



UNIVERSIDADE ESTUAL PAULISTA JÚLIO DE MESQUITA FILHO
FACULDADE DE CIÊNCIAS E LETRAS
DEPARTAMENTO DE CIÊNCIAS ECONÔMICAS

TRABALHO DE MONOGRAFIA
Curso de Ciências Econômicas

**BITCOIN: FUNCIONAMENTO E CARACTERÍSTICAS DE UMA
CRIPTOMOEDA**

Graduando: Muriel Pavan dos Santos

2016
ARARAQUARA-SP

Novembro de 2016.

Graduação em Ciências Econômicas pela Faculdade de Ciências e Letras de
Araraquara.



BITCOIN: FUNCIONAMENTO E CARACTERÍSTICAS DE UMA CRIPTOMOEDA

Muriel Pavan dos Santos

RA: 130894-7

ARARAQUARA-SP
NOVEMBRO DE 2016.

MURIEL PAVAN DOS SANTOS

**BITCOIN: FUNCIONAMENTO E CARACTERÍSTICAS DE
UMA CRIPTOMOEDA**

Trabalho de Monografia apresentada ao Prof. Dr. Rogério Gomes, como requisito final para a conclusão do curso de graduação em Ciências Econômicas, tendo como orientador de conteúdo o Prof. Dr. Rogério Gomes.

Agradecimentos

Agradeço aos professores que sempre mantiveram aceso meu senso crítico, ao Prof. Dr. Rogério Gomes, por aceitar um tema tão fora da curva, aos meus amigos (Tuvão, Wellington e Chun) por toda a ajuda durante a universidade e ao apoio dos meus pais durante todo o percurso da graduação.

Resumo

As criptomoedas são, de forma sucinta, uma nova forma de moeda. A Bitcoin, criada em 2009 por Satoshi Nakamoto, é a maior criptomoeda e a responsável por trazer ao mundo a tecnologia do *blockchain*. As chamadas moedas digitais são *peer-to-peer* e não dependem de um emissor central para validar e conferir as transações. Todo o software é de código aberto e seu funcionamento segue leis matemáticas. O presente trabalho tem caráter exploratório e pretende explicar o funcionamento básicos das criptomoedas, além de tentar encaixá-las dentro do conceito clássico e do conceito austríaco da *moeda*.

Palavras-chave: criptomoeda, *bitcoin*, *blockchain*.

Abstract

Cryptocurrencies are, in a succinct way, a new form of currency. The Bitcoin, which was created in 2009 by Satoshi Nakamoto, is the biggest cryptocurrency and the responsible for a new technology called blockchain. The digital currencies are peer-to-peer and don't need a central node in the transaction map to endorse and authenticate the transactions. The software is open-source and it works following mathematical principles. This paper is merely exploratory, explain only the basics about the cryptocurrency and also try to analyze if them can be called as "currency" using the 'classical' definition or if the austrian definition fits better.

Keywords: cryptocurrency, bitcoin, blockchain.

Sumário

Introdução.....	9
1. Origem e funcionamento das criptomoedas.....	10
1.1. Desdobramentos, regulações e legislações.....	18
2. As características econômicas das criptomoedas.....	23
2.1.1 A definição de moeda e características.....	23
2.1.2 A escassez e virtualidade.....	26
2.1.3 As críticas às criptomoedas.....	28
3. Síntese e comparativo entre os meios de pagamento.....	29
4. Referências Bibliográficas.....	32
5. Anexos e mídia digital consultada.....	34

Introdução

Qualquer leitor que checou as notícias dos cadernos de Economia ou Finanças nos últimos tempos pôde conferir, com tons de desconfiança, um termo bastante novo: um novo meio de pagamento virtual, o Bitcoin. A mídia econômica especializada e até alguns outros veículos têm tratado tal novidade mais como curiosidade, como um novo artifício do sistema econômico-monetário, do que como uma moeda. Mas, será válido chamá-la de moeda? O que seriam, exatamente, as criptomoedas? O que seriam, sinteticamente, as criptomoedas, especialmente a Bitcoin? Elas têm legalidade? Como surgiram? O que se pode comprar com elas? Quem é seu fiador ou avalista? Como funcionam tecnicamente? Essas talvez sejam os primeiros questionamentos sobre o projeto Bitcoin. Esta monografia, que possui o caráter exploratório, uma vez que foi concebida em um momento de abertura do mercado das moedas virtuais e, por isso, de escassa literatura sobre o assunto, procura abordar algumas dessas questões.

1. Origem e funcionamento das Criptomoedas

As criptomoedas¹ são, de modo sucinto, um meio de troca criptografado que funciona baseado em uma rede descentralizada de computadores conectados (uma rede peer-to-peer). Diferenciando-se do sistema bancário convencional, as criptomoedas não dependem de um órgão centralizador para controlar e verificar as transações. Toda distribuição e oferta de moedas é dada pelo sistema (código-fonte) da criptomoeda em questão. O termo “criptomoeda” foi cunhado em uma lista (mailing list) de discussões Cypherpunk² em 1998. Wei Dai³ (pseudônimo) publicou um manifesto idealizando uma rede de pagamentos que não dependesse de um órgão central controlador. Pouco tempo depois, surgia o Bit Gold⁴, uma espécie de precursor do Bitcoin que iniciou a utilização do *proof-of-work*. Utilizando-se do *proof-of-work*, da plataforma *peer-to-peer* (ponto-a-ponto), da criptografia, e do *blockchain* Satoshi Nakamoto criou, em 2009, o Bitcoin. Também conhecidas como moeda digital, ganharam notoriedade pública especialmente por atingir valor de mercado e algumas possibilidades especiais da utilização dessa moeda.

Antes da invenção da Bitcoin, todas as transações online (entre duas partes) necessitavam de três pontos de ligação. Por exemplo: pessoa A quer enviar dinheiro para pessoa B. Para tal, tanto a pessoa A quanto a pessoa B precisam de um serviço de um terceiro agente confiável, intermediário, C. Tal agente é responsável por debitar da conta da pessoa A a quantia que esta deseja enviar para a pessoa B e creditar esta mesma quantia na conta da pessoa B. Esse processo, claro, envolve taxas. Nota-se que, sem o intermediário, seria impossível evitar o clássico problema do “gasto-duplo” (clássico em Ciência da Computação). Quem garantiria que a pessoa A debitaria a quantia combinada de sua conta? Como seria feito o crédito em

1 CRIPTOMOEDA. Uma das primeiras manifestações da “grande mídia econômica” acerca das criptomoedas (neste caso, o Bitcoin). The Bitcoin. GREENBERG, Andy. Forbes, 20 abr, 2011. Disponível em <<http://www.forbes.com/forbes/2011/0509>>. Acesso em 09/09/2013.

2 CYPHERPUNK Grupo de pessoas que buscam a utilização da criptografia com fins de garantia de privacidade. Cypherpunk é a justaposição de duas palavras, cypher e punk, como um trocadilho para punks que utilizariam criptografia. Houve um grupo famoso que criou um mailing list para se comunicar, por volta do início da década de 90. Formou-se um fórum e, ali, Wei Dai rascunhou as primeiras idéias de como seria possível uma sociedade com um dinheiro sem um emissor central e criptografado.

3 WEI DAI (pseudônimo) era um entusiasta da criptografia que a via como meio de diminuir/contornar o controle estatal sobre a vida dos indivíduos de determinada sociedade. Disponível em <<http://www.weidai.com/bmoney.txt>>. Acesso em 09/09/2013.

4 Breve explicação em <https://en.bitcoin.it/wiki/Bit_Gold_proposal>. Acesso em 09/09/2013.

conta da pessoa B? Sempre se fez, até então, necessário um intermediador das transações que mantivesse um livro-razão com todo o histórico das transações e, assim, permitisse sempre o correto adereçamento das movimentações, visando evitar o gasto duplo. O Bitcoin surge subtraindo o intermediário C do processo, pois todos os usuários do Bitcoin carregam um registro histórico de **todas** as transações já realizadas no sistema Bitcoin. E cada nova transação precisa ser aprovada e registrada por **todo** o sistema para ser dada como válida. É como se cada usuário possuísse um livro-razão das trocas já realizadas na economia Bitcoin. Cada bitcoin despendida por um usuário, o horário, a quantia, todas essas informações ficam armazenadas nos computadores dos usuários. A diferença é que neste caso, esse arquivo é chamado de *blockchain*⁵ (cadeia de blocos, em português) e não livro-razão. Todas as movimentações de unidades bitcoin dentro do sistema são confrontadas contra o *blockchain* para assegurar que não exista gasto duplo. É exatamente neste ponto que o Bitcoin, para alguns, é revolucionário. Ele torna possível transações diretas de A para B sem intermediários e com custo muitíssimo reduzido quando comparado aos serviços bancários ou, ainda, serviços de envio de dinheiro entre países (Western Union, MoneyGram e outros).

