

JNT-FACIT BUSINESS AND TECHNOLOGY JOURNAL - ISSN: 2526-4281 QUALIS B1



**MINERAÇÃO DE CRIPTOMOEDAS: ESTUDO
COMPARATIVO PÓS-REGULAMENTAÇÃO DO
BITCOIN COM ALTERNATIVAS EMERGENTES**

**CRYPTOCURRENCIES MINING: COMPARATIVE
STUDY POST-REGULATION OF BITCOIN WITH
EMERGING ALTERNATIVES**

Kayo Alexandre LACERDA
Faculdade de Ciências do Tocantins FACIT
E-mail: kayo.look@hotmail.com

Leonardo da Silva CUNHA
Faculdade de Ciências do Tocantins FACIT
E-mail: leonardosilvai.silva@gmail.com

Cássio Cipriano NOGUEIRA
Faculdade de Ciências do Tocantins FACIT
E-mail: cassio.cipriano@faculadefacit.edu.br



RESUMO

As criptomoedas vêm ganhando cada vez mais espaço e revolucionando a forma de efetuar pagamentos e fazer investimentos através da internet. Também chamadas de “moedas virtuais”, estas são uma espécie de dinheiro existente apenas no âmbito virtual e que utilizam criptografia para garantir a segurança nas transações, impossibilitando sua falsificação, e também pode ser “minerado”, algo que, grosso modo, significa dizer que é possível fazer investimentos para aumentar o valor que se possui em criptomoedas, utilizando ferramentas específicas para tal finalidade. Este trabalho tem como objetivo realizar um estudo comparativo com a mineração de diferentes criptomoedas, demonstrando o seu funcionamento e maneiras de obtê-las através de computador pessoal, a fim de relatar a experiência e apresentar os resultados obtidos com tecnologias populares, como Bitcoin e Litecoin; e uma criptomoeda brasileira chamada Nióbio; demonstrando aspectos específicos na forma de minerar e no rendimento de cada uma das criptomoedas, analisando os impactos após a regulamentação do Bitcoin em alguns países.

Palavras-Chave: Criptomoedas. Mineração. Bitcoin. Estudo Comparativo.

ABSTRACT

Cryptocurrencies are gaining more and more space and revolutionizing the way of making payments and making investments through the internet. Also called “virtual currencies”, these are a kind of Money that exists only in the virtual sphere and that use cryptography to guarantee security in transactions, making it impossible to counterfeit, and can also be “mined”, something that, roughly speaking, means to say that it is possible to make investments to increase the value that one has in cryptocurrencies, using specific tools for this purpose. This work aims to carry out a comparative study with the mining of different cryptocurrencies, demonstrating their operation and ways of obtaining them through a personal computer, in order to report the experience and present the results obtained with popular Technologies, such as Bitcoin and Litecoin; and a Brazilian cryptocurrency called Nióbio; demonstrating specific aspects in the way of mining and the yield of each of the cryptocurrencies, analyzing the impacts after the Bitcoin regulation in some countries.

Keywords: Cryptocurrencies. Mining. Bitcoin. Comparative Study.

INTRODUÇÃO

A crescente adesão dos usuários da internet às compras virtuais proporciona o crescente surgimento de novas tecnologias, tais como as criptomoedas, que vem ganhando cada vez mais espaço e revolucionando a forma de efetuar pagamentos e fazer investimentos através da internet, de modo alheio às formas tradicionais de câmbio regulamentadas nos diferentes países ao redor do mundo. Nos últimos anos, a mídia deu ênfase às criptomoedas, principalmente ao Bitcoin, principal criptomoeda da atualidade, o que as tornou populares mundialmente e despertou a curiosidade em pessoas que ainda não conheciam sobre o assunto.

Conhecidas popularmente também como “moedas virtuais”, as criptomoedas são uma espécie de dinheiro existente apenas no âmbito virtual e que utilizam criptografia para garantir a segurança nas transações, impossibilitando a sua falsificação; e pode ser “minerado”, algo que, grosso modo, significa dizer que é possível fazer investimentos para aumentar o valor que se possui em criptomoedas, utilizando ferramentas específicas para tal finalidade. Devido a isso, tornou-se comum pessoas que ainda não sabem ao certo como funcionam as criptomoedas, interessarem-se mesmo assim pelo assunto, devido à possibilidade de ganhar, comprar ou de minerar o seu próprio dinheiro virtual em seus dispositivos pessoais, o que ficou bem mais atrativo após a recente regulamentação do Bitcoin em alguns países, tornando esta a criptomoeda mais valorizada do mercado.

