operações internacionais com rapidez e segurança. Segundo Tu e Meredith (2015, p.277), o *Bitcoin* “é um meio de troca criado e armazenado eletronicamente, sem possuir apoio de uma autoridade por parte do governo, banco central ou uma mercadoria como o ouro. Assim como as moedas tradicionais, o *Bitcoin*, pode ser usado para adquirir bens e serviços de qualquer pessoa que esteja disposta a aceitá- la como forma de pagamento”.

O conceito de criptomoedas surgiu no final dos anos 80, porém ela só virou assunto comum entre as pessoas após a criação *do Bitcoin* que se iniciou com um artigo publicado por Satoshi Nakamoto. Até o presente momento não existe nenhuma confirmação com 100% de certeza sobre quem realmente é Satoshi Nakamoto, todas as suas comunicações com os demais programadores do *Bitcoin* foram feitas através de servidores que não possibilitem nenhuma forma de rastreabilidade. Muito se especula sobre quem pode ser esse misterioso criador do *Bitcoin*.

Satoshi Nakamoto escreveu em 2008 um artigo no qual ele expõe a sua ideia de como deveria funcionar o modelo do *Bitcoin* a fim de buscar outros interessados para auxiliá-lo na programação do mesmo.

Neste artigo ele deixa claro que a sua intenção com o *Bitcoin* é de criar um sistema *peer-to-peer*, em tradução livre, “par-a-par”, na qual não necessite de uma terceira parte recebendo uma comissão para a realização de uma transação (Nakamoto, 2008).

> Uma transação de dinheiro puramente peer-to-peer permitirá pagamentos online serem enviados diretamente de um usuário para outro sem a necessidade de passar por alguma instituição financeira. A assinatura digital providencia parte da solução, porém o maior beneficio é perdido se for necessário de um terceiro para verificar e evitar o problema de double-spending (pagamento duplo). Para isso nós propomos uma solução ao problema de pagamento duplo usando a rede peer-to-peer. A rede cria um carimbo de horário em cada transação e envia para a continuidade do sistema criando uma hash-based proof-of-work, formando uma linha de informações que não podem ser alterados sem refazer o processo de proof-of-work. (Nakamoto, 2008, p. 1)

Segundo Nakamoto (2008), o *Blockchain* possibilitaria a criação de uma moeda na qual não haveria a necessidade de nenhuma instituição ou indivíduo controlar e gerenciar o sistema de pagamentos. Sendo assim, o sistema é todo mantido por pessoas anônimas espalhadas pelo mundo, onde ninguém teria a capacidade de controlar sozinho a demanda e a oferta de moeda. Com isso os indivíduos nao ficam reféns de um sistema que pode ser alterado com objetivo de favorecer um governo uma empresa ou até mesmo um individuo em especifico.

Com esse modelo, Nakamoto (2008) argumentou se haveria a necessidade da participação dos bancos na execução das transações financeiras entre usuários. Segundo o autor, a não participação de tais intermediários neste processo eliminaria os custos que estas instituições impõe ao sistema ao cobrarem para desempenhar a função de intermediador financeiro, além de minimizar os riscos referentes à capacidade dos mesmos honrar os compromissos financeiros perante os seus clientes.

Existem dois modelos de criptografia, o simétrico e o assimétrico. No modelo simétrico, a forma de verificação das informações e sua decodificação ocorre por meio de uma chave única na qual o usuário possui. Já no modelo de criptografia assimétrico, ele é feito por meio de duas chaves; uma chave de posse do usuário e

outra, chamada de chave pública, que deve ser utilizada simultaneamente com a chave privada (pertencente ao usuário) para o processo funcionar, uma vez que a chave pública e a chave privada são inversamente correspondentes, ou seja, tudo o que é cifrado pela chave pública é decifrado pela chave privada.

Com este modelo de criptografia assimétrico, que utiliza duas chaves, o usuário deve sempre zelar pelo armazenamento e segurança da sua chave privada, para evitar que ela seja roubada ou que seja esquecida, pois não há outra forma de recuperar suas "moedas" sem ela.

