Bitcoins: liberdade para transações financeiras com a Internet

Bruna Andreata Avelar
Francisco Chaves de Carvalho Marinho
Laila Kelly Costa Menezes
Marco Aurelio Felizardo de Andrade
Rafael Mizerani Couto Moreira
Wladston Viana Ferreira Filho

Resumo. *A ampla utilização e disponibilização de tecnologias criptográficas, juntamente com a internet, possibilitou a troca segura, anônima e distribuída de mensagens. Utilizando essas tecnologias como base, foi desenvolvido um protocolo para um sistema financeiro anônimo, seguro, distribuído, e sem controle central chamado Bitcoin. Hoje já são transacionados milhões de dólares cada dia em Bitcoins, e nos Estados Unidos e Europa muitos comércios e prestadores de serviços estão aceitando pagamentos nessa moeda. Essa plataforma tem um potencial imenso para aumentar as liberdades individuais dos cidadãos, caso seja amplamente utilizada, pois torna os bancos obsoletos ao disponibilizar um sistema seguro, privado e anônimo. O custo das transações é quase zero, e não há restrições para transações financeiras para outros países. Neste artigo será explicado como funciona, as vantagens e desvantagens, e serão mostrados exemplos de utilização.*

Palavras-chave: dinheiro virtual, criptografia, internet.

1. Introdução

O dinheiro já teve várias formas e representações nas diversas civilizações conhecidas. Sal, metais semipreciosos, cascas de mariscos difíceis de encontrar, certos tipos de pedras, entre outros. No final do século XIX, começou-se a utilizar cédulas impressas. Mesmo após a revolução tecnológica e cultural proporcionada pelo computador pessoal e pela Internet, a cédula de papel, aliada a sistemas financeiros controlados por estados soberanos, ainda é a forma utilizada para representar dinheiro.

A consolidação da Internet e da criptografia criou a base tecnológica para o desenvolvimento de um novo conceito de moeda, a cripto-moeda, que está ganhando popularidade e se mostrando como uma possibilidade ao dinheiro convencional. Enviar e receber cripto-moedas é uma operação análoga a enviar ou receber emails. E suas características marcantes e inovadoras incluem a ausência de um controle central através de um governo ou entidade centralizadora, a manutenção da privacidade, e o fato de serem objetos completamente digitais.

Uma cripto-moeda chamada Bitcoin conseguiu alcançar níveis de liquidez e popularidade para ser uma moeda global, colocando o conceito das cripto-moedas para a realidade. Hoje, o Bitcoin processa o equivalente a USD 750 mil em transações a cada hora e é possível comprar e vender Bitcoins em diversos mercados espalhados pelo mundo. A maioria das pessoas, no entanto, ainda desconhece ou possui entendimento errado sobre o funcionamento dessa nova moeda.

Neste trabalho, será explicado o funcionamento do sistema Bitcoin, serão avaliadas suas vantagens e desvantagens e serão mostrados exemplos reais de uso. O objetivo é esclarecer o funcionamento desta nova forma de moeda a fim de popularizar suas liberdades e apontar suas limitações em relação ao sistema financeiro tradicional.

2. O funcionamento da rede

Um conceito importante da rede Bitcoin é o endereço público. Um endereço público é representado por uma sequência de 35 caracteres, começando com 1. A título de exemplo, este é o endereço público utilizado pelo site wikileaks.org para o recebimento de donativos:

1HB5XMLmzFVj8ALj6mfBsbifRoD4miY36v

Para ocorrer a transferência de valores de um endereço público para outro (transação financeira) é necessária a existência de uma chave privada associada aos endereços. A chave privada só deve ser conhecida pelo criador do endereço público, já que somente este tem o direito de "gastar" seus Bitcoins. Uma vez que isto ocorra, é matematicamente impossível gastar Bitcoins alheios. A criptografia utilizada no processo de geração das chaves é forte e seriam necessários milhões de anos, utilizando os melhores supercomputadores que existem hoje, para conseguir encontrar uma chave privada de um endereço público. Por isso é importante ressaltar que, caso a chave privada de um endereço seja perdida, seus Bitcoins estarão perdidos de forma irrecuperável.