A mídia e os meios de comunicação, de modo geral, vêm explorando a popularidade das criptomoedas, por meio de propagandas veiculadas na TV e anúncios em sites e blogs, até sites de compras que já aceitam criptomoedas como forma de pagamento em seus produtos e serviços, numa busca por incentivar cada vez mais pessoas a aderirem a este novo e revolucionário tipo de investimento. Por outro lado, na prática, minerar criptomoedas não é algo tão simples quanto alguns anúncios e propagandas na mídia acabam mostrando. Neste sentido, este trabalho tem como objetivo realizar um estudo comparativo com a mineração de diferentes criptomoedas, demonstrando o seu funcionamento e as maneiras de obtê-las utilizando um computador pessoal, a fim de relatar a experiência e apresentar os resultados obtidos com tecnologias populares, como Bitcoin e Litecoin; e uma criptomoeda brasileira chamada Nióbio; a fim de demonstrar aspectos específicos na forma de minerar e no rendimento de cada uma das criptomoedas, analisando os impactos após a regulamentação do Bitcoin.

Este trabalho está caracterizado como uma pesquisa descritiva, definida por Rampazzo (2005, p. 53) como um tipo de pesquisa que “observa, registra, analisa e correlaciona fatos ou fenômenos (variáveis), sem manipulá-los; estuda fatos e fenômenos do mundo físico e, especialmente, do mundo humano, sem a interferência do pesquisador”, com abordagem quantitativa, que, segundo Collado *et. al.* (2013, p. 30), “utiliza a coleta de dados para testar hipóteses, baseando-se na medição numérica e na análise estatística para estabelecer padrões e comprovar teorias”. A técnica que será utilizada para a coleta de dados será a netnografia, que, segundo Kozinets (2010, p. 9-10), “[...] é uma forma especializada de etnografia adaptada às contingências específicas dos mundos sociais de hoje, mediados por computadores”, utilizando como aporte instrumental para a escrita etnográfica o diário de campo, definido por Oliveira (2014, p. 1) como um “dispositivo de registro das temporalidades cotidianas vivenciadas na pesquisa”.

O artigo está estruturado da seguinte forma: no primeiro tópico, é apresentado um breve histórico das transações comerciais, desde os tempos em que não existia moeda alguma, até o surgimento dos meios virtuais para tais transações; no segundo tópico, apresentam-se especificidades das criptomoedas, tais como mecanismos que garantem a segurança no uso das mesmas e os diferentes modos de obtê-las; no terceiro tópico, comenta-se sobre as três criptomoedas escolhidas para realizar este trabalho; no quarto tópico, são tratados detalhes de como a pesquisa foi desenvolvida e apresentam-se os resultados; no quinto tópico, têm-se as considerações finais; e por fim, as referências.

DO SURGIMENTO DA MOEDA ÀS TRANSAÇÕES NO AMBIENTE VIRTUAL

Os meios de pagamentos evoluíram muito no decorrer dos séculos. No passado, antes das moedas existirem, utilizava-se o escambo, uma prática da troca de serviços ou mercadorias. Com o passar do tempo, foram surgindo novas formas de efetuar pagamentos.

Há cerca de 10 mil a.C, começou-se a utilizar animais como moeda na troca de serviços e alimentações. No entanto, era pouco conveniente. Em 3 mil a.C, foi dado um passo muito importante, na Mesopotâmia, que substituiu uso de animais por medidas de grãos; e na China, África, Oceania e nas Américas, utilizavam conchas como moeda (ABDALLA, 2017, s/p).

A primeira moeda surgiu na China, fabricada em bronze. No entanto, a moeda, em seu formato atual de disco metálico, teve sua origem, na Lídia, atualmente território turco, feitas em metais preciosos, como ouro e prata, chamada *eléctron*. Devido ao uso excessivo de metais nas grandes transações comerciais, os chineses, que já haviam inventado o papel,

durante a dinastia Tang, começaram a utilizar dinheiro em papel, sendo os pioneiros no desenvolvimento dessas cédulas.

Na Suécia, o Banco de Estocolmo foi o primeiro banco europeu a imprimir e distribuir cédulas de dinheiro. Já no ano de 1920, devido ao avanço de automóveis, foi possível realizar viagens mais longas e cada vez mais frequente. Daí surgiu a necessidade de fazer pagamentos cada vez mais longe de domicílios bancários. Algumas lojas perceberam uma oportunidade e criaram os *Charge Cards* e *Charge Plates*, que consistiam em uma pequena placa em metal que apresentava o nome do titular impresso junto ao nome do estabelecimento, uma espécie de cartão de crédito primitivo.

