UNIVERSIDADE FEDERAL FLUMINENSE

Mauricio Gomes dos Santos

Moedas Virtuais e seu impacto na sociedade.

Niterói

2017

Mauricio Gomes dos Santos

Moedas Virtuais e seu impacto na sociedade.

Trabalho de Conclusão de Curso submetido ao Curso de Tecnologia em Sistemas de Computação da Universidade Federal Fluminense como requisito parcial para obtenção do título de Tecnólogo em Sistemas de Computação.

Orientadora:
Helga Dolorico Balbi

NITERÓI

Ficha Catalográfica elaborada pela Biblioteca da Escola de Engenharia e Instituto de Computação da UFF

S237 Santos, Mauricio Gomes dos
Moedas virtuais e seu impacto na sociedade / Mauricio Gomes dos Santos. – Niterói, RJ : [s.n.], 2017.
45 f.

Projeto Final (Tecnólogo em Sistemas de Computação) – Universidade Federal Fluminense, 2017.
Orientador: Helga Dolorico Balbi.

1. Sistema de computador. 2. Moeda virtual. 3. Criptografia de dados (Computação). I. Título.

CDD 004

2017

Mauricio Gomes dos Santos

Moedas Virtuais e seu impacto na sociedade.

Trabalho de Conclusão de Curso submetido ao Curso de Tecnologia em Sistemas de Computação da Universidade Federal Fluminense como requisito parcial para obtenção do título de Tecnólogo em Sistemas de Computação.

Niterói, 20 de Junho de 2017.

Banca Examinadora:

_____

Prof[a]. Helga Dolorico Balbi, Msc. – Orientadora
UFF - Universidade Federal Fluminense

_____

Prof. Vinicius Corrêa Ferreira, M.Sc. – Avaliador
UFF - Universidade Federal Fluminense

AGRADECIMENTOS

Dedico este trabalho primeiramente a deus que me deu saúde nessa jornada.

A minha orientadora Helga que me ajudou e estimulou nos momentos mais difíceis. Aos professores, tutores e todos os profissionais do sistema de ensino à distância do Cederj o meu muito obrigado.

A minha companheira Elaine Silva pela força e dedicação, aos meus pais que me deram base para tal feito e meu estimado filho Guilherme que me inspira todos os dias.

“O insucesso é apenas uma oportunidade para recomeçar com mais inteligência”.
Henry Ford.

RESUMO

Este trabalho tem por objetivo estudar os impactos de uma tecnologia que inovou a forma de realizar transações financeiras nos últimos anos, em específico as moedas virtuais de alta complexidade tecnológica, como por exemplo a Bitcoin, e descrever quais têm sido os posicionamentos adotados por uma série de áreas e jurisdições a esse respeito. Trata-se de uma aproximação mais palpável da linguagem da Tecnologia da informação e da economia aos operadores do Direito. O estudo estende-se na direção de propor uma reflexão acerca do significado de se reconhecer as moedas virtuais como uma moeda paralela – muito embora a discussão acerca de ser ou não moeda constitui apenas uma das discussões possíveis. A Bitcoin é um experimento de um novo modelo de moeda totalmente baseado em criptografia e que traz como novidade uma nova forma de se pensar a sua relação com a sociedade. Esta moeda virtual, pelas suas características intrínsecas baseadas em tecnologia, não pode ser controlada por nenhum grupo de pessoas, empresa ou governo. O trabalho apresentará a compreensão do seu surgimento no mercado e das suas particularidades e vantagens comparadas com outras moedas virtuais, que permitirá ao leitor a realização de uma análise plena e fundamental sobre o sistema de geração de moedas virtuais. A Bitcoin reforça seu potencial e suas limitações, principalmente no tocante aos desafios enfrentados à uma regulação eficaz. Também serão discutidas as inovações trazidas pela moeda eletrônica para o sistema financeiro atual e os seus impactos no campo jurídico, assim como a decorrência de crimes na INTERNET sob a utilização do anonimato proporcionado pelas características da Bitcoin que privilegiam a privacidade. O método utilizado para o desenvolvimento do trabalho é o dedutivo e a técnica de pesquisa é a bibliográfica, partindo-se de estudos sobre as características inovadoras da Bitcoin e sobre a resposta dos Governos a estes novos aspectos ainda desconhecidos para a maioria dos legisladores.

Palavras-chaves: Bitcoin; Direito; Moeda virtual; Moedas Paralelas; Novas Tecnologias; Regulamentação; Criptomoedas.

ABSTRACT

The purpose of this work is to study the impacts of a new technology in the way of carrying out financial transactions in recent years, in particular virtual currencies of high technological complexity, such as Bitcoin, and to describe the positions adopted by different areas and jurisdictions in this regard. It is a more palpable approximation of the language of the Information Technology and economics to the operators of the law. The study extends in the direction of reflecting on the significance of recognizing virtual currencies as a parallel coin - although the discussion of whether or not it is a currency is just one of the possible discussions. Bitcoin is an experiment in a new currency model totally based on cryptography that brings a novel way of thinking about its relationship with society. Any group of people, business or government cannot control this virtual currency, because of its intrinsic characteristics based on technology. The work will present the understanding of its emergence in the market and its particulars and advantages compared to other virtual currencies, which will allow the reader to carry out a full and fundamental analysis of this virtual coin generation system. Bitcoin reinforces its potential and its limitations, especially with regard to the challenges faced by effective regulation. This work aims to discuss the innovation brought by electronic money to the current financial system and its impacts in the legal field, as well as the occurrence of crimes on the Internet under the use of anonymity provided by the characteristics of Bitcoin that privilege privacy. The method used for this is the deductive and the research technique is the bibliographical one, starting from studies on the innovative characteristics of Bitcoin and on the response of the Governments to these new aspects that still unknown for the majority of the legislators.

Key words: Bitcoin; Right; Virtual currency; Parallel Coins; New technologies; Regulation; Crypto coin.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

MIT - *Massachusetts Institute of Technology*

P2P - *Point-to-Point*

TOR – Software livre que proporciona anonimato, privacidade e segurança para usuário navegar na internet.

Proof-of-stake - A mineração é proporcional ao número de moeda que o minerado detém

SUMÁRIO

1 INTRODUÇÃO

À primeira vista, não é nada fácil entender o que são Moedas Virtuais, tendo em vista que se trata de uma tecnologia inovadora com um conceito diferenciado, um dia inimaginável para o conceito humano e que quebra vários tabus.

As Moedas virtuais são uma forma de dinheiro como qualquer outro, como o Dólar ou o Real. Sua diferença está em sua criação, que parte de um princípio lógico digital, que não é controlado nem emitido por um governo. Sua cotação é determinada livremente por seus usuários, que ainda o geram, protegem e utilizam.

As moedas virtuais, especificamente o Bitcoin, moeda esta que será nossa base para esta dissertação, representam uma imensa revolução no mercado financeiro tornando possível a realização de transferências de A para B sem jamais precisar de um intermediário, como os Bancos por exemplo, tornando-se um marco no mundo capitalista e moderno dos tempos atuais.

Mas como funciona? Quais os benefícios e desvantagens em utilizar? Estas questões serão abordadas no decorrer do trabalho, que está organizado da seguinte forma: O segundo capítulo apresentará um breve histórico sobre as moedas virtuais. O terceiro capítulo tem como interesse justamente explicar o funcionamento deste sistema. Após o entendimento básico, o quarto capítulo apresentará um breve comparativo entre algumas moedas existentes no mercado, como Litecoin. Na sequência, no quinto capítulo, será apresentada uma visão econômica e jurídica acerca das moedas virtuais. É importante notar que se trata de duas áreas densas e com um grande conteúdo. Desta forma, serão abordadas de forma superficial, não sendo o foco principal do trabalho. O objetivo principal é mostrar o impacto que essa tecnologia trás para a sociedade. No sexto capítulo será apresentada uma ideia sobre o futuro das moedas virtuais e o que esperar em termos de inovação.

> Em definitivo, o Bitcoin é a maior inovação tecnologia desde a internet, é revolucionário, sem precedentes e tem o potencial de mudar o mundo de uma forma jamais vista. À moeda, ela e o futuro. Ao avanço da liberdade individual, é uma esperança e uma grata novidade [1]

2 HISTÓRICO DAS MOEDAS VIRTUAIS

Este capítulo trará uma breve descrição sobre as moedas virtuais, apresentando uma introdução sobre sua história, seu surgimento e suas motivações para sua implementação, apontando as diferenças básicas entre as muitas moedas existentes no mercado.

2.1 MOEDAS VIRTUAIS

Nos últimos anos, muito se tem ouvido falar de uma nova forma de transação financeira. Tal transação não envolve bancos centrais e governos e, com seu sucesso, tem ganhado admiradores e críticos. Essa nova modalidade se chama Moeda Virtual (ou *virtual currency* em inglês). Existem diversas moedas virtuais em uso atualmente, porém, a mais popular atualmente é o Bitcoin. Tendo isto em vista, esta moeda será utilizada como base principal para o desenvolvimento deste trabalho.

O termo, que para muitos ganhou vida por conta de jogos de realidade virtual, e o sucesso alcançado com o Bitcoin, que baseia-se em ideias mais avançadas da aplicação da criptografia para dinheiro, tiveram origem no início da década de 80, no princípio da internet, em 1983 [2] com David Chaum.

