SEGURANÇA DA MOEDA DIGITAL BITCOIN

Jeferson Schommer Scarton[1], Fagno Alves Fonseca[2], Mauro Henrique Lima de Boni[2]

[1]Acadêmico do curso de Sistemas para Internet - IFTO - Campus Palmas. e-mail: jscarton3108@gmail.com
[2]Professor do curso de Sistemas para Internet - IFTO - Campus Palmas. e-mail: fagno.fonseca@ifto.edu.br, mauro@ifto.edu.br

Resumo: Diante do surgimento da moeda digital Bitcoin, vários questionamentos sobre sua integridade são postos à frente de sua proposta em ser uma criptomoeda descentralizada. Com o propósito de analisar sua viabilidade e solidez perante as formas de pagamento mais amplamente utilizadas, este trabalho apresenta uma revisão narrativa dos seus aspectos de segurança, de modo que, seja possível compreender e conhecer seu funcionamento. Os resultados obtidos demonstram que o uso correto e dentro dos protocolos propostos pela moeda, pode trazer benefícios que outros meios de pagamento não disponibilizam.
Palavras–chave: bitcoin, criptomoeda, moeda digital, segurança

1. INTRODUÇÃO

A busca por tecnologias e o uso da internet vem aumentando todos os anos (ITU, 2016). A fim de proteger os dados na rede e a privacidade das pessoas, surgiu em meados do ano de 1993 o manifesto Cypherpunk (HUGHES, 1993), uma carta escrita por Eric Hughes onde fala principalmente da privacidade e da criptografia para haver uma sociedade aberta na era eletrônica. Em um trecho de sua carta, Hughes cita a importância de se ter transações anônimas e da garantia de que cada parte tenha conhecimento apenas do necessário para realizar a mesma.

A partir dessa premissa programadores do mundo todo começaram suas tentativas de desenvolver uma moeda eletrônica capaz de conceder anonimato aos usuários através de criptografia. Em 2008 um grupo de pessoas utilizando um pseudônimo conhecido como Satoshi Nakamoto (NAKAMOTO, 2008) fez um primeiro anúncio de que estava trabalhando em uma criptomoeda, uma moeda virtual baseada em criptografia e capaz de ter seu funcionamento de maneira descentralizada e sem a necessidade de um intermediário para realizar as transações. Às 18h15 do dia 3 de janeiro de 2009, nascia oficialmente o Bitcoin, 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, ou seja, totalmente descentralizado, pois antes do seu surgimento toda transação realizada pela internet utilizava um terceiro, como um banco, financeira, operadora de cartões entre outras que atuam na área (ULRICH, 2014).

Após sua criação poucos adeptos a tecnologia utilizavam a moeda digital. Os maiores utilizadores eram os desenvolvedores e entusiastas. Assim a moeda continuou sua luta pelo crescimento. Na passagem dos anos de 2011 e 2012, o Bitcoin se manteve como um grande ativo especulativo, porém com o crescente numero de membros em sua comunidade e adeptos no ano de 2013, após fatores como crise política, econômica e grande ajuda da mídia tecnológica, o Bitcoin teve ascensão ganhando atenção de instituições financeiras, fundos de investimento e até mesmo de governos. Porém, com a crescente busca dessa moeda digital ao final de 2013 e inicio de 2014, houve uma série de ataques a sites de carteiras digitais e casas de cambio da moeda (POPPER, 2015), na qual, foram relatados em vários jornais digitais como *The New York Times* e BBC Brasil, que trouxe a tona questionamentos sobre sua segurança.

Diante de tais fatos e questionamentos sobre sua segurança, objetivamos com esta pesquisa responder ao seguinte problema: O Bitcoin é seguro a ponto de ser viável como um meio concorrente às formas de pagamento mais utilizadas atualmente? Dessa forma, este trabalho apresenta informações quanto aos seus aspectos de segurança, de modo que, seja possível compreender e conhecer seu funcionamento, e entender os principais conceitos que envolvem sua criação.

