A CRIPTOMOEDA BITCOIN E SUAS TECNOLOGIAS

Vinícius Monteiro Galvão da Silva[1], Napoleão Povoa Ribeiro Filho[2]

[1]Estudante do Curso Superior de Tecnologia em Sistemas para Internet – IFTO. e-mail: <vinixsenior@gmail.com>
[2]Professor do Curso de Sistemas para Internet - IFTO. e-mail: <napoleao@ifto.edu.br>

Resumo: Criptomoedas são moedas digitais, que não existem na forma física, não são reguladas por nenhum tipo de órgão governamental e fornecem um certo tipo de anonimato para quem realiza uma transação. Tais moedas surgiram após diversos estudos e experimentos onde o objetivo era obter uma maior segurança e rapidez ao realizar transações por meios digitais. Hoje, essa tecnologia apresenta crescente aceitação em transações comerciais nos mais variados tipos de negócios. Porém, o seu entendimento ainda pode ser visto como um obstáculo para uma maior popularização da mesma. Este artigo tem por objetivo apresentar a origem as criptomoedas, explicar suas tecnologias e apresentar situações comerciais onde a mesma está sendo utilizada.

Palavras-chave: bitcoins, blockchain, criptomoedas, moeda digital

1 INTRODUÇÃO

Atualmente as transações financeiras (pagamentos, transferências, entre outras) realizadas com o dinheiro como conhecemos, são regulamentadas por algum tipo de órgão. No Brasil, é o Banco Central do Brasil o responsável por realizar tal regulamentação. Normalmente para realizar tais transações, existe algum tipo de custo para poder efetuá-las, como por exemplo o custo de realizar transferências bancárias por meio de TED e DOC (que são operações bancárias que têm como finalidade realizar transferências de valores entre instituições financeiras diferentes), que na maioria das instituições bancárias (como Banco do Brasil, Bradesco, Caixa Econômica Federal, entre outros) seu custo varia entre R$ 8,00 e R$ 16,00.

Baseado nesse contexto, sempre existiram tentativas de se realizar transações comerciais sem esse tipo de intervenção. O advento da internet e sua posterior popularização forneceram as tecnologias necessárias utilizadas em vários experimentos que tentaram excluir os bancos como mediadores de transações comerciais. Esses experimentos criaram moedas virtuais (só existiam em sistemas computacionais, não era impresso em papel moeda) que ficaram conhecidas como moedas digitais ou criptomoedas.

O projeto *Bit Gold* e o *B-money* são exemplos de tentativas de se criar um tipo de dinheiro virtual, mas nenhuma delas teve sucesso (ADVFN, s.d.). Tais iniciativas apresentaram problemas relacionados à segurança e confiabilidade. Talvez por isso não conseguiram se popularizar. Mas a partir desses primeiros esforços e utilizando tecnologias mais maduras, foi desenvolvido em 2008 o *Bitcoin*,

que resolveu o problema de gasto duplo, ou seja, quando há a utilização do mesmo *Bitcoin* ou outra criptomoeda por mais de uma vez em diferentes transações financeiras.

Considerando o contexto apresentado, este trabalho tem como finalidade explicar como a criptomoeda *Bitcoin* é gerada, as tecnologias envolvidas na geração do *Bitcoin*, bem como identificar atualmente em quais situações e negócios as criptomoedas já estão sendo aceitas.

2 JUSTIFICATIVA

Os motivos fundamentais que impulsionaram a criação do *Bitcoin* foram: um sistema financeiro instável e com elevado nível de intervenção estatal e a crescente perda de privacidade financeira (com as criptomoedas é possível realizar transações de forma anônima) (ULRICH, 2014). Em um determinado momento em que houve uma grande crise do sistema financeiro, tornou-se evidente que com o sistema bancário tradicional não havia liberdade financeira, pois não era possível gerenciar o próprio dinheiro da melhor forma, sem depender de grandes instituições como bancos e governos. E como já havia diversos estudos e experimentos sobre moedas que fossem desvinculadas de um órgão central, foi possível a criação do *Bitcoin* em 2008.

