

BITCOIN NA PRÁTICA

Igor Campos Alcantara¹, Rosemeire Soares de Sousa¹

¹Instituto Federal de Mato Grosso do Sul – Aquidauana-MS

campos_igor_7@hotmail.com, rosemeire.sousa@ifms.edu.br

Resumo

Bitcoin é um sistema de dinheiro totalmente virtual que não precisa de um governo, empresa ou grupo selecionado de pessoas para controlar suas transações monetárias. Atualmente existem muitas moedas virtuais em circulação, mas o Bitcoin é pioneiro no assunto e se tornou o mais acessível e de maior conhecimento entre os usuários de moedas virtuais. Esse sistema é tão inovador que é considerado como uma revolução tecnológica após a Internet, porém, quando falamos no tema Bitcoin, poucos entendem de fato o que é e como essa criptomoeda funciona no dia a dia. Neste trabalho serão abordadas as características do Bitcoin e o seu funcionamento.

Palavras-chave: Bitcoin, moeda-virtual.

Introdução

O Bitcoin, criado em 2008, divulgado fortemente a partir de 2009, é uma moeda de existência exclusivamente virtual, suas transações são realizadas somente por meio da internet, em um ambiente codificado. Essa espécie de moeda virtual, conhecida também como criptomoeda, é um software de código-aberto. Através de uma rede peer-to-peer (P2P) do inglês ponto a ponto, deu origem a outras moedas criptográficas, sistemas de pagamentos virtuais e uma infinidade de produtos e serviços derivados de sua tecnologia. O interesse pela pesquisa está relacionado ao fato de que a moeda Bitcoin é apresentada pelos seus investidores como uma moeda futurista, de valorização rápida, que não corre o risco de ser falsificada. Contudo, trata-se de uma moeda que não existe fisicamente, não pertence a nenhum país e não é regulada por nenhuma instituição financeira, é movimentada por meio de uma conta virtual e um aplicativo também virtual, que possibilita a transação e a troca das moedas em rede.

O objetivo desta pesquisa descreve sobre o uso e aplicação dos mecanismos tecnológicos que garantem a existência do Bitcoin e permitem transações financeiras, exclusivamente através da internet, entre pessoas que nunca se viram, a partir de qualquer computador ou dispositivo móvel (ULRICH, 2014).

Metodologia e desenvolvimento

O estudo teve início com as reuniões semanais dos integrantes do grupo de pesquisa Blockchain. Cada integrante trazia novas contribuições sobre a estrutura P2P, que possibilita a existência das criptomoedas de forma descentralizada por ser uma rede que, “não necessita de

uma autoridade central encarregada de criar as unidades monetárias e de verificar as transações realizadas, essa força computacional para manter a rede é provida diretamente pelos usuários” (MARQUEZIN, 2017); paralelamente, eram colhidas informações sobre o Bitcoin. Essas contribuições foram realizadas através de estudos bibliográficos, artigos de pessoas renomadas no assunto, debates, constantes questionamentos entre os membros participantes e consulta aos sites relacionados ao tema. À medida em que as informações se tornavam mais claras, eram adicionadas a um documento compartilhado. Tendo em vista o número de trabalhos pesquisados para entender o processo do bitcoin, identificamos a necessidade de um trabalho com essas informações detalhadas.

Resultados

Entender como funciona as carteiras Bitcoins é o primeiro passo para quem deseja ingressar nesse universo, pois um bom entendimento sobre essa tecnologia evita futuros problemas para aqueles que desejam ingressar no mundo das criptomoedas, afinal, os usuários são a principal fonte desse sistema, tanto para gerar, movimentar ou adquirir Bitcoins. Uma carteira de bitcoin é um software, aplicativo ou hardware capaz de gerenciar (guardar) suas chaves pública e privada. As carteiras não armazenam criptomoedas, na verdade, as moedas não estão armazenadas em um local. O que existe são registros na Blockchain informando quando a chave pública recebeu ou enviou algumas moedas, assim, para se ter acesso a esses registros faz-se necessário o uso das chaves. E a função dessas carteiras é justamente guardar essas chaves, de modo que elas não caiam em mãos erradas, principalmente a chave privada (senha). Torna-se necessário entender a diferença entre os diversos tipos de carteiras, todas com suas respectivas particularidades. Logo, não existe a melhor carteira, mas a mais recomendada para cada tipo de necessidade do usuário, conforme descrito a seguir:

- Desktop: É um programa (carteira) que roda no computador desktop ou notebook. A única desvantagem é necessitar de um PC. Pois uma vez infectado (vírus), todos os seus bitcoins podem ser perdidos (roubados por hackers).
- Mobile: Um aplicativo disponibilizado aos smartphones e tablets, levando muita praticidade nas transações do dia a dia. Sua desvantagem é ter que fazer um backup escrito das 12 ou 24 palavras fornecidas pela carteira e guardá-las em um local seguro, a fim de que, caso um dia seu

dispositivo (smartphone/tablet) seja roubado, poderá facilmente recuperar o seus bitcoins utilizando o backup escrito.

