INTERFACE TECNOLÓGICA

CRIPTOMOEDA VIRTUAL: o impacto do bitcoin no mundo

VIRTUAL CRYPTOCURRENCY: the impact of bitcoin in the world

Leonardo Poletto Donato – leo.donato007@gmail.com
Brazelino Bertolete Neto – brazelino.neto@fatectq.edu.br
Faculdade de Tecnologia de Taquaritinga (FATEC) – SP – Brasil

RESUMO

Ao longo dos anos, obtiveram-se vários avanços em todas as áreas da tecnologia, tais como mensagens eletrônicas, redes sociais, aprimoramento da capacidade visual para uso medicinal, internet das coisas e afins. Agora chegou o momento de o dinheiro ser digital também, mas não pelo fato que já conhecemos, como *internet banking*, mas por uma nova metodologia, da moeda não ter seu estado físico, somente digital, ser de pessoa para pessoa, além de ter uma proposta de segurança maior por ser criptografada. Este artigo tem o intuito de apresentar o que é a criptomoeda virtual, focado em *Bitcoin*, o surgimento, propósito e quais estão sendo seus impactos mundiais, já que é uma nova maneira de se ter e guardar dinheiro. O objetivo é de informar sobre o porquê de ela estar muito valorizada atualmente, seus benefícios e malefícios na sociedade, o porquê de ela se tornar o dinheiro do futuro e, assim, mostrar sua inovadora funcionalidade.

Palavras-chave: Criptomoeda. *Bitcoin*. Economia. Moeda virtual. Dinheiro.

ABSTRACT

Over the years, several advances have been made in all areas of technology such as electronic messaging, social networking, visual enhancement for medical use, internet of things and others. Now the time has come for money to be digital too, but not in a way that we already know it, internet banking, for instance, but through a new methodology, of the currency not having its physical state, only digital, being person to person, besides having a higher security proposal for being encrypted. This article aims at presenting what the virtual cryptocurrency is, focused on Bitcoin, the emergence, purpose and what its global impacts are, since it is a new way of having and saving money. The objective is to inform why it is highly valued today, its pros and cons in society, why it tends to become the money of the future and, so, showing its innovative functionality.

Keywords: Cryptocurrency. *Bitcoin*. Economy. Virtual currency. Money.

1 INTRODUÇÃO

Este artigo tem a finalidade de apresentar o conceito de criptomoeda virtual, com foco na moeda *Bitcoin*, que está em uso crescente desde sua criação.

As pessoas tendem a criar algumas resistências à transição do que é real para o digital. Este artigo expõe que, com um certo conhecimento, o conceito de moeda virtual pode ser algo promissor no futuro, pois já vem evoluindo nos dias atuais.

Pagliery (2014) diz que a ideia do *Bitcoin* já vem causando impacto, porque representa uma maneira totalmente nova de pensar sobre o dinheiro, e tem o potencial de transformar algo que é um elemento fundamental da história humana.

Esta pesquisa tem o objetivo de mostrar o que é *bitcoin*, como foi o seu surgimento e alguns de seus propósitos, expondo, ainda, como é o funcionamento de seu sistema, tais como o método de transação, sua criptografia e o porquê de ser seguro para o uso. O sistema *Bitcoin* lista todas as transações, sendo um sistema que mantém o anonimato de seus usuários. Também conta com vários usuários chamados de mineradores, que recebem novas moedas pelos trabalhos realizados ao quebrarem a criptografia proposta, validando, assim, as transações efetuadas e usando sua capacidade computacional como forma de trabalho. E serão expostas, ainda, algumas falhas de segurança e problemas causados pela moeda, e, por fim, serão apresentadas as perspectivas econômicas, o seu crescimento e posicionamento no mercado.

Com o avanço da tecnologia em todas as áreas e quesitos, há mais um avanço, dessa vez na área econômica, na qual o dinheiro existirá apenas digitalmente.

2 REFERENCIAL TEÓRICO

> O *Bitcoin* é uma forma de dinheiro, assim como o real, o dólar ou o euro, com a diferença de ser puramente digital e não ser emitido por nenhum governo. O seu valor é determinado livremente pelos indivíduos no mercado. Para transações online, é a forma ideal de pagamento, pois é rápido, barato e seguro. Você lembra como a internet e o e-mail revolucionaram a comunicação? Antes, para enviar uma mensagem a uma pessoa do outro lado da Terra, era necessário fazer isso pelos correios. Nada mais antiquado. Você dependia de um intermediário para, fisicamente, entregar uma mensagem. (ULRICH, 2014, p. 16).