A rede Bitcoin mantém ainda um arquivo contendo todas as transações já realizadas para todos os endereços do sistema. Este arquivo é público e conhecido por todos os utilizadores da rede Bitcoin. É a lista pública de transações. Desta forma, as transações são transparentes e todos possuem conhecimento completo de todas as operações. O anonimato e a privacidade ficam garantidos por que não é possível saber quem é o detentor de cada endereço público, ou seja, quem está gerando as transações, ou quem possui determinado valor.

Transações são validadas somente se o endereço público possuir Bitcoins e se esses Bitcoins nunca tiverem sido gastos anteriormente. Isso é garantido através da lista pública de transações. Além disto, as transações são irreversíveis: uma vez que esteja inclusa na lista pública, não há como desfazê-la. Opcionalmente, pode-se incluir também uma taxa na transação: um valor adicional a ser pago para a própria rede Bitcoin para estimular o seu rápido processamento.

3. Gerando Bitcoins

No sistema financeiro tradicional, dinheiro é obtido em troca de produtos ou serviços. O mesmo ocorre no sistema de Bitcoin. Para receber as cripto-moedas, o usuário deve contribuir na efetivação das transações oferecendo sua capacidade de processamento.

Aproximadamente a cada 10 minutos, algum usuário que está processando operações publica um novo bloco contendo novas transações. Cada bloco contém também uma transação especial, de geração, que efetivamente cria novos Bitcoins e os atribui a um

endereço público, criado pelo gerador do bloco. Assim o usuário é recompensado recebendo todas as taxas de transações processadas mais os Bitcoins criados.

Entretanto, moedas não serão geradas infinitamente. O número decresce a cada novo bloco, já que o protocolo prevê a criação de uma quantidade limitada de Bitcoins. Esta quantidade é prevista para ser alcançado em 2140, sendo que em 2030 o número já seria irrisório.

A rede Bitcoin é hoje a rede computacional distribuída mais poderosa do mundo, com uma capacidade de processamento de 150 Petaflops. O computador mais rápido do mundo (o japonês K Computer) possui uma capacidade de 10 Petaflops.

4. Vantagens e desvantagens

Como sempre ocorre com tecnologias recém-criadas, o sistema Bitcoin também apresenta um lado positivo e um negativo. Suas principais vantagens estão na possibilidade de um usuário realizar transações financeiras sem intermédio de bancos ou outras empresas. Isso elimina gastos com taxas e impostos tanto em operações nacionais quanto internacionais. Mesmo que exista a taxa para transações, o usuário tem liberdade para escolher se deve ou não pagá-la. E, caso escolha pagá-la, é o próprio usuário que determina o valor considerado justo. Além disso, o dinheiro fica livre de barreiras como a aprovação de crédito ou congelamento de conta.

Por outro lado suas desvantagens estão intimamente relacionadas ao fato da nova moeda não ser assegurada ou aprovada por nenhum governo. Como o valor de qualquer moeda é geralmente definido pela confiança que o mercado tem sobre mesma, conforme a confiança flutua o valor do Bitcoin também flutua. Isso faz com que a moeda valha em um dia RS$ 7,00, no outro RS$ 30,00 e no outro RS$ 20,00. Outro problema constantemente citado consiste no caso em que usuários têm seu endereço público e sua chave privada roubados ao mesmo tempo. Apesar de o sistema em si ser seguro ele não impede esse tipo ameaça. Isto, entretanto, é um problema que pode ser contornado com medidas simples de segurança como proteger seus arquivos com senhas fortes e criptografia.

