

# BITCOIN: O DINHEIRO COM TECNOLOGIA DE FONTE ABERTA EM REDE PONTO-A-PONTO\*

Fabio Machado de Oliveira – Universidade Estadual do Norte Fluminense

Maria Eugênia Ferreira Totti – Universidade Estadual do Norte Fluminense

Vanuza de Silva Pereira Ney – Universidade Federal Fluminense

**RESUMO:** Esse trabalho apresenta uma tecnologia de rede ponto-a-ponto que está em crescente consolidação, um sistema eletrônico de pagamento que usa um protocolo de criptografia aberto para validar suas transações, denominado Bitcoin, tendo este uma proposta de virtualização completa da moeda excluindo a participação de instituições certificadoras como governos e órgãos financeiros nas garantias de operações virtuais com dinheiro real. Em seguida são apresentados os artefatos tecnológicos que sustentam a eliminação do intermediário confiável e suas taxas de cobrança na mediação de pagamentos online. Apoiado em teóricos como: Satoshi Nakamoto, Jack Weatherford e outros, iremos abordar questionamentos a respeito da aceitação e adesão ao Bitcoin nas diversas perspectivas impactadas com essa nova tecnologia, principalmente em países que enfrentam inflação e crises financeiras. Observar o fenômeno de flutuação sempre crescente da cotação do Bitcoin, bem como, os agentes externos que influenciam nessas oscilações. Contribuir para a formação de uma consciência holística dessa nova tecnologia, que encontra fomento na sociedade em rede e que a cada dia está mais conectada foi o principal sentido desse trabalho, contribuindo para o avanço da fronteira do conhecimento no ciberespaço e a constante conquista de consciência e cidadania na internet.

**PALAVRAS-CHAVE:** Bitcoin. Moeda Virtual. Novas Tecnologias.

## INTRODUÇÃO

As antigas civilizações conhecidas já utilizaram diversos meios e formas de representações para materializar o dinheiro, bem como, agregar valor nessas definições, por meio de objetos como pedras, metais preciosos e até mesmo o sal.

Na obra *A História do Dinheiro*, Weatherford (1999) mostra o valor metafórico do dinheiro quando diz que este representa uma criação humana com vários fins. Para o autor o dinheiro constitui uma via que os seres humanos adotaram para estruturar sua existência no mundo, bem como, suas relações sociais.

A compreensão de Mattar (2006) corrobora com essa ideia, quando ele diz que “o dinheiro ‘atravessa’, por assim dizer, todo o consumo”. Uma chave para compreender a importância do dinheiro na vida das pessoas precisa considerar as diferentes perspectivas metafóricas das moedas. A representação simbólica do dinheiro por artefatos físicos é natural no mundo real, contudo com a constante expansão do ciberespaço e a consolidação da internet como seu principal expoente, já era

---

\* XI EVIDOSOL e VIII CILTEC-Online - junho/2014 - <http://evidosol.textolivre.org>

esperada uma demanda reprimida por novas formas de representação do dinheiro acompanhando os formatos e padrões estabelecidos no mundo virtual.

A criptografia e as redes ponto-a-ponto fundamentam as bases tecnológicas para o desenvolvimento de um novo conceito de moeda, a cripto-moeda, que obedece a um rígido e ao mesmo tempo simples protocolo de funcionamento, que expressa a forma como deve ser emitida, armazenada e transmitida, sendo esta última, análoga a uma operação de enviar e receber e-mails. Outra característica marcante está no uso de tecnologias de fonte aberta, mais conhecidas como *open source* que sustentam essa cripto-moeda chamada Bitcoin.

A ausência de um controle central mediado por um governo ou instituição financeira agregando seus impostos e taxas administrativas, bem como a manutenção da privacidade durante seu uso e o fato de serem objetos totalmente digitais, confere o crescente aumento de popularidade ao Bitcoin, se mostrando como uma alternativa as moedas convencionais e mais adequado as novas tecnologias da informação e comunicação.

Neste estudo, será apresentado o sistema Bitcoin, suas concepções tecnológicas e seus paradoxos entre o mundo real e o virtual, suas vantagens e desvantagens. O objetivo é mostrar suas liberdades e alertar sobre suas limitações, contribuindo para uma formação de opinião esclarecida e no uso consciente dessa nova tecnologia.

## 1 O BITCOIN E SUAS PARTICULARIDADES

O sistema Bitcoin funciona sobre uma rede estruturada ponto-a-ponto, que segundo Shirky (2000) é constituída por clientes e servidores desempenhando o mesmo papel no mesmo nível de atuação e nunca um papel fixo ou centralizado como pode ser vista na Figura 01.