Ulrich (2014) descreve o mecanismo de como se processa esta operação:

> "[...]Tal mecanismo exige que a cada usuário sejam atribuídas duas "chaves", uma privada, que é mantida em segredo, como uma senha, e outra pública, que pode ser compartilhada com todos. Quando a Maria decide transferir bitcoins ao João, ela cria uma mensagem, chamada de "transação", que contém a chave pública do João, assinando com sua chave privada. [...] A criptografia de chave pública garante que todos os computadores na rede tenham um registro constantemente atualizado e verificado de todas as transações dentro da rede Bitcoin, o que impede o gasto duplo e qualquer tipo de fraude. " (Ulrich, 2014, p. 18-19)

O *Bitcoin* é muito conhecido devido à sua grande volatilidade, e porque tem sido alvo de intenso debate e estudos. Também, é conhecido por ser um "ativo" desejado por investidores (que possuem consciência dos riscos e ganhos) e curiosos - na sua maioria composto por pessoas com pouco conhecimento do mercado de criptomoedas - que almejam lucros rápidos e fáceis.

O gráfico abaixo demonstra, utilizando *candle sticks* mensais, a medida da valorização do Bitcoin entre os períodos de 2012 a 2017, com valores expressos em reais.

Figura 2 – Valorizaçao da Bitcoin

Fonte https://www.mercadobitcoin.com.br/graficos

As sucessivas altas no valor das criptomoedas tem atraído a atenção de diversos investidores que têm aplicado seus recursos nesta espécie de “ativo”. Esta nova modalidade de “ativo financeiro” transformou-se no centro das atenções dos principais mercados do mundo, e diariamente ouve-se falar através de jornais, revistas e periódicos, sobre os perigos, oportunidades e sobre o futuro deste novo “investimento”. (EFE, 2017)

É importante comentar que o objetivo desse trabalho não é o de verificar qual a razão da valorização dos Bitcoins, mas sim de apresentar sua definição, seu histórico e argumentar se o uso em larga escala desta criptomoeda é possível em um futuro próximo como um dos principais meios de pagamento.

3.5 Mineração de bitcoin

Um dos pontos que difere o *Bitcoin* das moedas tradicionais como o dólar ou o euro, pois não possui uma entidade para imprimir ou controlar sua base monetária. Sendo assim, como é criado o Bitcoin e como é regulada a sua quantidade? (Rosic, 2016)

O meio de obtenção do *Bitcoin* é chamado de mineração, cujo processo, basicamente, consiste em adquirir digitalmente a propriedade de determinado número de criptomoedas a partir de um intenso processamento computacional realizado pelo *hardware* do computador de uma pessoa que realiza essa operação. Nakamoto (2008) utilizou como metáfora a mineração de ouro para criar o seu processo de controle da base monetária.

Para o sistema de *blockchain* funcionar é necessário que tenham computadores realizando verificações constantes dos blocos que estão sendo criados a fim de permitir maior segurança para os seus usuários.

. Sendo assim, a forma como foi desenvolvida a mineração de *Bitcoins* visava incentivar os indivíduos a realizarem essas verificações, oferecendo como recompensa um determinado número de *Bitcoins* a cada número X de verificações realizadas. Esse *Bitcoin* adicional que o minerador recebe é “uma moeda” que não fazia parte da base monetária existente anterior, portanto, verifica-se uma ampliação da base monetária com a mineração.

Essa mineração vem se tornando a cada ano mais complexa de ser realizada devido ao aumento no número de verificações necessárias. Para os mineradores existem dois pontos principais que os fazem decidir quanto se é ou não vantajoso a mineiraçao dos *bitcoins*. (Kobbie, 2017)

A primeira questão é qual o custo da energia elétrica e multiplicado pela quantidade necessária para se minerar uma bitcoin, nos últimos anos empresas estão produzindo hardware especifico para a mineração de bitcoin com o avanço da tecnologia esses hardwares tem uma menor quantidade de calor e por consequência menor consumo energético para o processamento de informações necessárias na mineração.