Em 1994, houve a primeira transação de moeda eletrônica, a partir do *DigiCash* [3] de David Chaum. Em 1998, o *b-money* [4] de Wei Dai inovava garantindo privacidade e que cada moeda seria única: com um complexo sistema de códigos divididos em duas chaves, uma pública e uma privada, para que houvesse uma transação, onde a parte recebedora deve oferecer seu código público para a parte pagadora em sua carteira e o envio das moedas à carteira do recebedor.

Outros sistemas similares foram sendo desenvolvidos a partir do então, como o D-Cash e o BitGold, entre outros. O BitGold [5] do ano 2005, de Nick Szabo trazia artifício para evitar clonagem de moedas e a operacionalidade do sistema, modalidade que ficou conhecida como prova-de-trabalho (*proof-of-work*): as transfe-

rências eram realizadas instantaneamente, mas existiam os “mineradores”, ou seja, pessoas que usavam seus computadores para “Validar” as transações feitas, decodificando suas criptografias, cobrando módicas taxas entre as transações.

De fato, a ideia de uma moeda autônoma e eletrônica surgiu nos meados de 1998, através “*Manifesto Cypherpunk*” [6], um texto de autoria do programador Eric Hughes que defendia o uso de criptografia para proteger a privacidade na era da informação.

Na prática nenhum dos sistemas foram aplicados: Na roda da evolução das moedas criptografadas, em 2008 um artigo foi lançado com o conceito do Bitcoin, por Satoshi Nakamoto, revelando todo o código de programação, de modo acessível a todos, e explicando seu funcionamento [7].

Nakamoto foi além das tentativas e erros dos conceitos anteriores, com uma junção de chaves públicas e privadas de B-money e a prova-de-trabalho do BitGold, ele resolveu um grande problema: Um sistema de validação que ficou conhecido como *Blockchain*, que será tratado com mais profundidade adiante. Hughes afirmava que se deve garantir que somente as partes interessadas tenham conhecimento da transação financeira.

Outro exemplo famoso é o Litecoin [8], que surgiu em 2011 e destaca-se por ser bem mais leve do que o Bitcoin. O processamento de blocos, ocorre a cada 2,5 min segundos, contra os 10 min do Bitcoin, entre outras diferenças que serão abordadas mais adiante.

O Peercoin [9] é uma moeda digital experimental que, como o Bitcoin, usa tecnologia peer-to-peer para operar. O *software* foi lançado sob licença da MIT, que é uma concessão de permissão gratuita para uso de software, arquivos e outros criado por advogados do Instituto Tecnológico de Massachusetts. Os Peercoin são enviados facilmente através da internet, sem confiar em terceiros, e seu custo é bem baixo comparado a outras moedas.

> Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions....(MIT license first paragraph.) [10]

O Feathercoin [11], criada em Abril de 2013, por bitcointalk.org, uma marca que ficou registrada após sofrer vários ataques devastadores, conhecidos como “51 por cento”. Esses ataques tem o poder suficiente para criar sua própria cadeia de bloqueios, com isso gera gastos duplos, confirmações de transações não se confirmam e corrompem a rede [12]. Esses ataques invalidam os blocos, produzidos por mineradores, assim levando duplicatas da moeda. Em Setembro deste mesmo ano, após atualizar seus clientes para uma versão de *software* corrigida para evitar ataques “51 por cento”, a Fearthercoin expandiu seus serviços para Holanda, África do sul e República Tcheca.

As moedas virtuais têm várias motivações, uma delas é instabilidade econômicas dos países. Recentemente, os preços das moedas subiram devido ao aumento da procura por moedas virtuais na China, que passa por uma fase de incertezas econômicas. Na crise de 2008, o sistema financeiro global estava à beira de um colapso diante de uma crise que afetou grandes potências mundiais como os EUA, Itália e outros. Esta foi a data de lançamento do Bitcoin.

O uso crescente desta tecnologia é um ponto importante, visto que diversas empresas estão aceitando este tipo de pagamento via moedas virtuais, como as empresas de grande porte Dell Computadores [13], Amazon, AliExpress, E-bay entre outras. Nota-se, também, as altas valorizações das moedas, principalmente do Bitcoin, que chegou a ser negociado por R$ 849 reais em Junho de 2015 e, no mesmo período deste ano de 2016, já era negociado a R$2.262, ou seja, a uma variação de 166% [14]. Mas a grande motivação, sem dúvida, é o fato de representar uma moeda descentralizada, livre impostos e sem o controle de um banco central conforme o “Manifesto Cypherpunk” relata.

3 TECNOLOGIAS UTILIZADAS.

Este capítulo introduz as tecnologias implementada nas moedas virtuais, inovações no mercado financeiro e seu funcionamento.

3.1 IMPLEMENTAÇÃO DAS MOEDAS VIRTUAIS.

A tecnologia e funcionamento por trás das moedas virtuais se aprimoram a cada dia, códigos são reescritos e novas moedas são lançadas. A Bitcoin será referência para a apresentação deste capítulo. Conforme descrito anteriormente, as moedas virtuais são utilizadas em transações *online* e compras de produtos e serviços pela Internet. É bom ressaltar, novamente, que nenhum governo ou banco central controla seu fluxo.

A Bitcoin inicialmente surgiu, como um protótipo de moeda eletrônica para pagamentos online. As inovações possibilitavam realizar transações diretamente entre duas partes, sem a necessidade de envolvimento de instituições financeiras para a validação das transações.

O modelo de estrutura tecnológica da Bitcoin é a principal novidade em relação ao modelo financeiro atual. Baseia-se em uma rede *peer-to-peer*, muito utilizada para troca de dados na Internet, como o compartilhamento de músicas e vídeo, por exemplo. A criptografia é usada para assegurar a integridade de todos os dados trafegados. Diferente do compartilhamento de músicas e outros, que o foco está na segurança do usuário e não na segurança das informações, a rede Bitcoin foca em ambos, tanto na privacidade dos seus usuários, isso não quer dizer que seja infalível, como na segurança de que as trocas monetárias transacionadas na rede são confiáveis.

Essa confiança é demonstrada e denominada *Blockchain*, que contém o histórico de todas as transações já realizadas na rede. Quer dizer que funciona como um “livro registro” que mostra publicamente o histórico de todas as negociações feitas pelas chaves públicas. É um processo de validação por meio de concorrência das transações em blocos encadeados, cuja decodificação se dá em função dos

blocos vizinhos. Os mineradores, para receber novos lotes de moedas e taxas, recebem esses blocos para serem decodificados, com o intuito de validar em massa as transações efetuadas.

Deste modo, o *hardware* do minerador que conseguir de fato decodificar o bloco de transações receberá uma recompensa (maior a capacidade de processamento deste dispositivo, mais chance tem de decodificar primeiro e ser recompensado).

As transações são efetuadas após verificação das chaves públicas e das chaves privadas, essas por sua vez são mantidas em sigilo como senha de banco. É com a chave privada que a transação será autenticada. Ao se verificar a chave pública, o qual todos da rede têm acesso, é necessário encontrar-se a chave privada do benificiário, e só assim a troca de carteira é homologada e a transferência da Bitcoin é concretizada. Está atividade será registrada, carimbada com data e hora e fixada em um bloco do *Blockchain*.

A Figura 1 mostra uma transação entre João e Maria. João decide transferir Bitcoin para Maria. Para isso, ele gera uma mensagem que se chama “transação”, contendo a chave pública de Maria, que está assinada com a chave privada do mesmo. A rede Bitcoin por sua vez tem acesso livre à chave pública de João. Ao se verificar esta chave pública de João é visto que de fato a transação foi assinada com a chave privada e a negociação é validada. Assim, a troca é autenticada e Maria passa a ser o novo proprietário do fundo.

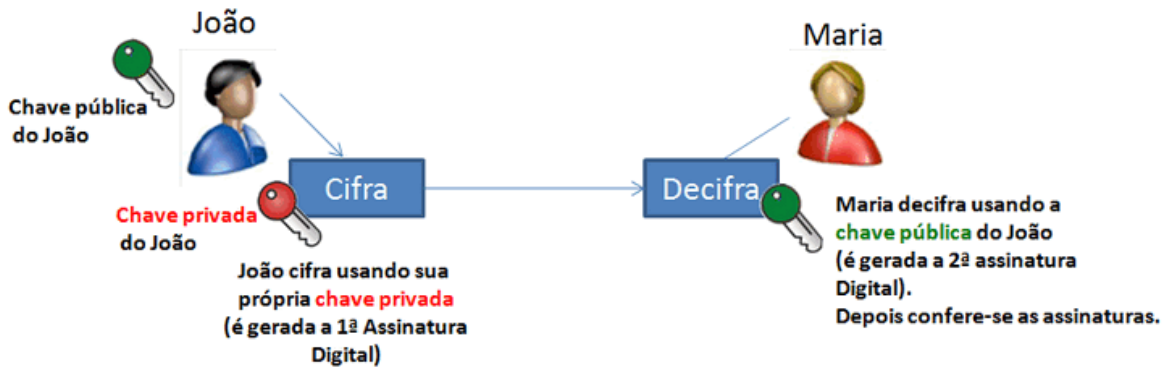

Figura 1: Validação da chave pública e privada [15]

O histórico de negociações é assegurado através das chaves públicas (códigos alfanuméricos) que não são vinculados a nenhum usuário. No entanto, as chaves podem ser facilmente rastreadas pelo endereço de IP. Para não correr esse risco e preservar a privacidade dos usuários, é possível utilizar *softwares* como o TOR [16], é um software que tem como o objetivo garantir uma navegação segura na INTERNET, analisar o tráfego de dados na rede e sobre tudo proteger os usuários contra *malwares* que ameacem os dados pessoais e a privacidade. *Malware* é qualquer parte de um software que tenha em seu código uma escrita para causar danos a dados ou dispositivos de terceiros, exemplos são cavalo de troia e *worm*.