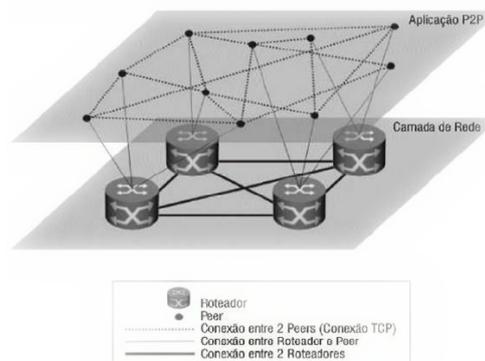


Figura 01 – Topologia de Rede Ponto-a-Ponto

Fonte: Coutinho (2006).<sup>1</sup>

Os dados que trafegam nessa rede são criptografados em um endereço público representado por um vetor de 35 caracteres, mais conhecido como chave pública e cada Bitcoin é representado nessa sequência, que a título de exemplo pode ser vista aqui: 19i8kQxp8DwjdbSWvUG6aWWmfK2BkNARTL. Este endereço também pode ser representado com o *QR-code*, isto é, um tipo de código de barras bidimensional mostrado na Figura 02:

<sup>1</sup> Disponível em: [http://www.gta.ufrj.br/grad/06\\_2/gustavo/roverlay.htm](http://www.gta.ufrj.br/grad/06_2/gustavo/roverlay.htm); Acesso em março de 2014.



Figura 02 – QR Code 2005 bar code

Fonte: ISSO/IEC.<sup>2</sup>

Segundo Nakamoto (2008), o Bitcoin é uma moeda eletrônica definida como uma cadeia de assinaturas digitais e as transferências de valores ocorrem com o envio do código assinado digitalmente para o próximo proprietário e adicionado ao fim da moeda, pois a rede Bitcoin mantém um arquivo contendo todas as transações efetuadas de todos os endereços públicos do sistema, podendo o recebedor verificar as assinaturas para confirmar a cadeia de propriedade. Nessa transferência é necessária a existência de uma chave privada associada aos endereços públicos e esta chave privada só é de conhecimento do criador desse endereço público ou chave pública. É a lista de endereços públicos de transações que confere transparência a todas as operações, já o anonimato e a privacidade ficam garantidos, pois não é possível saber quem é o dono de cada endereço público.

Em seu artigo que define o protocolo de funcionamento do Bitcoin, Nakamoto (2008) explica que cada novo usuário conectado a rede ponto-a-ponto Bitcoin recebe toda a lista de transações e contribui com o processamento de novos blocos contendo novas transações, aproximadamente, em intervalos de 10 minutos, cada bloco apresenta uma transação diferente, de geração, que controla a criação de novos Bitcoins e os atribui a um endereço público, gerado pelo criador do novo bloco. Outro ponto importante é observar que essa geração não é infinita e sim controlada pelo próprio protocolo do sistema, como foi explicado e estima-se que em 2140 atinja seu máximo.

Para Duarte (2014), o Bitcoin é como qualquer moeda atual hoje no mundo e possui todo um aparato tecnológico que lhe confere confiança e sua aceitação é exponencial graças a sua transparência nas transações e ainda a fuga da volatilidade, inflação e incertezas governamentais que afetam as moedas convencionais.

## CONCLUSÃO

Expor as ameaças dos “hackers” que sempre exploram possibilidades de ganhar dinheiro utilizando suas habilidades e conhecimentos avançados nesse universo, serve de alerta para os entusiastas despreparados e desinformados, pois apesar de toda segurança do Bitcoin as vulnerabilidades podem partir do fator humano.

Muitas ameaças rondam a difusão do Bitcoin e de acordo com Piropo (2014) os governos não veem com bons olhos o crescimento de um sistema monetário sobre o qual não tem controle, isto é, poder interferir na emissão de moedas, delimitar o fluxo de negociações internacionais e taxar operações financeiras. Outro ponto sensível está na possibilidade de “lavagem” de dinheiro, que assim como no sistema tradicional, sempre encontra uma forma de se realizar, enfim como não deixaria de acontecer com toda nova tecnologia, pode ser usada para o bem ou para o mal.

Em dezembro de 2013 o governo da China tomou uma atitude que influenciou na cotação do Bitcoin, proibiu suas instituições financeiras oficiais de usarem Bitcoin, levando a uma desvalorização de 54,4% em apenas duas semanas. A cotação caiu dos US\$ 1147,25 de 04/12/2013

<sup>2</sup> Disponível em: [http://www.iso.org/iso/catalogue\\_detail?csnumber=43655](http://www.iso.org/iso/catalogue_detail?csnumber=43655); . Acesso em março de 2014.

até o valor de US\$ 522,23 em 18/12/2013, entretanto sua recuperação foi rápida, atingindo em meados de janeiro de 2014 o patamar de US\$ 800,00. Para Piropo (2014) O mais importante é que mesmo diante de tantas incertezas quem adquiriu Bitcoins entre janeiro e outubro de 2013 se beneficiou muito, com uma valorização nesse período que variaram de US\$ 13,13 até US\$ 125,49.