Mesmo com esses avanços nos equipamentos ainda assim uma elevação no preço da energia pode e deve impedir com que muitos usuários continuem a minerar considerando que tal aumento impacta diretamente sua rentabilidade. A questão da

maior complexidade das minerações também faz com que diversos usuários que hoje conseguem minerar utilizando seus computadores sejam expelidos do sistema caso não realizem novos investimentos em equipamentos mais modernos, potentes e eficientes.

A outra questão é o preço da bitcoin, como o resultado e recompensa da mineração é a obtenção de uma nova bitcoin, o preço da mesma no mercado é um fator chave para se considerar a viabilidade ou não da mineração portanto podemos afirmar que a abrupta valorização da moeda teve como resultado um maior incentivo a novos mineradores ou até mais investimento em Hardware especifico para mineração como placas de vídeo processadores, dos mineradores atuais.

A título de curiosidade em novembro de 2017 foi verificado que se todas as máquinas ligadas ao bitcoin fossem considerada uma nação ela seria a 61 nação em consumo de energia do mundo, tendo um consumo superior que o de 20 nações europeias. (Ribeiro, 2017)

Para controlar a quantidade de criação de moedas o sistema recalcula a cada 2016 blocos que são aproximadamente 2 semanas. Caso a quantidade de mineradores tenha aumentado muito o sistema envia fórmulas mais complexas para serem resolvidas, aumentando o tempo para a criação de cada moeda.

Consequentemente, o lucro dos mineradores é reduzido devido a quantidade maior de tempo demandado para a mineração e também devido aos maiores gastos necessários com energia elétrica e na aquisição de *hardwares* mais potentes para realizar tal processo. A figura abaixo ilustra tal processo.