A seguir, este artigo está estruturado nas seguintes seções: 2)Material e Métodos, 3)Criptomoeda Bitcoin, subdividido em 3.1)Bloco, 3.2)Blockchain, 3.3)Prova de Trabalho, 3.4)Mineração, 3.5)Carteiras Digitais, 4)Segurança do Bitcoin, 5)Resultados e Discussão 6)Conclusões.

2. MATERIAL E MÉTODOS

Esta pesquisa trata-se de uma revisão narrativa, a qual tem intenção de descrever o desenvolvimento e o estado da arte quanto ao tema abordado, permitindo adquirir conhecimento de forma rápida com um baixo custo de tempo (ROTHER, 2007). Quanto às fontes de dados, não são pré-determinadas e especificas sendo mais abrangentes e deixando a escolha sujeita a perspectiva do pesquisador (CORDEIRO, OLIVEIRA, *et al.*, 2007). Neste sentido, buscou-se identificar na literatura, os principais estudos realizados quanto ao tema em questão desde a sua criação, abordando os principais riscos e vulnerabilidades.

Cabe ainda observar que distinto de uma revisão sistemática não é abordado alguma falha específica, assim reunindo trabalhos a cerca desta, mas sim a agregação de dados a respeito dos principais ataques e acontecimentos que colocaram em duvida a integridade da moeda durante toda a passagem de tempo entre sua criação e os dias atuais.

3. CRIPTOMOEDA BITCOIN

A criptomoeda Bitcoin é algo diferente do que estamos acostumados com a moeda comum. Uma carteira Bitcoin contendo suas moedas digitais pode ser simplesmente copiada como qualquer arquivo digital, bem como pode ter um backup. Com isso devemos pensar em segurança de maneira diferente, pois diferencia dos meios de pagamentos que estamos habituados a utilizar (ANTONOPOULOS, 2014).

A segurança é o estado de estar seguro, isto é, ter proteção contra aqueles que desejam o mal de forma intencional ou não (WHITMAN e MATTORD, 2011). Na esfera da segurança da informação, seria garantir a confidencialidade e integridade das informações de forma que apenas o proprietário tenha acesso.

Tendo em conta tal definição de segurança podemos confrontar sua aplicação ao Bitcoin, mas antes de iniciar é preciso entender alguns conceitos de termos e tecnologias usadas pela criptomoeda de modo a facilitar o entendimento no decorrer do estudo.

3.1 BLOCO

O bloco é o agrupamento de transações, cada bloco contém um carimbo de tempo e uma assinatura do bloco anterior. Seu cabeçalho engloba um hash, ou seja, uma sequencia de bits utilizados para realizar um calculo que prova sua originalidade, desta forma tendo uma prova de trabalho, validando assim as transações. Depois de validado o bloco é adicionado a blockchain principal (ANTONOPOULOS, 2014).

3.2 BLOCKCHAIN

A blockchain é onde fica armazenada toda a contabilidade do Bitcoin, de forma publica. Ela é composta pelos blocos adicionados pelos mineiros. A blockchain detém todas as informações de forma completa, sobre endereços e saldos desde o bloco gênese até o bloco mais recente, organizados de forma cronológica (SWAN, 2015).

Todos os mineiros tem uma copia da blockchain, assim que um novo bloco é validado bem como adicionado ao livro caixa (assim também conhecido), ele é atualizado para todos os nós da rede a fim de que tenham conhecimento, adotando assim a blockchain que contêm o maior número de blocos.

3.3 PROVA DE TRABALHO

A prova de trabalho é um problema matemático dado pelo algoritmo SHA256 (GILBERT e HANDSCHUH, 2004) que é distribuído na rede Bitcoin, a fim de que os mineiros possam encontrar a solução (ANTONOPOULOS, 2014). Ao decifrar o problema o mineiro gera um novo bloco. A dificuldade da prova de trabalho é ajustada a cada 2016 blocos a fim de que seja gerado em média um bloco a cada dez minutos.