Os primeiros cartões de crédito surgiram em 1950, pelo empresário Fred McNamara, que, ao passar por um constrangimento em um jantar, ao tentar pagar sua conta, percebeu que havia esquecido sua carteira no hotel que estava hospedado. O incidente o fez pensar que ele, um empresário de grande prestígio, não poderia ficar refém apenas do dinheiro que possuía no bolso. Após diversas reuniões com amigos e seu sócio, foi lançado o primeiro cartão de crédito, chamado *Diners Club Card*.

No ano de 1970, os cartões de créditos foram padronizados com uso de tarjas magnéticas, graças a tecnologia ATM, que foi utilizada pela primeira vez em 1967 pela agência *Barclays Bank*, em Londres, que permitia aos estabelecimentos verificar as transações eletronicamente. No início do ano de 1990, chegaram os cartões com chips, chamados de *SmartCards* (ou EMV), devidamente protegidas por protocolos criptográficos, dando mais segurança nas transações. Em agosto do ano de 1995, foi realizada a primeira compra online com cartão de crédito em um site.

O ato de comprar pela internet surgiu a partir da difusão do *e-commerce* (comércio eletrônico), no início dos anos noventa, quando a internet começou a se popularizar como rede mundial e, então, grandes varejistas passaram a explorar esse ambiente como um novo nicho para expandir seus negócios. As compras virtuais tornaram-se ainda mais importantes após a mudança para a Web 2.0¹, em meados dos anos dois mil, proporcionando uma maior interatividade entre as empresas e seus clientes, aprimorando o marketing digital e facilitando as formas de pagamento no meio eletrônico, por meio do uso de cartões de crédito e débito no ambiente virtual e até mesmo o surgimento de

¹ A ideia da Web 2.0 foi introduzida em uma conferência do O'Reilly Media Group em 2004. [...] Desde a sua introdução, a Web 2.0 tornou-se a lógica cultural para o comércio eletrônico, com uma série de práticas empresariais que buscam captar e explorar a cultura participativa [...] Os princípios da Web 2.0 motivam o público a participar da construção e da customização de serviços e mensagens, em vez de esperar que as empresas lhes apresentem experiências completas formadas em sua totalidade (JENKINS, 2014, p.79).

serviços de pagamentos totalmente online, tais como o mundialmente conhecido *PayPal*, o brasileiro PagSeguro, o *PicPay*, entre outros.

Com lançamento do site eletrônico Amazon.com, a internet que até então era utilizada apenas como uma ferramenta de pesquisa se abriu para uso comercial. Em 1997 a empresa Amazon, tornou-se a primeira empresa varejista no ambiente virtual. Devido à popularização das compras virtuais, em 1998, é lançada a primeira carteira virtual chamada “PAYPAL”, uma *startup* criada no estado da Califórnia, por Peter Thiel e Max Levchin, com intuito de realizar transações no ambiente virtual livre do controle governamental (ABDALLA, 2017, s/p).

Mesmo com intenção de realizar transações virtuais livres e sem o controle governamental, serviços como o PayPal ainda não têm toda essa liberdade, devido à dependência que possuem de realizar transações utilizando o dinheiro comum, que é impresso e controlado pelo governo e distribuído pelos bancos e demais instituições financeiras regulamentadas. A verdadeira independência e liberdade surgiram somente em 2008, com o nascimento da primeira aplicação de *blockchain*, que de origem às criptomoedas.

CRIPTOMOEDAS

Criptomoedas são moedas totalmente virtuais e independentes de qualquer órgão público ou privado e com um alto valor de mercado. São utilizadas para fazer negociações online diretamente de um usuário para outro, protegidas por uma tecnologia conhecida como *blockchain*.

A primeira criptomoeda a surgir foi a Bitcoin, em 2009, mas a ideia da existência de um dinheiro descentralizado e digital surgiu em 1993, no Manifesto Sypherpunk, um texto escrito por um programador chamado Eric Hughes, que defendia o individualismo e privacidade dos usuários na rede, além da existência de maneiras para fazer transações anônimas de forma descentralizada sem nenhum tipo de controle do governo.

Devemos defender nossa própria privacidade se planejamos ter alguma. Devemos nos juntar e criar sistemas que permitem que transações anônimas aconteçam. As pessoas têm defendido sua própria privacidade por séculos com sussurros, escuridão, envelopes, portas fechadas, apertos de mão secretos e mensageiros. As tecnologias do passado não permitiam uma privacidade forte, mas tecnologias eletrônicas permitem (HUGHES, 1993, s/p).

A partir desse manifesto, programadores do mundo inteiro se dedicaram à criação de moedas eletrônicas, que funcionam em plataformas que usam a criptografia para

fornecer o anonimato nas transações entre usuários, permitindo a criação de vários tipos de criptomoedas.