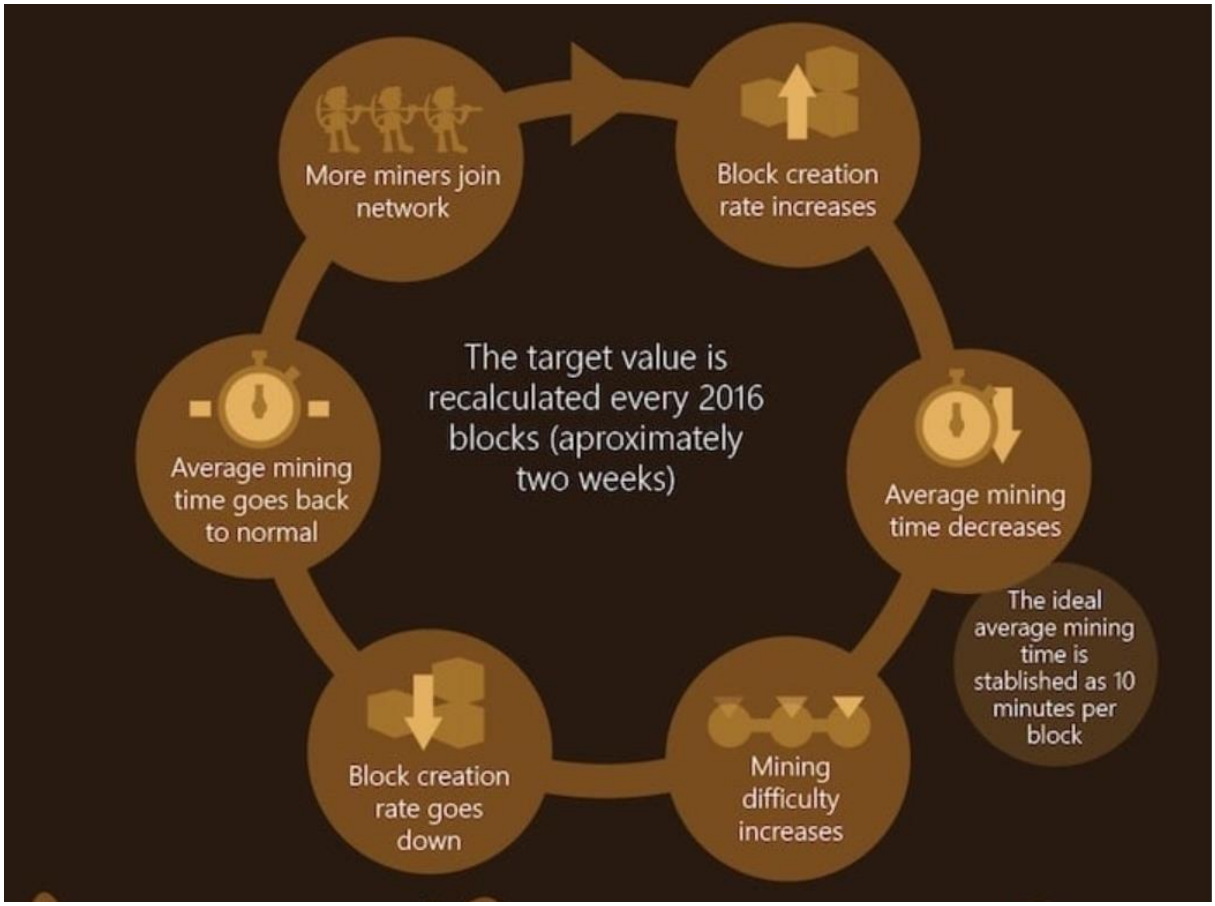

Figura 3- Mineração de bitcoin
Fonte - https://www.bitcoinmining.com/

Com o *blockchain* o sistema de *Bitcoins* autorregula a quantidade de moeda que está sendo emitida. Além disso, o *blockchain* possui em sua programação um mecanismo para reduzir a quantidade de *Bitcoin* a ser minerado pela metade entre um ano e outro, e assim é possível determinar o número máximo de *Bitcoins* que podem ser criados. Nakamoto (2008) previu que a quantidade de Bitcoins que podem ser produzidos é de 21 milhões de unidades até 2140. (Nakamoto, 2008)

Em resumo uma mineração é o processamento e validação de transações de bitcoin realizada por computadores de diversas pessoas ao redor do mundo tendo como recompensa 1 bitcoin por tal tarefa. E essa bitcoin adicional é a forma na qual se possibilita o crescimento da base monetária de bitcoin na qual tem um crescimento a taxas decrescentes.

4 Silk Road e Bitcoin

Os *Bitcoins* nem sempre foram associadas à valorização e especulação do mercado como ocorre hoje em dia. Inicialmente, elas eram conhecidas por serem moedas utilizadas para realizar operações não legais no “mercado negro”, para aquisição de produtos ilegais e para a contratação de serviços criminosos ou suspeitos. O caso mais famoso foi o do site chamado *Silk Road* - em tradução livre caminho da seda.

Segundo Bearmen (2015), em 2011 Ross Ulbricht teve a ideia de associar a possibilidade de transações anônimas com o *Bitcoin* e o anonimato da *internet* utilizando *TOR* (um navegador alternativo de *Internet* que não deixa rastros digitais usualmente utilizado por quem quer acessar a chamada “*Deep Web”).*

Com o TOR o que ocorre é que ao dar um comando para buscar uma determinada informação, esse comando não é enviado diretamente para a busca da informação, mas sim é enviado para diversos computadores ao redor do mundo até que seu comando não seja mais possível de ser rastreado e então para a informação solicitada. (Vieira, 2013)

Ao ligar essa forma anônima de navegar na internet com o anonimato oferecido pelo meio de pagamento *Bitcoin* o *Silk Road* se tornou o ambiente perfeito para o comércio de produtos ilegais, em sua maioria drogas como cocaína, heroína, LSD, dentre outras formas de psicotrópicos que eram anunciadas no site, compradas com *Bitcoin* e enviadas pelo correio para seus destinatários finais, tudo sem, teoricamente, deixar rastros.

O site foi fechado pelo *FBI* em 2013 após uma intensa investigação onde Ross Ulbricht foi preso em flagrante com seu computador logado, como administrador, no *Silk Road*. Alguns meses depois o site foi reaberto com uma versão chamada de *Silk Road* 2.0 que também foi fechado pelo *FBI* e seu outro administrador preso. Atualmente, ainda existem diversos sites que utilizam TOR e criptomoedas para comercializar produtos ilegais (Bearman, 2015).