Outro ponto interessante são as outras aplicações para essa estrutura Bitcoin (*blockchain*) criada. Uma vez que todo um sistema **garante** alguma informação, as possibilidades são infinitas. Para fins práticos, essa garantia se dá através de uma assinatura carimbada, com data, hora e detalhes de um determinado fato/ponto/transação em questão e, claro, com respaldo de todo o sistema. O conceito é tão revolucionário que há empresas as quais estão utilizando-se do blockchain para fins não-financeiros como: **Ascribe**⁶ - reivindicação de propriedade sobre arquivos digitais (como desenhos, textos e quaisquer outros tipos de arte/ciência que estejam em formato digital) e claro, conseqüentemente a venda de propriedades digitais, **BitProof**⁷ - marcação de hora/data/autoria de documentos digitais, virtualmente tornando o sistema dos atuais cartórios obsoletos, já que garante a autenticidade notarial através do blockchain, **Uproov**⁸ – aplicativo para celulares que faz a marcação da hora/data/localização nas fotos/vídeos tirados pelo

5 É possível conferir toda a blockchain da Bitcoin no seguinte endereço <<https://blockchain.info/pt>>

6 Site da empresa **ASCRIIBE**: <<https://www.ascribe.io/>>.

7 Site da empresa **BitProof** <<https://bitproof.io/>>.

8 Site da empresa **UpROOV** <<https://uproov.com/>>.

usuário, tornando possível **provar** que algo aconteceu perto do usuário ou naquele momento em questão, ou seja, tornando realmente **autênticos** aquelas fotos e/ou vídeos, **Colu**⁹ – basicamente a utilização do blockchain para criar outros ativos financeiros que não as bitcoins, como uma outra criptomoeda ou moeda para utilização de maneira local (como acontece em algumas regiões do Brasil), **Warranter**¹⁰ – utiliza-se do blockchain para gerar garantias em produtos vendidos no varejo, atualmente a LG e a GoPro já utilizam estes serviços, **Everledger**¹¹ – faz uso do blockchain para acompanhar diamantes de maneira individual, desde a mina onde ele fora minerado até o consumidor final, resolvendo problemas de longuíssima data no ramo de seguros, uma vez que cada diamante recebe um certificado e este provê as verificações necessárias às seguradoras, proprietários, requerentes e até órgãos legais, **Filament**¹² – o avanço real da IoT (internet of things), a empresa utiliza hardwares minúsculos que são “colados” em todos os tipos de eletrônicos/objetos e estes dispositivos serão registrados no blockchain tendo sua própria identidade e podendo se comunicar com outros objetos/rede através da internet e dos micropagamentos em bitcoins, **Provenance**¹³ – talvez a maior e mais ambiciosa aplicação do blockchain, este aplicativo “marca” toda as informações e a história de um determinado produto passando por toda a cadeia de suprimento, onde e a que horas ele fora produzido, por quais outros locais passou, quais empresas o negociaram e etc, **IBREA**¹⁴ – não são uma empresa, mas sim um grupo cyberativistas que visa modernizar todos os processos imobiliários do mundo atualmente, querem transferir as escriturações, registros de imóveis e até mesmo cauções em para o sistema Bitcoin e, assim, fazer uso do blockchain, evitando fraudes e agilizando as transações. Há ainda uma miríade de outras empresas que estão fazendo uso do *blockchain* para as mais diversas necessidades humanas, mas esse não é o foco, neste mo.

O *blockchain* é o coração e plataforma na qual o Bitcoin se sustenta. É essencialmente o banco de dados (apresentado sob a forma de um livro-razão) onde **todos** os usuários do sistema o possuem e cada nova transação/adição de dados

9 Site da empresa **COLU** <<https://www.colu.com/>>.

10 Site da empresa **WARRANTER** <<http://www.warranteer.com/>>.

11 Site da empresa **everledger** <<https://www.everledger.io/>>.

12 Site da empresa **Filament** <<https://filament.com/>>.

13 Site da empresa **Provenance** <<https://www.provenance.org/>>.

14 Site do grupo **IBREA (International Blockchain Real Estate Assn.)** <<http://www.ibtcrea.org/>>.

deve ser confirmada e aceita por todos os usuários. Assim, o *blockchain* cresce a cada operação realizada dentro do sistema. Quase todos os outros bancos de dados disponíveis no mundo são passíveis de deleções em seus registros e adulterações. No *blockchain*, isso não ocorre e é matematicamente impossível. Ou seja, em qualquer setor onde é necessário que um grupo **confirme** determinado fato ou acontecimento, o *blockchain* é viável. Por isso, ele é revolucionário, pois sintetiza a **confiança** em um mundo onde sempre as confirmações são feitas por terceiros e de maneira centralizada. Não é difícil imaginar a emissão de documentos de identidade tendo sua veracidade baseada no *blockchain*, ou então, como uma poderosíssima ferramenta contra a corrupção, uma vez que cada transação realizada dentro do sistema é facilmente auditável e virtualmente imutável.

O **Ethereum**¹⁵ é uma moeda digital que nasceu com o fim específico de executar os chamados *smart contracts*, utilizando-se de uma estrutura muitíssimo semelhante ao *blockchain*, mas focando nas outras “utilizações não-financeiras” através da **retenção**. Retenção, neste caso, é a aplicação do *chargeback* nas transações através dos *smart contracts*. Na concepção de seus criadores, essa criptomoeda é um computador de escala mundial à prova de adulterações e que permite aos usuários uma plataforma segura para executar contratos, confirmar posses, programar de maneira segura e distribuída, uma vez que tudo será registrado ao longo de seu *blockchain*. Os *smart contracts* são um pequeno programa de computador (algumas linhas de código) que ficam **armazenadas** no *blockchain*, quando algum outro participante da comunidade (pode até mesmo ser algum outro *smart contract*) comunica-se com aquele pedaço de informação, ele é executado. Estando no *blockchain*, todos os membros interessados, ou seja, aqueles que acompanham aquela linha de blocos, saberão exatamente o que esse programa faz e qual é o seu estado atual. Mas como isso poderia ser útil? Isso adereça uma pequena questão relativa aos *chargebacks*, já que não é possível realizá-los de maneira autômata no *blockchain* do Bitcoin. O *smart contract* do Ethereum permite implementar essa retenção dentro do *blockchain* de maneira automática, transparente e fiável. As próprias linhas de código de um *smart contract* podem possuir uma carteira e participar o processo transacional. Exemplo de

15 Site do projeto **Ethereum** <<https://www.ethereum.org/>>.

aplicação em um e-commerce: o indivíduo A realiza uma compra de um produto do indivíduo B. Ambos assinam a transação e o *smart contract* está presente. Quando o indivíduo A recebe o produto, ele remete o dinheiro às linhas de código (ao *smart contract*, no caso) e este realiza a transferência para o vendedor. Ou seja, é possível realizar a **retenção** dentro da própria estrutura de *blockchain*. Isso, mais uma vez, elimina a necessidade de um terceiro agente no processo. Podemos expandir essa lógica para outros processos, como prazos de confirmação/inscrição, prazos de devolução de produtos comprados, pagamentos periódicos, crowdfunding e etc. Tudo pode ser programado nesses *smart contracts* e a intervenção humana em quaisquer pontos nunca será necessária. É a tecnologia pavimentando o caminho para os futuros processos burocráticos (os quais, é claro, deixarão de sê-lo e demandarão cada vez menos tempo). As possibilidades, como descritas e explanadas, são muitas. O Ethereum foi financiado como um projeto de *crowdfunding* e suas moedas são as *ether*. Atualmente tornou-se a segunda maior *altcoin*¹⁶ do mundo, ultrapassando em popularidade e utilização a *litecoin*.

O funcionamento do Bitcoin é uma tarefa um tanto complicada de se explicar. O sistema abarca uma miríade de conceitos e campos do conhecimento humano e, por ser absolutamente recente, está encoberto sob o véu das desconfianças e desconhecimentos. Por ser algo matemático, imaterial (incorpóreo), o Bitcoin (e as bitcoins) muitas vezes não são vistos como o que, de fato, são: simples moedas digitais. Podemos considerá-los moedas? Mais adiante, precisamente no Capítulo 2, o presente trabalho discorrerá acerca disto. No terceiro capítulo, será feito um comparativo simples e sintético entre os atuais meios de pagamento e o que as criptomoedas (em especial o Bitcoin) têm a oferecer.

O sistema Bitcoin se dá, como descrito anteriormente, sobre uma plataforma peer-to-peer. A seguir, faremos uma breve explanação da plataforma com o objetivo de facilitar o entendimento do funcionamento do sistema.

O peer-to-peer é uma arquitetura de rede (online, portanto) onde cada um dos usuários da rede funcionam tanto como clientes (receber conteúdo) quanto como servidores (prover conteúdo). Tal arquitetura pode proporcionar, caso seja interessante aos fins da rede, o anonimato entre todos os nós (peers) da rede. As

¹⁶ *Altcoin* ou *alternative cryptocurrencies* são criptomoedas alternativas às bitcoins. Surgiram depois e com base no projeto Bitcoin (utilizando-se do *blockchain*).

redes p2p (peer-to-peer) estão há muito estabelecidas e são largamente utilizadas na internet. São mais conhecidas pela quantidade de conteúdo ilegal que carregam e, especialmente, pela facilidade que qualquer usuário encontra em baixar (fazer o download) de tais conteúdos. O sistema torrent, o qual é mais conhecido e popular, também utiliza a arquitetura de rede peer-to-peer.

O Bitcoin é uma rede peer-to-peer e, portanto, não possui autoridade central com encargos para emitir, verificar e/ou gerenciar as transações. Todo o processo de verificação das transações (conferência das bitcoins no *blockchain*) se dá através do *proof-of-work* de usuários que disponibilizam poder computacional ao sistema. Tais usuários são denominados “mineradores”. O termo é emprestado dos mineradores de ouro, pois estes usuários são recompensados com as novas bitcoins criadas pelo sistema. A cada dez minutos, uma quantidade definida e conhecida por todos é introduzida no sistema distribuída de maneira aleatória entre os mineradores, usuários que cederam potencial computacional para estruturar o funcionamento da rede. A “mineração” se dá na realização do *proof-of-work*.

O *proof-of-work* é uma espécie de enigma matemático lançado pelo sistema onde os computadores “disputam” quem encontrará primeiro a solução de um determinado problema. Sem entrar em termos mais específicos, o sistema Bitcoin trabalha com o *solution-verification proof-of-work protocol*. Ou, em linhas mais palatáveis, o sistema lança o enigma e aguarda até receber a resposta correta de algum dos mineradores. Para tentar tornar este conceito mais simples, podemos imaginar que o enigma seja a busca de mais casas decimais para o “número π ”, onde o prêmio em bitcoins iria para o primeiro usuário a conseguir alcançar a quingentésima casa após a vírgula. O próximo desafio, ilustrativamente, seria alcançar a milésima. No outro, alcançar a milionésima casa após a vírgula. E assim por diante. Outro exemplo é a analogia com a busca de números primos, como Ken Tindell¹⁷ colocou: o enigma se transcreveria na busca de números primos cada vez maiores. Há uma criptomoeda recente, a Primecoin¹⁸, que utiliza este método e, inclusive, já bateu todos os recordes previamente estabelecidos pela Universidade de Tennessee que guardavam uma lista dos 5.000 maiores números primos. Porém,

17 TINDELL, Ken. Geeks Love The Bitcoin Phenomenon Like They Loved The Internet In 1995. Disponível em <<http://www.businessinsider.com/how-bitcoins-are-mined-and-used-2013-4>> Acesso em 09/09/2013.