3.4 MINERAÇÃO

A segurança do Bitcoin é garantida pela prova de trabalho, resolvida por uma rede organizada, onde os participantes são conhecidos como mineiros (EYAL e SIRER, 2013). Cada mineiro é responsável por manter a rede Bitcoin e a blockchain. A participação requer poder de processamento que é calculado em taxa de hash, que é a capacidade de realizar cálculos por segundo. Para incentivar o mineiro são dadas recompensas em Bitcoins a cada transação validada, porém quando ele soluciona uma prova de trabalho criando assim um novo bloco, ganha novos Bitcoins que são gerados junto com a descoberta. Sendo assim, o processo de criação de blocos é denominado mineração e os participantes mineiros (EYAL, 2015).

A gratificação por originar um novo bloco se iniciou com 50 Bitcoins e a cada 210.000 blocos (aproximadamente quatro anos) ela é reduzida pela metade, em 2012 foi reduzida para 25 Bitcoins (ANTONOPOULOS, 2014), e atualmente a prova de trabalho gratifica o mineiro com 12,5 Bitcoins a cada bloco gerado. Atingindo desta maneira no ano de 2140 a geração do último Bitcoin, finalizando assim com um total de 21 milhões de Bitcoins gerados.

3.5 CARTEIRAS DIGITAIS

Wallets ou carteiras digitais são softwares responsáveis por armazenar as chaves das moedas de propriedade do utilizador (ANTONOPOULOS, 2014). Fazem-se necessárias para realizar

transações na rede Bitcoin. Existem vários modelos para as diferentes plataformas de sistemas e dispositivos. A comunidade Bitcoin recomenda algumas exibindo suas principais características, juntamente está o manual de boas praticas, mas cabe ao usuário definir qual atende melhor as suas necessidades (BITCOIN, 2016).

4. SEGURANÇA DO BITCOIN

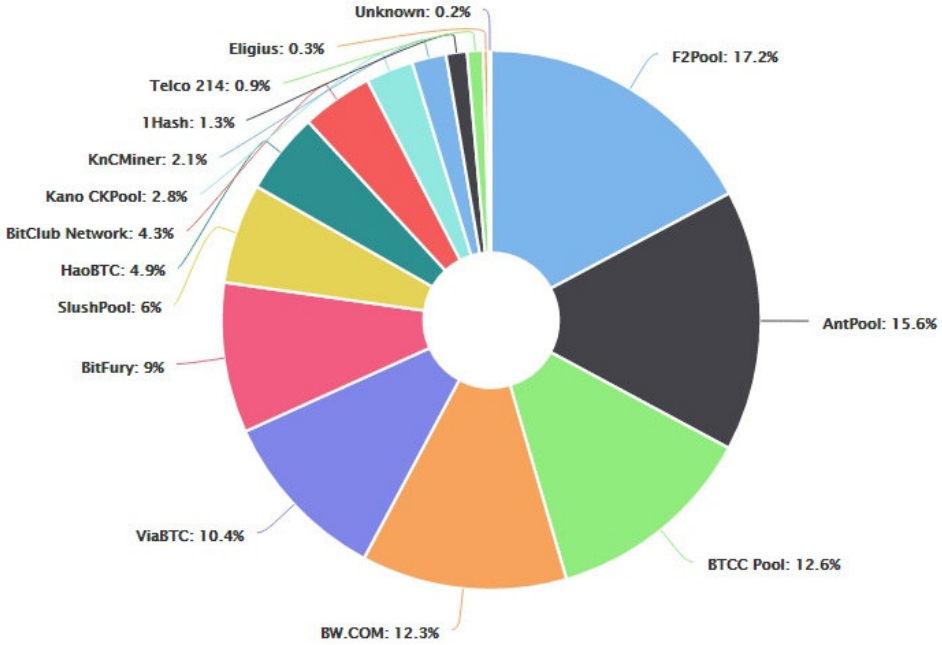
Desde seu lançamento até os presentes dias, Satoshi afirmou que o Bitcoin teria problema se o poder de processamento de algum ataque ou minerador mal intencionado obtivesse mais de 50% de toda a rede (BITCOIN, 2016). Durante seu inicio nos anos de 2009 e 2010 a preocupação de Satoshi era muito grande devido a taxa de hash da rede ser pequena, um ataque de força bruta seria facilmente prejudicial à rede, porém no início a moeda não despertou muita atenção, isso fez com que a rede se mantivesse e seus dados permanecessem íntegros (POPPER, 2015).