As criptomoedas, por sua ausência de vínculo com uma autoridade central ou possibilidade de influência do Estado, tornou-se uma ferramenta de importante relevância para evitar oscilações de câmbio causadas por crises internas, especialmente as causadas por motivos políticos, cuja tendência é sempre a busca por moedas estrangeiras que não seriam afetadas por tais circunstâncias (OLIVEIRA et. al, 2019). As criptomoedas, assim como o Real e o Dólar, também podem ser utilizadas para comprar bens e serviços.

Nesse sentido, pode-se perceber a importância do estudo sobre as criptomoedas, sua relevância no mercado financeiro atual, e também sua aceitação em diferentes tipos de transações comerciais.

3 METODOLOGIA

A pesquisa deste trabalho é de caráter exploratório, pois tem como objetivo buscar informações para ter uma maior familiaridade e assim buscar os principais estudos relacionados ao tema proposto. Quanto à abordagem, trata-se de uma pesquisa qualitativa, pois serão apresentados conceitos e análises sobre o tema. E quanto aos procedimentos metodológicos, esta é uma pesquisa bibliográfica já que o trabalho será elaborado com base em materiais já publicados, como livros, artigos científicos e reportagens relacionadas ao tema.

4 REFERENCIAL TEÓRICO

4.1 Como a criptomoeda Bitcoin é gerada

Bitcoin é uma moeda digital *peer-to-peer* (par a par ou, simplesmente, de ponto a ponto), de código aberto, que não depende de uma autoridade central para controlar fazer o seu gerenciamento. Ponto a ponto, significa que os computadores dos usuários são os "pontos", e conectam-se entre si formando uma rede descentralizada. Conforme explica (FOXBIT, 2020), em uma rede descentralizada não há a dependência de grandes corporações ou do governo para efetuar transações, cobrar altas taxas ou colocar limites de tempo entre transações.

O sistema *peer-to-peer* do *Bitcoin* permite que não haja a necessidade de qualquer intermediário para a confirmação das transações financeiras. Ou seja, uma pessoa pode transferir determinada quantia em *Bitcoin* para qualquer lugar do mundo sem que seja necessário que uma instituição financeira registre esta transação.

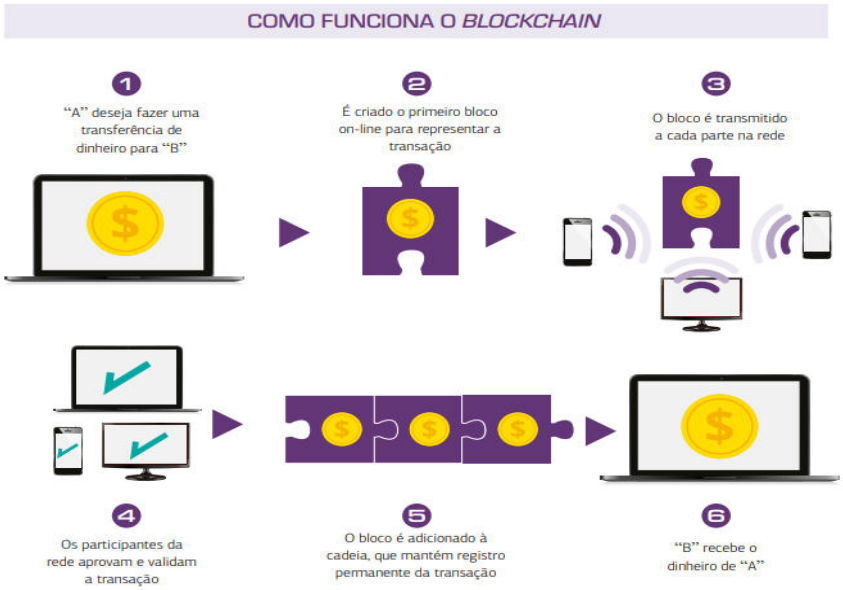
O meio de obtenção do *Bitcoin* é chamado de mineração, cujo processo, basicamente, consiste em adquirir digitalmente a propriedade de determinado número de criptomoedas a partir de um intenso processamento computacional realizado pelo hardware do computador de uma pessoa que realiza essa operação (REIS, 2017). Esse processo de mineração é caracterizado por adicionar registros ao livro razão público do *Bitcoin*, conhecido como *Blockchain*. Tal tecnologia é uma cadeia de blocos que confirma as transações da criptomoeda para toda a rede, evitando assim os gastos duplos ou reuso da criptomoeda (NETO; MATARAZZO, 2020).