18 Site do projeto Primecoin <<http://primecoin.io/>>.

o enigma é, no caso do Bitcoin, buscar uma seqüência de dados (um bloco) que produza um certo padrão particular quando confrontado com o algoritmo do tipo “*hash*”. O “*hash*”, para facilitar o entendimento, pode ser pensado como uma fechadura. Uma vez confirmado o padrão, o prêmio vai para o minerador que encontrou aquela determinada seqüência. E, caso o bloco tenha sido usado para verificar¹⁹ uma transação, o minerador também recebe uma pequena taxa de serviço, em u.m. (unidades monetárias) corrente do sistema (no caso da criptomoeda Bitcoin, as bitcoins). É importante notar que a dificuldade dos “enigmas” aumenta e fica cada vez mais difícil encontrar a combinação. É necessário ressaltar que o *proof-of-work* não é uma tecnologia nova. O método “*hashcash*” surgiu para tentar combater o spam de e-mails, logo não início da popularização dos e-mails nos anos 2000. O remetente “gastava” aproximadamente 1s para processar um enigma simples antes de enviar um e-mail qualquer e isso, é claro, frenava o ímpeto do spam desmesurado²⁰. O “*hash*” pode ser traduzido como um somatório ou resumo de um número de tamanho fixo, o qual se relaciona com um código maior. Tal qual uma chave e fechadura, ou os últimos dois dígitos do CPF, os quais permitem verificar se todo o código (do CPF, no caso), é válido. Essa característica é fundamental e irreversível, ou seja, não é possível obter o código original a partir do “*hash*”.

No início do funcionamento do sistema Bitcoin, era possível minerar vários blocos com uma capacidade computacional trivial, como um computador doméstico. Com a “corrida pelo bitcoin”²¹²²²³ (especialmente em meados de 2013, quando a moeda valorizou de maneira expressiva), a dificuldade se tornou tamanha que, assim como o ouro, a mineração se tornou atividade profissional e também acabou criando um novo mercado, com novas empresas, fornecedores, tecnologia própria para mineração, serviços de manutenção de *mining rigs* (dispositivos de mineração),

19 Alguns blocos são utilizados somente para verificar a transação e conferir a integridade de “corrente de blocos”. No caso de um bloco assim (que é gerado de tempos em tempos segundo o próprio sistema), o agente que descobrir a combinação recebe uma pequena quantidade de u.m. do sistema em questão.

20 Apenas para ilustrar, para enviar 100.000 e-mails, que é uma lista minúscula, seriam necessárias quase 28 horas, tornando o spam algo inviável. Infelizmente essa prática não foi implementada

21 Inside the Race to Build the World’s Fastest Bitcoin Miner. Disponível em <<https://www.wired.com/2013/04/bitcoin-mining-rigs/>>. Acesso em 10/09/2013.

22 WILE, Rob. Bitcoin Mining Is Becoming A Professional, Industrial, Nordic Enterprise. Disponível em <<http://www.businessinsider.com/bitcoin-iceland-pool-2013-12>> Acesso em 22/12/2013.

23 POPPER, Nathaniel. Into The Bitcoin Mines. Disponível em <https://dealbook.nytimes.com/2013/12/21/into-the-bitcoin-mines/?_r=1> Acesso em 22/12/2013.

serviços de resfriamento de *mining rigs* e etc.

O processo de mineração de bitcoins possui um limite. No lançamento da plataforma, Nakamoto estipulou que somente serão criadas 21 milhões de bitcoins²⁴ e, como é a quantidade de moedas que entrará no sistema é perfeitamente previsível, as últimas unidades monetárias (os últimos “satoshis”, 0,00000001 BTC) de bitcoin serão coletadas no ano de 2140. A dificuldade de mineração, a qual já fora explanada anteriormente, funciona para calibrar a quantidade de bitcoins a serem mineradas. Essa dificuldade é ajustada para que o sistema gere aproximadamente 1 novo bloco a cada dez minutos. Se os mineradores resolverem o enigma muito rapidamente, o sistema aumenta a dificuldade do enigma para que este seja resolvido em aproximadamente dez minutos. Caso os mineradores demorem demais, o sistema automaticamente reduz a dificuldade. Com o objetivo de compelir os mineradores a darem sustentação ao sistema, mesmo após toda a mineração das bitcoins disponíveis, será possível consegui-las através do prêmio de verificação das transações (que é advindo da minúscula taxa cobrada nas transações).

As transações entre os indivíduos não são, necessariamente, anônimas, mas primordialmente realizadas através de um pseudônimo. Cada usuário possui uma carteira com um endereço alfanumérico (chave pública) de 33 dígitos e uma chave privada (espécie de senha). Este endereço identifica o usuário dentro da rede Bitcoin. Para aumentar a privacidade, nada impede que um usuário crie várias e várias carteiras. Como todas as transações são confirmadas e gravadas no *blockchain* é possível, ao menos em teoria, identificar os usuários da rede. As transações se dão quando um usuário A assina a chave pública do usuário B usando sua própria chave privada. Neste processo, o usuário A assinala a quantidade de criptomoedas a serem transferidas e aguarda o processo de confirmação. Tal mecanismo cria uma transferência e esta irá para o bloco, onde será confirmada por todos os mineradores e, uma vez confirmada, será registrada no livro razão (*blockchain*) de todos os usuários da rede da criptomoeda em questão.

Dentre as já citadas vantagens das criptomoedas, o mais importante é a ausência de um agente intermediário nas transações. A ausência desse agente se transcreve em menores custos de transação. Há algumas outras vantagens que se

24 Informação direta do *whitepaper*. Disponível em <<https://bitcoin.org/bitcoin.pdf>>. Acesso em 09/09/2013.

desdobram desse fator, como a possibilidade de remessas de dinheiro em locais onde há estrangulamento de capitais por parte dos agentes, onde o governo estatal impede remessas ou comercialização com outra moeda que não seja a de curso forçado (casos semelhantes ocorreram recentemente na Argentina e Grécia).²⁵²⁶²⁷²⁸²⁹³⁰

1.1. Desdobramentos, regulações e legislações

Os ASIC (Application-specific integrated circuit, ou Circuito Integrado de Aplicação Específica) são circuitos integrados (uma espécie de hardware) que é customizado para um uso particular. No caso da mineração de criptomoedas, são hardwares especializados em fazer os cálculos buscando a obtenção do prêmio. Há uma miríade de empresas e de produtos³¹ atuando neste ramo o que, segundo alguns³², é uma espécie de confirmação da solidez do ecossistema econômico das criptomoedas, especialmente do Bitcoin. Além dos produtos específicos para mineração de criptomoedas, há também as conseqüências mercadológicas da criação de um novo método de pagamentos. Empresas investindo em softwares baseados nas Bitcoins, programação na nuvem para utilização dos pagamentos, criação de tokens físicos com chaves privadas e que contém criptomoedas, empresas trabalhando somente com criptomoedas (custo de transação

25 PAGLIERY, Jose. Greeks are Rushing into Bitcoin. Disponível em <<http://money.cnn.com/2015/06/29/technology/greece-bitcoin/>>. Acesso em 23/12/2013.

26 MOUNT, Ian. Bitcoin: Greece's New euro workaround? Disponível em <<http://fortune.com/2015/07/10/greece-bitcoin-bitchain/>>. Acesso em 23/12/2013.

27 DARWISH, Muhammad. Greece's Cash Crisis is Bitcoin's Boost. Disponível em <<https://www.bloomberg.com/news/articles/2015-07-08/greece-s-cash-crisis-is-bitcoin-s-boost-ibuhh68t>>. Acesso em 23/12/2013.

28 GILSON, David. Farmers help bitcoin grow organically in Argentina. Disponível em <<http://www.coindesk.com/farmers-help-bitcoin-grow-organically-argentina/>>. Acesso em 23/12/2013.

29 CRETIAZ, José. Bitcoin: fiebre argentina por la máquina de dinero digital. Disponível em <<http://www.lanacion.com.ar/1596773-bitcoin-pasion-argentina-por-la-nueva-maquina-de-hacer-billetes-digitales>>. Acesso em 23/12/2013.

30 MCCOMB, Dave. Using Bitcoin to Get the Dolar Blue Rate in Argentina. Disponível em <<http://www.discoverbuenosaires.com/bitcoin-argentina>>. Acesso em 23/12/2013.

31 Lista comparativa dos ASICs no mercado disponível em <https://en.bitcoin.it/wiki/Mining_hardware_comparison>. Acesso em 23/12/2013.

32 Gavin Andresen argumenta que o surgimento de mercados que dão sustentação ao bitcoin é a maior prova de que o sistema está se tornando sólido. É necessário extrema confiança dos agentes para utilizar a moeda, mas é necessário ainda mais confiança para montar negócios que funcionam somente por causa da moeda. A entrevista está disponível em <<https://twit.tv/shows/triangulation/episodes/103>>. Acesso em 20/12/2013.

extremamente baixo, perto de 0), serviços educacionais para trading entre criptomoedas e mais uma infinidade de serviços, produtos, acessórios, plataformas e arquiteturas que somente são possíveis devido ao surgimento dessas novas *cryptocurrencies*. Além disso, há também todo um ecossistema acadêmico que se formou ao redor da moeda para discuti-la e estudar suas principais conseqüências e impactos nos mais variados campos da humanidade, como os possíveis impactos legais e jurídicos, geopolíticos, econômicos, sociais e etc.

Desde o surgimento e posterior alvoroço causado pelo Bitcoin, os órgãos reguladores vêm discutindo³³ maneiras de controlar/suprimir o uso das bitcoins. Essa preocupação é real pois a natureza do sistema permite que a compra e venda de quaisquer produtos, serviços, envio de remessas e etc sejam feitas de maneira completamente desconexa do sistema financeiro tradicional e controlado pelo governo. Dentre as possibilidades indesejadas, podemos destacar o uso das bitcoins: para o comércio de bens ilegais, como armas, drogas, pornografia, serviços proibidos; lavagem de dinheiro; evasão fiscal e etc. Além das questões relativas à natureza desse novo meio de pagamentos, a simples existência de uma alternativa matematicamente **segura** ao sistema financeiro tradicional já é uma questão passível de preocupação por parte dos órgãos reguladores, pois as novas criptomoedas podem surgir como **concorrentes** às moedas forçadas e de curso legal. Assim, elas podem vir afetar a eficácia de uma política fiscal e monetária e vir a aumentar os riscos financeiros do sistema tradicional. Ainda sobre os usos “especiais” desse sistema, é interessante citar o caso do *SilkRoad*, um mercado negro onde é possível comprar quaisquer tipos de itens proibidos e ilegais (drogas, armas e etc) também apelidado de “e-bay do mercado negro”³⁴. O site foi fechado pelo FBI em maio de 2013 mas depois de poucos meses, outros administradores do site reforçaram a segurança (só é possível acessar o site através da *DeepWeb*) e o relançaram, sendo assim ele continua operacional até os dias atuais. Neste caso específico, a saída estatal para lidar com estes problemas é o combate clássico à pirataria, tráfico de armas, tráfico de drogas (isto é, busca e apreensão). Porém, há um outro problema bastante maior: os serviços e conteúdos puramente

33 Lista de como cada país se porta perante o Bitcoin disponível em <https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country>. Acesso em 20/11/2016.