- Web ou Online: São carteiras armazenadas na “nuvem” que podem ser acessadas de qualquer dispositivo conectado à internet. O ponto negativo é que o usuário não detém total poder sobre suas criptos, uma vez que suas chaves – pública e privada – ficam armazenadas no próprio servidor (nuvem). Portanto, se algum hacker invadir tal servidor, provavelmente você perderá seus bitcoins.
- Hardware: São dispositivos físicos eletrônicos, geralmente em formato USB, embora façam transações online suas chaves ficam armazenadas offline. É ideal para quem procura segurança. Sua principal desvantagem é o preço.
- Papel: Nada mais do que as chaves pública e privada impressas em papel, garantindo assim, mais segurança ao usuário. Vale ressaltar que para uma melhor garantia de segurança certifique-se de que estas chaves sejam geradas offline.

Para a sua própria segurança o ideal é que você tenha no mínimo duas carteiras. Uma contendo um saldo menor, a qual poderia ser usada para pequenas transações diárias como pagamento de uma compra de pães por exemplo, semelhante a um cartão de débito. E a outra servindo para você guardar o restante de seu saldo (caso seja alto), semelhante a uma conta poupança. Assim, caso acontecer da sua carteira ser roubada, não perderá todo seu dinheiro. Após decidir qual carteira atenderá melhor a necessidade do usuário, o processo para a criação de uma carteira poderá ser realizada por meio da ferramenta bitaddress.org.

Aos usuários que querem minerar Bitcoins existem três opções: hardware, software e sistema operacional próprio de mineração:

- Hardware: equipamentos que são utilizados para mineração que contém chips ASIC que é uma sigla para Circuito Integrado de Aplicação Específica, que possuem como uma única função a realização do cálculo de hash SHA-256. Eles oferecem desempenhos 100 vezes maior que outros equipamentos mais comuns. Existem fabricantes especializados em fabricação deste tipo de hardware, como por exemplo, Bitmain, AsicMiner, CoinTerra TerraMiner IV, Virtual Mining Corp.
- Software: Os softwares de mineração permitem que o usuário utilize o hardware que tem disponível para mineração. O BFGMiner, por exemplo, é um software de mineração projetado para o Hardware da ASIC, e é compatível com dispositivos FPGAs, mas também pode ser utilizado em um PC normal. Ele, está disponível para o Windows e todas as principais distribuições do Linux, podendo também ser instalado em um Raspberry Pi.

- Sistemas Operacionais: Além de hardware e software, o usuário pode também instalar um sistema operacional, que utilizará todo o poder computacional do sistema para uso exclusivo da mineração. Os criadores do Brains OS, que é um sistema operacional utilizado para mineração, afirmam que ele é o primeiro sistema de mineração de código aberto criado no mundo.

Logo quando surgiu o Bitcoin era possível minerar em um computador comum, mas logo depois foram investidos milhões de dólares em poder computacional tornando um a mineração através da CPU ou até mesmo GPU uma atividade inviável.

Considerações Finais

O Bitcoin se apresenta como uma inovação futurista que, possibilita aos usuários se livrarem de taxas bancárias e juros de cartões, tornando possível realizar transações monetárias, exclusivamente pela internet. Sem risco de fraude ou prejuízo, garante ao investidor sigilo, segurança e privacidade. Contudo, há evidências de riscos e prejuízos no investimento em Bitcoin, posto que, a moeda digital é totalmente auto financiada pelos seus participantes, não tem propriedade intelectual e não há regulação desse mercado.

Agradecimentos

Agradecemos ao IFMS *Campus* Aquidauana, pelo incentivo às pesquisas, disponibilizando recursos tecnológicos para o desenvolvimento dos estudos.

Referências

MARQUEZIN, Alicia Pereira. **Evolução Monetária**: Um estudo sobre a demanda pelo Bitcoin. Porto Alegre, Universidade Federal do Rio Grande do Sul, 2017.

ULRICH, Fernando. **Bitcoin a moeda na era digital**. São Paulo: Instituto Ludwig Von Mises Brasil, 2014, 123p.

Disponível em:

<https://www.criptofacil.com/carteira-bitcoin-guia-definitivo-para-sua-carteira-digital-passo-a-passo/> Acesso em: 25 de mar. 2019.

Disponível em:

<https://www.bitaddress.org/bitaddress.org-v3.3.0-SHA256-dec17c07685e1870960903d8f58090475b25af946fe95a73af88408cef4aa194.html> Acesso em: 25 de mar. 2019.

MENDES, Ana Carolina Camargo. **Moeda Eletrônica Bitcoin**: Análise do Uso na Cidade de Brasília – DF.

Disponível

<https://www.nucleodoconhecimento.com.br/tecnologia/moeda-eletronica-bitcoin> em: Acesso em: 27 de mar. 2019.