Em 2010 Laszlo Hanecz, um engenheiro de software, resolveu testar pela primeira vez a robustez da rede Bitcoin, tentou quebrar o sistema adquirindo mais de 50% do poder de processamento da rede. Com isso ele descobriu que a GPU - processador Gráfico do computador era muito melhor para realizar as provas de trabalho que a unidade central de processamento do computador - CPU. Porém ele percebeu que com a obtenção da maior parte das moedas elas perderiam o valor. Após ele trocar alguns e-mails com Satoshi se tornou um ajudante no projeto da moeda digital (POPPER, 2015).

Conseguinte em 2011, a supremacia dos ataques se conteve a casas de cambio da moeda e empresas de Bitcoin, que de alguma forma armazenavam os Bitcoins de seus clientes. Uma ênfase é dada a Mt. Gox uma casa de cambio da moeda digital que detinha a maior parte das transações. Em um desses ataques um hacker conseguiu acesso às carteiras dos clientes, transferindo os Bitcoins para uma carteira de sua propriedade. Como o limite de transferência de cada cliente era de mil dólares, ele começou vender grandes quantidades de Bitcon a preços bem inferiores do praticado pelo mercado, isso fez o valor do Bitcoin cair rapidamente, assim ele realizou maiores retiradas de Bitcoins das carteiras dos clientes da Mt. Gox (POPPER, 2015).

Com o crescente numero de adeptos ao Bitcoin, nos anos de 2011 e 2012 a mineração foi se tornando algo difícil, pois ao passo que aumentava a quantidade de mineiros a dificuldade era ajustada, diminuindo a probabilidade de minerar um novo bloco. Assim começou a formar-se grupos de mineração denominados *pools* de mineração, onde vários colaboradores unem seus poderes de processamento a fim de conseguir minerar novos blocos, no qual a recompensa é dividida de acordo a taxa de hash de cada integrante. Atualmente diferentes *pools* detêm a maior parte do poder de processamento do Bitcoin como visto na Figura 1.

Figura 1- Porcentagem do poder de processamento em hash dos *pools*



Fonte: Blockchain info (BLOCKCHAIN, 2016)

Utilizando-se desta tática a renda de cada mineiro é estável e continua, pois colocar-se a minerar sozinho traria um baixo rendimento, podendo atingir apenas um bloco por ano (CHAUDHARY, FEHNKER, *et al.*, 2015).

Perante 2013 foi afirmado que não seria necessário 1/2 do poder de processamento da rede Bitcoin e sim que com apenas 1/4, ou seja, 25% se conseguiria atingir a blockchain com um ataque chamado mineração egoísta. Este estudo diz que um *pool* de mineradores com intenção de atacar consegue minerar um novo bloco, porém não disponibiliza para o restante da rede, tentado assim criar uma bifurcação, onde sua ramificação é a maior. Tendo em mão uma blockchain maior ela usaria para validar transações com gasto duplo, ou seja, gastando a mesma moeda várias vezes, logo após disponibilizaria para o restante da rede, fazendo com que os mineiros adotem como sendo a blockchain correta (EYAL e SIRER, 2013).

Ao final do ano de 2013 o Bitcoin atingiu o maior valor já registrado pela moeda, mais de mil dólares por unidade de Bitcoin, isso desencadeou um brusco aumento de contas e usuários, da mesma forma um crescente fluxo nas casas de cambio. A vista disso no inicio de 2014 a casa de cambio Mt. Gox novamente foi alvo de ataques de hackers. Eles exploraram uma falha nos identificadores de transações, alterando os destinos das moedas para carteiras diferentes das originalmente indicadas. Este fato gerou o maior desastre envolvendo Bitcoins até o presente, cerca de 400 milhões de dólares em Bitcoins simplesmente sumiram (POPPER, 2015).