34 Monetarists Anonymous. Disponível em <<http://www.economist.com/node/21563752>>. Acesso em 09/09/2013.

digitais não são passíveis do tratamento clássico e são, na prática, dificílimos de serem sanados. No caso da evasão fiscal, o problema também é patente e sem solução, pois a transferência de fundos através do sistema Bitcoin não é facilmente rastreável, fazendo com que este sistema seja, segundo o professor da Universidade da Flórida, Omri Marian, o novo “paraíso fiscal”³⁵ dos maiores sonegadores.

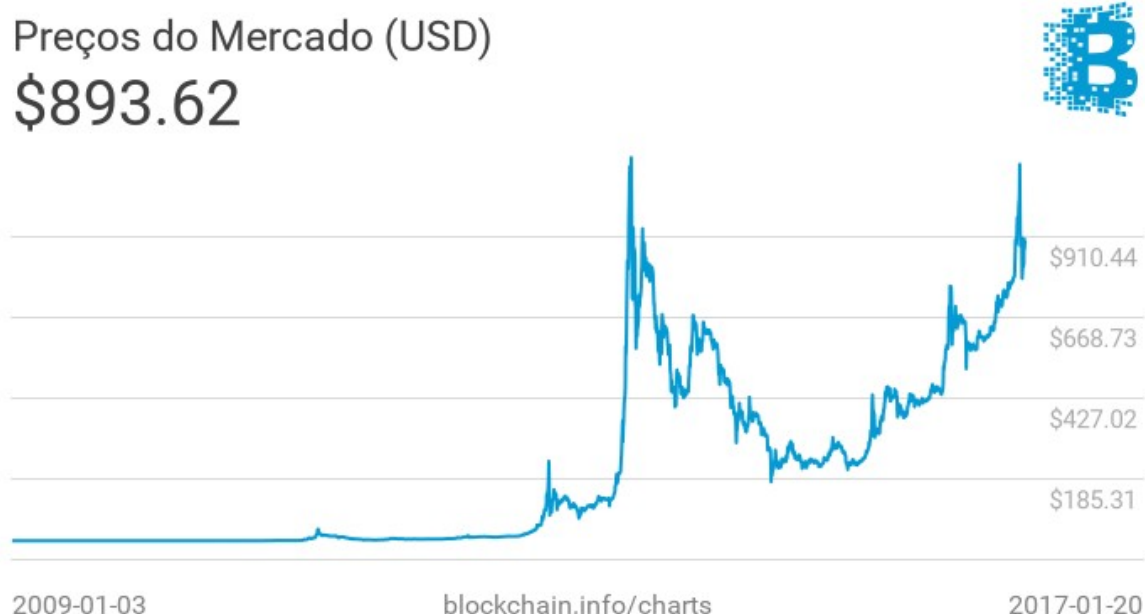
A regulação das criptomoedas ainda é, na maioria dos países, inexistente ou extremamente fraca em razão da própria natureza do Bitcoin. Uma vez que é impossível influenciar **diretamente** no sistema e/ou na quantidade de moedas, a única maneira que os governos ou outros órgãos reguladores podem utilizar é através da taxaçaõ nas casas de câmbio e isto tende a compelir os usuários a permanecerem no sistema Bitcoin. Ainda assim, quando tais medidas são realizadas, isso mostrou um certo impacto no sistema, uma vez que o câmbio da bitcoin flutuou de maneira expressiva. Por exemplo, aconteceu quando o governo chinês em dezembro 2013 decidiu proibir³⁶ as companhias nacionais de pagamento e instituições financeiras de realizar transações em bitcoins/criptomoedas, restando somente aos indivíduos o direito de utilizar as bitcoins. Esta proibição causou a maior volatilidade que o ativo já havia visto até então, quando perdeu quase 50% do seu valor de mercado em apenas um dia. Até o início de 2015 a moeda passou por uma grande volatilidade, com quedas seguidas de apreciações especulativas. De 2015 até 2017 a moeda vivenciou baixa volatilidade (para padrões de par moeda-moeda) e valorizou de forma quase que contínua (em um horizonte-prazo mensal).

35 MARIAN, Omri. Are Cryptocurrencies Super Tax Havens? Disponível em <http://repository.law.umich.edu/mlr_fi/vol112/iss1/2/>. Acesso em 23/12/2013.

36 CAMPI, Monica. China proíbe bitcoin por temer lavagem de dinheiro. Disponível em <<http://exame.abril.com.br/tecnologia/china-proibe-bitcoin-por-temer-lavagem-de-dinheiro/>>. Acesso em 23/12/2013.

Segue o gráfico do preço da bitcoin em USD:

Gráfico 1.1 – O preço da bitcoin em dólares 2009-2017.



Esta aparente estabilidade vem atraindo cada vez mais usuários ao sistema e difundindo com mais violência a tecnologia do *blockchain* e dos *smart-contracts* mencionados anteriormente. O tamanho do mercado Bitcoin ainda é pequeno, cerca de 15 bilhões de dólares. A somatória de *market-capitalization* das maiores criptomoedas não chega a 20 bilhões de dólares³⁷. Faz sentido se preocupar com a possibilidade de uma substituição monetária (utilização das criptomoedas em detrimento das moedas clássicas, de curso forçado)? Todos os dados indicam que não, ainda é muitíssimo cedo para se preocupar com isso. No entanto, podemos discorrer sobre alguns riscos que surgirão conforme o avanço desse novo conceito monetário se sintetizar.

Há o risco mais claro de uma possível substituição monetária: o risco sistêmico. Neste caso, a economia de maneira geral seria impactada caso houvesse uma modificação real do nível de demanda dos indivíduos pelos passivos públicos e dos bancos, causando problemas no controle dos agregados monetários. A possível ineficácia da política monetária poderia se estender para a política cambial gerando

³⁷ Capitalização de mercado da maioria das *cryptocurrencies* que existem atualmente disponível em <<https://coinmarketcap.com/>>. Acesso em 09/09/2016.

a disfuncionalidade do sistema monetário tradicional. É possível ir além e pensar conseqüências ainda mais graves. Uma vez que os agregados monetários se descontrolam e o tradicional meio de pagamento deixa de ser utilizado, como mensurar os indicadores econômicos de desenvolvimento, de saúde monetária e etc? Como mensurar o PIB? Como mensurar a inflação? Sem tais variáveis e indicadores, como firmar contratos? Como balizar investimentos? Em suma, a substituição monetária só ocorreria caso a capitalização de mercado das criptomoedas excedesse ou fosse expressiva frente a capitalização das moedas de curso forçado. Apenas para fins comparativos, as estimativas sugerem que há quase 180 trilhões de dólares em ativos no mundo e apenas 18 bilhões de dólares em criptomoedas. Ou seja, no presente os riscos mencionados não possuem chance de se concretizarem. No entanto, esses riscos podem tornar-se reais em uma escala diminuta, como em países e/ou municípios onde a economia tende a fugir do curso forçado (países com inflação galopante, por exemplo). Isso é realidade em países como o Chipre, Argentina e a Grécia. No caso da Argentina, devido às estrangulações ao mercado de capitais e à inflação, muitos argentinos viram nas bitcoins (mesmo com sua volatilidade) uma alternativa válida ao peso e isso fez do país o líder em utilização das bitcoins em toda a América Latina³⁸, fazendo com que até o UBER aceitasse bitcoins³⁹.

Explenados algumas das mais patentes conseqüências do surgimento e desdobramento das criptomoedas, é válido afirmar que a maioria dos Estados nacionais possui uma postura de certa tolerância⁴⁰ com o Bitcoin. No caso brasileiro ainda não há nenhuma disposição oficial do governo acerca da matéria, mas entende-se que as bitcoins e demais criptomoedas **devem** ser declaradas e, no caso de trading e possíveis lucros, as normas de tributação da renda variável se aplicam às criptomoedas.

38 DYNIEWICZ, Luciana. Com crise e inflação, Buenos Aires lidera em bitcoin na América Latina. Disponível em <<http://www1.folha.uol.com.br/tec/2016/07/1788250-com-crise-e-inflacao-buenos-aires-lidera-em-bitcoin-na-america-latina.shtml>>. Acesso em 04/07/2016.

39 JANSEN. UBER da Argentina agora aceita Bitcoin e luta pela continuação do serviço. Disponível em <<https://guiadobitcoin.com.br/uber-da-argentina-agora-aceita-bitcoin-e-luta-pela-continuacao-do-servico/>>. Acesso em 06/07/2016.

40 Existe um site especializado em condensar todas as informações acerca da postura legal dos países frente ao Bitcoin e outras *cryptocurrencies* e seu endereço é <<http://bitlegal.io/>>. Acesso em 06/07/2016.

2. As características econômicas das criptomoedas

O surgimento das criptomoedas, especialmente o Bitcoin, culminou por levantar rejeição pela maioria do público “comum”. Essa rejeição, esse medo, são naturais, visto a essência de algo tão novo e desconectado da concepção tradicional sobre o funcionamento do dinheiro e da cognição do que é dinheiro/moeda. Esta nova moeda digital possui uma complexidade técnica e tecnológica jamais vistas, as quais, justificam tais reações. É como tentar explicar a internet, em seu surgimento no final dos anos 80, para uma população sem qualquer entendimento básico do que são os computadores ou de como funciona a computação (ciência) de maneira geral. As criptomoedas, nesse sentido, estão no mesmo pé que a internet quando do surgimento desta última. A maioria da mídia foca em seus potenciais pontos negativos que inebriam as discussões acerca deste novo conceito monetário. É necessário trazer esta discussão ao campo acadêmico e analisá-la sob o viés da ciência econômica.