Antes de alcançarem a mídia, as criptomoedas eram bastante utilizadas na *Deep Web*, pelo simples fato de a maioria delas fornecerem um certo nível de anonimato, quando utilizadas com cautela, não podendo ser descoberto quem é o dono daquele dinheiro. Um exemplo é o uso por redes criminosas, procurando uma maneira de lavar seu dinheiro sem serem rastreadas.

As criptomoedas deixaram de ser algo restrito à *Deep Web* após a regulamentação do Bitcoin, primeiramente no Japão, em 2017, por motivos de ter o controle contra crimes financeiros e promover uma segurança maior para seus investidores, fazendo o controle das transações e afastando o anonimato que algumas moedas proporcionam, regulamentando seu uso no país, podendo ser submetido à prisão o indivíduo que for pego oferecendo serviços envolvendo a moeda sem ter licença fornecida pelo estado.

Após a regulamentação no Japão, outros países procuram regulamentar a moeda, inclusive o Brasil. Segundo Edgar (2017, s/p), “[...] no Brasil, existe um projeto de lei que pretende oficializar o reconhecimento das moedas virtuais como ‘arranjos de pagamento’, submetendo a sua regulação expressa e diretamente ao Banco Central”. Há países que vão além, como a Inglaterra, que pretende criar uma criptomoeda própria para uso nacional. Apesar de alguns países serem a favor da regulamentação, também existem os que são totalmente contra o uso das criptomoedas, tais como a China e a Coreia do Sul, que procuram formas de proibir a utilização das criptomoedas em seus territórios, podendo virar pauta de assunto nas próximas reuniões do G20.

Blockchain

Esta é uma das plataformas utilizadas para o funcionamento da rede de várias criptomoedas existentes, popularizada através do Bitcoin, que utiliza a tecnologia. Foi construída tendo em mente quatro principais características arquiteturas: segurança das operações, descentralização de armazenamento/computação, integridade de dados e imutabilidade de transações (BRAGA *et. al.*, 2016, p. 3).

Blockchain funciona através de uma rede descentralizada, chamada *peer-to-peer* (ou ponto-a-ponto, em português, que define uma rede que faz a comunicação entre dois pontos na internet), onde todos os usuários são responsáveis por manter a base de dados. Cada pessoa nessa rede representa um “nó” e tem como papel guardar e validar as transações ocasionadas por clientes que utilizam alguma moeda digital. Assim, se, por

ventura, um dos “nós” perdermos todas as informações armazenadas em sua máquina, ainda haverá todos os outros com esses dados disponíveis, mantendo a integridade da operação. Outra vantagem do *blockchain* é a segurança, pois todos os “nós” têm a tarefa de validar as transações que ocorrem na rede, diferente de um banco, que só tem a própria organização como meio de validação. Depois de ocorrido, as operações são registradas em uma espécie de “livro”, de forma criptografada garantindo a segurança das informações.

Mineração

A mineração de criptomoedas é a atividade de verificar as transações feitas com moedas virtuais, realizadas pelos consumidores das mesmas. Todas as atividades são registradas em *blockchain*. Na mineração, os computadores são interligados por uma rede específica, onde existem vários outros usuários minerando alguma criptomoeda. Dessa maneira, as máquinas conectadas a essa rede são como “nós” da rede, sendo responsáveis pelo controle dos dados, garantindo a segurança no compartilhamento das informações da moeda, não dependendo de um nó central apenas, pois as mesmas informações são armazenadas em todos os computadores, de forma descentralizada.

As pessoas responsáveis por essa atividade são chamadas de mineradores e utilizam softwares criados especificamente para fazer o gerenciamento da mineração. Essas aplicações possuem um algoritmo que emite códigos com valores criptografados, chamados de *hash* — qualquer algoritmo que mapeie dados grandes e de tamanho variável para pequenos dados de tamanho fixo e que, por esse motivo, são conhecidas por resumirem o dado, tendo como sua principal aplicação a comparação de dados grandes ou secretos —, que consistem em equações altamente complexas realizadas no ato de minerar alguma moeda.

Quando alguém consegue decifrar algum código primeiro, recebe uma fração da moeda como recompensa. Porém, todo esse esforço pode se tornar uma tarefa difícil, já que para fazer mineração é preciso equipamentos específicos, trazendo gastos significativos com a aquisição desse material, além do grande consumo de energia, podendo não proporcionar o lucro esperado. No entanto, existem vários métodos diferentes para se minerar criptomoedas, cada um com suas vantagens e desvantagens e adequam-se às necessidades dos diferentes tipos de usuários.