Quando ocorreu o primeiro fechamento do *Silk Road* as pessoas temiam que o preço do *Bitcoin* fosse desvalorizar de forma abrupta devido à importância do site e a crença de que *Bitcoin* eram quase que exclusivas para tal finalidade. O que se provou depois errado pois a desvalorização foi muito pequena, mas até hoje *Bitcoin* é o meio de pagamento mais utilizado para crimes na *internet* (Roberts, 2017).

5 Regulamentação de criptomoedas

Um dos aspectos que mais podem influenciar sobre o futuro das criptomoedas é a forma como elas serão regulamentadas.

Os idealizadores dessas criptomoedas, tais como Wei Dai e Nakamoto, objetivavam criar um sistema de pagamentos que não tivesse a interferência do governo, no qual tanto o governo como as instituições bancárias não fossem necessárias para promover o seu funcionamento.

A expansão do volume de negociaões com as criptomoedas aumentou tanto – especialmente com o *Bitcoin* - que, atualmente, parece impossível manter este sistema sob o controle das instituições jurídicas e regulatórias, nacionais e internacionais. Muitos veem esta interferência institucional como uma tentativa de barrar o crescimento das moedas virtuais, enquanto que outros acreditam que tal medida pode gerar legitimidade à este tipo de “moeda”, permitindo o seu crescimento e consolidação (Joshi, 2017)

Sejam quais forem as consequências de tais medidas, observa-se que moedas com tamanho volume de negociação e valores unitários necessita de regulamentação para garantir o correto funcionamento do mercado e para a proteção dos próprios demandantes deste tipo de “ativo”.

Um dos motivos mais usados para justificar a regulamentação das criptomoedas é para evitar a existência de “lavagem de dinheiro” e para coibir que essa seja um meio de pagamento usado por pessoas que queiram obter e fornecer produtos ou serviços ilegais de forma anônima.

Sendo assim, é preciso debater os aspectos que envolvem a regulamentação das criptomoedas e os reais motivos para a adoção de tais medidas. A forma como será feita a regulamentação impacta diretamente sobre o futuro uso deste tipo de moeda.

As regulamentações das criptomoedas, como o *Bitcoin,* estão sendo realizadas de forma diferente em diferentes países. Alguns países proíbem o uso das criptomoedas, alegando ilegalidade e sujeitando os utilizadores desta forma de transação monetária à prisão. Um exemplo desta forma de controle é exercida pelo governo de Bangladesh que utiliza as leis de lavagem de dinheiro como referência para adotar tal postura frente à utilização de criptomoedas.

Outros países, tal como a Irlanda, permitem o uso de tais moedas virtuais sem que ocorra nenhum tipo de regulamentação.Já o Estados Unidos possui uma onda de regulamentação das criptomoedas com diferentes regras a depender da definição dos legisladores de cada estado.

5.1 Criptomoedas e o governo

Como vimos até o momento algumas criptomoedas como no caso da bitcoin podem e são mais seguras para armazenar a quantidade monetária de criptomoedas. Ou seja, se uma pessoa possui 1 bitcoin ela tem mais garantia e segurança de manter esse bitcoin que se um indivíduo possuir 1 real na sua conta do banco, isso não quer dizer que o seu valor monetário está mais seguro em bitcoins que em reais, apenas que é mais difícil de um hacker roubar seu 1 bitcoin que seu 1 real no sistema do banco.

Mas de qualquer forma o seu valor monetário pode reduzir drasticamente no bitcoin e até o momento não é possível afirmar qual a opção mais segura para se preservar o valor monetário bitcoin ou outras moedas. Mesmo que esse fosse o objetivo teríamos que primeiramente definir com relação a moeda de qual país que queremos comparar, ou até mesmo se a melhor opção é comparar com outra moeda ou com outros investimentos considerando o fato de muitas pessoas estarem utilizando bitcoins como uma forma de investir seu dinheiro e não apenas preservar seu valor. (Joshi, 2017)

De qualquer forma a questão que fica agora é de como fica o governo com relação as criptomoedas, se as criptomoedas não necessitam de nenhum agente para controlá-las e são em grande parte anônimas como fica a relação delas com o governo. Nem o governo nem nenhuma pessoa tem a capacidade de controlar a bitcoin por exemplo sendo assim vemos que caso essa se torne a unidade monetária global do futuro eles perderão uma importante capacidade de expandir ou reduzir a base monetária, algo importante para algumas economias se financiarem ou atuarem durante crises.

