TCC: ARAGON, MATHEUS, 2018

Tema: CRIPTOMOEDA: UMA ANÁLISE DA UTILIZAÇÃO DO BITCOIN NA SOCIEDADE CONTEMPORÂNEA

Referencia bibliográfica: ARAGON, Matheus. **CRIPTOMOEDA: UMA ANÁLISE DA UTILIZAÇÃO DO BITCOIN NA SOCIEDADE CONTEMPORÂNEA.** Orientador: Prof. Mari Néia Valicheski Ferrari, Ma. 2018. 54 f. TCC (Graduação) - Curso de Gestão da Tecnologia da Informação, INSTITUTO FEDERAL DE SANTA CATARINA, Florianópolis, 2018. Disponível em: https://repositorio.ifsc.edu.br/bitstream/handle/123456789/394/TCC%20%20Matheus%20Aragon.pdf?sequence=1&isAllowed=y. acesso em: 20 abr. 2023.

Pontos principais

|  |  |  |
| --- | --- | --- |
| Pagina | Texto | Comentário |
| 15 | Segundo Nakamoto (2008), em seu artigo intitulado “Bitcoin: A Peer-to-Peer Electronic Cash System”, o Bitcoin é uma moeda virtual e descentralizada, ou seja, não é uma moeda física e nem controlada por nenhum banco central.  O Bitcoin é produzido de forma descentralizada por milhares de computadores, mantidos por empresas que fornecem a capacidade de suas máquinas para a criação do Bitcoin e validação de transações, em um processo chamado de mineração (ANTONOPOULOS, 2014). A rede Bitcoin utiliza a arquitetura de redes de computadores peer-to-peer, na qual cada um dos nós da rede funciona tanto como cliente tanto quanto servidor. Para proteger a rede Bitcoin, é utilizado o protocolo PoW[1] (Proof-of-work), que previne a rede de ataques cibernéticos. O Bitcoin utiliza ainda a tecnologia Blockchain, um sistema de banco de dados distribuído. (NAKAMOTO, 2008) |  |
| 16 | Devido à sua alta volatilidade, o Bitcoin passou a ser frequentemente classificado como um ativo financeiro, o que se afasta de seu propósito original, que era de atuar como moeda de troca em transações econômicas. Além disso, ainda causa incertezas acerca da sua empregabilidade e se seu uso é vantajoso frente aos meios de pagamentos tradicionais. |  |
| 17 | Essa alta valorização do Bitcoin chamou a atenção da mídia e de algumas grandes empresas, como a Dell e a PayPal, que passaram a aceitá-lo como meio de pagamento. De acordo com o site coinmap (coinmap.org, 2018), mais de 13.000 locais já o aceitam como meio de pagamento  Devido à grande popularização da moeda, alguns países já reconhecem o Bitcoin como meio de pagamento legítimo, como por exemplo a Alemanha, onde as pessoas podem utilizar o bitcoin2 para realizar suas transações sem pagar impostos |  |
| 21 | De acordo com Hubbard e O’Brien (2010), “a definição econômica de moeda é qualquer ativo que as pessoas estão dispostas a aceitar em troca de bens e serviços ou pelo pagamento de dívidas”.  A moeda possui 3 funções básicas, sendo elas: meio de troca, unidade de conta e reserva de valor. (NUNES, 2016).  A moeda como meio de troca representa a sua capacidade de ser utilizada como meio de pagamento para a compra de bens ou serviços. (NUNES, 2016). Como exemplifica Hubbard e O’Brien (2010), “quando o supermercado local aceita sua nota de US$5 em troca de pão e leite, a nota de US$5 está servindo como um meio de troca comercial”.  A função de unidade de conta se refere ao fato da moeda fornecer um padrão para que as mercadorias sejam cotadas no mercado, ou seja, ser o instrumento pelo qual os valores das mercadorias são medidos. (NUNES, 2016). Segundo Hubbard e O’Brien (2010), esta função traz benefício, pois “reduz a necessidade de cotar muitos preços diferentes no comércio”.  A função de reserva de valor se refere à possibilidade da moeda ser guardada de forma a transferir a capacidade de compra para o futuro, ou seja, permitir que o poder de compra se mantenha com o tempo. (NUNES, 2016). Além disto, a reserva de valor é uma forma de se medir a riqueza. (HUBBARD E O’BRIEN, 2010). |  |