A rede mantém o registro de transações constantemente atualizado e analisado, o que impede as fraudes e os gastos duplos. Tudo isso só é possível por causa da criptografia de chave pública.

A rede peer-to-peer (tradução livre, pessoa para pessoa) é um dos fatores para o sucesso das moedas virtuais. Ela é totalmente dependente dos seus usuários para funcionar por ser uma rede descentralizada, isso porque os dados não ficam armazenados em um servidor central. Em uma rede descentralizada, cada ponto ou nó da rede tem a função de cliente ou de servidor, e todos os nós são igualitários, pois ambos têm a mesma informação. Cada usuário compartilha pedaços de informações com os outros usuários da rede. Isso garante maior disponibilidade e performance, adaptação às falhas, deixando a comunicação rápida e reduzindo os custos relacionados a infraestrutura.

Na Figura 2 existem três modelos de topologia. No caso da rede centralizada, a transferência de informações parte de um único ponto, um exemplo clássico seria o sistema de televisão, onde um transmissor no caso uma antena, envia informações que são captadas por receptores, no caso os televisores, que captam essas informações geradas por esse único ponto central na rede. A rede descentralizada funciona como uma árvore, ou seja, do centro da rede, informações são geradas e transferidas para nós intermediários, que passam armazenar, atualizar e transferir essas informações para o usuário final. Por último, na rede distribuída todos os usuários podem ser emissores ou destinatários das informações, mas para ser um emissor o mesmo tem que ter as informações solicitadas pelo destinatário da informação, exemplo de uma rede distribuída é a rede *torrent,* que disponibiliza diversos arquivos na rede, filmes, livros e outros.

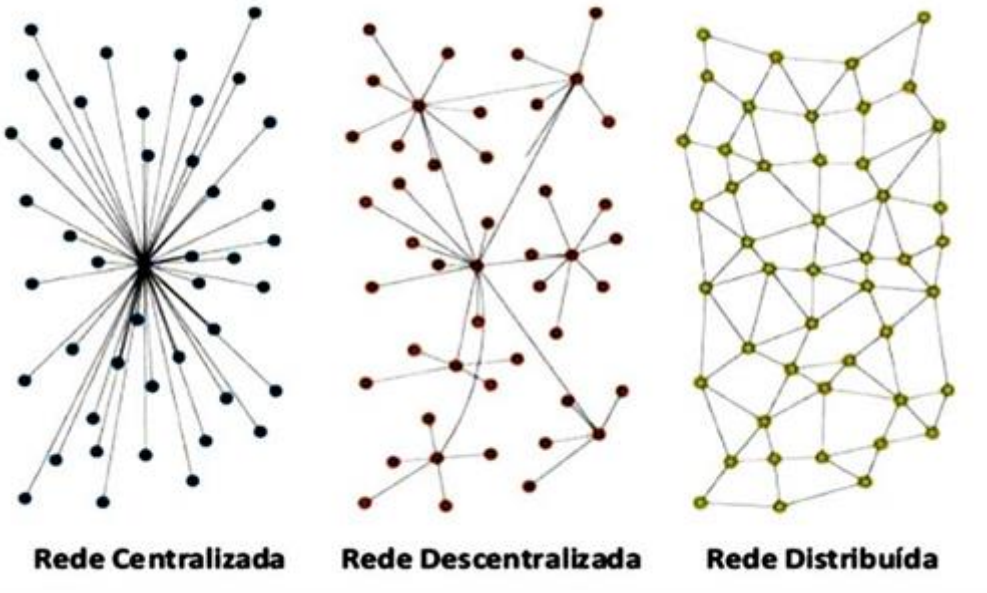

Figura 2: Exemplo de topologia de redes. [17]

The term peer-to-peer, or P2P, means that the computers that participate in the network are peers to each other, that they are all equal, that there are no "special" nodes, and that all nodes share the burden of providing network services. The network nodes interconnect in a mesh network with a "flat" topology. There is no server, no centralized service, and no hierarchy within the network. Nodes in a peer-to-peer network both provide and consume services at the same time with reciprocity acting as the incentive for participation. Peer-to-peer networks are inherently resilient, decentralized, and open. The preeminent example of a P2P network architecture was the early Internet itself, where nodes on the IP network were equal. Today's Internet architecture is more hierarchical, but the Internet Protocol still retains its flat-topology essence. Beyond bitcoin, the largest and most successful application of P2P technologies is file sharing with Napster as the pioneer and BitTorrent as the most recent evolution of the architecture.
The term "bitcoin network" refers to the collection of nodes running the bitcoin P2P protocol. In addition to the bitcoin P2P protocol, there are other protocols such as Stratum, which are used for mining and lightweight or mobile wallets. These additional protocols are provided by gateway routing servers that access the bitcoin network using the bitcoin P2P protocol, and then extend that network to nodes running other protocols. For example, Stratum servers connect Stratum mining nodes via the Stratum protocol to the main bitcoin network and bridge the Stratum protocol to the bitcoin P2P protocol. We use the term "extended bitcoin network" to refer to the overall network that includes the bitcoin P2P protocol, pool-mining protocols, the Stratum protocol, and any other related protocols connecting the components of the bitcoin system. [18]

A arquitetura de rede peer-to-peer é muito mais que uma escolha de topologia, ela tem um papel [19] essencial para o funcionamento da Bitcoin, ela garante a distribuição do *Blockchain* a todos os seus usuários. Por meio deste sistema, todos os usuários da rede são mantidos com uma cópia atualizada das negociações ocorridas. Ou seja, toda e qualquer nova transação que venha a ocorrer é transmitido a todos os membros em um registro único e compartilhado, o que torna redundante e desnecessário a existência de um servidor central. Além do Bitcoin, a maior e bem-sucedida aplicação de moeda virtual que utiliza esta tecnologia peer-to-peer, temos o *Napster* e o *BitTorrente* que fazem compartilhamento de arquivos.

Devido a esta característica da Bitcoin, não é possível que ela seja controlada por nenhuma pessoa, empresa ou organização, o que acaba frustrando tentativas de criar legislações específicas sobre algo que não pode ser regulado, pelo menos não da maneira como o dinheiro tradicional é.

O *Blockchain* é um grande livro caixa que contém todas as transações. Qualquer nova transação é analisada e salva neste banco de dados, e isso assegura que não ocorram gastos duplos.

AFigura 3 demonstra o ciclo para um minerador ter acesso a um novo bloco. Antes de acessar um novo bloco, o minerador dever cumprir todas as tarefas que estão no bloco atual. Estas tarefas são problemas que devem ser solucionados de forma difícil e trabalhosa para o protocolo funcionar. Sua solução leva em torno de dez minutos. Já a verificação desta solução deve ser mais rápida e fácil, essa tarefa é retratada na Figura 4.

Após a conclusão destas tarefas, o minerador poderá acessar um novo *Blockchain*, tudo isso serve para evitar fraudes no sistema. A Figura 5 traz o número de transações realizadas no dia 04/06/2017 que foi de 278.912 operações com valor total negociado de $41 milhões. A energia gasta para solucionar os blocos foi de 5.432,357 *Terahertz* e a cotação do Bitcoin era de 1BTC para $2667,54 dólares.

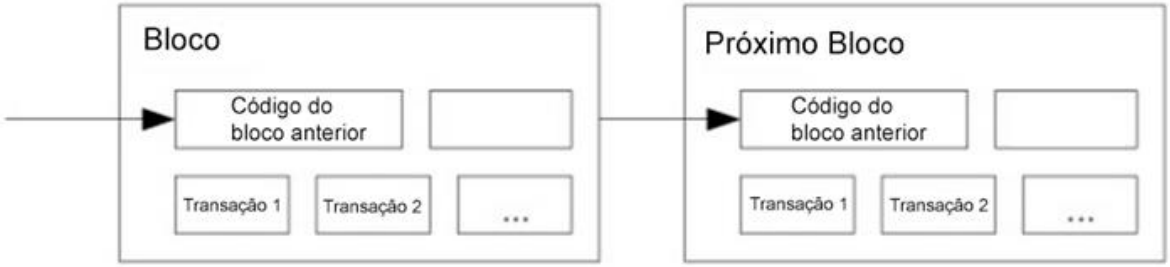

Figura 3: Validação das transações prova de trabalho; (*Proof-of-Work*) [20]

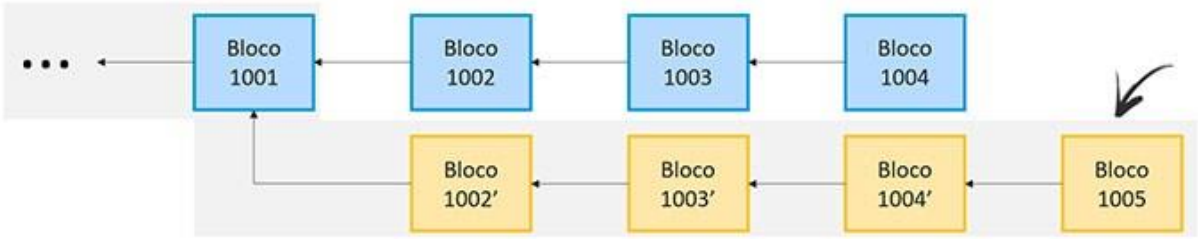

Figura 4 Sequencia de bloco distribuídos [21]

Figura 5: Número de transações por dia. [22]

Todas as transações que ocorrem na economia Bitcoin são registradas em uma espécie de livro-razão público e distribuído chamado de *Blockchain* (corrente de blocos, ou simplesmente um registro público de transações), o que nada mais é do que um grande banco de dados público, contendo o histórico de todas as transações realizadas. Novas transações são verificadas contra o *Blockchain* de modo a assegurar que os mesmos Bitcoins não tenham sido previamente gastos, eliminando assim o problema do gasto duplo [23].