De acordo com Ulrich (2014), a invenção do *Bitcoin* é revolucionária porque, pela primeira vez, o problema do gasto duplo pode ser resolvido sem a necessidade de um terceiro. O *Bitcoin* distribui o imprescindível registro histórico a todos os usuários do sistema via uma rede *peer-to-peer*. Todas as transações que ocorrem na economia *Bitcoin* são registradas em uma espécie de livro-razão público distribuído, chamado de *Blockchain*.

Além disso, o que possibilitou sua criação foi uma situação econômica e um sistema financeiro instável com um elevado nível de intervenção estatal, o que gerou a oportunidade

para o lançamento dessa nova ideia de dinheiro. O colapso financeiro em 2008, uma crise mundial vinda dos Estados Unidos da América, possibilitou a entrada do *Bitcoin*, com a internet já funcionando melhor e a população mais conectada também.

O intuito, segundo Ulrich (2014), era de fazer um sistema de trocas monetárias mais seguro com a implementação de um banco de dados para controle, sendo ele *peer-to-peer*, as moedas com criptografia, de código aberto e totalmente descentralizada. O cidadão, nos dias atuais, não tem controle algum sobre seu próprio dinheiro, ficando dependente do governo, principalmente em tempos de crises financeiras.

"Este é o paradigma do atual milênio: crescente perda de privacidade financeira; autoridades monetárias centralizadas e opressivas que abusam do dinheiro, isentas de qualquer responsabilidade; e bancos cúmplices e coadjuvantes no desvario monetário" (ULRICH, 2014, p. 37).

Por anos, cientistas da computação tentaram desenvolver equações matemáticas e técnicas para um sistema de pagamento que funcionasse integralmente na internet. Então Satoshi Nakamoto criou uma combinação de várias técnicas e conhecimentos da área para, assim, desenvolver uma arquitetura de rede a permitir que equações matemáticas e a criptografia servissem aos usuários.

Nakamoto (2009), em sua publicação na *P2P foundation*, explica a motivação para a criação da criptomoeda, dizendo que a raiz do problema com a moeda tradicional é que ela precisa de muita confiabilidade em terceiros, como agências bancárias, para funcionar. Precisa-se de confiança em um banco central para que não se desvalorize a moeda. Mas a história das moedas respaldadas por governos, e não pela paridade com o ouro (moedas *fiat*), mostra inúmeras violações de confiança. Os bancos devem ser confiáveis para manterem o nosso dinheiro e transferi-lo eletronicamente, mas o emprestam em bolhas de crédito com apenas uma fração de reserva. Com moedas criptografadas, sem a necessidade de confiar em um intermediário ou em terceiros, o dinheiro se torna seguro, e as transações, sem esforço.

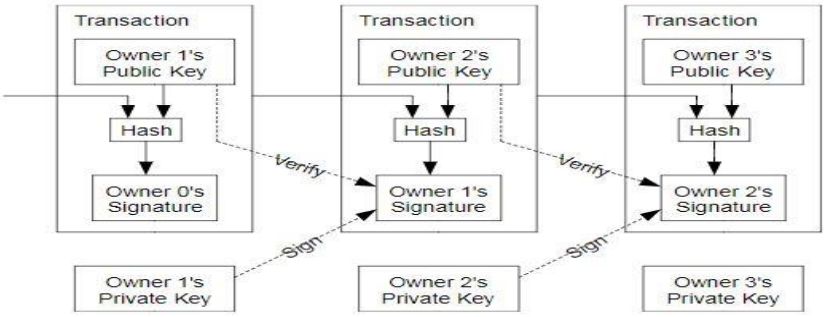
3 PROCEDIMENTOS METODOLÓGICOS

Nessa pesquisa, foram utilizados livros especializados no assunto, artigos jornalísticos e o documento teórico do criador da moeda.