Em suas análises Piropo (2014) também destaca outro momento de forte impacto na cotação de Bitcoins, fato esse ocorrido durante a crise financeira de Chipre, quando o governo daquele país anunciou um confisco compulsório de 6,7% a 10% nos depósitos bancários, semelhante ao Plano Color no Brasil. Posteriormente ocorreu uma imensa demanda para comprar Bitcoins partindo de Chipre, pois as pessoas não estavam tão seguras em relação a atitudes do governo e das instituições financeiras. Nesse episódio o Mt. Gox, que era a maior entre as casas de câmbio de Bitcoins, teve que suspender suas operações alegando manutenção em seus servidores, entretanto essa atitude foi para acalmar o mercado Bitcoin. Quando as operações foram retomadas, novamente a cotação passou a subir, oscilou por um período curto e depois se estabilizou.

Notadamente, toda vez que algum governo age contra o sistema Bitcoin de forma voluntária ou involuntária, no caso de Chipre, se estabelece uma turbulência em sua cotação, contudo a moeda acaba se estabilizando com o passar do tempo, registrando uma cotação menor que a anterior, porém o novo patamar de estabilização é sempre maior que o último patamar estável. Esses dados podem ser vistos na Figura 03.



Figura 03 – Variação da cotação do bitcoin por ano.

Fonte: B. Piropo (2014).<sup>3</sup>

## REFERÊNCIAS

BOHANNAM, Paul. The impact of Money on an African subsistence economy. In: G. Dalton (org), Trial na peasant economies. Readings in economy anthropology. New York: The Natural History Press. Pp. 123-35, 1967. URL <[http://dornsife.usc.edu/tools/mytools/PersonnelInfoSystem/DOC/Faculty/ANTH/publication\\_1003708\\_9664.pdf](http://dornsife.usc.edu/tools/mytools/PersonnelInfoSystem/DOC/Faculty/ANTH/publication_1003708_9664.pdf)>. Acessado em 10/03/2014.

CAMPOS, Andres Cisneros. Estudio de la red Bitcoin. 2013. URL <<http://openaccess.uoc.edu/webapps/o2/bitstream/10609/23341/6/acisneroscTFM0613memoria.pdf>>

<sup>3</sup> Disponível em: <http://www.techtudo.com.br/artigos/noticia/2014/02/bitcoin-oscilacoes-da-cotacao.html>; Acesso em março de 2014.

>. Acessado em 11/03/2014.

CERF, V. G. & KAHN R. E., "A protocol for packet network interconnection", IEEE Trans. Comm. Tech., vol. COM-22, V5, 1974, pp. 627-641.

ROHR, Altieres & GOMES, Helton Simões. Moeda virtual bitcoin começa a ganhar espaço no comércio brasileiro. Portal G1. URL <<http://g1.globo.com/tecnologia/noticia/2014/02/moeda-virtual-bitcoin-comeca-ganhar-espaco-no-comercio-brasileiro.html>>. Acessado em 18/02/2014.

DUARTE, George. Primitive Money. In: G. Dalton (org) Tribal na peasant economies. Readings in economy anthropology. New York Press, 1967 pp.254-81. URL <[http://www.bylany.com/kvetina/kvetina\\_etnoarcheologie/literatura\\_esaje/5\\_literatura\\_obchod.pdf](http://www.bylany.com/kvetina/kvetina_etnoarcheologie/literatura_esaje/5_literatura_obchod.pdf)>. Acessado em 13/12/2013.

GIBSON, Willian. Neuromancer. São Paulo: Aleph, 2003.

LÉVY, Pierre. A Inteligência Coletiva. São Paulo: Ed.34, 2000.

\_\_\_\_\_. Cibercultura. São Paulo: Editora 34, 1999.

\_\_\_\_\_. A inteligência coletiva: por uma antropologia do ciberespaço. São Paulo: Loyola, 1998.

NAKAMOTO, Satoshi. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. URL <<http://bitcoin.org/bitcoin.pdf>>. Acessado em 15/10/2013.

NEIBURG, Federico. 2007. As moedas doentes, os números públicos e a antropologia do dinheiro. Mana. URL <<http://dx.doi.org/10.1590/S0104-93132007000100005>>. Acessado em 10/12/2013.

MONTEIRO, Silvana Drumond. 2007. O Ciberespaço: o termo, a definição e o conceito. DataGramZero. URL <[http://www.dgz.org.br/jun07/Art\\_03.htm](http://www.dgz.org.br/jun07/Art_03.htm)>. Acessado em 13/03/2014.

PIROPO, Benito. 2013. Bitcoin: oscilações da cotação. Techtudo. URL <<http://www.techtudo.com.br/artigos/noticia/2014/02/bitcoin-oscilacoes-da-cotacao.html>>. Acessado em 18/02/2014.

SHIRKY, Clay. What's P2P and What's not. Openp2p.com, 24/11/2000. URL <<http://www.openp2p.com/pub/a/p2p/2000/11/24/shirky1-whatisp2p.html>>. Acessado em 13/04/2014.

WEATHERFORD, John. A História do Dinheiro – Do arenito ao cyberspace. São Paulo, Negócio Editora, 1999.