O crescimento dos *pools* de mineração também trouxeram problemas para o Bitcoin, em 2014 um deles conhecido como GHash.IO atingiu cerca de 50% de todo poder de processamento da rede Bitcoin. Nada de errado foi feito, porém com todo esse poder GHash.IO poderia

simplesmente realizar uma venda de Bitcoins, e ao ter em posse uma blockchain maior que a correta publica-la, por conseguinte anulando a venda e ficando com os Bitcoins e o valor de venda (EYAL, 2015).

Outra fissura conhecida como bloco de sabotagem envolve *pools* de mineração. Nessa situação um *pool* **A** para prejudicar *pool* **B** coloca um minerador infiltrado, assim se esse minerador conseguir a solução da prova de trabalho ele não revela a **B**, prejudicando assim os lucros de todos os membros e dando mais chances de **A** encontrar a solução e ganhar a recompensa (EYAL, 2015).

As crises políticas e o monopólio do governo sobre o dinheiro em alguns países fez o interesse por utilizar o Bitcoin aumentar, alguns governos proíbem o acesso à moeda digital (ULRICH, 2014), porém o uso do Bitcoin é alcançado muitas vezes pelo navegador Tor. Um projeto de servidores voluntários que permite uma privacidade maior de navegação através de tuneis sem identificação (TOR, 2016). Mas o uso do Tor acabou deixando uma brecha. Foi explorada uma regra do Bitcoin, onde permite oito conexões de saída com outros nós da rede. Através de algumas técnicas um atacante consegue isolar um nó honesto da rede, passando a controlar suas transações (BIRYUKOV e PUSTOGAROV, 2015).

Atualmente devido ao alto custo de eletricidade e a necessidade de hardware especifico para mineração, muitos mineiros estão migrando para mineração nas nuvens. Um mineiro aluga ou arrenda o poder de processamento em hash de empresas especializadas em mineração, pagando com Bitcoins, tendo a intenção de obter lucro depois de algum tempo (KRISHNAN, SAKETH e TEJ, 2015). Porém alguns sites de mineradoras após um tempo em funcionamento simplesmente ficam *offline*, deixando seus mineiros com o prejuízo. Foi o que aconteceu em 2016 com a mineradora em nuvem Hashocean, que deixou aproximadamente 700.000 assinantes sem notícias e com a perda de seus Bitcoins investidos (OGUNDEJI, 2016).

Apesar das passagens citadas, levar em consideração os mecanismos que o Bitcoin adota para solução de problemas e bloqueio de falhas é de grande valia. Bitcoin tem uma política de código fonte aberto, onde qualquer pessoa pode ajudar no seu desenvolvimento assim como na manutenção, bastando apenas se cadastrar e seguir regras proposta pela comunidade (BITCOIN, 2016). Uma dessas políticas adotadas é conhecida como BIP (*Bitcoin Improvement Proposal*), ou seja, proposta de melhoria Bitcoin, com essa metodologia qualquer um pode propor melhorias para a moeda a fim de ajudar a comunidade, basta apenas seguir métricas definidas e enviar a proposta, caso seja de grande importância será aceita, e o autor será citado nesse BIP. Atualmente no diretório de desenvolvimento do núcleo Bitcoin consta 152 BIP's documentados (BITCOIN, 2016).

Existem também mecanismos de envio de falhas, assim como canais de notícias, que são atualizados com qualquer problema ocorrido no Bitcoin. Um exemplo é a bifurcação de 2015 que lá esta documentada, juntamente com o motivo, medidas a serem tomadas pelos usuários e quais atitudes foram executadas para solucionar o problema (BITCOIN, 2015).

5. RESULTADOS E DISCUSSÃO

Este estudo limita-se em destacar os principais fatos sobre a segurança da moeda digital Bitcoin, como forma objetiva de avaliar a integridade do mesmo, respondendo algumas duvidas e contribuindo com a ponderação e uso de novos adeptos a essa tecnologia.

Os estudos foram unanimes, mostram que os ataques concentram-se principalmente sobre os softwares utilizados pelos clientes, seja para gerencia suas moedas, ou para investir. O foco é onde se centraliza grandes quantidades de usuários e moedas, a fim de conseguir um roubo de grande parte delas. Também mostram a exploração de uma possível bifurcação da blockchain utilizando-se de algumas estratégias a fim de alcançar duplicidade de gastos sem a percepção do restante da rede.