3.1 Funcionamento e Criptografia

A funcionalidade da moeda, em termos transacionais, dá-se basicamente quando o proprietário decide transferir o *bitcoin* para alguém, assinando digitalmente sua transação juntamente com o sistema de *hash* (algoritmo de dispersão que cifra os dados para manter sua integridade), colocando, ao final, a chave pública do beneficiário. Abaixo, há a representação visual do funcionamento das transações:

Figura 1 – Representação do método transacional



Fonte: Nakamoto, 2008, p. 2.

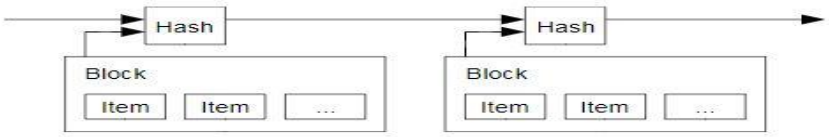
Para começar a usufruir dessas funcionalidades, de acordo com Grinberg (2012 *apud* BARBOSA *et al*., 2016, p. 43), os indivíduos que desejam ter seu arquivo *Bitcoin* e transacionar no sistema *Bitcoin* podem fazer o *download* de um programa que detenha o protocolo do sistema. O programa pode operar em diferentes dispositivos, como o computador ou celular, realizando operações diretas com o arquivo *Bitcoin* por meio destes mecanismos. Outra forma de transação é a criação de uma conta em um site que exerça a função de comercialização de moeda, um mercado de *bitcoin*. Este site funciona de forma muito parecida com uma corretora de bolsa de valores, encaminhando ordens de compra e venda de ações de empresas de capital aberto, em que o usuário, além de administrar, pode comprar e vender *bitcoins*.

Segundo Finardi (2017), as carteiras (*wallets*) são os principais canais de comunicação do sistema *Bitcoin*, são os arquivos que comprovam quantos *bitcoins* o usuário detém. A carteira é baseada no conceito de chave pública/privada, em que a chave privada fica armazenada localmente (como uma senha bancária), e a chave pública é o endereço registrado no *Blockchain*.

Nakamoto (2008) diz que o problema é o fato de o beneficiário não poder verificar se o proprietário gastou duas vezes a mesma moeda. Assim, para que não precisassem de um sistema

central para controle, os usuários deveriam estar cientes e informados de todas as transações realizadas, criando-se, dessa forma, uma solução com um servidor *timestamp*, que trabalharia com blocos de itens para serem marcados, publicando o *hash* e provando que os dados estavam presentes no momento informado.

Figura 2 – Representação do servidor timestamp

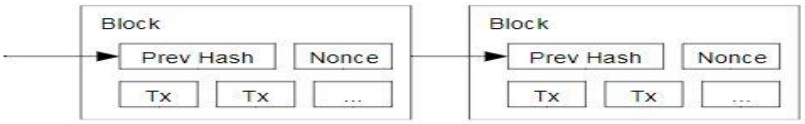


Fonte: Nakamoto, 2008, p. 2.

De acordo com Nakamoto (2008), para a implementação do servidor, foi necessária a criação do sistema *proof-of-work* (algoritmo que define a dificuldade da mineração da criptomoeda), que funciona, de forma resumida, quando um valor passa pelo sistema *hash* ele tem seu caminho começado pelo número de *bits* igual a zero. Após, é adicionado um *nonce* criptográfico (um número arbitrário que só pode ser usado uma vez) que influencia o resultado do *hashing*, e, é testado até que seja encontrado o resultado em *bits* esperado.

Quando o usuário realiza alguma tarefa, é gerado um *token*, uma espécie de prova de trabalho, criando uma ordem criptográfica ao usuário. Esse *token* contém a dificuldade e a assinatura do usuário que o gerou, é uma confirmação do valor do trabalho feito.

Figura 3 – Representação do sistema proof-of-work



Fonte: Nakamoto, 2008, p. 3.

O modelo do sistema *Bitcoin* utiliza o método de criptografia assimétrica com uma função criptográfica *hash*, que irá exigir de seus usuários da rede um *proof-of-work* (protocolo utilizado para prevenção de ataques cibernéticos).

Para conseguir levar o sistema a se tornar público, Nakamoto implementou o método assimétrico, que intercala chaves privadas e públicas. De acordo com Machado (2010 *apud* BARBOSA *et al*., 2016, p. 53), a chave privada irá funcionar como se fosse a identificação de seu titular, e a pública serve de parâmetro geral para troca de comunicações. Portanto, utiliza-

se esse método, pois terá a necessidade de uma chave privada para decifrar a codificação criada por uma pública, sendo semelhante o procedimento para o caso que for da pública para a privada.