2.1.1 A definição de **moeda** e características

É válido afirmar que as bitcoins e outras criptomoedas são, de fato, moedas? O que é, por definição, uma “moeda”? De maneira sintética e simplista, a moeda é um bem especial dentro de determinada economia mercantil, baseada na troca de mercadorias, que possui três características ou propriedades: ela deve ser um **meio de troca**, isto é, possuir liquidez dentro de um mercado específico, intermediar o movimento das mercadorias, permitindo que elas circulem; deve ser uma **unidade de conta**, ou seja, deve ser divisível e/ou quantificável ao ponto de ser o referencial nos processos de trocas voluntárias (todas as mercadorias têm seu valor expresso em termos de uma única mercadoria, a moeda); deve servir como **reserva de valor**, em outras palavras, ela deve resguardar o poder de compra através do tempo, deve possuir a qualidade de se “armazenar” a riqueza. Além dessas três características essenciais, o bem que se dispôr a ser transacionado como moeda deve ainda: possuir escassez (por motivações óbvias) e ser tangível aos usuários (ser portátil de alguma maneira). Segundo Mises, um bem qualquer torna-se moeda quando

existe sua demanda é cada vez maior e, portanto, sua liquidez vai tornando “máxima”⁴¹. Isto é, sua liquidez (pode ser trocada imediatamente por qualquer outra mercadoria) aumenta a um ponto em que o mercado (os indivíduos) tende a entesourar o bem para utilizá-lo futuramente como um meio de troca. Portanto, compreende-se que o bem em questão adquire a função de “reserva de valor”, uma vez que os indivíduos desenvolvem uma preferência por guardar este bem para futuramente utilizá-lo como meio de troca. Dentre todas as funções da moeda, a mais importante é de servir como meio de troca, já que as outras funções decorrem diretamente desta, segundo a visão austríaca. Há casos onde a moeda pode perder alguma de suas propriedades e, ainda assim, continuar a ser utilizada (especialmente se ela for de curso forçado). Ocorreu algo engenhoso em 1994 no Brasil, com o Plano Real. Em razão da alta inflação e desvalorização diária da moeda em circulação, o papel da “unidade de conta” foi exercido pela Unidade Real de Valor (URV) – conversão diária da URV (meio de conta) em Cruzeiro (meio de pagamento). Assim, a antiga moeda também não servia como reserva de valor. Isso, segundo Mises⁴², só é possível em um ambiente de curso forçado da moeda e onde o governo causou um descontrole da economia ao tentar forçar pacotes econômicos para “corrigir” problemas. Ou seja, foi necessário que o mesmo governo criasse ou outro aparato que carregasse as características de uma moeda. Ressalte-se que o mercado pode vir a eleger outros bens como reservas de valor, como metais, imóveis, títulos e etc. Apenas para ilustrar, a prata, o ouro e outros metais preciosos foram utilizados como meio de troca por séculos e, atualmente, restringem-se a mais uma reserva de valor. No entanto, não há liquidez imediata, pois é necessário trocá-los por moeda e, então, adquirir outra mercadoria. A função unidade de conta é uma consequência direta de sua característica basal e primordial: o meio de troca, segundo os austríacos. Quando os indivíduos se dispõem a realizar as trocas com determinado bem, eles tomam como referência a precificação dos outros bens em função do bem de liquidez “máxima” (a moeda, no caso).

41 MISES, Ludwig von. *The Theory of Money and Credit. Part One – The Nature of Money*. Mises explica detalhadamente a natureza do dinheiro como conhecemos e explica o teorema da regressão na “Part One” de sua principal obra, sendo mais especificamente os capítulos I ao V.

42 MISES, Ludwig von. *The Theory of Money and Credit. Part One – The Nature of Money*. Mises explica detalhadamente a natureza do dinheiro como conhecemos e explica como o estado influencia todo o sistema ao eleger uma moeda de curso forçado e tentar 'controlar' a economia através de planos econômicos na “Part One” de sua principal obra, sendo mais especificamente os capítulos I ao V.

As moedas surgiram de maneira orgânica ao sistema mercantil, uma vez que facilitam as relações comerciais interindividuais de um determinado sistema. Inicialmente, as moedas surgiram com o intuito de serem meros meios de troca. O teorema da regressão⁴³ de Mises afirmar que todo e qualquer tipo de bem que vier a se transformar em moeda precisa, primeiramente, servir como meio de troca. Para que seja considerado um meio de troca, um bem primeiramente deve ser considerado com valor, ou seja, possuir valor de uso. Em síntese: o valor de uso de determinado bem antecede o valor de troca daquele bem em específico. Podemos citar o *sal*, o qual possuía um grande valor como mercadoria (conservação de alimentos) e, posteriormente, devido à sua alta liquidez, tornou-se um meio de troca, visto que todos os indivíduos aceitavam intermediar suas trocas baseando-se em uma quantidade específica de *sal*.

Nesta perspectiva, é válido afirmar que as bitcoins são moedas? Tiveram elas valor como mercadorias? Na perspectiva deste estudo: sim, elas tiveram. No início da plataforma, mais especificamente no começo de 2009, o sistema Bitcoin foi avançando e vários usuários, entusiastas de criptografia, *geeks*, *nerds*, anarquistas, anarcocapitalistas, sujeitos que, segundo Fernando Ulrich⁴⁴, compraram bitcoins como maneira de protestar contra o *status quo* e etc. O cenário cultural e econômico (pós-crise financeiro de 2008) do surgimento do Bitcoin contribuiu, de início, para que esta nova moeda estivesse envolta e associada a uma grande quantidade de qualidades subjetivas, como: símbolo resistência ao poder financeiro global, símbolo de resistência ao poder estatal, símbolo do avanço da criptografia, surgimento de um novo meio de pagamentos *cool* (o qual somente entusiastas de tecnologia poderiam utilizar), símbolo da privacidade (caso Wikileaks) e etc. Em suma, houve demanda real pelas bitcoins no surgimento do sistema, é a prova de que as bitcoins possuíam valor de uso antes de, como se observa atualmente, possuírem valor de troca. A primeira real transação com bitcoins por bens reais ocorreu em maio de 2010⁴⁵, quando o usuário 'laszlo' adquiriu uma pizza por 10 mil bitcoins (interessante

43 MURPHY, Robert. A Origem do dinheiro e de seu valor. Disponível em <<http://www.mises.org.br/Article.aspx?id=209>>. Acesso em 09/09/2013.

44 Fernando Ulrich é um libertário e ávido defensor de políticas liberais no Brasil. Associado ao Instituto Mises Brasil, ele foi um dos primeiros a discutir seriamente o Bitcoin no país. Ele comenta em seu livro (ULRICH, Fernando. Bitcoin: A Moeda na Era Digital) que a bitcoin, no início, tornou-se um bem-símbolo de protesto às forças do estado e esse foi exatamente um dos motivos de ele ser tão demandado.

45 História resumida do Bitcoin disponível em <<https://en.bitcoin.it/wiki/History>>. Acesso em 09/09/2013.

reafirmar que todas as transações estão descritas no *blockchain*). Desde então, as bitcoins foram utilizadas para comprar absolutamente tudo, de eletrônicos e *gadgets* às casas, carros, mansões, serviços e etc. Atualmente as bitcoins são aceitas em todos os grandes centros urbanos do mundo⁴⁶ e possuem especial demanda em países com estrangulamento de capitais e/ou moedas de curso forçado extremamente depreciadas e controladas pelos governos (caso da Argentina, Chipre, Grécia e outros). Assim, as bitcoins (e demais criptomoedas que já possuem grande aceitação como a Litecoin, Ethereum e Ripple) podem servir de “refúgio seguro” de “moedas/ativos em descrédito”. Nesse sentido, podem exercer o papel de meio de troca e reserva de valor, ou seja, receber a nomeação de moedas segundo a visão tradicional. Já segundo a visão austríaca, como estas criptomoedas passaram pelo crivo do teorema da regressão e foram primordialmente meios de troca, elas podem ser consideradas moedas.

2.1.2 A escassez e virtualidade

Outra característica comum às moedas é a escassez. A emissão do papel-moeda como conhecemos é controlado pelo estado. O ouro (e quaisquer outros metais que já foram moedas-commodities) possui a escassez “controlada” pela natureza, ou seja, sua oferta é dada e praticamente inelástica (oferta decrescente e com um ritmo mais ou menos conhecido). Questionou-se, especialmente por parte da mídia econômica *mainstream*, se as bitcoins, seriam, de fato, bens escassos. Graças ao já discutido *blockchain*, o Bitcoin trouxe para o mundo digital, pela primeira vez na história, a escassez autêntica dos bens digitais. Esse último se dá através da prevenção do gasto duplo, uma vez que toda a cadeia de mineradores *peer-to-peer* deve confirmar a transação. A escassez é legítima e matemática uma vez que é impossível todo o sistema autenticar uma transação onde ocorreria gasto duplo. Baseando-se na escassez legítima, surgiram várias empresas utilizando-se desta tecnologia para prover serviços os quais podem se beneficiar da

46 Locais onde as bitcoins são aceitos ao redor do globo disponível em <<https://coinmap.org>>. Acesso em 09/09/2013.

confiabilidade e **escassez** real de um bem digital. Uma vez que o *blockchain* é matematicamente seguro, é impossível que uma mesma bitcoin seja gasta mais de uma vez e, portanto, as bitcoins possuem essa mesma característica de uma moeda “tradicional”. No entanto, pela estrutura, o “multiplicador bancário” é algo mais difícil de ocorrer e muito se discute no fórum oficial do Bitcoin se em algum momento isso irá ocorrer. Seria necessário que o mercado aceitasse uma outra criptomoeda ou um *smartcontract* com validade em bitcoins. Ou seja, seria necessário que ocorresse com as criptomoedas o que ocorreu com a moeda tradicional. Mas é algo difícil de ocorrer, visto que o motivo principal que fez com que os indivíduos passassem a aceitar “comprovantes de depósito”, cheques e etc foi a facilidade que estas formas de pagamento trouxeram ao mundo. O Bitcoin torna desnecessário esses outros meios de pagamento uma vez que é imaterial, incorpóreo e não precisa de um agente com fé para realizar o resguardo do valor.