4.2 O funcionamento da tecnologia blockchain

O *Blockchain* surgiu com a criptomoeda *Bitcoin* e tinha por objetivo ser um livro-razão onde todas as transações financeiras de todos os usuários de *Bitcoin* ficassem armazenadas de forma a não ocorrer a utilização de uma mesma criptomoeda em transações financeiras diferentes. E, como já apresentado anteriormente, não ser necessário um órgão centralizador para validar as transações financeiras efetuadas (DE LUCENA; HENRIQUES, 2016). Alguns dados importantes que são armazenados no *Blockchain* são: a quantia de *Bitcoins* que foi transacionada ou qualquer outra criptomoeda, quem enviou, quem recebeu, em que data a transação foi feita e também qual bloco ela está armazenada.

De acordo com a figura 1 apresentada a seguir, "A" deseja realizar a transferência de uma criptomoeda para "B". Em seguida é criado um bloco que representa a transação e posteriormente esse mesmo bloco é adicionado ao grande conjunto de blocos que se chama *Blockchain*. É no *Blockchain* que todas as transações com criptomoedas são registradas.

Figura 1 - Como funciona a tecnologia *Blockchain*



Fonte: Diniz (2017)

O *Blockchain* é uma cadeia de registros imutáveis, públicos e distribuídos. Cadeia porque os registros estão cuidadosamente encadeados uns aos outros por meio de chaves públicas (chaves que podem ser amplamente disseminadas), entradas e saídas. Imutáveis porque uma vez que o registro é inserido na cadeia, ele não pode mais ser alterado. Públicos porque a única condição necessária para que um cidadão possa ter acesso aos registros do *Blockchain* é que ele tenha acesso à internet. E distribuídos porque esta cadeia de registro não está armazenada em um único servidor central, ao contrário, está replicada em milhões de máquinas distribuídas pelo mundo todo e nenhuma empresa ou indivíduo pode reivindicar a propriedade destes registros (PIRES, 2016).

O *Blockchain* permite o registro de transações como se fosse um livro contábil (local onde ficam armazenados todos os registros de caráter financeiro e econômico). É através do uso do *Blockchain* que se garante a privacidade e segurança das transações feitas com *Bitcoin* e outras criptomoedas. A privacidade é garantida porque os dados são criptografados permitindo que

informações confidenciais sejam difíceis de serem acessadas. Também existe a garantia de segurança devido ao fato de que as informações que estão no *Blockchain* não podem ser alteradas. Os registros no *Blockchain* podem ser visualizados por qualquer pessoa, mas não é possível ver o que foi enviado nem quem enviou, apenas quando houve o envio.

4.3 O que é uma carteira digital?

As carteiras digitais (*wallets*), são aplicativos de computador/smartphone/Web capazes de guardar chaves privadas (que é um número alfanumérico codificado em diferentes formatos de acordo com a carteira em uso) e gerenciar um conjunto de endereços, acompanhando o valor total deles e realizando as operações de criar, assinar e enviar transações (RODRIGUES, 2016). As chaves privadas são conhecidas apenas pelo proprietário.

A carteira digital, possui o mesmo funcionamento de uma conta corrente utilizada em bancos, podendo enviar e receber valores em *Bitcoin*. Como afirma (LOURENÇO; VICENTE, 2018), no momento da movimentação da moeda, um registro é enviado ao *Blockchain*, onde armazena todas as transações feitas das moedas digitais.

4.4 O grau de segurança das criptomoedas através de sua criptografia assimétrica

Criptografia é uma codificação de qualquer informação armazenada num computador, onde essa informação só pode ser lida por quem detenha a senha da sua codificação. Ela possibilita que haja confidencialidade, autenticidade e integridade dos dados que circulam na rede (VICENTE, 2017). Dessa forma, os dados devem ser restritos e estar somente disponíveis para usuários autorizados. Para que os *Bitcoins* sejam transferidos de forma segura, a rede Bitcoin utiliza a criptografia assimétrica (NAKAMOTO, 2008). Na criptografia assimétrica há uma chave pública e privada.