| 22 | O Bitcoin é a primeira moeda digital descentralizada do mundo, criada por Satoshi Nakamoto. Ela teve seu White Paper3 publicado em um fórum em 2008, com seu lançamento em código aberto para o público em geral em janeiro de 2009. Ela é produzida por milhares de computadores, mantidos por pessoas que emprestam a capacidade de suas máquinas para criar bitcoins e registrar todas as transações feitas, em um processo conhecido por mineração (NAKAMOTO, 2008). Para proteger as transações realizadas na rede Bitcoin, é utilizada criptografia assimétrica, que funciona com o esquema de chaves públicas e privadas de Whitfield Diffie e Martin Hellman, que permite a autenticidade, privacidade e integridade da rede. (NAKAMOTO, 2018)  Todas as transações que ocorrem no Bitcoin são registradas em uma espécie de livro caixa público e distribuído chamado de Blockchain (corrente de blocos), o que nada mais é do que um grande banco de dados público, contendo o histórico de todas as transações relacionadas. (ULRICH, 2014).  Além do processo de mineração, é possível adquirir bitcoins comprando-os de corretoras. Os bitcoins ficam armazenados em uma espécie de carteira, que pode ser física ou virtual, |  |
| 23 | O processo de “nascimento” do bitcoin é chamado de mineração. Este é um processo em que os computadores mineradores conectados à rede Bitcoin competem entre si para resolver cálculos matemáticos. Quem ganha, valida um bloco de transações na rede e recebe uma fração da moeda que foi criada no processo. O nível é ajustado pela rede, para que a moeda consiga cumprir o plano de expansão que lhe foi atribuída, que é de ter 21 milhões de unidades até 2140 (ULRICH, 2014).  (...)  Quanto mais bitcoins são criados pelo processo de mineração, mais difícil fica sua criação, ou seja, mais cálculos os computadores da rede precisam realizar antes de processar um bloco de bitcoins. Ulrich (2014), faz um paralelo entre a mineração e os números primos, uma vez que é relativamente fácil achar os menores, porém a medida em que são encontrados, fica mais difícil de encontrar os maiores |  |
| 24 | Uma vez que o último bitcoin for minerado, os mineradores serão recompensados com taxas de serviço, em vez de novos bitcoins. Isso garante que os mineradores ainda tenham um incentivo de manter a rede operando após a extração do último bitcoin. (ULRICH, 2014)  A atividade de mineração atingiu a marca total de 29,05 TWh[3] (Terawatt-hora) gastos em novembro de 2017, o que representa 0,13% de toda a energia consumida no mundo. No último ano, essa atividade gastou cerca de US$ 1,5 bilhão em eletricidade. (DIGICONOMIST, 2017).  Bitcoin, uma vez que o fato de ser uma moeda intangível e desregulamentada gera desconfiança sobre a criptomoeda. (PROOF, 2018) |  |
| 25 | A tecnologia Blockchain surgiu junto com o Bitcoin, em 2008. O Blockchain foi pensado como uma forma segura para se transferir bitcoins e trazer confiabilidade à rede |  |
| 26 | A tecnologia Blockchain têm como principais propriedades a descentralização, uma vez que dispensa a necessidade de uma terceira parte para fazer a transação; a integridade, pois todos os conjuntos de dados são replicados em diferentes pontos da rede de maneira segura; e a transparência, visto que todas as transações registradas na blockchain são públicas. (SAMPAIO, et al., 2018).  Segundo Pereira (2016), a criptografia é um conjunto de técnicas empregadas para cifrar mensagens, as quais são decifradas por meio de uma chave. Desta forma, somente emissor e emissário conseguem ter acesso ao conteúdo enviado, enquanto que terceiros apenas conseguem visualizar códigos aleatórios sem conseguir extrair nada daquilo.  