Figura 6: Resumo dos custos de mineração. [24]

Os mineradores têm como objetivo encontrar uma sequência numérica que se somará às informações sobre transações feitas com Bitcoin. O produto disso será o que chamam de "*hash*".

Alguns dados de mineração são ilustrados na Figura 6. O que mais chama atenção é o total da receita dos mineradores de $6,7 Milhões de dólares, com um custo por transação efetuada de $23,77 dólares.

O *hash* é apenas um número, o Bitcoin estabelece um valor máximo para o *hash*. O Bitcoin trabalha com números extremamente grandes, mas, para fins de exemplo, vamos supor que o hash não pode ser maior do que 8. Quando o minerador encontrar um "*nonce*" que faz o bloco ter um hash 6, por exemplo, ele propaga isso para a rede. O bloco está resolvido e pode integrar a corrente de blocos.
Blocos de Bitcoins devem levar, em média, 10 minutos para terem seu "*nonce"* encontrado. Caso os mineradores estejam encontrando o "*nonce"* muito rapidamente, o valor máximo (8, no exemplo) é diminuído, para dificultar o trabalho. Caso os mineradores estejam muito lentos, o valor máximo é aumentando, facilitando o trabalho, pois o número de *hashes*

válidos aumenta. Esse ajuste é proporcional e é calculado pela rede periodicamente, baseando-se na velocidade média de geração de cada bloco. Pelo seu trabalho, os mineradores ganham uma quantidade de Bitcoins. Atualmente, esse valor é de 25, mas ele será diminuído pela metade quando a rede atingir determinado número de blocos, até que moedas não sejam mais geradas. O minerador também fica com o "troco" de todas as transações do bloco, caso esse troco não tenha sido "devolvido" ao pagador na transação. Caso dois mineradores encontrem um *nonce* juntos ou quase juntos, a rede terá dois blocos válidos em circulação. Eventualmente, um novo bloco será gerado, mas ele referenciará apenas o *hash* de um dos blocos anteriores. O bloco que sobrou, chamado de "bloco órfão", é descartado. Se a transação foi incluída apenas no bloco órfão, ele terá que ser novamente incluída em um bloco futuro, o que pode fazer com que uma transação leve mais de 30 minutos até ser oficialmente parte do histórico do Bitcoin [25].

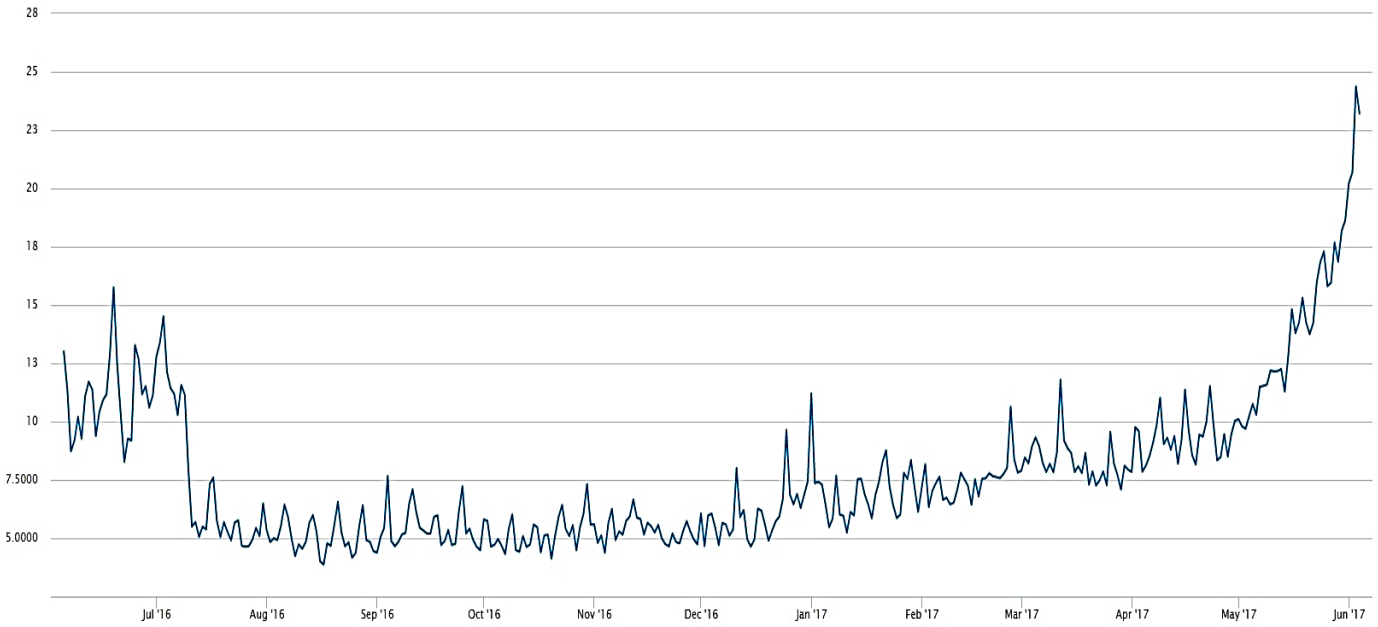

Figura 7: Custo da mineração ao logo de 2016 a 2017. [24]

Na Figura 7, pode-se observar o aumento no custo da mineração ao longo de um ano. Em Junho de 2016 o custo chegou a $15 dólares. Já em Junho de 2017, chegou aos atuais $25 dólares. Uma ilustração do passo a passo de uma transação de Bitcoin é mostrada na Figura 8 onde o usuário Bruno efetua a compra de um celular na loja virtual de Paula, que aceita Bitcoin. O custo do aparelho celular é de Um Bitcoin. Deve ser observado o destaque que o minerador tem na validação da transação ao encontrar o *hash*.

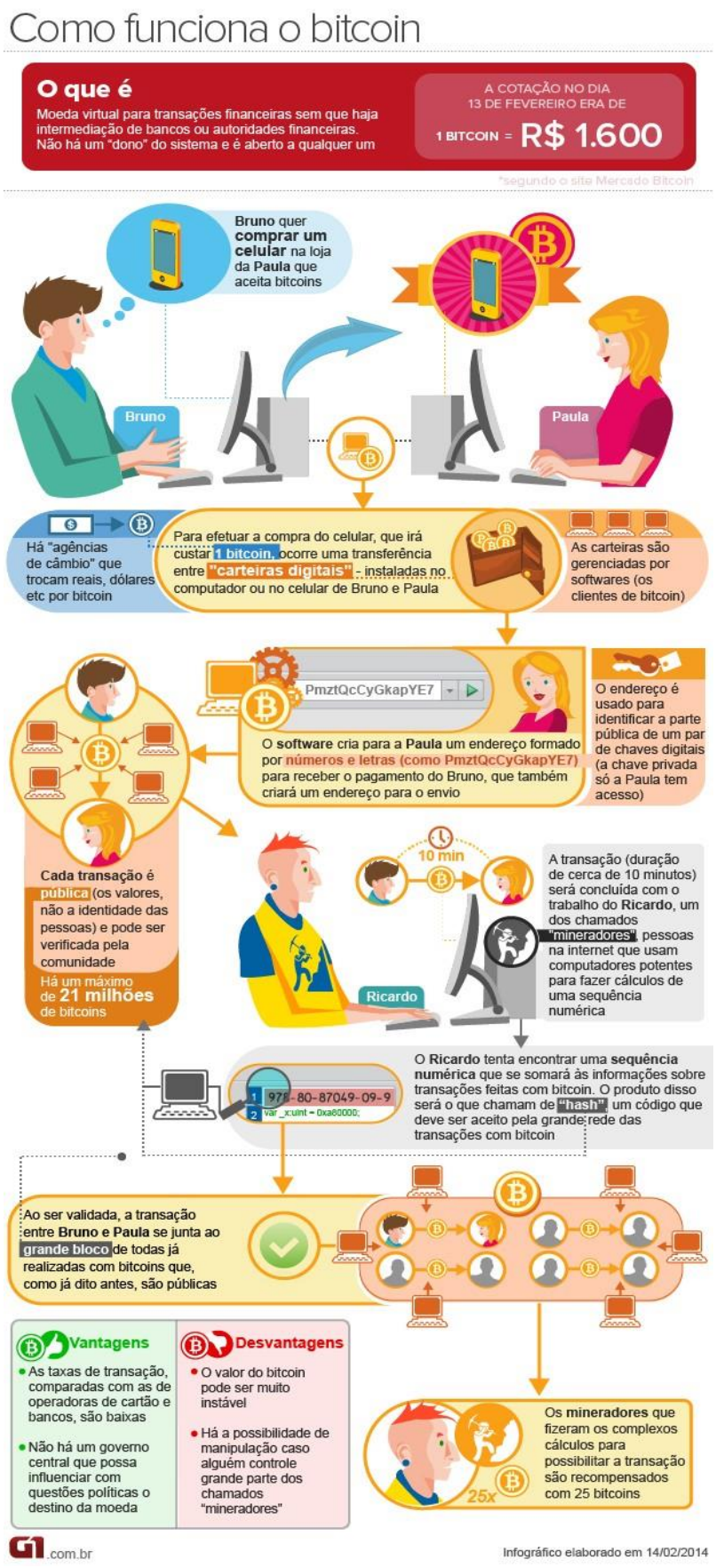

Figura 8: Diagrama do funcionamento do Bitcoin [25]

É muito caro operar como um mineiro. No nível de dificuldade atual, encontrar um único bloco leva à computação de cerca de 10 a 20 hashes. A cada dez minutos, complexos problemas matemáticos são lançados no sistema. Atualmente, a primeira máquina que decifrá-los recebe como remuneração 12,5 novos Bitcoins. A cada quatro anos, a recompensa diminui. Em 2012, eram 25 Bitcoins por problema decifrado. Em 2020, já é certo que o valor vai reduzir para 6,25 [26].