Tais chaves são geradas aos pares, e é praticamente possível gerar uma das chaves tendo posse da outra. E quanto maior a quantidade de bits de uma chave, mais complexas são as chaves geradas e mais seguro é o processo que as utiliza.

A chave privada utilizada na carteira virtual do usuário deve ser mantida em segredo por ele e protegida preferencialmente por senha. Contudo, uma vez perdida, não há como recuperá-la, pois não tem como gerar uma chave privada a partir de uma chave pública (VICENTE, 2017).

4.5 Negócios e situações que estão aceitando negociar com criptomoedas

Moedas digitais como *Bitcoin* e *Bitcoin cash* podem ser usadas para pagamentos de bens e serviços sem barreiras de distância ou necessidade de validação por instituições financeiras. Eles também não são reembolsáveis, o que evita estornos, como seria o caso da carteira digital de pagamentos *PayPal* e outros meios de troca controlados centralmente. De acordo com (O TEMPO, 2020), existem algumas empresas que aceitam criptomoedas atualmente, que são:

1 - Paypal: o Bitcoin é aceito pelo *PayPal* como forma de pagamento. É executado através de processadores de pagamento como *GoCoin*, *Coinbase* e *BitPay*. Eles são uma das primeiras empresas a começar a aceitar criptomoedas como pagamento por transações concluídas através deles.

2 - Microsoft: foi uma das primeiras grandes empresas a aceitá-las como método de pagamento em 2014. Atualmente, permite comprar aplicativos para *Xbox* e *Windows* resgatando criptomoedas no *BitPay* (companhia fundada em 2011 que oferece soluções de pagamentos e recebimentos em Bitcoin).

3 - Tesla: a empresa de automóveis de sucesso já aceita Bitcoins como forma de pagamento. A empresa declarou que vários usuários compraram o Tesla Model S por meio dessas criptomoedas.

4 - Expedia: a popular agência de viagens online aceita pagamento por reservas de voos e hotéis via bitcoin, embora as transações feitas depois de iniciadas não possam ser canceladas.

5 - Wordpress: por alguns anos, essa plataforma para a construção de sites, blogs, portais e e-commerces (lojas virtuais) começou a aceitar criptomoedas para a compra de melhorias em seus planos e serviços.

6 - Overstock.com: é uma enorme empresa de varejo online que começou a aceitar bitcoin em 2014. Você pode comprar quase tudo, como *gadgets* (dispositivos eletrônicos) e móveis, entre muitas outras categorias. A Overstock também aceita outras criptomoedas como *Ethereum*, *Litecoin*, *Monero*, *Bitcoin Cash* e *Dash*.

5 CONSIDERAÇÕES FINAIS

Diante do exposto, foi possível entender que havia uma grande intervenção estatal no sistema financeiro, bem como não havia privacidade financeira (possibilidade de realizar transações de forma anônima) e essas foram as principais motivações que levaram a criação das criptomoedas. Também foi possível identificar e entender o funcionamento das principais tecnologias envolvidas na sua geração ou quando a mesma é transferida entre carteiras digitais. Por fim, foi possível perceber que vários tipos de negócios já aceitam o *Bitcoin* como moeda na venda dos seus produtos ou serviços.

O *Bitcoin* se apresenta como uma alternativa real às moedas convencionais que comumente utilizamos. Oferece segurança e anonimato quando utilizada e ainda ultrapassa as barreiras regionais que existem por não precisarem de validação por terceiros. Devido a esses fatores, tal criptomoeda está cada vez mais se mostrando significante para uma parcela maior da população mundial.

REFERÊNCIAS

REIS, Luis Filipe Gold Coelho de et al. **Criptomoedas: uma análise se as criptomoedas são o futuro do dinheiro.** Disponível em: https://www.acervodigital.ufpr.br/handle/1884/55424. Acesso em: 22 jun. 2020.