Passado, a "assinatura digital", como é conhecido esse processo, inicia-se a função criptográfica *hash*, que é chamada de "impressão digital" do *bitcoin*. Segundo Champagne (2014 *apud* BARBOSA *et al*., 2016, p. 58), a função criptográfica *hash* é um complexo algoritmo matemático que transforma, por exemplo, uma sequência numérica com propriedades matemáticas próprias. Aos olhos de quem não tem conhecimento, parecerá algo totalmente aleatório. O resultado dessa função é chamado de *digest*, a cada envio realizado o *digest* será totalmente diferente.

A função *hash*, utilizada pelo *Bitcoin*, é a *SHA-256*, que tem como base a *SHA-2*. Essa função é implementada para aplicações de segurança e protocolos, nesse caso, é usada para verificar transações e calcular o *proof-of-work*.

A seguir, mostra-se um algoritmo, exemplificando essa função para criptografar senhas:

Figura 4 – Algoritmo SHA-2 em JAVA

```
package teste;

  import java.io.UnsupportedEncodingException;
  import java.security.MessageDigest;
  import java.security.NoSuchAlgorithmException;

  public class TesteAlgoritmo {

          public static void main(String args []) throws NoSuchAlgorithmException, UnsupportedEncodingException {

                    String senha = "admin";

                    MessageDigest algorithm = MessageDigest.getInstance("SHA-256");
                    byte messageDigest[] = algorithm.digest(senha.getBytes("UTF-8"));

                    StringBuilder hexString = new StringBuilder();
                    for (byte b : messageDigest) {
                      hexString.append(String.format("%02X", 0xFF & b));
                    }
                    String senhahex = hexString.toString();

                    System.out.println(senhahex);
          }

  }
```

Fonte: Medeiros, 2017.

3.2 *Blockchain* e Mineradores

> O *Blockchain* é o livro-razão público de todas as transações do *Bitcoin* que foram executadas. Está em constante crescimento à medida que os mineradores adicionam novos blocos (a cada 10 minutos) para gravar as mais recentes transações. Os blocos são adicionados no *Blockchain* em uma ordem linear e cronológica. Cada nó completo (isto é, cada computador conectado à rede *Bitcoin* usando um cliente que executa a tarefa de validação e retransmissão de transações) possui uma cópia do *Blockchain*, que é baixado automaticamente quando um minerador se junta à rede *Bitcoin*. O *Blockchain* possui informações completas sobre endereços e saldos do bloco gênese (as primeiras transações já executadas) para o bloco recentemente completado. O *Blockchain* como um livro-razão público significa que é fácil consultar

> qualquer explorador de blocos (como o https://blockchain.info/) para transações associadas a um endereço *Bitcoin* específico, por exemplo, você pode procurar seu próprio endereço *wallet* (carteira) para ver a transação na qual você recebeu seu primeiro *Bitcoin*. (SWAN, 2015, p. X).

"O *Blockchain* é, portanto, um registro em ordem cronológica de todas as transações que ocorreram na rede e foram compiladas e validadas pelos mineradores. É público, único, replicado e compartilhado pelos participantes do sistema. " (ULRICH, 2017).

> Uma operação envolvendo *Bitcoins* precisa de pelo menos três partes: um usuário que tenha emitido uma ordem de transferência de um bitcoin, um usuário de destino do bitcoin enviado e um conjunto de usuários, mineradores (*miners*) que irão verificar e validar a operação realizada entre as duas partes. (BARBOSA *et al*., 2016, p. 49).

De acordo com Moser (2013 *apud* BARBOSA *et al*., 2016, p. 50), da mesma forma que, para a criação de uma carteira de *bitcoins*, não é necessária a identificação do usuário titular para a formação de blocos de informação, os mineradores também não precisarão se identificar, bastando o pseudônimo estipulado no momento da criação da carteira. É nesse sentido que o sistema *Bitcoin* é apontado como um sistema anônimo, pois a identidade de seus usuários não é um pressuposto de seu funcionamento, apenas a publicidade das transações é.