A mineração é realizada por redes de computadores superpotentes. Em 2008, um Bitcoin era negociado por US$ 589 dólares. Em dezembro de 2013, um Bitcoin chegou a valer US$ 1.147 dólares e atualmente passa dos US$ 2000 dólares [27]. Com esse ágio nos valores negociados e com a alta rentabilidade, grandes empresas, gigantes da tecnologia, *startups* e companhias globais com anos de mercado travam uma "corrida digital" em busca dos melhores e mais potentes data *centers*. Eles funcionam 24 horas por dia, ininterruptamente, e passam por melhorias contínuas para resolver cada vez mais rápidas novas equações que garantam mais dinheiro virtual.

> Em todo o mundo, são feitos em torno de 1.500 quadrilhes de cálculos por segundo. Esse volume supera em duas mil vezes a força computacional dos 500 supercomputadores que existem no planeta [28].
> O volume anual negociado em 2016 foi de R$ 363 milhões. O índice é 45% superior aos R$ 113 milhões registrados em todo o ano passado. Percebe-se um crescimento constante e forte de volume no Brasil que permite iniciarmos as projeções de volume para 2017 com potencial para atingir um total entre R$ 650M e R$ 1B [29].

A Figura 9 mostra um gráfico da cotação do dia 05 de Junho de 2017. Na abertura do pregão, os valores eram de $2,513 dólares. O pregão fechou com uma alta de 3,91%, alcançando os valores de $2,835 dólares. A Figura 10 demonstra a alta valorização da moeda nos últimos 6 meses passando da casa dos $2,000 dólares em Maio de 2017. É possível notar que a variação em um 1 ano foi de 344,22%.

Fechamento Anterior	2.528,97	Compra	2.634,9	Var. Diária	2.530 - 2.641,53
Abertura	2.513,02	Venda	2.635	52 semanas	482 - 2.740,86
Variação 1 ano	344,22%				

Figura 9: Cotação do Bitcoin na data 05/06/2017. [30]

Fechamento Anterior	2.528,97	Compra	2.634,9	Var. Diária	2.530 - 2.641,53
Abertura	2.513,02	Venda	2.635	52 semanas	482 - 2.740,86
Variação 1 ano	344,22%				

Figura 10: Cotação do Bitcoin para o intervalo de um ano [30].

A Figura 11 apresenta um comparativo de rentabilidade entre fundos de investimentos nos anos de 2014, 2015 e 2016. Os resultados mostram o alto desempenho do mercado Bitcoin comparado com outros investimentos que incluem ouro, CDI e ações no Ibovespa.

Aplicações			
Investimento	**Rentabilidade %**		
	de 31dez14 até 12dez16	**2015**	**2016 Até 12 dezembro**
Bitcoin - Mercado Bitcoin	200,66	100,77	49,75
Ibovespa	18,34	-13,31	36,52
CDI	28,18	13,24	13,19
Poupanca	17,14	8,15	8,30
Ouro	22,78	33,63	-8,12
Dolar Ptax Venda	26,86	47,01	-13,70
Euro Real	10,83	31,71	-15,85
Fonte Economatica			

Figura 11: Comparativo com outros sistemas monetários em 2016 [31]

A Figura 12 mostra um gráfico com a evolução dos ganhos com Bitcoin em um ritmo acelerado, acompanhado pelo mercado de ações Ibovespa e uma leve alta nos investimentos de poupança e CDI. Já o ouro e Euro apresentaram uma leve queda no último ano.

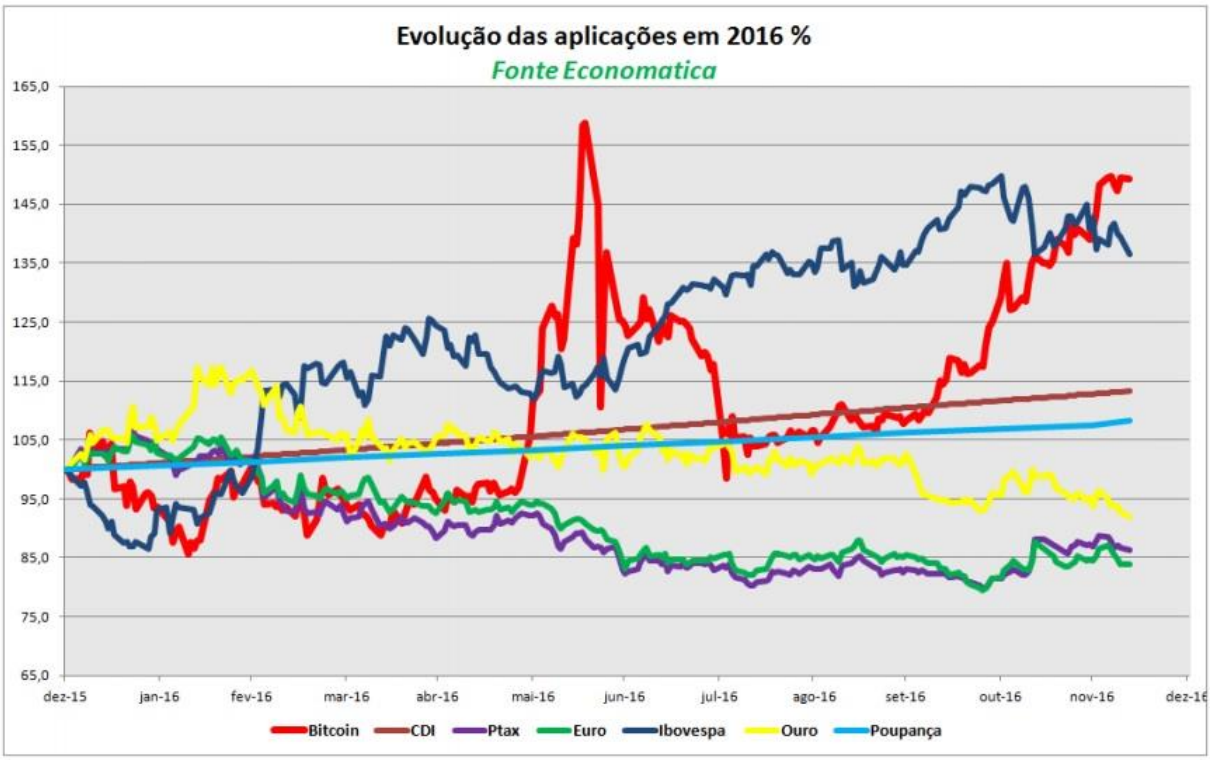

Figura 12: Evolução das aplicações no ano de 2016. [31]

Como descrito anteriormente para solucionar as tarefas durante a mineração, são exigidas máquinas superpotentes e dedicadas. É essencial uma ótima placa de vídeo e uma boa ventilação para manter os equipamentos sem superaquecimento. Muitos dos mineradores, por este fato, não utilizam gabinetes para proteger seus *hardwares* como mostra a Figura 13. Não há necessidade de um processador potente visto que não influência muito. Já as placas de vídeo devem ter uma atenção redobrada conforme mostra a Figura 14.

Figura 13: Hardware linkados de mineração. [20]

Figura 14: Placas dedicadas para mineração. [20]

4 MOEDAS PARALELAS

Com o sucesso do Bitcoin novas moedas foram criadas, dando opção de escolha aos clientes e mineradores. Este capitulo traz algumas dessas moedas que vieram para complementar e agitar o mercado.

4.1 LITECOIN

O Litecoin [32] é uma ferramenta de comércio que complementa o Bitcoin. Litecoin é uma moeda virtual peer-to-peer que permite pagamentos instantâneos com um custo baixo para qualquer indivíduo na rede. Como o Bitcoin, o Litecoin é uma rede descentralizada e sem autoridades centrais. A matemática mantém a rede segura e favorece os indivíduos a manterem controle de suas próprias finanças. Possui confirmação de transações mais rápidas e melhor eficiência de armazenamento comparado com a moeda líder Bitcoin, também baseada na matemática.

O código é aberto lançando sobre licença MIT [10] isso garante que o usuário consiga executar, modificar e copiar o programa, e distribuí-lo.

A codificação de carteira permite que o usuário possa segurar suas chaves privadas na carteira, e assim, poderá visualizar as transações e o saldo de conta. A preocupação com segurança é alta, para evitar ataques a carteiras de clientes através de vírus e troianos, mas também como um controle de conformidade antes de enviar pagamentos.