Além da escassez, outro aspecto que foi colocado como possível ponto negativo à existência e continuidade das criptomoedas: sua intangibilidade. Porém, este não é novidade ao sistema financeiro atual, uma vez que a maior parte da moeda tradicional é fundamentalmente escriturária, isso é, moeda multiplicada pelos bancos através do sistema de reserva fracionária. Praticamente toda a moeda escritural atualmente já é, de certo forma, digital, visto que são apenas registros contábeis digitais nas contas bancárias do sistema financeiro. Além disto, a maioria das transações rotineiras utilizam-se da moeda escritural em detrimento da moeda física. É claro que essa intangibilidade poderia ser um empecilho à utilização das criptomoedas, visto que ainda há uma parcela da população que utiliza a moeda material, isto é, não possuem cartões de crédito e/ou não possuem contas no sistema financeiro tradicional⁴⁷. Para este público em específico, é possível produzir moedas físicas que possuam o lastro em bitcoins. Isso já existe e várias empresas produzem moedas que contêm a tecnologia do Bitcoin, uma vez que detêm a chave privada e chave pública para realizar a transação. As três principais moedas físicas que contêm bitcoins e estão em circulação são: as moedas Casascius⁴⁸, as moedas

47 Dos Brasileiros, apenas 64% tem conta em banco. Disponível em <<http://www.clientesa.com.br/estatisticas/58750/dos-brasileiros-64-tem-conta-no-banco/ler.aspx>>. Acesso em 20/11/2016.

48 Site do projeto Casascius disponível em <<https://www.casascius.com/>>.

Denarium⁴⁹ e as moedas Satori⁵⁰.

2.1.3 As críticas às criptomoedas

Como citado no capítulo 1, é possível conhecer, através do código fonte da criptomoeda, a quantidade, a velocidade, as taxas e todo o funcionamento das unidades monetárias do sistema. No caso do Bitcoin, é sabido que a oferta crescerá de maneira escalonada até o máximo de 21.000.000 (21 milhões) de unidades e, caso seja necessário mais unidades monetárias, é possível dividir cada bitcoin em unidades menores de maneira ininterrupta. O gráfico 2.1 a seguir mostra a entrada de bitcoins no mercado de 2009 (surgimento da bitcoin) até 25/11/2016.

Gráfico 2.1 – Evolução da bitcoin em circulação: 2009 - 2016



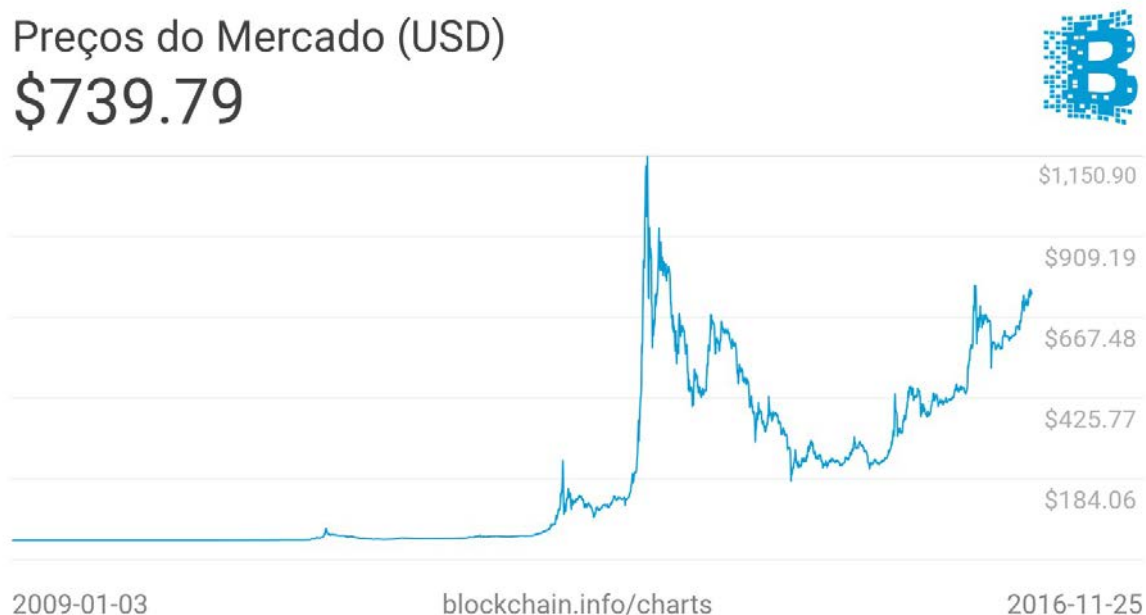
A curva, no início, não seguiu a distribuição esperada pois não haviam transações e usuários suficientes para que o sistema liberasse as bitcoins, ou seja, elas não eram mineradas. O primeiro câmbio que se tem registro de uma bitcoin por dólares fora realizada em outubro de 2009 a uma taxa de 1.309,03 bitcoins por um dólar, relação alcançada ao calcular-se o custo com energia elétrica, depreciação do hardware necessário para a mineração (computador utilizado para fazer o *proof-of-work* em

49 Site do projeto DENARIUM disponível em <<https://denarium.com/>>.

50 Site do projeto Satori disponível em <<https://satoricoin.jp/en/>>.

questão) e demais custos. Essa é uma das bases *reais* de precificação do bitcoin, uma vez que as outras apreciações e depreciações acontecem puramente devido às especulações de mercado. Como é possível observar pelo gráfico 2.2 abaixo, a cotação ainda é muito volátil, mas há uma tendência de valorização

Gráfico 2.2 – Cotação da bitcoin 2009-2016



O pico da valorização alcançado em 2013 (USD 1.150,90) foi reflexo de uma espécie de bolha. Em pouquíssimos meses a cotação subiu de maneira estrondosa, chamando a atenção da mídia da pior maneira possível. Alguns disseram que a bolha seria o fim de todo o projeto Bitcoin e desse “sonho da agenda libertária”⁵¹ (Krugman fora um destes, chegando a afirmar “Bitcoin is EVIL”. Mas, como é possível observar, a moeda voltou a se valorizar em relação ao dólar estadunidense. A moeda atingiu seu menor patamar em janeiro de 2015 (USD 184,06) e, desde então, está com a cotação em ascensão. Aparentemente a mídia tem um fator preponderante na cotação, uma vez que notícias acerca do Bitcoin tendem a inflacionar a cotação e alimentar variações no preço. As discussões acerca do Bitcoin abarcaram os conceitos relativos às moedas, como o lastro. Alguns argumentam que pelo fato de a bitcoin ser um bem *digital* e não possuir lastro, ela

51 KRUGMAN, Paul. The Conscience of a Liberal. Disponível em <http://krugman.blogs.nytimes.com/2013/12/28/bitcoin-is-evil/?_r=0>. Acesso em 10/01/2014.

não poderia, de fato, tornar-se uma moeda. Mas, será que o lastro é algo realmente necessário? As moedas tradicionalmente usadas são *fiduciárias*, ou seja, não possuem lastro e não possuem valor intrínseco. Sendo assim, as bitcoins também não necessitariam de lastro algum. Acerca dessa questão do lastro, Ulrich (2014) escreveu:

“...a constatação de que o bitcoin é desprovido de lastro leva inúmeros economistas a taxar a moeda digital de débil e inerentemente defeituosa. A realidade é que o Bitcoin tornou evidente algo até hoje pouco compreendido: lastro não é uma necessidade teórica de uma moeda, apenas uma técnica empírica cujo principal serviço foi o de servir como restrição às práticas imprudentes de banqueiros e às investidas inflacionistas do estado no gerenciamento da moeda.”

Há ainda algumas outras considerações acerca das criptomoedas, como a dependência que todas elas têm de duas outras estruturas: a eletricidade e internet. Essa dependência é realmente uma falha no projeto? Ela poder vir a impossibilitar a utilização das criptomoedas em uma escala maior? Definitivamente não. *Todas* as moedas tradicionais já são, em maior ou menor grau, digitais. Todo o sistema financeiro atual já existe e convive com essa dependência. A bitcoin seria tão somente mais um ativo a utilizar-se desta estrutura e, portanto, essa dependência não é um impedimento ao projeto.

3. Síntese e comparativo entre os meios de pagamento

Por fim, é adequado postular que as criptomoedas, em seu atual estado, são “superiores” aos demais meios de pagamento/moedas? Isso é algo bastante difícil de afirmar, a começar pelo conceito do que é ser superior ou não. É inegável que as bitcoins e demais criptomoedas servem bem a alguns fins específicos e são muitíssimos utilizados em algumas situações singulares. Como denotado, para os Austríacos, a definição de moeda é o meio de troca *universalmente* aceito, que possui capacidade de contabilizar os gastos (funcionar como unidade de conta) e funcionar como uma reserva de valor. Ulrich (2014) sintetizou de maneira bastante clara as principais diferenças/semelhanças entre o Ouro, o papel-moeda (moeda

física tradicional) e as criptomoedas (a Bitcoin, no caso). Vide Quadro 1. Segue sua síntese:

Quadro 1 – Atributos dos bens-moedas

Atributos	Ouro	Papel-moeda	Bitcoin
1. Durabilidade	Alta	Baixa	Perfeita
2. Divisibilidade	Média	Alta	Perfeita
3. Maleabilidade	Alta	Alta	Incorpóreo
4. Homogeneidade	Média	Alta	Perfeita
5. Oferta	Limitada pela natureza	Ilimitada e controlada politicamente	Limitada matematicamente
6. Dependência de terceiros fiduciários	Alta	Alta	Nula

“O Bitcoin é, simplesmente, uma forma de moeda superior a todas as demais. Incorpora a escassez relativa do ouro, aliada à instantânea transportabilidade e divisibilidade dos substitutos de dinheiro (especialmente aqueles na forma digital moderna), prescindindo de inúmeros terceiros fiduciários – como bancos, casas de liquidação e entidades interbancárias internacionais –, eliminando, assim, o risco da contraparte.”

Em suma: as bitcoins podem ser consideradas moedas, muito embora ainda não possuam o caráter *universal*, visto que sua utilização ainda se dá de maneira restrita quando comparada com outros meios de pagamento. Além disso, a volatilidade dificulta o uso da moeda como unidade de conta, visto que ela ainda passa por um processo de consolidação. Ainda assim, elas são facilmente cambiáveis por outros meios de pagamento (câmbio acessível) e possuem características únicas quando comparadas às outras moedas. A natureza descentralizada, o livro-razão compartilhado entre todos os usuários e aberto a consultas, o fato de se privar de terceiros fiáveis no processo de confirmação das transações e etc caracteriza-se como pontos positivos. A proposta dessas moedas trouxe também uma plataforma incrível para várias outras áreas das ciências (o *blockchain*), cuja evolução está permitindo o surgimento de produtos e negócios nunca antes concebidos.