Mineração com CPU

Com o surgimento da primeira moeda virtual, os primeiros softwares para mineração permitiam utilizar as CPUs instaladas em computadores comuns. Um computador com um modelo de processador moderno pode fazer milhões de *hashs*, mas atualmente usar este recurso não é muito vantajoso, pelo fato de que as velocidades de processamento dos processadores, mesmo os modernos, são baixas em relação ao número de transações que ocorrem atualmente, tornando o processo de mineração tão lento que a quantidade de criptomoeda minerada se torna menor que a quantidade de recursos gastos no processo de mineração, como o gasto com energia devido ao tempo que o computador precisar ficar ligado, tornando a atividade um prejuízo.

Mineração com GPU

Este método utiliza a Unidade de Processamento Gráfico (GPU), que começou a ser utilizada depois que o uso de CPUs causou frustrações por seu baixo desempenho. A velocidade de processamento das GPUs é drasticamente melhor do que das CPUs. Segundo Marques (2017), “enquanto uma CPU pode executar 4 instruções de 32 bits por clock, uma GPU pode executar 3.200 destas operações ao mesmo tempo. GPUs foram feitas para ter uma alta vazão e alto paralelismo, ambos podem ser úteis na mineração”.

157

Mineração com FPGA

Trata-se de uma placa com vários circuitos integrados e processadores lógicos que se equipara a uma GPU em questão de processamento, sendo então mais rápido que processadores, mas tem ainda a vantagem de consumir pouca energia sem perder o desempenho. Porém, deve ser configurada de maneira correta para poder retirar todo o potencial da placa.

A Mineração ASIC

ASIC são computadores construídos com chips ASIC (*Application Specific Integrated Circuits*), que são circuitos integrados desenvolvidos para fazerem tarefas específicas e integram placas-mãe, com o objetivo de minerar criptomoedas. Além disso, essas placas possuem processadores superpotentes, que conseguem fazer milhares de cálculos por segundo. No entanto, com toda essa potência, há um alto consumo de eletricidade. Quanto maior a potência do ASIC, maior o consumo.

Serviços de mineração em nuvem (cloud)

Com a alta demanda de usuários querendo se tornar mineradores, empresas passaram a alugar poder de processamento de grandes centros de dados remotos, para executar mineração de criptomoedas em nuvem. O serviço é mais voltado para pessoas que não podem ou simplesmente não querem investir em hardware e arcar com altos gastos de energia, mas almejam obter criptomoedas, então contratam esse serviço e pagam pelo poder e tempo de processamento.

Mineração com computadores alheios

Hackers desenvolveram métodos de minerar criptomoedas usando o poder de processamento de outras pessoas sem o consentimento, através de softwares maliciosos que infectam os computadores por meios de sites, prejudicando o desempenho das máquinas infectadas. Em vez do lucro dessa atividade ir para os donos dos computadores, vai para os hackers.

CRIPTOMOEDAS SELECIONADAS PARA O ESTUDO

A primeira criptomoeda foi criada em 2009, após o começo da crise financeira nos Estados Unidos. Porém, um ano antes, Satoshi Nakamoto lançou um artigo falando do funcionamento dessa nova moeda.

Muitos acreditam que ele é o criador por trás dessa moeda digital. O único problema é que este autor não existe, Satoshi Nakamoto é um pseudônimo. Não se sabe, contudo, quem está por trás desse pseudônimo – nem mesmo se é apenas um indivíduo ou vários. Especulações existem, mas até o momento, não há nenhuma confirmação (CALDERON, 2017, p. 86).

Calderon (2017) defendia a ideia da criação de uma rede exclusiva para a moeda, seguindo a tecnologia *peer-to-peer*, que permitiria a troca do dinheiro diretamente de um usuário para o outro sem precisar passar por uma instituição financeira ou banco. Desde então, pelo mundo inteiro vem surgindo diferentes tipos de moedas virtuais, tornando-as populares pela facilidade de negociação e pelo seu alto valor de mercado, quando trocadas diretamente por dinheiro físico.

Bitcoin

Segundo SETTI *et. al.* (2017, s/p), “[...] ocorreu na Flórida, no ano de 2010, a primeira transação com Bitcoin, quando um programador em uma compra online, oferece a outro uma moeda totalmente virtual no pagamento de uma pizza, dando assim início à era do Bitcoin”. No começo de sua vida, o Bitcoin não tinha um valor econômico. Era utilizada como produto de troca apenas, após essa primeira transação e, graças ao modo como as informações se propagam na internet, de maneira espantosa e extremamente rápida, a moeda foi ganhando seu espaço, sendo espalhada pelos internautas uma nova maneira de se ganhar dinheiro, acumulando assim entusiastas e curiosos pelo assunto.