De outro lado se ninguém consegue controlar essa moeda como que um governo pode bloquear ela. Temos um caso recente onde o governo chinês famoso por bloquear diversas empresas de internet decidiu banir também a bitcoin.

Esse bloqueio não ocorre na bitcoin mas sim nas chamadas casas de câmbio que negociam a bitcoin, para um indivíduo comprar ou vender um determinado valor de bitcoin ele deve então ir até uma dessas chamadas casas de câmbio e trocar ou seu valor monetário do pais por bitcoins ou suas bitcoins por determinado valor monetário. Ao bloquear essas casas de câmbio você torna mais difícil a continuidade das operações desse dinheiro em seu país. (Wildau, 2017)

6 Criptomoedas e o que precisam para sobreviver

Para uma criptomoeda se tornar o meio de pagamento mainstream ela necessita que as empresas desenvolvam 3 itens, casas de câmbio, carteiras virtuais e sistema de pagamentos. As casas de câmbio seriam os locais (sites ou físicos) onde o usuário pode trocar suas moedas através da cotação do dia, as carteiras virtuais são a segunda parte do processo muitas vezes já oferecidas junto com as casas de câmbio que são formas nas quais as pessoas podem armazenar suas bitcoins de forma simples e segura. (Cannucciari, 2017)

Como demonstrado anteriormente as bitcoins funcionam com a criptografia aleatória onde o usario deve manter a sua chave privada em segurança, porém devido o risco de caso o usuário perca a chave ele não tenha mais como acessar seus bitcoins algumas carteiras virtuais estão mantendo essas chaves de segurança privada com elas além do usuário para oferecer uma forma de recuperar tais informações. A recomendação mais segura, no entanto, permanece sendo manter a chave privada única e exclusivamente com o usuário final detentor de suas bitcoins.

Outro item importante para a propagação das criptomoedas são de criar sistemas de pagamentos nos quais aceitem as mesmas de forma simples e segura, até o momento temos visto alguns sites na internet ainda de forma pouco significativa aderirem a esse modelo. E quando procuramos lojas físicas que aceitem criptomoedas vemos que seu número é ainda menor, para um desenvolvimento saudável e correto desses sistemas de pagamentos. Faz se necessário uma atuação do governo em termos de regulamentação para maior credibilidade do mesmo.

7 Riscos Imprevisíveis

As criptomoedas tem se mostrado até o presente momento como uma forma extremamente segura contra-ataques de hackers o que pode justificar a confiança de muitos na mesma, porém devemos sempre considerar que a tecnologia está em constante aprimoramento e de forma exponencial.

Sendo assim considerar que uma moeda como o caso do bitcoin que já está programada e não permite com que nenhum individuo ou instituição a manipule não tenha alguma forma de hacker até a data onde ela está programada para crescer 2140 parece muito utópico.

Essa constatação não torna a criptomoedas como algo impossível de se tornarem a moeda do futuro mas apenas coloca uma questão de até quando elas serão tal moeda, mesmo que não tenhamos agora uma resposta para tal pergunta é importante considerarmos esse ponto.

A base dessa moeda se dá pela forma de criptografia conhecida e usada atualmente, novos modelos de criptografia podem aparecer deixando a bitcoin por exemplo desatualizada ou até mesmo hackeável.

Outro sistema de segurança advém dos chamados blockchains e como o próprio Satoshi Nakamoto coloca em seu artigo White paper (2008) a única forma de hackear esse sistema é tendo uma máquina com poder de processamento superior ao de 50% da rede de *blockchain* algo que com o modelo atual parece impossível mas com o desenvolvimento dos computadores quânticos pode ser mais uma questão a ser abordada.