Como foi abordado, a arquitetura do sistema *Bitcoin* é descentralizada. Portanto, o sistema é mantido pela cooperação dos demais membros de sua rede, chamados de mineradores (*miners*).

De acordo com Swan (2015), os mineradores são os nós responsáveis por operarem o sistema *Bitcoin*, após verificada a validade das transações, atualizando o *Blockchain*. Eles competem entre si para a formação de blocos de informação e sua inclusão. Apesar de estarem trabalhando simultaneamente para a construção de um novo bloco de informações, apenas um deles será selecionado para incluir o seu bloco no *Blockchain*.

Quando algum usuário realiza uma transação, a operação será validada por mineradores, que recebem a "comissão pelo trabalho", equivalente a uma fração da transação.

Segundo Swan (2015), os mineradores têm de resolver uma complexa equação matemática que irá demandar tempo de processamento computacional. Essa solução tem uma sequência numérica única. Todos os mineradores concorrem entre si para incluírem o seu bloco de informações, mas só aquele que encontrar a solução poderá colocar o seu bloco, publicando as transações que ele validou. Estará apto a receber a comissão pela validação e inserção no

bloco, chamada de *block reward*, que é a premiação pela inserção no bloco de informações no *Blockchain* e o processo de criação de novos *bitcoins*.

"O protocolo do sistema *Bitcoin* é que regula o grau de dificuldade para a resolução destas equações matemáticas para a formação dos blocos de informação, equilibrando a dificuldade de modo que, a cada 10 minutos, um bloco novo seja criado. " (CHAMPAGNE 2014 *apud* BARBOSA *et al*., 2016, p. 57).

Tabela 1 – Tempo estimado para um dado usuário gerar bitcoins baseado na capacidade computacional

Capacidade computacional	Tempo médio necessário	Geração por dia (BTC)
5 MHashes/s	43 anos e 45 dias	0,0032
20 MHashes/s	10 anos e 285 dias	0,0127
100 MHashes/s	2 anos e 57 dias	0,0635
500 MHashes/s	157 dias e 9 horas	0,3177
2.000 MHashes/s	39 dias e 8 horas	1,2706
10.000 MHashes/s	7 dias e 20 horas	6,3532
50.000 MHashes/s	1 dia e 13 horas	31,7661

Fonte: Barbosa *et al*., 2016, p. 46.

Como já foi exposto, cada minerador tem o objetivo de resolver equações complexas para incluir seu bloco no *Blockchain*, sendo recompensado por *bitcoins* (*block reward*) e pelas transações que ele validou. Essa equação é conhecida como *proof-of-work* (prova de trabalho).

De acordo com Barbosa *et al*. (2016), o *proof-of-work* será resultado da resolução da equação matemática proposta pelo sistema *Bitcoin* para validar a sequência numérica gerada pela função *hash*. O resultado disso tudo será uma nova sequência numérica específica que também está na base hexadecimal e com dezesseis zeros. Esses zeros são uma maneira de o protocolo *Bitcoin* reconhecer que se trata de um *proof-of-work*.

3.3 Problemas e Falhas de Segurança

Existem algumas situações que ocasionam problemas no sistema *Bitcoin*. Segundo Barbosa *et al*. (2016), existe um problema que envolve um gasto redundante para carteiras diferentes, que pode aparecer depois de um resultado *proof-of-work* de dois mineradores e,

assim, criar, temporariamente, duas versões no *Blockchain*, colocando em risco a credibilidade, pois criará operações sem registro. Outro problema é, de acordo com Barbosa *et al*. (2016), qualquer que seja sua ação sobre seus arquivos, seja por ataque de hackers ou por uma exclusão acidental, as moedas serão perdidas e nunca mais poderão ser recuperadas.

Tagiaroli (2014) diz que usuários maliciosos podem utilizar programas que impedem a vítima de acessar o próprio conteúdo e só a liberam diante de um pagamento. Na maioria das vezes, pedem em *bitcoin*. Também ocorre, com frequência, o uso de *botnets* para conseguirem as moedas. Os *cybercriminosos* instalam softwares maliciosos em vários computadores sem consentimento e usam a capacidade computacional remotamente para minerar *bitcoins*. Também há o comércio ilícito, acessado somente pelo navegador *Tor*, que oferece drogas e serviços de assassinatos, todos pagos em *bitcoins*.