Especialistas em comportamento e consumo citam ainda outra explicação para tanto frisson em torno da moeda virtual: a sensação de lidar diretamente com suas economias, sem intermediação (e intervenção) de governos, bancos e outras empresas. Algo que nasceu com um espírito libertário como o que levou à criação do Napster, em 1999. Na época, o programa que permitia trocas de músicas entre pessoas de todo o mundo (*peer to peer*) explodiu ao empoderar o usuário. Acusado de incentivar a pirataria e derrubar os lucros do mercado fonográfico, o Napster morreu dois anos depois por decisão da Justiça (SETTI *et. al.*, 2017, s/p).

A moeda *open source* inicialmente começou a ser utilizada em financiamentos no lado obscuro da internet, conhecido como *Deep Web*. Grupos de hackers e do narcotráfico a utilizavam como forma de receber pagamentos pelos crimes que cometiam, se aproveitando do anonimato e dificuldade de rastreamento proporcionado pela moeda. Com o tempo, deixou de ser uma moeda exclusiva da *Deep Web* devido à sua regulamentação em alguns países, aceitação em diversos estabelecimentos e os diversos grupos que passaram a dedicar-se à sua mineração. Hoje o Bitcoin continua sendo a moeda mais minerada do mundo, devido ao seu valor comercial e às diversas maneiras de adquirir a moeda.

Litecoin

Criada em 2011 por Charles Lee, Litecoin é uma criptomoeda descentralizada, ou seja, não depende de nenhum órgão regulamentador para estar em funcionamento. Lee é um ex-engenheiro de software da Google.

Lee decidiu reescrever o Bitcoin, buscando corrigir algumas das falhas que via no desenvolvimento da moeda criptográfica. Em uma incursão anterior na arena das moedas alternativas, Lee tentou lançar a moeda Fairbrix, que fracassou justamente por conta de instabilidades técnicas. Em outubro de 2011, ele liberou uma cria mais aperfeiçoada, que viria a

ser conhecida como Litecoin e seria futuramente simbolizada pela prata, em oposição ao ouro no qual o Bitcoin se inspira. A ideia é justamente essa, ser a prata para o ouro do Bitcoin – ou seja, uma opção mais leve e abundante (BITCOIN BRASIL, 2013, s/p.).

Litecoin é considerada por muitos, mais rápida na realização de suas transações do que seu suposto rival. Assim, o Litecoin foi ganhando seu espaço no mercado das criptomoedas e entusiastas até mesmo das comunidades do Bitcoin, chegando a ser a segunda moeda mais minerada do mundo. Porém, nunca alcançou o patamar de preços do Bitcoin.

Apesar de sua construção ser baseada na estrutura Bitcoin, o Litecoin foi construído tentando ser uma melhoria, proporcionando um número superior de moedas que podem ser mineradas, além do que a corrente de blocos utilizada no Litecoin permite lidar com um número maior de transações, graças à geração mais constante desses blocos o que permite essa frequência elevada.

O Litecoin ainda tem um grande caminho pela frente para alcançar um alto nível de valorização. Apesar de já haver alguns estabelecimentos físicos e digitais que fazem a troca de Litecoin, os números são baixíssimos, além do que a moeda ainda não transmite o nível de confiança desejado entre os usuários e mineradores. Entretanto, o Litecoin apresenta muito potencial e uma elevada estabilidade em comparação ao Bitcoin.

160

Nióbio

Nióbio é uma criptomoeda totalmente brasileira que possui seu código aberto, permitindo a integração de diversos profissionais diferentes em seu desenvolvimento. A moeda foi criada em 2017 e seu nome faz referência ao minério Nióbio, onde, segundo Alvarenga (2013), “cerca de 98% de suas reservas estão localizadas no Brasil, país de criação da moeda”. Foi desenvolvida por uma equipe de doze profissionais e sua estrutura tem como base outra criptomoeda, chamada Bytecoin, que compartilha o mesmo algoritmo de mineração do Bitcoin. Porém, diferente do Bitcoin, a Nióbio utiliza a tecnologia Cryptonote para evitar a centralização de mineradores e para misturar as transações, dificultando o rastreamento possibilitando maior anonimato.

De acordo com a equipe da Nióbio Cash (2017), “[...] a moeda tem como objetivo incentivar pesquisas em torno do minério Nióbio, onde 5% dos lucros das criptomoedas adquiridas serão revertidas em um fundo que é destinado aos financiamentos dessas pesquisas”.