DE LUCENA, Antônio Unias; HENRIQUES, Marco Aurélio Amaral. **Estudo de arquiteturas dos blockchains de Bitcoin e Ethereum.** 2016. Disponível em: https://www.sps.fee.unicamp.br/sites/default/files/departamentos/dca/eadca/eadcaix/artigos/lucena_henriques.pdf. Acesso em: 22 jun. 2020.

ULRICH, Fernando. **Bitcoin-a moeda na era digital.** Journal, volume, v. 2, p. 239, 1892. Disponível em: https://fasam.edu.br/wp-content/uploads/2016/06/Bitcoin-A-Moeda-na-Era-Digital.pdf. Acesso em: 17 jul. 2020.

RODRIGUES, Elias Italiano. **Estudo sobre Bitcoin: escalabilidade da blockchain.** Disponível em: http://www.elias19r.com/files/cv/tcc1-monografia_7987251.pdf. Acesso em: 08 jul. 2020.

VICENTE, Rafael José. **A Criptomoeda Como Método Alternativo Para Realizar Transações Financeiras.** Maiêutica-Tecnologias da Informação, v. 2, n. 01, 2017. Disponível em: https://publicacao.uniasselvi.com.br/index.php/TI_EaD/article/view/1692/806. Acesso em: 08 jul. 2020.

PIRES, Timoteo Pimenta. **Tecnologia Blockchain e suas aplicações para provimento de transparência em transações eletrônicas.** 2016. Disponível em: https://www.bdm.unb.br/bitstream/10483/16252/1/2016_TimoteoPimentaPires_tcc.pdf. Acesso em: 24 jul. 2020.

NETO, Angelo Pisani; MATARAZZO, Gustavo. **BITCOIN, ETHEREUM E XRP: UMA ANÁLISE HISTÓRICA DAS CRIPTOMOEDAS E SUAS TECNOLOGIAS.** Revista Ciência em Evidência, v. 1, n. 1, p. 27-41, 2020. Disponível em: https://ojs.ifsp.edu.br/index.php/cienciaevidencia/article/view/1559/1033. Acesso em: 9 set. 2020.

OLIVEIRA, Francisco Cardozo; GIBRAN, Sandro Mansur; MORAES, Felipe Américo. **BITCOIN: O POTENCIAL DISRUPTIVOS DAS CRIPTOMOEDAS NA ECONOMIA.** Administração de Empresas em Revista, v. 2, n. 16, p. 64-85, 2020. Disponível em: http://revista.unicuritiba.edu.br/index.php/admrevista/article/view/4139/371372485. Acesso em: 14 set. 2020.

LOURENÇO, Tatiana; VICENTE, Joyce Cristina. Bitcoin: **A Moeda Digital que Constitui uma rede inovadora de Pagamentos.** 2018. Disponível em: http://repositorio.unifafibe.com.br:8080/xmlui/handle/123456789/81. Acesso em: 14 set. 2020.

NAKAMOTO, Satoshi. 2008. **Bitcoin: A Peer-to-Peer Electronic Cash System.** 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 15 set. 2020.

O TEMPO. **Pagamentos com criptomoeda agora são aceitos pelas principais marcas.** 2020. Disponível em: https://www.otempo.com.br/economia/pagamentos-com-criptomoeda-agora-sao-aceitos-pelas-principais-marcas-1.2311519. Acesso em: 21 set. 2020.

DINIZ, Eduardo Henrique. **Emerge uma nova tecnologia disruptiva.** GV EXECUTIVO, v. 16, n. 2, p. 46-50, 2017. Disponível em: http://bibliotecadigital.fgv.br/ojs/index.php/gvexecutivo/article/view/68676/66265. Acesso em: 24 set. 2020.

FOXBIT. **O que é descentralização: um passo rumo ao futuro**. 2020. Disponível em: https://foxbit.com.br/blog/o-que-e-descentralizacao-um-passo-rumo-ao-futuro/. Acesso em: 5 nov. 2020.

ADVFN. **Criptomoedas: História.** Disponível em: https://br.advfn.com/investimentos/criptomoedas/historia. Acesso em: 5 nov. 2020.