O surgimento das criptomoedas foi a consequência de um colapso monetário a nível global, o qual chegou ao seu auge com a crise financeira de 2008. Sendo assim, o Bitcoin e outras criptomoedas são uma resposta da sociedade à imposição monetária por parte dos governantes. As criptomoedas são uma resposta de liberdade à imposição governamental do curso forçado. Nakamoto, em seu *whitepaper*, comentou:

“O problema básico com a moeda convencional é toda a confiança necessária para fazê-la funcionar. Precisamos confiar que o banco central não desvalorizará o dinheiro, mas a história das moedas fiduciárias está repleta de quebras dessa confiança. Bancos têm a obrigação de guardar nosso dinheiro e transferi-lo eletronicamente, mas eles o emprestam em ondas de bolhas de crédito com uma mera fração em reserva. Temos que confiar-lhes com nossa privacidade, confiar que não deixarão ladrões de identidade drenar nossas contas.”

4. Referências Bibliográficas

VAIDHYANATHAN, Siva. **The Anarchist in the Library**. Basic Books; Edição: Pbk. (11 de maio de 2005).

FRIEDMAN, David D.. **The Machinery of Freedom**. Chu Hartley LLC; Edição: Third Edition (8 de julho de 2014). Nota: o autor é filho do ultraconhecido Milton Friedman.

BLOCK, Walter. **Defending the Undefendable**. Fox & Wilkes; Edição: 2 (1 de junho de 1991).

RAND, Ayn. **Capitalism: The Unknown Ideal**. Signet; Edição: Reissue (15 de julho de 1986).

MURPHY, Robert P.. **Chaos Theory - Two Essays on Market Anarchy**. Ludwig von Mises Institute (17 de março de 2011).

LONG, Roderick T.. **Anarchism-Minarchism**. Editora Routledge (março de 2013).

Projeto Original da Bitcoin:

NAKAMOTO, Satoshi. **BitCoin - A Peer-to-Peer Eletronic Cash System**. Disponível em: <<http://article.gmane.org/gmane.comp.cryptography.general/12588>> Acesso em: 01 set. 2013.

Artigos que tratam das criptomoedas:

BARBER, Simon; BOYNEM, Xavier; SHI, Elaine; UZUN, Ersin. **Bitter to Better — How to Make Bitcoin a Better Currency**. University of California, Berkeley. Disponível em: <<https://eprint.iacr.org/2012/584.pdf>> Acesso em: 10 ago. 2013.

RON, Dorit; SHAMIR, Adi. **Quantitative Analysis of the Full Bitcoin Transaction Graph**. The Weizmann Institute of Science, Israel. Disponível em: <<https://eprint.iacr.org/2012/584.pdf>> Acesso em: 12 ago. 2013.

KING, Sunny; NADAL, Scott. PPCoin: **Peer-to-Peer Cryptocurrency with Proof-of-stake**. Disponível em: <https://archive.org/stream/PPCoinPaper/ppcoin-paper_djvu.txt> Acesso em: 19 ago. 2013.

ANDROULAKI, Elli; KARAME, Ghassan O.; ROESCHLIN, Marc; SCHRER, Tobias; CAPKUN, Srdjan. **Evaluating User Privacy in Bitcoin**. NEC Laboratories Europe, Heidelberg, Germany. Disponível em: <<https://eprint.iacr.org/2012/596.pdf>> Acesso em: 25 ago. 2013.

MIERS, Ian; GARMAN, Christina; GREEN, Matthew; RUBIN, Aviel D.. Zerocoin - **Anonymous Distributed E-Cash from Bitcoin**. The Johns Hopkins University Department of Computer Science, Baltimore, USA. Disponível em: <<http://zerocoin.org/media/pdf/ZerocoinOakland.pdf>> Acesso em 01 set. 2013.

Relatório do Department of the Treasury (USA) sobre o assunto:

FINANCIAL CRIMES ENFORCEMENT NETWORK. Application of FinCEN's **Regulations to Persons Administering, Exchanging, or Using Virtual Currencies** disponível em: http://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf> Acesso em: 10 de set. 2013.

Relatório do Banco Central Europeu:

EUROPEAN CENTRAL BANK. **Virtual Currency Schemes** <disponível em: <http://www.ecb.int/pub/pdf/other/virtualcurrencyschemes201210en.pdf>> Acesso em: 01 set. 2013.

5. Anexos

Mídia digital consultada:

5.1. Notícias acerca das Criptomoedas (invariavelmente citam Bitcoins):

MELIK, James. **Digital currency: Brave new world or criminal heaven?** Disponível em: <<http://www.bbc.co.uk/news/business-19785935>> Acesso em: 05 out. 2013.

SIMONITE, Tom. **Bitcoin Isn't the Only Cryptocurrency in Town** Disponível em: <<http://www.technologyreview.com/news/513661/bitcoin-isnt-the-only-cryptocurrency-in-town/>> Acesso em: 01 out. 2013.

LEE, Timothy. B. **An Illustrated History of Bitcoin Crashes.** Disponível em: <http://www.forbes.com/sites/timothylee/2013/04/11/an-illustrated-history-of-bitcoin-crashes/?utm_campaign=forbestwittersf&utm_source=twitter&utm_medium=social> Acesso em: 10 out. 2013.

GUADAMUZ, Andres. **We need decentralized cryptocurrencies, we just don't need bitcoin.** Disponível em: <<http://www.technollama.co.uk/we-need-decentralized-cryptocurrencies-we-just-dont-need-bitcoin>> Acesso em: out. 2013.

MATONIS, Jon. **Bitcoin Casinos Release 2012 Earnings.** Disponível em: <<http://www.forbes.com/sites/jonmatonis/2013/01/22/bitcoin-casinos-release-2012-earnings/>> Acesso em: out. 2013.

SIDEL, ROBIN. **Bitcoin Investors Hang On for the Ride.** Disponível em: <http://online.wsj.com/article/SB10001424127887324345804578426692340390104.html?mod=googlenews_wsj> Acesso em: out. 2013.

Mining Digital Gold. Disponível em: <<http://www.economist.com/news/finance-and-economics/21576149-even-if-it-crashes-bitcoin-may-make-dent-financial-world-mining-digital>> Acesso em: out. 2013.

HOUGH, Jack. **The Currency That's Up 200,000%.** Disponível em: <<http://www.smartmoney.com/invest/stocks/the-currency-thats-up-200000-1307029053200/>> Acesso em: out. 2013.

WALLACE, Benjamin. **The Rise and Fall of Bitcoin.** Disponível em: <http://www.wired.com/magazine/2011/11/mf_bitcoin/> Acesso em: out. 2013.

Bitcoin, The Nationless electronic cash beloved by hackers, bursts into financial mainstream. Disponível em: <<http://www.foxnews.com/tech/2013/04/11/bitcoin-electronic-cash-beloved-by-hackers/>> Acesso em: out. 2013.

WOODHILL, Louis. **Bitcoins are digital collectibles, not real money.** Disponível em: <<http://www.forbes.com/sites/louiswoodhill/2013/04/11/bitcoins-are-digital-collectibles-not-real-money/>> Acesso em: out. 2013.

PLUMMER, Brad. **Yes, Bitcoin is Volatile. But it's still got defenders.** Disponível em: <<http://www.washingtonpost.com/blogs/wonkblog/wp/2013/04/11/yes-bitcoin-is-volatile-its-still-got-defenders/>> Acesso em: out. 2013.

ZEITLIN, Matthew. **Bitcoin's Wild Ride Show It's Not Real Money.** Disponível em: <<http://www.bloomberg.com/news/2013-04-11/bitcoin-s-wild-ride-shows-its-not-real-money.html>> Acesso em: out. 2013.

KRUGMAN, Paul. **Golden Cyberfettters.** Disponível em: <<http://krugman.blogs.nytimes.com/2011/09/07/golden-cyberfettters/>> Acesso em: out. 2013. Texto de Krugman sobre as Bitcoins.

SUROWIECKI, James. **Cryptocurrency.** Disponível em: <<http://www.technologyreview.com/review/425142/cryptocurrency/>> Acesso em: out. 2013.

<http://www.mail-archive.com/search?l=cryptography@metzdowd.com&q=from:%22Satoshi+Nakamoto%22> - **Mailing List** com idéias originais de Nakamoto.

The Beginner's Guide to Bitcoin – Everything You Need to Know. Disponível em: <<http://www.monetarism.co.uk/the-beginners-guide-to-bitcoin-everything-you-need-to-know/>> Acesso em: out. 2013.

LEE, Timothy. B. **New Money Laundering Guidelines Are A Positive Sign For Bitcoin.** Disponível em: <<http://www.forbes.com/sites/timothylee/2013/03/19/new-money-laundering-guidelines-are-a-positive-sign-for-bitcoin/>> Acesso em: set. 2013.

FAIOLA, Anthony; FARNAM, T. W. **The Rise of the Bitcoin: Virtual Gold or Cyber-bubble?** Disponível em: <http://articles.washingtonpost.com/2013-04-04/world/38280106_1_bitcoin-satoshi-nakamoto-monetary-policy> Acesso em: set. 2013.

TRAVERSE, Nick. **The Number: \$141.** Disponível em: <<http://www.newyorker.com/online/blogs/newsdesk/2013/04/the-number-141.html>> Acesso em: out. 2013.

SALMON, Felix. **The Bitcoin Bubble and the Future of Currency.** Disponível em: <<https://medium.com/money-banking/2b5ef79482cb>> Acesso em: out. 2013.

ESTES, Adam Clark. **Bitcoin is Now a BILLION Dollar Industry.** Disponível em: <<http://www.theatlanticwire.com/business/2013/03/bitcoin-now-billion-dollar-industry/63667/>> Acesso em: out. 2013.

BUSTILLOS, Maria. **The Bitcoin Boom.** Disponível em:

<<http://www.newyorker.com/online/blogs/elements/2013/04/the-future-of-bitcoin.html>>

Acesso em: out. 2013.

LOWENTHAL, Thomas. **Bitcoin: Inside the encrypted, peer-to-peer digital currency.** Disponível em: <<http://arstechnica.com/tech-policy/2011/06/bitcoin-inside-the-encrypted-peer-to-peer-currency/>> Acesso em: out. 2013.