Para que os bitcoins sejam transferidos de forma segura, a rede Bitcoin utiliza a criptografia assimétrica. (NAKAMOTO, 2008). A diferença entre criptografia simétrica e assimétrica é que na simétrica os algoritmos simétricos de uma chave (um pedaço de informação que controla a operação de um algoritmo) são usados tanto para criptografar quanto para descriptografar, enquanto que na criptografia assimétrica há duas chaves, sendo uma a chave pública, para encriptar as mensagens, e a privada, para desencriptar. As chaves são completamente independentes uma das outras. (ANTONOPOULOS, 2014) |  |
| 27 | O princípio central do Bitcoin é a descentralização, e isto tem suas implicações na segurança. Em um modelo centralizado, como um banco tradicional, a responsabilidade do sistema é do próprio banco, diferentemente de um sistema descentralizado como o Bitcoin, onde esta responsabilidade é de todos os usuários finais. (ANTONOPOULOS, 2014). |  |
| 28 | Para receber, armazenar, proteger e gastar bitcoins é necessário possuir uma espécie de carteira. Esta carteira é meramente um aplicativo, site ou dispositivo que contém uma chave privada que permite acessar o endereço onde os bitcoins do usuário estão guardados (TUWINER, 2018). As principais carteiras de bitcoins são a carteira de hardware e a carteira online.  Uma carteira de hardware é um dispositivo físico eletrônico, desenvolvido com o propósito de proteger bitcoins. Para que os bitcoins destas carteiras possam ser gastos, eles precisam estar conectados ao computador, telefone ou tablete. Carteiras de hardware mantém as chaves privadas em um ambiente off-line, sendo desta maneira protegidas de malwares e cibercriminosos. Para ter acesso a carteira de hardware, seria necessário roubar a carteira em si. (TUWINER, 2018)  Já as carteiras web armazenam as chaves privadas online, onde a carteira é criptografada por uma senha escolhida pelo usuário. Pelo fato de ser online, ela possui um menor nível de segurança quando comparado com as carteiras de hardware. (TUWINER, 2018) |  |
| 29 | O modelo bancário tradicional atinge um nível de privacidade ao limitar o acesso à informação ao partes envolvidas e o terceiro de confiança. A necessidade de anunciar publicamente todas as transações da rede Bitcoin exclui esse método, mas a privacidade ainda pode ser mantida quebrando-se o fluxo de informações de outro modo: mantendo as chaves públicas anônimas. O público pode ver que alguém está enviando uma quantia para outra pessoa, mas sem informações que vinculem a transação a qualquer pessoa. Isto é semelhante ao nível de informação divulgado pelas bolsas de valores, em que o tempo e o tamanho dos negócios individuais, a operação, é tornada pública, mas sem dizer quem eram as partes (NAKAMOTO, 2018  (...)  De acordo com Nakamoto (2008), o problema do modelo de privacidade do Bitcoin é que, caso o dono de uma chave seja descoberto de alguma forma, é possível verificar todas as transações que este usuário realizou na rede.  Para acessar os bitcoins guardados em uma carteira digital, é necessário possuir uma chave, uma sequência de caracteres aleatórios (KELLY, 2015). Se esta chave for perdida ou roubada, não é possível de forma alguma recuperar os bitcoins. |  |
| 33 | Devido à forma como o algoritmo da rede Bitcoin funciona, onde, quanto mais bitcoins são minerados, mais difícil fica minerá-los, esta atividade está praticamente restrita a grandes empresas de mineração (KELLY, 2017). Atualmente, o modo mais fácil de comprar/vender bitcoins são através de corretoras de bitcoin.  Devido à forma como o algoritmo da rede Bitcoin funciona, onde, quanto mais bitcoins são minerados, mais difícil fica minerá-los, esta atividade está praticamente restrita a grandes empresas de mineração (KELLY, 2017). Atualmente, o modo mais fácil de comprar/vender bitcoins são através de corretoras de bitcoin. |  |