4 RESULTADOS E DISCUSSÕES

Para Ulrich (2014 *apud* BARBOSA *et al*., 2016, p. 105), o *Bitcoin* é uma forma de moeda superior às demais, pois incorpora a escassez do ouro atrelada à transportabilidade e divisibilidade dos substitutos do dinheiro de forma instantânea, prescindindo de inúmeros terceiros fiduciários, como bancos, eliminando-se, assim, o risco da contraparte.

Quadro 1 – Comparação das características das moedas

Atributos	**Ouro**	**Papel-moeda**	***Bitcoin***
1. Durabilidade	Alta	Baixa	Perfeita
2. Divisibilidade	Média	Alta	Perfeita
3. Maleabilidade	Alta	Alta	Incorpórea
4. Homogeneidade	Média	Alta	Perfeita
5. Oferta (Escassez)	Limitada pela natureza	Ilimitada e controlada politicamente	Limitada matematicamente
6. Dependência de terceiros fiduciários	Alta	Alta	Baixa ou quase nula

Fonte: Barbosa *et al*., 2016, p. 105.

Leal (2017) aponta que a moeda está em alta desde a implementação do novo software (*SegWit*), que tem como objetivo tornar as transações de *bitcoins* mais leves, o que aumentaria a quantidade de transações que poderiam ser incluídas em cada bloco. Em 14/08/2017, já estava valendo US$ 4.263 (cerca de R$ 13.500) e, de acordo com a Redação do Olhar Digital (2017), essa cotação passou a valer mais que todo o real em circulação no Brasil. O total em reais é de R$ 218,69 bilhões, ao passo que o *Bitcoin* já tinha chegado a R$ 220,8 bilhões.

Américo (2017) apurou, em sua reportagem, que a Câmara dos Deputados criou uma comissão para discutir a regulamentação de moedas virtuais no Brasil e analisar a entrada do *bitcoin* nas modalidades de pagamento reguladas pelo Banco Central.

A declaração do imposto de renda, como "outros bens e direitos", já pode ser realizada, mas uma possível regulamentação e controle do Banco Central iria excluir umas de suas principais características, que é a independência de terceiros para funcionarem, como aponta Kleina (2017) em sua reportagem.

Em contrapartida, nos Estados Unidos, uma reportagem de Américo (2016) mencionou que uma juíza federal qualificou o *bitcoin* como dinheiro real em uma decisão de um processo criminal de ataque de *hackers* contra o banco JP Morgan e outras empresas.

O *Bitcoin* já está adentrando no mercado atual também. Os serviços financeiros do Japão já estavam considerando reconhecê-lo como representante real de dinheiro a fim de melhorar a proteção de seus consumidores, e, com isso, Sumares (2016) fez uma reportagem informando que uma empresa japonesa de serviços *bitcoin*, *Coincheck*, em parceria com a empresa que opera várias usinas de eletricidade no Japão, lançou um recurso que habilita a seus usuários a opção de pagarem as contas de luz. Também há um desconto para alguns usuários mais frequentes. Além disso, o próximo passo será firmar mais parcerias que permitirão aos usuários conseguirem pagar contas de gás, água e de internet móvel.

5 CONSIDERAÇÕES FINAIS

Pode-se constatar, ao final desse artigo, que o *bitcoin* tem potencial para revolucionar a economia mundial, por mais que haja alguns problemas a serem solucionados.

Ainda que demore o entendimento sobre o funcionamento e as dificuldades que isso pode causar para a sociedade se adequar a esse novo método monetário, as perspectivas são muito boas e concretas, uma vez que tudo em nossa vida cotidiana migra para ser algo digital,

assim como migramos do telefone fixo para o smartphone, da loja para o e-commerce, do contato pessoal ao contato via internet e, em todos esses exemplos, a sociedade acatou e se adequou.

Portanto, é preciso atentar para uma possível revolução econômica, como já vem acontecendo, mas nem todos têm acesso e conhecimento de como obterem e utilizarem a moeda, sendo esse fato um obstáculo à usabilidade do *bitcoin* para certa parte da população mundial.