Bitcoin – A peer-to-peer digital currency. Disponível em: <<http://www.wired.co.uk/news/archive/2011-05/16/bitcoin-p2p-currency>> Acesso em: set. 2013.

Bitcoin – A Virtual Money Created by CPU Cycles. Disponível em: <<http://lwn.net/Articles/414452/>> Acesso em: out. 2013.

O'LEARY, Naomi. **Bitcoin, the City trader's Anarchic new toy.** Disponível em: <<http://www.reuters.com/article/2012/04/01/traders-bitcoinidUSL6E8ET5K620120401>> Acesso em: out. 2013.

TINDELL, Ken. **Geeks Love the Bitcoin Phenomenon Like They Loved the Internet in 1990s.** Disponível em: <<http://www.businessinsider.com/how-bitcoins-are-mined-and-used-2013-4>> Acesso em: out. 2013.

Programador cria meio para usar Bitcoin como selo de autenticidade. Disponível em: <http://idgnow.uol.com.br/internet/2013/05/24/programador-cria-meio-para-usar-bitcoin-como-selo-de-autenticidade/?utm_source=feedly> Acesso em: set. 2013.

O'BRIEN, Matthew. **Bitcoin Is No Longer a Currency.** Disponível em: <<http://www.theatlantic.com/business/archive/2013/04/bitcoin-is-no-longer-a-currency/274859/>> Acesso em: out. 2013.

FOX, Justin. **Building a Better Coin.** Disponível em:

<<http://blogs.hbr.org/fox/2013/04/building-a-better-bitcoin.html>> Acesso em: out. 2013.

PLANES, Alex. **What the Bitcoin Crash Can TeACH Us About Money and Investing.** Disponível em: <<http://www.fool.com/investing/general/2013/04/11/what-the-bitcoin-crash-can-teach-us-about-money-an.aspx>> Acesso em: out. 2013.

Monetarists Anonymous. Disponível em: <<http://www.economist.com/node/21563752>> Acesso em: out. 2013.

GREENBER, Andy. **Crypto Currency.** Disponível em: <<http://www.forbes.com/forbes/2011/0509/technology-psilocybin-bitcoins-gavin-andresen-crypto-currency.html>> Acesso em: out. 2013.

PECK. Morgen. Bitcoin: **The Cryptoanarchist's Answer to Cash.** Disponível em: <<http://spectrum.ieee.org/computing/software/bitcoin-the-cryptoanarchists-answer-to-cash/0>> Acesso em: out. 2013.

KRUGMAN, Paul. **Adam Smith Hates Bitcoin.** Disponível em: <<http://krugman.blogs.nytimes.com/2013/04/12/adam-smith-hates-bitcoin/>> Acesso em: out. 2013.

KRUGMAN, Paul. **The Antisocial Network.** Disponível em: <http://www.nytimes.com/2013/04/15/opinion/krugman-the-antisocial-network.html?_r=0> Acesso em: out. 2013.

BOESLER, Matthew. **ANALYST: The Rise Of Bitcoin Teaches A Tremendous Lesson About Global Economics.** Disponível em: <<http://www.businessinsider.com/global-economics-lesson-from-bitcoin-2013-3>> Acesso em: out. 2013.

QUIGGIN, John. **The Bitcoin Bubble and a Bad Hypothesis.** Disponível em:

<<http://nationalinterest.org/commentary/the-bitcoin-bubble-bad-hypothesis-8353>>

Acesso em: out. 2013.

Fundação Bitcoin quer dobrar o tamanho de sua equipe. Disponível em:

<<http://idgnow.uol.com.br/internet/2013/06/03/fundacao-bitcoin-quer-dobrar-o-tamanho-de-sua-equipe-para-quatro/>>

Acesso em: nov. 2013.

MATONIS, Jon. **The Politics of Bitcoin Mixing Services.** Disponível em:

<<http://www.forbes.com/sites/jonmatonis/2013/06/05/the-politics-of-bitcoin-mixing-services/>>

Acesso em: nov. 2013.

STEADMAN, Ian. Wary of Bitcoin? A Guide to some other cryptocurrencies.

Disponível em: <<http://arstechnica.com/business/2013/05/wary-of-bitcoin-a-guide-to-some-other-cryptocurrencies/>>

Acesso em: nov. 2013.

5.2 Notícias sobre algumas das conseqüências do avanço da viabilidade das criptomoedas:

MADRIGAL, Alexis. C. **Libertarian Dream? A Site Where You Buy Drugs With Digital Dollars.** Disponível em:

<<http://www.theatlantic.com/technology/archive/2011/06/libertarian-dream-a-site-where-you-buy-drugs-with-digital-dollars/239776/>>

Acesso em: nov. 2013.

CHEN, Adrian. **The Underground Website Where You Can Buy Any Drug Imaginable.** Disponível em:

<<http://gizmodo.com/5805928/the-underground-website-where-you-can-buy-any-drug-imaginable>>

Acesso em: nov. 2013.

BALL, James. **Silk Road: the online drug marketplace that officials seem powerless to stop.** Disponível em:

<<http://www.guardian.co.uk/world/2013/mar/22/silk-road-online-drug-marketplace>>

Acesso em: nov. 2013.

GREENBER, Andy. **Wikileaks Asks For Anonymous Bitcoin Donations.** Disponível em: <<http://www.forbes.com/sites/andygreenberg/2011/06/14/wikileaks-asks-for-anonymous-bitcoin-donations/>> Acesso em: out. 2013.

COHN, Cindy. **EFF And Bitcoin.** Disponível em: <<https://www.eff.org/deeplinks/2011/06/eff-and-bitcoin>> Acesso em: set. 2013.

LEE, Timothy. B. US regulator: **Bitcoin exchanges must comply with money-laundering laws.** Disponível em: <<http://arstechnica.com/tech-policy/2013/03/us-regulator-bitcoin-exchanges-must-comply-with-money-laundering-laws/>> Acesso em: out. 2013.

Paypal considers bitcoins. Disponível em: <<http://bitcoinmagazine.com/paypal-considers-bitcoin/>> Acesso em: out. 2013.

The Pirate Bay and other p2p sharing platforms are accepting bitcoins. Disponível em: <<http://bitcoinmagazine.com/the-pirate-bay-accepting-bitcoin-donations/>> Acesso em: out. 2013.

COX, Jeff. Bitcoin Bonanza: **Cyprus Crisis Boosts Digital Dollars.** Disponível em: <<http://www.cnbc.com/id/100597242>> Acesso em: out. 2013.

Bitcoin in Spain – The currency run. Disponível em: <<http://www.wired.co.uk/news/archive/2013-03/20/bitcoin-spain-currency-run>> Acesso em: out. 2013.

SALYER, Kirsten. **Fleeing the Euro for Bitcoins.** Disponível em: <<http://www.bloomberg.com/news/2013-03-20/fleeing-the-euro-for-bitcoins-.html>> Acesso em: out. 2013.

WARNER, Bernhard. **Jittery Spaniards Seek Safety in Bitcoins.** Disponível em:

<<http://www.businessweek.com/articles/2013-03-20/jittery-spaniards-look-for-safe-haven-in-bitcoins>> Acesso em: out. 2013.

GREENBER, Andy. **Founder Of Drug Site Silk Road Says Bitcoin Booms And Busts Won't Kill His Black Market.** Disponível em: <<http://www.forbes.com/sites/andygreenberg/2013/04/16/founder-of-drug-site-silk-road-says-bitcoin-booms-and-busts-wont-kill-his-black-market/>> Acesso em: out. 2013.

RASKIN, Max. **Dollar-less Iranians Discover Virtual Currency.** Disponível em: <<http://www.businessweek.com/articles/2012-11-29/dollar-less-iranians-discover-virtual-currency>> Acesso em: out. 2013.

COOGAN, Peter. **Bitcoin Botnet Mining.** Disponível em: <<http://www.symantec.com/connect/blogs/bitcoin-botnet-mining>> Acesso em: out. 2013.

HIGGINS, Stan. **Gaming Platform Steam Now Accepting Bitcoin.** Disponível em: <<http://www.coindesk.com/video-game-platform-steam-now-accepting-bitcoin/>> Acesso em: abr. 2016.

Cibercriminosos brasileiros investem em golpes para roubar bitcoins. Disponível em: <<http://idgnow.uol.com.br/internet/2013/05/23/cibercriminosos-brasileiros-investem-em-golpes-para-roubar-bitcoins/>> Acesso em: out. 2013.

SPOTNIKS. **Dominica se torna o primeiro país a adotar o Bitcoin como moeda corrente.** Disponível em: <<http://spotniks.com/dominica-se-torna-o-primeiro-pais-adotar-o-bitcoin-como-moeda-corrente/>> Acesso em: 28 ago. 2014.

SILVA, Juliana A. L. **Norueguês investe R\$59 em bitcoins e compra apartamento com rendimentos.** Disponível em: <<http://www.infomoney.com.br/minhas-financas/planeje-suas-financas/noticia/3031573/noruegues-investe-bitcoins-compra>>

apartamento-com-rendimentos> Acesso em: 30 out. 2013.

PLANETA CARRO. **Tesla Model S é comprado apenas com bitcoins.** Disponível em: <<http://quatorrodas.abril.com.br/blogs/planeta-carro/2013/12/07/tesla-model-s-e-comprado-apenas-com-bitcoins/>> Acesso em: 8 dez. 2013.

COSTA, Antonio Luiz M. C. **Bitcoin, a TELEXFREE dos ricos, cultos e descolados?** Disponível em: <<http://www.cartacapital.com.br/blogs/antonio-luiz/bitcoin-a-telexfree-dos-ricos-cultos-e-descolados-3305.html>> Acesso em: 26 ago. 2013.

KLEINA, Nilton. **Shift, o novo cartão de débito para pagar com bitcoins nos EUA.** Disponível em: <<https://www.tecmundo.com.br/bitcoin/89695-shift-novo-cartao-debito-pagar-bitcoin-eua.htm>> Acesso em: 22 nov. 2015.

5.3 Lista de sites que trabalham com bitcoin ou apontam locais os quais aceitam diretamente as bitcoins:

http://www.americanbanker.com/issues/177_176/bitpay-signs-1000-merchants-to-accept-bitcoin-payments-1052538-1.html

<http://www.paritynews.com/web-news/item/690-the-internet-archive-starts-accepting-bitcoin-donation>

<https://bitpay.com/> e <https://bitpay.com/visa/> - Utilizar bitcoins no cartão de crédito tradicional