| 39 | No Brasil, não há nenhuma lei especifica sobre moedas virtuais. Porém, há um projeto de lei de 2015 (PL[7] 2303/2015) do deputado Aureo, que defende a regulamentação das criptomoedas. O projeto está, atualmente, sendo avaliado por uma comissão especial. (R7, 2017) Apesar do Bitcoin não possuir nenhum amparo jurídico específico até o presente momento, o posicionamento oficial do governo é de que é preciso declará-lo no imposto de renda, uma vez que, por regra, pessoas físicas precisam declarar todos os bens e direitos acima de R$ 1 mil. (EPOCA, 2018). Além disso, a CVM[8] proibiu a compra de criptomoedas por fundos de investimentos, afirmando que tais criptomoedas não podem ser qualificadas como ativos financeiros. (ESTADAO, 2018). |  |
| 42 | Em relação às suas propriedades, o bitcoin apresenta algumas vantagens em relação a padrões monetários, como o ouro e o papel-moeda. No quesito durabilidade, o bitcoin supera tanto o ouro quanto o papel-moeda. Por ser uma moeda digital, o bitcoin não sofre alteração espacial ou temporal. (ULRICH, 2014). Sobre a divisibilidade, o bitcoin possui, atualmente, 8 casas decimais (NAKAMOTO, 2008), possuindo uma divisibilidade muito maior do que o papel-moeda e o ouro. Em relação a maleabilidade, pelo fato do bitcoin ser algo intangível, esta propriedade não se aplica a ele, enquanto que o ouro é o elemento conhecido mais maleável. (ULRICH, 2014). O bitcoin apresenta homogeneidade matemática (por definição), sendo praticamente impossível de falsificá-lo, enquanto que o ouro depende de averiguações para comprovar sua pureza. O papel-moeda, apesar de homogêneo, pode ser mais facilmente falsificado. (ULRICH, 2014). Em relação a oferta, o bitcoin é limitado ao número de 21 milhões de unidades (BLOCKCHAIN, 2018), enquanto que o ouro tem uma limitação pela natureza. Já o papel-moeda é ilimitado, embora tenha sua fabricação controlada pelo governo. Criado justamente para eliminar a necessidade de uma terceira parte, o bitcoin não tem dependência de terceiros fiduciários (NAKAMOTO, 2008), como é o caso do papel-moeda e do ouro, que jamais poderiam eliminar terceiros fiduciários. (ULRICH, 2014) (...) Levando-se em conta a comparação de propriedades entre o bitcoin, ouro e o papel-moeda, pode-se dizer que o bitcoin é superior aos outros dois |  |
| 44 | e o bitcoin realiza esta função(Meio de Troca), embora com muito menor liquidez quando comparado com moedas correntes locais. Neste último ano |  |
| 45 | O principal obstáculo para que o bitcoin possa realizar esta função (Unidade de conta) é sua alta volatilidade.  Embora o bitcoin não sirva atualmente como unidade de conta, não é impossível que no futuro ele possa vir a realizar esta função. Isto dependerá de alguns fatores, como a sua regulamentação ao redor do mundo, a atenuação de sua volatilidade e a ampliação de seu uso. (ULRICH, 2014). |  |
| 46 | Ainda que desperte inseguranças, o bitcoin cumpre a função de reserva de valor, a longo prazo. A |  |
| 48 | apesar do bitcoin ter sido criado por Satoshi Nakamoto com a ideia de facilitar as pequenas transações, atualmente ele não é adequado para este fim, visto que a taxa de transação está por volta de US$3, ocasionando sua pouca utilização em transferências de pequeno porte quando comparado a outros meios de pagamentos.  o Bitcoin atua como meio de troca e reserva de valor, porém não é reconhecido como unidade de conta. | Conclusão |