REFERÊNCIAS

AMÉRICO, Juliana. **Bitcoin é dinheiro real, decide juíza em caso de ataque de hackers**. Disponível em: <https://olhardigital.com.br/pro/noticia/bitcoin-e-dinheiro-real-decide-juiza-em-caso-de-ataque-de-hackers/62310>. Acesso em: 21 ago. 2017.

AMÉRICO, Juliana. **Câmara cria comissão para discutir regularização da bitcoin**. Disponível em: <https://olhardigital.com.br/noticia/camara-cria-comissao-para-discutir-regularizacao-da-bitcoin/68678>. Acesso em: 21 ago. 2017.

BARBOSA, Tatiana Casseb Bahr de Miranda et al. **A revolução das moedas digitais:** bitcoins e altcoins. São Paulo: Revoar, 2016. 359 p.

CABRAL, Rafael. **Tudo sobre o Bitcoin: a história, os usos e a política por trás da moeda forte digital**. Disponível em: <http://gizmodo.uol.com.br/tudo-sobre-o-bitcoin/>. Acesso em: 08 jun. 2017.

FINARDI, Israel. **Como criar uma carteira Bitcoin?**. Disponível em: <https://www.criptomoedasfacil.com/como-criar-uma-carteira-bitcoin/>. Acesso em: 30 ago. 2017.

KLEINA, Nilton. **Deputados brasileiros vão discutir regulamentação e imposto para bitcoins**. Disponível em: <https://www.tecmundo.com.br/bitcoin/117285-deputados-brasileiros-discutir-regulamentacao-imposto-bitcoins.htm>. Acesso em: 21 ago. 2017.

LEAL, Milton. **Proposta de melhoria do bitcoin recebe sinal verde e preço dispara**. Disponível em: <https://www.criptomoedasfacil.com/proposta-de-melhoria-do-bitcoin-recebe-sinal-verde-e-preco-dispara/>. Acesso em: 17 ago. 2017.

MEDEIROS, Higor. **Como funciona a Criptografia Hash em Java**. Disponível em: <http://www.devmedia.com.br/como-funciona-a-criptografia-hash-em-java/31139>. Acesso em: 08 ago. 2017.

NAKAMOTO, Satoshi. **Bitcoin**: A Peer-to-Peer Electronic Cash System. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 02 ago. 2017.

NAKAMOTO, Satoshi. **Bitcoin open source implementation of P2P currency**. 11/02/2009. Disponível em: <http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?xg_source=activity>. Acesso em: 09 jun. 2017.

OLHAR DIGITAL, Redação. **Ainda em crescimento, bitcoin já vale mais do que todo o real em circulação**. Disponível em: <https://olhardigital.com.br/pro/noticia/ainda-em-crescimento-bitcoin-ja-vale-mais-do-que-todo-o-real-em-circulacao/70394>. Acesso em: 17 ago. 2017.

PAGLIERY, Jose. **Bitcoin and the future of money**. Chicago: Triumph Books, 2014. 257 p.

SCHIAVON, Guto. **Mineração de Bitcoin:** Entenda como funciona. Disponível em: <https://foxbit.com.br/blog/mineracao-de-bitcoin-entenda-como-funciona/>. Acesso em: 14 ago. 2017.

SUMARES, Gustavo. **Japão aceitará pagamento de contas de luz em bitcoin**. Disponível em: <https://olhardigital.com.br/pro/noticia/japao-aceitara-pagamento-de-contas-de-luz-em-bitcoin/62483>. Acesso em: 08 ago. 2017.

SWAN, Melanie. **Blockchain**: Blueprint for a New Economy. California: O'Reilly Media, Inc., 2015. 149 p.

TAGIAROLI, Guilherme. **Com promessa de anonimato, bitcoin ganha espaço em atividades criminosas**. Disponível em: <https://tecnologia.uol.com.br/noticias/redacao/2014/03/18/com-promessa-de-anonimato-bitcoin-ganha-espaco-em-atividades-criminosas.htm>. Acesso em: 28 ago. 2017.

ULRICH, Fernando. **Bitcoin: a moeda na era digital**. São Paulo: Instituto Ludwig von Mises Brasil, 2014. 106 p.

ULRICH, Fernando. **Bitcoin ou blockchain?**. 05/05/2015. Disponível em: <http://www.infomoney.com.br/blogs/cambio/moeda-na-era-digital/post/4020628/bitcoin-blockchain>. Acesso em: 11 ago. 2017.