Cabe observar que a grande maioria das vitimas culpou a Mt. Gox, em razão que não havia nada de errado com o protocolo Bitcon (POPPER, 2015). A literatura aponta que nos principais ataques as casas de cambio, os utilizadores desses serviços tinham consciência de que o problema estava no gerenciamento de suas moedas e não de fato no código do Bitcoin. Quanto aos ataques a blockchain, todos têm foco de alterar algum bloco a fim de conseguir realizar gastos duplos.

Em relação aos ataques, ambos têm a finalidade de conseguir de forma ilícita moedas de outros, com o propósito de obter enriquecimento pessoal, não objetivando acabar com o sistema Bitcoin, pois assim de nada valeria as moedas usurpadas, e seus esforços seriam em vão. Em nenhuma das tentativas de fraude fica evidenciado o interesse e a possibilidade de dizimar o sistema Bitcoin.

Desse modo, podemos afirmar que na avaliação da segurança do Bitcoin, devem ser enfatizados aspectos relacionados aos ataques. Pois os desejos são de obter Bitcoins de forma contraria do proposto pelos protocolos da moeda digital. E que indiferente do ataque, nenhum deles tem como objetivo extinguir o projeto da moeda digital, já que com isso ele não obteria lucro algum. Diante de tais fatos, correções e prevenções podem ser sugeridas e desenvolvidas, com intuito de minimizar tais acontecimentos e corrigir possíveis falhas.

Embora alguns prejuízos possam ser contabilizados, seja por ataques ou uso de maneira inexata a sua proposta, o Bitcoin pode ser largamente utilizado, fato que nos direciona a incentivar o seu uso, com vistas em suas características únicas e particulares tais como a descentralização.

6. CONCLUSÕES

Conclui-se que a moeda digital Bitcoin pode garantir segurança na sua utilização, desde que seguidas às recomendações propostas por seus protocolos. Falhas são suscetíveis assim como em qualquer outro sistema de moeda ou forma de pagamento mais amplamente utilizada. As principais falhas aqui citadas estão relacionadas ao agrupamento de informações, seja por uso de softwares de investimento ou gerenciamento de moedas digitais, ou pelo agrupamento de mineradores, ferindo assim um dos principais conceitos do Bitcoin, a descentralização.

O uso da moeda sem seu devido conhecimento também pode acarretar perdas, pois a simples escolha de uma carteira digital não confiável pode fazer toda a diferença na utilização e na experiência de uso do Bitcoin. Desafios de segurança específicos de uma moeda digital também são encontrados, sendo comparada a um arquivo digital, uma pessoa simplesmente pode apagar seus Bitcoins sem querer, e como consequência perdê-los (ULRICH, 2014). Seu correto

armazenamento é de notável importância já que armazenar de forma incorreta também poderia promover o roubo das moedas por softwares maliciosos.

A criptomoeda Bitcoin adota boas técnicas de prevenção e correção de erros. Com a crescente quantidade de usuários, a busca pela estabilidade desta é de grande interesse e valia para todos, pois sua falha causaria grandes prejuízos. O uso consciente do Bitcoin pode trazer muitos benefícios, tal como realizar transferência de valores entre dois pontos distintos no globo, já que com acesso a internet é possível a qualquer momento efetuar uma transação de forma imediata. Isto posta, todos ganham com redução de taxas hoje pagas a terceiros, que cobram por uma necessária intermediação para realizar transações como compra e venda.

Mesmo sem ter esgotado as fontes de pesquisa foi possível abordar sobre os principais desafios encontrados pela moeda digital Bitcoin durante esses mais de sete anos que esta em circulação. Nesse escopo foi apontado como ela reage e se mantém até o presente trabalho. Diante de tais informações fica aberto a possibilidade de novos estudos sobre a centralização e descentralização que podem ocorrer na moeda digital Bitcoin. Pois diante dos fatos, a dificuldade de mineração deve aumentar a cada nova taxa hash de processamento inserido na rede, um estudo sobre tal problemática será de grande prestígio.