ESTUDO COMPARATIVO

Para a realização do estudo, foram determinadas três criptomoedas distintas: a Nióbio Cash, por ser uma tecnologia criada no Brasil; a Litecoin por ser uma moeda popular, que já esteve em segundo lugar no ranking mundial de criptomoedas mais utilizadas; e o Bitcoin, por ser a criptomoeda mais popular e valorizada atualmente, além de ter sido a pioneira.

O estudo consistiu em minerar as três criptomoedas em dois computadores pessoais, que chamaremos de computador K e computador L, com configurações de hardware suficientes para minerar qualquer criptomoeda por meio de Mineração com CPU. Ambos os PCs utilizados possuem 8 GB de Memória RAM, processador Intel Core i5 com clock de 2,5 GHz, HDs de 1 TB — estando o computador K com 620 GB de espaço livre e o computador L com 600 GB livre —, e sistema operacional Microsoft Windows 10 Pro instalado.

Foi determinado um cronograma para a realização da coleta dos dados, que compreendeu os dias 21 a 26 de maio de 2018, e horários diferentes durante dia e noite para realizar a mineração das criptomoedas, bem como monitorar o andamento das atividades: das 8:00h da manhã às 16:00h da tarde com computador L, utilizando uma conexão de internet de 10 Mbps (Megabytes por segundo) de velocidade, e no período da noite, das 23:00h às 7:00h da manhã do dia seguinte, no computador K, com uma conexão de internet de 10 Mbps.

Para conseguir trabalhar com as três criptomoedas dentro do cronograma estabelecido para a coleta dos dados, que compreendeu seis dias, este período teve que ser fragmentado em dois dias para minerar cada criptomoeda. A primeira moeda minerada foi a Nióbio Cash. Para esta tarefa, foi utilizada uma aplicação que equipes de desenvolvedores da própria moeda mantém disponível em seu site, chamada Miner que tem como papel não só fazer a mineração da moeda, mas também armazená-las, funcionando como um tipo de carteira virtual. O fato de tratar-se de uma ferramenta disponibilizada pela própria organização mantenedora da Nióbio Cash foi determinante na escolha por utilizá-la.

Apesar da aplicação possuir uma interface simples e de boa usabilidade, disponibilizando uma aba exclusiva para mineração, fazendo-nos crer que aparentemente seria fácil minerar a Nióbio, ele se mostrou muito demorado, tomando todo tempo estipulado para a coleta de requisitos somente para que o programa tivesse que sincronizar

todos os blocos de transações já feitos desde a criação da criptomoeda, sendo isto um pré-requisito para a mineração.

Após 16 horas de trabalho no computador L, sem desliga-lo, a sincronização estava em 58.233 de 88.183 blocos e ainda não havia sido concluída, tornando-se inviável minerar a moeda no tempo estabelecido, devido à sincronização dos blocos se dar lentamente, travando muitas vezes, com várias horas sem nenhum aumento significativo, chegando ao final desse prazo faltando 29.950 blocos. No computador K, mesmo deixando a máquina ligada 24 horas, durante dois dias, a sincronização não foi concluída. A ferramenta até dispõe da possibilidade de deixar o programa sincronizando e minerando ao mesmo tempo. Porém, julgamos não ser uma opção viável em computadores pessoais, devido o computador K ter superaquecido com o alto uso do processador e, por motivos de segurança, se autodesligava para manter a integridade física de seus componentes internos, interrompendo as atividades de sincronização e mineração.

Devido aos problemas enfrentados, buscou-se alternativas para realizar a mineração da Nóbio Cash. No entanto, a criptomoeda ainda possui maneiras muito restritas para sua mineração. Além do programa próprio, pode se utilizar os *pools*, que consiste em plataformas online de terceiros, onde milhares de usuários se juntam para minerar uma determinada criptomoeda, tornando a dificuldade de mineração menor. Entretanto, com os *pools*, a tarefa se torna muito complicada para um usuário iniciante, pois são necessários conhecimentos específicos para operar tais ferramentas.

Após tentativas de mineração com a criptomoeda Nióbio, passou-se para a Bitcoin. Como não há uma equipe por trás da Bitcoin, logo não há um programa e nem uma carteira virtual específica que leva o nome da mesma. Sendo assim, para fazer mineração, foi escolhido um programa de terceiros, chamado Nicehash, e a carteira a ser depositado a quantia de Bitcoins minerados também é da mesma desenvolvedora da aplicação, por ter maior compatibilidade e menor risco de ocorrer problemas com os depósitos, além de ter a opção de acompanhar o desempenho da atividade pelo próprio site da carteira. Nicehash é uma aplicação fácil de configurar e, diferente do programa para mineração fornecido pela equipe da moeda Nióbio Cash, não há uma necessidade sincronizar blocos para iniciar a mineração, tornando melhor a experiência com o aplicativo, fazendo que o tempo entre a instalação e o começo da mineração seja consideravelmente mais curto.