Os mineradores têm como recompensa inicial 25 moedas por bloco. É seguida a lógica da moeda líder de mercado, a quantidade de moedas geradas fica reduzida à metade a cada 4 anos (840.000 blocos). Mas a rede Litecoin é projetada para produzir cerca de 4 vezes o número de unidades do que Bitcoin, ou cerca de 84 milhões de Litecoins.

4.2 PEERCOIN

O Peercoin é uma proposta ambiciosa de ser a criptomoeda mais segura e com um custo baixo de energia. Sua proposta é criar moedas a partir de quaisquer dispositivos, ou seja, para criar um Peercoin só é preciso um dispositivo. Isto é possível, pois a criação é feita com base nas Peercoins que o usuário detém em vez da capacidade de processamento disponível.

Também conhecido como PPCoin, é uma criptomoeda *peer-to-peer* que utiliza ambos os sistemas *proof-of-stake and proof-of-work*.

Proof-of-stake foi criada como uma alternativa à *proof-of-work* para lidar com questões inerentes a esta última. Devido ao alto consumo de energia para resolver os blocos de transação no método *proof-of-work*, no sistema *proof-of-stake*, a mineração é proporcional ao número de moeda que o minerador detém, por exemplo, se um mineiro possui 2% de Peercoin disponível teoricamente ele poderá minar apenas 2% dos blocos.

Neste sistema, não há a necessidade de uma classe de mineradores autenticando as transações. Em contrapartida, qualquer dispositivo que tenha uma carteira da moeda ajudaria nas validações dessas transações, isso atestaria as propriedades de cada carteira existente, e teria chances de receber novos lotes de moeda proporcionalmente à quantidade de moeda acumulada na carteira [33].

Não diferente das outras moedas do mercado, ela segue os padrões de licença MIT. A gestão de transações e emissão de dinheiro é realizada coletivamente pela rede.

> Uma das primeiras implementações bem-sucedidas de uma criptografia distribuída, descrita em 1998 por Wei Dai,. Baseando-se na noção de que o dinheiro é qualquer objeto, ou qualquer tipo de registro, aceito como pagamento de bens e serviços e reembolso de dívidas em um determinado país ou contexto socioeconômico, Bitcoin é projetado em torno da ideia de usar criptografia para controlar a criação e transferência de dinheiro, em vez de confiar nas autoridades centrais [34].

PPCoin é a quarta maior moeda virtual minerada por capitalização de mercado, tendo um limite de mercado de US $30 milhões a partir de julho de 2014, segundo dados do próprio site [9]. Ela tem uma característica única, pois a mesma foi projetada para atingir uma taxa de inflação anual de 1%. Essa característica, jun-

tamente com o aumento da eficiência energética, visa permitir uma maior escalabilidade a longo prazo. Ao contrário das suas concorrentes, a Peercoin não tem um limite rígido no número de moedas possíveis.

O protocolo para determinar qual cadeia de blocos concorrente ganha como corrente principal foi trocado para usar a idade da moeda consumida. Aqui cada transação em um bloco contribui sua idade consumida da moeda à contagem do bloco. Isso contrasta com uso do método *proof-of-work* que é a principal cadeia do Bitcoin, enquanto que o trabalho total da cadeia de blocos é usado para determinar a cadeia principal.

A conclusão é que, ao contrário das outras moedas, a *Peercoin* é de mais fácil mineração, porque ela não depende da capacidade de processamento de seu computador. O processo de mineração é feito com base nas *Peercoins* que se detém. Na parte de segurança a Peercoin também mostra grande apelo, segundo os fundadores.

> Cada vez que a sua criação de moedas gerar um bloco, as suas moedas ajudam a controlar a rede. Para que um ataque à rede tivesse sucesso, um utilizador malicioso teria que controlar a maior parte das moedas geradas por criação, o que poderia afetar negativamente o seu próprio investimento". [35]

A Peercoin ainda oferece uma recompensa aos usuários, criar a moeda lhe permite ganhar 1% ao ano. A criação de moedas é feita com base nas moedas existentes nos últimos 30 dias sendo a taxa maximizada após 90 dias, ou seja, ao gerar moedas frequentemente seus ganhos vão se acumulando [9].

5 VISÃO ECONÔMICA E JURÍDICA

Este capítulo tratará de debater as perspectivas de mercado e movimentos de organizações financeiras e jurídicas de alguns países em relação às moedas virtuais.

5.1 VISÃO ECONÔMIA

A Bitcoin surgiu como uma proposta tecnológica para substituir o papel moeda para partes de transações ou até mesmo cogitar ser um dia a moeda de troca mais utilizada. Com o avanço das tecnologias e a crise monetária de 2008, as moedas virtuais ganharam força [36].

Os debates são inevitáveis diante de perspectivas e de incertezas que giram em torno dessa nova tecnologia, quais mudanças trarão para a vida das pessoas e para as relações comercias.

Além dos aspectos econômicos, surgem muitas dúvidas em relação a como uma moeda digital se encaixaria nas legislações atuais e como se daria a sua regulamentação ou não em um cenário em que atualmente a oferta monetária é controlada a partir de um monopólio do Estado.

Os problemas decorridos do monopólio estatal para controle e emissão de moeda podem ser considerados a inflação e o ciclo econômicos causados pela manipulação da base monetária e expansão de crédito viam bancos e venda de títulos de dívida pública para financiamento de gastos públicos [37]. Todos estes problemas não afetam a programação do código da Bitcoin e demais moedas virtuais.

A utilização desse sistema de pagamento e recebimento amplia o mercado monetário, pois tem a capacidade de gerar uma nova oferta monetária na economia, e quanto maior a quantidade de dinheiro em uma economia, menor o poder de compra com cada unidade monetária elevando o risco de abalar o êxito e efetividade da política monetária e sua implementação. Com o desuso da moeda local, em tese poderia levar ao decréscimo da moeda local [38].

A ampla substituição da moeda emitida pelo banco central por moedas virtuais privadas poderia significantemente reduzir o tamanho dos balancetes das autoridades monetárias e, portanto, também sua habilidade em influenciar as taxas de juros de curto prazo, pilar básico das políticas monetárias modernas. Implicando diretamente nas manobras e mudanças de juros pelos bancos centrais pela economia, e o controle sobre moeda e crédito poderia tornar-se menos efetivo [38].

Apesar de apresentar inúmeras vantagens sobre as moedas em circulação, o uso de moedas virtuais também apresenta riscos para a sociedade, como a possibilidade de transacionar sob anonimato, crimes relacionados à lavagem de dinheiro e roubo de dinheiro virtual a partir de um grande desnivelamento de conhecimento entre os usuários da rede.

Os legisladores de todo o mundo precisam primeiramente entender o conceito inovador trazido pela moeda tecnológica, para depois, refletir sobre os benefícios e malefícios que uma regulação traria para a sua relação com a sociedade.

Hoje, autoridades de vários países já têm debatido e como novas moedas virtuais devem ser reguladas, particularmente no que concerne a questões de lavagem de dinheiro e de financiamento ao terrorismo.

Em 2014 na Rússia, autoridades já se posicionaram sobre a ilegalidade de tratar Bitcoins e assemelhados como moeda paralela ao Rublo [39], mas novos estudos e o próprio vice-ministro das finanças, Alexey Moiseev, disse que as autoridades responsáveis já consideram a regulamentação de criptomoedas, afim de combater a sonegação e lavagem de dinheiro no país [40]. Decorre que pessoas físicas ou jurídicas não podem usar sistemas de pagamentos anônimos, em concorrência (ilegal) à moeda doméstica oficial. Nos EUA, as agências de segurança têm se preocupado com possíveis ligações com o terrorismo e tráfico de armas, devido ao uso em ataques de *Dark Web*. Porém, foram duramente criticadas por analistas e apoiadores da moeda, que acusaram as agências de enganar o público [41]. Em Junho de 2015 Nova York se tornou uma das primeiras cidades norte americanas a regulamentar o Bitcoin, chamada de *BitLicense's* em uma ação que de início beneficiou vinte uma empresas [42] .

> *BitLicense's* This Part contains regulations relating to the conduct of business involving Virtual Currency, as defined herein, in accordance with the superintendent’s powers pursuant to the above-stated authority.[[42].p3]

O Banco Central do Brasil esclarece que a utilização das chamadas moedas virtuais e a incidência, sobre elas, de normas aplicáveis aos sistemas financeiros e de pagamentos têm sido temas de debate internacional e de manifestações de autoridades monetárias. Não são emitidas nem garantidas por uma autoridade monetária. Algumas são emitidas e intermediadas por entidades não financeiras e outras não têm sequer uma entidade responsável por sua emissão. Nem garantia de conversão para a moeda oficial, tampouco são garantidos por ativo real de qualquer espécie [43].

> Em nota o Banco Central do Brasil informa que, embora o uso das chamadas moedas virtuais ainda não se tenha mostrado capaz de oferecer riscos ao Sistema Financeiro Nacional, particularmente às transações de pagamentos de varejo (art. 6º, § 4º, da Lei nº 12.685/2013), o Banco Central do Brasil está acompanhando a evolução da utilização de tais instrumentos e as discussões nos foros internacionais sobre a matéria – em especial sobre sua natureza, propriedade e funcionamento –, para fins de adoção de eventuais medidas no âmbito de sua competência legal, se for o caso [43].

Para um país de moeda instável, como foi sempre o caso do Brasil, parece indispensável que a lei reguladora discipline eficientemente e dê o curso legal à moeda. Naturalmente, faz parte do arranjo institucional alguma regra de estabilização monetária, evitando processos inflacionários que, no limite, desencadeiem quadros de hiperinflação e leve à perda da função básica de reserva de valor da moeda. A determinação do valor da moeda virtual é prejudicada, pois não constitui mercado organizado com liquidez e uso mais amplo.