REFERÊNCIAS

ANTONOPOULOS, A. M. **Mastering Bitcoin**. 1. ed. Sebastopol: O'Reilly Media, 2014.

BIRYUKOV, A.; PUSTOGAROV, I. Bitcoin over tor isn't a good idea. **Proceedings - IEEE Symposium on Security and Privacy**, 2015. 122-134.

BITCOIN, P. Bitcoin. **Some Miners Generating Invalid Blocks**, 2015. Disponivel em: <https://bitcoin.org/en/alert/2015-07-04-spv-mining>. Acesso em: 08 ago. 2016.

BITCOIN, P. Bitcoin. **Bitcoin Developer Guide**, 2016. Disponivel em: <https://bitcoin.org/en/developer-guide>. Acesso em: 08 ago. 2016.

BITCOIN, P. Bitcoin. **Bitcoin Improvement Proposals**, 2016. Disponivel em: <https://github.com/bitcoin/bips>. Acesso em: 08 ago. 2016.

BITCOIN, P. Bitcoin. **Choose your Bitcoin wallet**, 2016. Disponivel em: <https://bitcoin.org/en/choose-your-wallet>. Acesso em: 08 ago. 2016.

BLOCKCHAIN, I. Blockchain. **Distribuição da Taxa de Hash**, 2016. Disponivel em: <https://blockchain.info/pt/pools>. Acesso em: 08 ago. 2016.

CHAUDHARY, K. et al. Modeling and Verification of the Bitcoin Protocol. **Electronic Proceedings in Theoretical Computer Science**, 2015. 46-60.

CORDEIRO, A. M. et al. Revisão sistemática: uma revisão narrativa. **Revista do Colégio Brasileiro de Cirurgiões**, 2007. 428-431.

EYAL, I. The Miner ' s Dilemma. **36th IEEE Symposium on Security and Privacy**, 2015. 89-103.

EYAL, I.; SIRER, E. G. Majority is not enough - Bitcoin mining is vulnerable. **CoRR**, 2013. 436-454.

GILBERT, H.; HANDSCHUH, H. Security Analysis of SHA-256 and Sisters. **Selected Areas in Cryptography**, 2004. 175-193.

HUGHES, E. **A cypherpunk's Manifesto**, 1993. Disponivel em: <https://w2.eff.org/Privacy/Crypto/Crypto_misc/cypherpunk.manifesto>. Acesso em: 08 ago. 2016.

ITU. Committed to connecting the world. **World Telecommunication - Indicators database**, 2016. Disponivel em: <http://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx>. Acesso em: 08 ago. 2016.

KRISHNAN, H.; SAKETH, S.; TEJ, V. Cryptocurrency Mining – Transition to Cloud. **International Journal of Advanced Computer Science and Applications**, 2015. 115-124.

NAKAMOTO, S. Bitcoin. **Bitcoin A Peer-to-Peer Electronic Cash System**, 2008. Disponivel em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 08 ago. 2016.

OGUNDEJI, O. The Cointelegraph future of money. **Major Bitcoin Miner Disappears Along with Millions of Dollars Worth of Bitcoin**, 2016. Disponivel em: <https://cointelegraph.com/news/major-bitcoin-miner-disappears-along-with-millions-of-dollars-worth-of-bitcoin>. Acesso em: 08 ago. 2016.

POPPER, N. **Digital Gold - Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money**. 1. ed. [S.l.]: HarperCollins Publishers, 2015.

ROTHER, E. T. Revisão sistemática X revisão narrativa. **Acta Paulista de Enfermagem**, jun. 2007. 5-7.

SWAN, M. **Blockchain Blueprint for a New Economy**. 1. ed. Sebastopol: O'Reilly Media, 2015.

TOR, P. Tor. **Anonymity Online**, 2016. Disponivel em: <https://www.torproject.org>. Acesso em: 08 ago. 2016.

ULRICH, F. **Bitcoin - a moeda na era digital**. 1. ed. São Paulo: Mises Brasil, 2014.

WHITMAN, M. E.; MATTORD, H. J. **Principles of Information Security**. 4ª Edição. ed. Boston: Course Technology Press, 2011.