Como colocado no título tais riscos são imprevisíveis e tentar determinar sua probabilidade de acontecer parece algo próximo do impossível, porém não considerá-los seria um tanto ingênuo de nossas partes.

9 Conclusão

O objetivo desse trabalho era de buscar entender se as criptomoedas serão a moeda do futuro, porém com o decorrer do mesmo surgiram mais dúvidas que respostas a tal pergunta.

No final de 1800 foi realizado um estudo em Nova York que foi publicado pelo New York times na época de que existia uma preocupação muito grande em como a cidade lidaria em 100 anos com a quantidade de cavalos e por consequência fezes de cavalo na cidade. Estudiosos na época alertavam para o fato de que com o aumento constante na quantidade de cavalos as doenças advindas das fezes também se elevariam.

Atualmente tal informação parece algo irreal e vemos que o meio de transporte foi substituído pelo automóvel, porém os estudos na época não tinham informações suficientes para conseguir identificar que tal fenômeno ocorreria e então fizeram uma projeção considerando as informações do passado.

Assim como esse estudo, acredito que concluir esse trabalho com uma resposta exata e afirmativa sobre as criptomoedas serem ou não a moeda do futuro não levaria em conta mudanças futuras que podem e vem ocorrendo.

Foi observado que as criptomoedas possuem um sistema de blockchain em seu funcionamento que as torna mais seguras contra ataques hackers que qualquer outro sistema de segurança bancário utilizado atualmente. Isso demonstra que pode e está havendo uma mudança nos sistemas de segurança do mundo para esse novo blockchain, mas não prova que devido a essa maior segurança os bancos passaram a utilizar alguma criptomoeda existente.

Foi possível verificar que as criptomoedas possuem as três características básicas de uma moeda sendo elas, I. Meio de troca, instrumento intermediário de aceitação geral. II. Unidade de conta, e III. Reserva de valor. Isso é importante pois

prova que elas possuem então o mínimo necessário para se tornarem uma moeda, mesmo que o fator meio de troca com aceitação geral seja possível questionar até onde é considerada essa aceitação geral da bitcoin.

Os fatores principais que chamaram a atenção e que parecem ser os maiores determinantes sobre o futuro das criptomoedas são, se elas possuem um valor de uso e como os governos estão agindo com a regulamentação das mesmas.

Ao observar o fenômeno da bitcoin (criptomeoda mais famosa e de maior volume) vemos que a maioria das manchetes de jornais e revistas abordam o tema devido a sua valorização abrupta. Isso demonstra que o maior interesse das pessoas que buscam a moeda é de especulação e ganhos financeiros elevados, tal fato não pode ocorrer infinitamente levantando então a questão de o que as pessoas que estao comprando a bitcoin para valorização farão quando a mesma parar de valorizar, ou diminuir a sua valorização.

Caso tal moeda tenha um valor de uso real, ou seja, tenha aceitação e permita usuários a realizarem compras utilizando a mesma como meio de pagamento evitaria uma redução na demanda da mesma mantendo assim o seu preço estável e oferecendo um possível futuro para a mesma.

Porém, para isso ocorrer é necessário que exista um crescimento nos meios de pagamento que aceitam criptomoedas. Até o momento quase no fim de 2017, poucos estabelecimentos aceitam criptomoedas e os que aceitam chegam a ser mostrados em manchetes de jornal como algo inovador. Caso seja observado no futuro um aumento significativo de locais que aceitem criptomoedas e que o mesmo se torne algo corriqueiro, é então plausível afirmar que estamos em uma direção de tornar as criptomoedas a moeda do futuro.

O outro fator considerado um dos principais determinantes do futuro das criptomoedas é a regulamentação governamental das mesmas, até hoje não se tem uma forma única de regulamentação, existem alguns países que a proíbem e outros que as liberam ignorando sua existência ou com regulamentações já definidas. Enquanto não houver uma maior certeza a respeito de como as criptomoedas serão regulamentadas não será possível definir o seu futuro.