5. Exemplos de uso

Desde que surgiu em 2008, o mercado que depende e suporta Bitcoins tem se desenvolvido. Se no início do processo eram raros os que se aventuravam em realizar a venda de seus produtos utilizando a nova moeda, hoje já existem desde restaurantes em Nova York até casas de câmbio como a Mt. Gox. Além disso, a cripto-moeda desempenha um importante papel no aumento de liberdades de cidadãos que vivem em países totalitários, como o Irã, ou em países que dificultam transferências bancárias para além de seus territórios, como a China.

Futuramente, o sistema Bitcoin pode ter ainda um papel de destaque no sistema financeiro africano. Em países como Quênia e Nigéria em que a economia cresce sem o devido acompanhamento do sistema bancário, não é incomum encontrar-se grandes redes de cambistas ilegais que realizam pagamentos transfronteiriços. A estratégia de maior sucesso até então tem sido o sistema de pagamento por telefonia móvel, onde se

realizam transferências bancárias através de mensagens de texto. Desta forma o Bitcoin aliado à telefonia móvel poderia oferecer uma estrutura mais segura e rápida para transferências a qualquer parte do globo.

Entretanto, não existem apenas aplicações éticas ou legais para a cripto-moeda. Na verdade o sistema Bitcoin ganhou notoriedade devido a sua utilização para ações ilegais como compra de drogas através de uma espécie de mercado negro online: o Silk Road. Após o senador americano Charles Schumer aparecer na impressa fazendo duras críticas ao sistema, diversas pessoas passaram a ter conhecimento sobre a nova tecnologia e a utilizá-la. Porém o uso de dinheiro em atividades ilegais não é um privilégio dos Bitcoins. Na verdade, este é um problema enfrentado por todo tipo de moeda de troca e para minimizá-lo é necessário encontrar meios para punir os criminosos.

6. Conclusão

Como toda nova tecnologia o sistema Bitcoin é motivo de críticas ou de discursos eufóricos. Entretanto, o que a história nos ensina é que não há como prever se no futuro a cripto-moeda cairá no esquecimento ou se firmará como um sistema monetário alternativo. Ela apresenta vantagens e nichos específicos para seu desenvolvimento, mas apresenta também desvantagens e pontos que devem ser aperfeiçoadas. Contudo a ideia que este sistema introduz é ao menos importante para reacender a discussão de um problema que a muito aflige nosso país: a quantidade absurda de impostos e juros bancários e a falta de liberdade dos cidadãos brasileiros perante esse assunto.

7. Bibliografia

[1] NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Eletronic Cash System*. Disponível em: http://bitcoin.org/bitcoin.pdf Acesso em: 14 de maio de 2012.

[2] *Bitcoin*. Wikipédia, a enciclopédia livre. Flórida: Wikimedia Foundation, 2012. Disponível em: http://en.wikipedia.org/wiki/Bitcoin Acesso em: 14 de maio de 2012.

[3] KOHN, Stephanie. *Bitcoin: A Moeda Digital*. Olhar Digital, julho de 2011. Disponível em: http://olhardigital.uol.com.br/produtos/digital_news/noticias/bitcoin_a_moeda_digital Acesso em: 14 de maio de 2012.

[4] SIMONITE, Tom. *Bitcoin Busca Nova Vida na África*. Technology Review, março 2012. Disponível em: http://www.technologyreview.com.br/read_article.aspx?id=39951&pg=2 Acesso em: 14 de maio de 2012.

[5] SMAAL, Beatriz. *Bitcoin: O Dólar da Internet*. Tecmundo, junho de 2011. Disponível em: http://www.tecmundo.com.br/dinheiro/10951-bitcoin-o-dolar-da-internet.htm Acesso em: 14 de maio de 2012.

[6] SERRANO, Filipe. *Lastro em Bits*. Link Estadão, junho de 2011. Disponível em: http://blogs.estadao.com.br/link/lastro-em-bits/ Acesso em: 14 de maio de 2012.

[7] KIST, Cristine. *O Dinheiro do Futuro*. Super Interessante, ed. 297, novembro de 2011. Disponivel em: http://super.abril.com.br/tecnologia/dinheiro-futuro-647372.shtml Acesso em: 14 de maio de 2012.