A Receita Federal entende que Bitcoin é um ativo como qualquer outro e, portanto, ganhos decorrentes da variação da sua cotação seriam tributáveis. A moeda virtual também seria declarada no Imposto de Renda, como ouro e dinheiro. A Figura 15 apresenta uma evolução nos preços do Ouro e do Bitcoin nos últimos 3 anos, até que, em Janeiro de 2017, o valor de mercado do Bitcoin alcançou os valores do ouro.

> A Receita Federal, por sua vez, determinou que os contribuintes que possuírem bitcoins deverão prestar as pertinentes informações por meio da declaração do Imposto de Renda, sujeitando-se eventual ganho de capital, se houver, à tributação aplicável. Tal manifestação baseia-se na equiparação dos bitcoins a ativos financeiros para fins tributários. [44]

Figura 15: Comparativo da valorização do Ouro e Bitcoin. [45]

5.2 VISÃO JURÍDICA

Com a ciência jurídica não se tem um cenário diferente. O Direito tem, entre outras funções, o papel de regulamentar, quando necessário, as relações sociais desenvolvidas entre uma sociedade, viabilizando o convívio pacífico e ordeiro.

No entanto, como é sabido, a humanidade está constantemente em processo de evolução, modificando-se quase que diariamente, criando novas relações jurídicas e, por vezes, deixando outras. Criminosos têm se utilizado do espaço virtual para a comercialização de armas, drogas e a propagação de seus negócios ilegais, com a vantagem da utilização de pseudônimos que impossibilitem ou, ao menos tornem extremamente dificultosa a identificação dos usuários ou com criação de contas anônimas.

As vantagens da descentralização do controle emissão sobre a Bitcoin, no entanto, pode ser consideradas também um ponto fraco.

Dependendo da perspectiva de análise, pode-se chegar à conclusão de que a Bitcoin é uma porta aberta para a prática ilícita com o uso desta tecnologia. O crime de lavagem de dinheiro tem tomado grandes proporções com o passar dos anos.

Atividade criminosa consiste no afastamento dos bens/valores financeiros auferidos através do cometimento dos tipos penais.

Em 2011 foi sancionada pela presidenta Dilma Rousseff, a Lei N.º 12.737, que dispõe sobre a tipificação criminal de delitos informáticos. Nesta Lei, conhecida como “Lei Carolina Dieckmann”, tipifica-se a invasão de dispositivo informático que tenha a finalidade de obter, adulterar ou destruir dados sem a autorização do proprietário; a interrupção de serviço telemático; falsificação de cartão de crédito, entre outros. No entanto, ante a grande quantidade de delitos cometidos diariamente através da internet, pode-se dizer que a legislação, neste momento, estaria apenas engatinhando para uma longa caminhada que tem por objetivo principal, garantir a segurança dos usuários que necessitam dos milhares de serviços online e outros mecanismos digitais.

> Convém ainda destacar, que a convenção não obsta aos Estados signatários a criação das medidas legislativas que acharem necessárias para a prevenção e repressão dos cibercrimes, demonstrando ainda, que ao aderir à convenção é possível criar uma “relação de circulação” entre o direito material e processual que permeia a era dos crimes eletrônicos, para que a partir de uma legislação específica seja possível buscar procedimentos eficazes e concretos ao tratamento desses delitos. [46]

Portanto, tem-se como principal problema dos crimes cometidos no meio virtual a falta de uma legislação específica e ampla, capaz de observar a maior parte das condutas, dentro de suas peculiaridades, características e complexidade em que são desenvolvidas.

> Embora, por um lado, as autoridades devam assegurar a solidez do sistema e a proteção dos investidores, por outro devem também procurar evitar a criação de obstáculos ou impedimentos à circulação das moedas virtuais no país, favorecendo o avanço e a disseminação dos códigos criptográficos, que, conforme sugerem especialistas, ainda poderão ser aproveitados para diversas outras finalidades em favor da segurança e eficiência das operações econômicas. [44]

No Brasil, a regulamentação das ações via web encaminham-se especificamente aos crimes praticados neste cenário, uma vez que, segundo a economia estatal, o uso das Bitcoins, especificamente no momento atual, ante a sua restrição

de alcance e pouca aceitação como meio de troca, não é capaz de ameaçar as moedas oficiais como o Real, Euro e Dólar.

6 FUTURO DAS MOEDAS VIRTUAIS

Há inúmeras vantagens que fazem de uma moeda virtual um excelente complemento no meio financeiro. É preciso enxergar o Bitcoin de forma menos exclusiva, mas sim como complementária às formas de dinheiro existentes nos tempos atuais. Não se pode afirmar se esse fenômeno irá perdurar. Se sobreviverá a outros anos, ou décadas, a desafios como colapso em seus valores e migração de usuários para outra moeda iminente. Conforme escreveu a revista Britânica The Economist, sobre o tema Bitcoin, “mas há grande probabilidade de que alguma forma de dinheiro digital deixará uma marca duradoura no ambiente financeiro” [47].

São irrefutáveis as inúmeras vantagens trazidas pelas moedas virtuais. Exemplo disso é a redução substancial nos custos de transações financeiras, além das transferências instantâneas, realizando essas e outras operações sem interferências de terceiros e gerando ganho na privacidade dos clientes.

A cada dia, mais empresas passam aceitar essa forma de transação, principalmente na área de tecnologia e entretenimento e varejo [48] .

> Como resultado, estima-se que mais de 16 milhões de Bitcoins estejam em circulação atualmente, e já se tem notícia até mesmo de redes de empréstimos de Bitcoins, como a BTCjam, plataforma que intermedia empréstimos de Bitcoins entre seus usuários na modalidade P2P e movimentou mais de US$13 milhões até hoje. [44]

Contudo, é provável que o crescimento das moedas virtuais continue por inúmeros fatores, como o crescente uso da Internet e das comunidades virtuais, o aumento do comércio eletrônico de bens, maior privacidade ou anonimato, custos de transação mais baixos que o pagamento tradicional, operações mais rápidas, entre outros. Assim sendo, os formuladores de políticas deveriam considerar a moeda virtual como uma nova categoria, deixando seu desenvolvimento livre.

Mas fica a dúvida, se como moeda, poderá o Bitcoin e outras moedas virtuais, ampliar sua liquidez e sua relevância no sistema financeiro atual. Na teoria de seus idealizadores, como Satoshi Nakamoto criador do Bitcoin, a resposta é sim!

Potencial para tanto as moedas virtuais têm. Pois com a escassez do ouro e de matérias-primas para confecção de papel moeda, além da dificuldade de transportar e estocar, é possível que a adoção do Bitcoin seja fortificada e ampliada, bem como sua liquidez.

7 CONCLUSÕES E TRABALHOS FUTUROS

Este trabalho apresentou detalhes sobre o surgimento e funcionamento das moedas virtuais. A principal moeda virtual da atualidade é o Bitcoin, que foi utilizada como base para desenvolvimento do trabalho. Novas moedas que estão ganhando mercado também foram apresentadas comparativamente ao Bitcoin. Informações acerca dos campos econômico e jurídico relativos a estas novas moedas também foram discutidas, ressaltando os pontos mais interessantes e posicionamentos dos países nos quais as moedas virtuais ganharam mercado. Por fim, uma previsão relativa ao futuro e o que se pode esperar das moedas virtuais nos próximos anos, foi apresentada.

A evolução no sistema de comércios passou pelo sistema de troca de bens e serviços, evoluiu para metais preciosos, chegando aos modelos atuais de papel moeda, até alcançar as transações eletrônicas. Apesar da aparência unicamente digital das novas moedas virtuais, as atuais formas do dinheiro assemelham-se em muito com estas novas moedas. A maior parte da massa monetária no mundo moderno manifesta-se de forma digital.

Embora, em termos práticos, os esquemas de moeda virtual sejam apenas uma evolução, apresentam mudanças substanciais quando comparadas com as moedas e pagamentos reais.

O enorme crescimento no acesso e uso da internet têm como resultado inúmeras inovações técnicas por detrás desses esquemas. O Bitcoin introduziu inovações inimagináveis para mente humana. Como um sistema totalmente descentralizado, compartilhamento em sua malha de rede, único e universal para todos os usuários em qualquer parte do planeta.

Seu sucesso transformou o Bitcoin e outras moedas virtuais em um sistema monetário eficiente e acessível. Países antes opositores passaram a se render a essa nova modalidade de transação vide caso de Rússia.

O movimento de construção e desconstrução a partir das inovações não se restringiria apenas às tecnologias, tal como o advento do computador pessoal que fez com que as máquinas de escrever entrassem em desuso, mas também seria

possível que instituições jurídicas e sociais entrassem neste processo, de modo a exigir uma constante adaptação destas instituições às novas inovações tecnológicas.

Entre as vantagens da Bitcoin para a sociedade está a possibilidade de ampliação de serviços financeiros, a proteção contra inflação e o confisco por parte do governo e os baixos custos. A partir do amadurecimento das moedas virtuais, uma provável regulamentação a fortalecerá ou a enfraquecerá, de acordo com as regras que a sociedade de cada país.

Com um código elegante o Bitcoin, que conta com mecanismos regulatórios próprios, o fator preponderante da descentralização, e a questão da transparência consubstanciada na existência do *Blockchain* parecem aproximá-lo de um exemplo empírico de que a existência e manutenção da confiança, em um sistema monetário, não necessariamente exige a presença de um Estado como garantidor último de uma ordem econômica.