Concluindo assim que as criptomoedas possuem grandes possibilidade de se tornarem a moeda do futuro, mas que para isso ocorrer devemos observar alguns fatores supracitados, não incentivando a aplicação em criptomoedas como um meio

de investimento rentável e com certeza de ganhos mas sim como uma aposta altamente arriscada.

REFERÊNCIAS

Assange, J. (2012). *Liberdade e o Futuro da internet Cypherpunks .* Sao paulo: Boitempo.

ALMEIDA, P. B. O futuro da competição monetária: O comportamento da moeda Bitcoin e o seu impacto sobre as politicas de Bancos Centrais. 2016. Disponível em: <https://repositorio.ufsc.br/bitstream/handle/123456789/167758/339958.pdf?sequence=1>.
Acesso em: 01/04/2017.

BANCO CENTRAL DO BRASIL (BACEN). BC esclarece sobre riscos decorrentes da aquisição das chamadas "moedas virtuais" ou "moedas criptografadas". Brasília, 2014
Disponível em:
<https://www3.bcb.gov.br/normativo/detalharNormativo.do?method=detalharNormativo&N=
114009277>. Acesso em: 01/05/2017

Bearman, J. (15 de 10 de 2015). *Wired*. Fonte: Wired: https://www.wired.com/2015/04/silk-road-1/

Bitcoin.org. (2015). Fonte: https://bitcoin.org/en/faq#what-is-bitcoin

Cannucciari, C. (Diretor). (2017). *Banco ou Bitcoin* [Filme Cinematográfico].

Dai Wei http://www.weidai.com/bmoney.txt

EFE, A. (2017). *G1*. Fonte: https://g1.globo.com/economia/mercados/noticia/febre-do-ouro-digital-no-japao-faz-valor-do-bitcoin-disparar-no-mundo.ghtml

Gold, L. (Diretor). (2017). *Testes da vida academica* [Filme Cinematográfico].

Joshi, D. (20 de 10 de 2017). *Business insider* . Fonte: http://www.businessinsider.com/blockchain-cryptocurrency-regulations-us-global-2017-10

Kelly, B. (2017). *Forbes*. Fonte: Forbes : https://www.forbes.com/sites/briankelly/2017/10/24/why-bitcoin-matters-more-than-blockchain/#594ac5bb37ac

LAAN, Cesar Rodrigues van der. É Crível uma Economia Monetária Baseada em Bitcoins? Limites à disseminação de moedas virtuais privadas. Senado Federal. Texto
para Discussão nº 163. 2014. Disponível em:
<https://www12.senado.leg.br/publicacoes/estudos-legislativos/tipos-de-estudos/textos-paradiscussao/td163/view>.
Acesso em: 01/04/2017

Maulid, H. (2008). The Implementation of Blind Signature in Digital Cash. pp. 2-6.

Nakamoto, S. (2008). Bitcoin a Peer-to-Peer Eletronic Cash Sistem. p. 1.

NAKAMOTO, S. Bitcoin: A Peer-to-Peer Eletronic Cash System. (S.L.). 2008 Disponível
em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 01/04/2017

Roberts, J. J. (2 de 10 de 2017). *Fortune*. Fonte: Fortune: http://fortune.com/2017/10/02/bitcoin-sale-silk-road/

Rosic, A. (21 de 12 de 2016). *Hufffington post*. Fonte: huffpost: https://www.huffingtonpost.com/ameer-rosic-/what-is-bitcoin-mining-a-_b_13764842.html

Tapscott, D. (2013). *Blockchain Revolution.* New York: An imprint fo penguin Radom house LLC.

Vieira, L. (21 de 11 de 2013). *Techtudo*. Fonte: Techtudo: http://www.techtudo.com.br/tudo-sobre/tor.html

Wildau, G. (7 de 9 de 2017). *Fianancial Times*. Fonte: https://www.ft.com/content/d576e4e4-c374-11e7-a1d2-6786f39ef675

YERMSCK, D. Is Bitcoin a Real Currency? An economic appraisal. Cambridge. National
Bureau of Economic Research nº 19747, 2013. Disponível em:
<http://www.nber.org/papers/w19747>. Acesso em: 13/09/2016