Trabalhos futuros podemos nos aprofundar em novos métodos de trabalho e de tarefas a partir de uma nova lógica de algoritmo que foque ainda mais na segurança evitando ataques, gastos duplos ou fraudes e aumentar oferta de moedas virtuais utilizando números hexadecimal, visto que todas em operação hoje têm um tempo de vida já definido.

8 BIBLIOGRAFIA

1. ULRICH, F. Bitcoin A Moeda Na Era Digital. [S.l.]: [s.n.], 2014. p. 16.
2. CHAUM, D. Security without Identification: bitcoin and Cryptocurrency technologies. [S.l.]: Cursera, 09 Feb 2016. p. 08-09.
3. CHAUM, D. Digicash Press Release: World's first electronic cash payment over computer networks, 1994. Disponivel em: <https://w2.eff.org/Privacy/Digital_money/?f=digicash.announce.txt>. Acesso em: 07 Set 2016.
4. DAI, W. B-money, 1998. Disponivel em: <http://www.weidai.com/bmoney.txt.>. Acesso em: 07 Set 2016.
5. SZABO, N. Bit Gold, 2005. Disponivel em: <unenumerated.blogspot.com.br/2005/12/bit-gold.html>. Acesso em: 03 Out 2016.
6. HUGHES, E. A Cypherpunk`s Manifesto. Disponivel em: <w2.eff.org/Privacy/Crypto/Crypto_misc/cypherpunk.manifesto>. Acesso em: 09 Set 2016.
7. NAKAMOTO, S. Bitcoin: A Peer-to-Peer Eletronic Cash System, 2008. Disponivel em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 19 Mai 2017.
8. LITECOIN, E. D. D. Disponivel em: <https://litecoin.info/Main_page>. Acesso em: 27 Abri 2017.
9. PEERCOIN, E. D. D. Disponivel em: <https://peercoin.net/assets/paper/peercoin-paper.pdf>. Acesso em: 28 Abr 2017.
10. LAWRENCE, R. Open Source Licensing. [S.l.]: [s.n.], p. 85.
11. GITHUB, E. D. D. D. Disponivel em: <https://github.com/wrapperband/FeathercoinWalletGuide>. Acesso em: 2 Abr 2017.
12. BRADBURY, D. **coindesk**. Disponivel em: <http://www.coindesk.com/feathercoin-hit-by-massive-attack/>. Acesso em: 28 Nov 2016.
13. LULLEZ, R. Disponivel em: <http://www.negociecoins.com.br/lojas-aceitam-bitcoins>. Acesso em: 10 Set 2016.
14. JASEN. Disponivel em: <http://guiadobitcoin.com.br/10-motivos-para-investir-em-bitcoin-em-2016/>. Acesso em: 10 Set 2016.
15. TELLES, R. Disponivel em: <http://www.rtell.com.br/Pcp/paginas/redes/dredes44.htm>.
16. ANDERSON, M. **Tor**. Disponivel em: <www.torproject.org/>. Acesso em: 27 Abr 2017.
17. EICHEMBERGER, R. **sinapse**. Disponivel em: <https://conectarinteragircomunicar.wordpress.com/>. Acesso em: 05 Junho 2017.
18. ADAMS, P., 2013. Disponivel em: <http://chimera.labs.oreilly.com/books/1234000001802/ch06.html>.

Acesso em: 03 Junho 2017.

19. ULRICH, F. Bitcoin: a moeda na era digital. São Paulo: Instituto Ludwig Von Mises, 2014. p. 45.
20. DANN. Disponivel em: <http://dann.com.br/bitcoin-guia-definitivo-parte-13-ideologia-e-estrutura-da-rede/>. Acesso em: 3 Junho 2017.
21. PROOF, E. D. D. **Proof**. Disponivel em: <http://www.proof.com.br/blog/blockchain/>. Acesso em: 05 Junho 2017.
22. SMITH, P. **Blockchain**. Disponivel em: <https://blockchain.info/pt>. Acesso em: 05 junho 2017.
23. ULRICH, F. Bitcoin: Moeda da era Digital. [S.l.]: [s.n.], p. 18.
24. CARY, N. Disponivel em: <https://blockchain.info/stats>. Acesso em: 05 Junho 2017.
25. ROHR, A. **G1**, 2014. Disponivel em: <g1.globo.com/tecnologia/noticia/2014/02/entenda-como-e-uma-transacao-com-moeda-virtual-bitcoin.html>. Acesso em: 09 Set 2016.
26. GOMES, H. **G1**, 2016. Disponivel em: <http://g1.globo.com/tecnologia/noticia/2016/07/emissao-de-bitcoins-cai-pela-metade-pela-2-vez-na-historia-da-moeda.html>. Acesso em: 26 Maio 2017.
27. DOUBLERBTC, E. D. D. Disponivel em: <https://doublerbtc.us>. Acesso em: 05 Mai 2017.
28. SMITH, P. Disponivel em: <https://blockchain.info/pt/charts>. Acesso em: 22 Mai 2017.
29. BITVALOR, E. D. D. **Bitvalor**. Disponivel em: <http://bitvalor.com/files/Relatorio_Mercado_Brasileiro_Bitcoins_Dezembro2016.pdf>. Acesso em: 22 Maio 2017.
30. ROTH, E. **Investing**. Disponivel em: <https://br.investing.com/currencies/btc-usd>. Acesso em: 05 Junho 2017.
31. TOLOTTI, R. **Infomoney**. Disponivel em: <http://www.infomoney.com.br/welcome?returnurl=http%3A//www.infomoney.com.br/mercados/bitcoin/noticia/5925969/bitcoin-sobe-200-anos-melhor-ativo-entre-principais-aplicacoes-brasil>. Acesso em: 05 Junho 2017.
32. PAGE, L. Disponivel em: <https://litecoin.org/pt/>. Acesso em: 22 Maio 2017.
33. SOPHI. Proof of Stake FAQ, 2017. Disponivel em: <https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ>. Acesso em: 26 Maio 2017.
34. BRASIL, E. D. D. B. Bitcoin Brasil, 2017. Disponivel em: <https://bitcoinbrasil.wiki/bitcoin/>. Acesso em: 26 Abril 2017.
35. PEERCOIN, E. D. D. **Peercoin**. Disponivel em: <https://peercoin.net/minting.php?locale=pt_BR>. Acesso em: 26 Abril 2017.
36. NICOLAIS. Disponivel em: <https://www.extension.harvard.edu/inside-extension/how-use-real-estate-trends-predict-next-housing-bubble>. Acesso em: 22 Maio 2017.

37. DORNELAS, A. Notícia De Economia e Finanças Volume 2. [S.l.]: [s.n.], 2013. p. 205-206.
38. LAAN, C. V. D. Disponivel em: <https://www.brasil-economia-governo.org.br/2015/01/20/deve-o-governo-regular-bitcoins-riscos-e-limites-no-uso-de-moedas-virtuais-privadas/>. Acesso em: 23 Maio 2017.
39. DILLET, R. Disponivel em: <https://techcrunch.com/2014/02/07/russia-bans-bitcoin/>. Acesso em: 24 Maio 2017.
40. JASEN, 2017. Disponivel em: <https://guiadobitcoin.com.br/russia-planeja-oficializar-e-regulamentar-o-bitcoin-em-2018-para-lutar-contra-a-lavagem-de-dinheiro/>. Acesso em: 24 Maio 2017.
41. CHRYS, 2017. Disponivel em: <http://www.btcsoul.com/2017/03/09/wall-street-journal-bitcoin-dinheiro-terrorismo-exagero/>. Acesso em: 24 Maio 2017.
42. YORK, D. O. F. S. N., 2015. Disponivel em: <http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf>. Acesso em: 24 Maio 2017.
43. MENDES, A. L., 2014. Disponivel em: <https://www3.bcb.gov.br/normativo/detalharNormativo.do?method=detalharNormativo&N=114009277>. Acesso em: 15 Fev 2017.
44. SOUZA, A. G. N. E. M. M. D. Estadão, 2017. Disponivel em: <http://politica.estadao.com.br/blogs/fausto-macedo/o-avanco-das-moedas-virtuais/>. Acesso em: 24 Maio 2017.
45. PINTO, P. **pplware**. Disponivel em: <https://pplware.sapo.pt/informacao/moeda-virtual-bitcoin-ja-vale-mais-que-ouro/>. Acesso em: 05 Junho 2017.
46. SILVA, A. K. C. D. E-gov, 2015. Disponivel em: <http://www.egov.ufsc.br/portal/conteudo/o-estudo-comparado-dos-crimes-cibern%C3%A9ticos-uma-abordagem-instrumentalista-constitucional>. Acesso em: 24 Maio 2017.
47. LUCAS, E. The Economist, 2013. Disponivel em: <http://www.economist.com/news/finance-and-economics/21576149-even-if-it-crashes-bitcoin-may-make-dent-financial-world-mining-digital>. Acesso em: 25 Maio 2017.
48. LULLEZ, R. Negociecoins. Disponivel em: <https://www.negociecoins.com.br/lojas-aceitam-bitcoins>. Acesso em: 25 Maio 2017.

Unsupported source type (DocumentFrom InternetSite) for source 17Ab.

Unsupported source type (DocumentFromInternetSite) for source 17Ab.

50. P2P, O. C. M. B. D. **UFRJ**. Disponivel em: <https://www.gta.ufrj.br/grad/04_1/p2p/index.html#Topic21>.