Antes de começar a minerar Bitcoin, é preciso fazer um teste de benchmark para atestar qual o melhor algoritmo de mineração se adequa à máquina utilizada — algo que vai depender muito da configuração de hardware do computador, mas geralmente o

algoritmo mais utilizado para a tarefa de Mineração com CPU é o algoritmo Cryptonightv7. O teste deve ser feito com um uma internet estável. Do contrario, o programa se encerrará sozinho, o que acabou ocorrendo no computador L, onde o programa falhou todas as vezes ao tentar prosseguir com o teste. Após a tentativa falha, o computador L foi levado ao local onde o computador K estava e foi possível ter a confirmação de que o problema era realmente a rede, já que, com uma banda de acesso maior e estável, foi possível realizar o teste de benchmark sem nenhum problema, liberando o programa para a mineração e podendo retornar ao ambiente de teste do computador L.

A empresa Nicehash, além de disponibilizar um miner para trabalhar com a Bitcoin, também disponibiliza em seu site uma carteira virtual onde é possível manter as moedas recebidas pelo trabalho, além de manter atualizado o desempenho com todos os detalhes possíveis, como, por exemplo, rentabilidade, eficiência de trabalho, estatísticas de mineração, entre outras, dando ao usuário uma visão geral sobre a atividade.

Ao iniciar a mineração, é executada uma tela de comando onde se mostra a velocidade de processamento, trazendo relatórios de desempenho no intervalo de um minuto, além de mostrar quando o programa encontra blocos, podendo ser acompanhado também pelo site.

Apesar do problema com o teste de benchmark ter sido resolvido com uma rede estável, o computador L não mostrou nenhum progresso, diferente do computador K, que além de mostrar resultados, conseguiu minerar uma quantidade de 0,0000000600 Bitcoins, equivalendo a 0,04 USD na cotação do dólar daquele dia.

A terceira e última criptomoeda a ser minerada foi a Litecoin. Em seu site, há disponível um aplicativo que, de início, pensou-se ser uma aplicação que permitia a mineração, mas era apenas de carteira para depósitos da moeda. Após uma busca sem sucesso por programas que possibilitavam fazer mineração da criptomoeda, optou-se pela mineração por *pool*. Em pesquisas na internet por tutoriais de como entrar e utilizar esses mineradores deparamo-nos com vários materiais que recomendavam utilizar o *pool* disponível pelo site www.litecoinpool.org.

Para começar a minerar com o *pool*, é necessário ter uma conta de usuário em uma carteira virtual, para receber as moedas, e fazer o cadastro no *pool*, onde é registrado o endereço da carteira. Após esse cadastro, o site disponibiliza um download com os arquivos necessários para começar a minerar, podendo escolher se quer utilizar a CPU ou a GPU do computador. Ao abrir o arquivo, o programa mostra uma tela de comando onde

começa a procurar por blocos de transações disponíveis, mostrando avisos quando os blocos são 100% interceptados e também no momento que ocorre algum erro na interceptação dos blocos, além de mostrar a velocidade do clock dos núcleos do processador a cada momento. Já na plataforma web, pode fazer o acompanhamento detalhado do desempenho com a fração adquirida da moeda e estatísticas de trabalho da conta, mostrando o número de hashes que foram feitos em períodos diários, semanais e mensais, além dos pagamentos pendentes.

Diferente do Bitcoin a mineração nos dois computadores ocorreu sem nenhum problema de internet, executando os aplicativos sem complicações, mostrando todas as informações necessárias para fazer o acompanhamento de todo o processo, conseguindo gerar um lucro de 0,00000030 Litecoins, que equivale a 0,0000300 USD. Entretanto, a carteira escolhida para tentar fazer o depósito das moedas mineradas na plataforma, a Litecoin Core, disponibilizada no site oficial do Litecoin, se mostrou incompatível com a *pool*, não recebendo a quantia da criptomoeda adquirida.

RESULTADOS E DISCUSSÕES

A partir dos resultados, foram observados alguns critérios, que serão considerados no estudo comparativo entre as três criptomoedas utilizadas. São eles:

- Popularidade: o quanto cada uma das criptomoedas analisadas é popular e conhecida;
- Disponibilidade de Material: em termos de livros, artigos, sites, blogs, vídeos, entre outros tipos de materiais que existem sobre cada uma das criptomoedas analisadas;
- Disponibilidade de Ferramentas: em termos de programas, carteiras, *pools*, entre outros tipos de ferramentas que existem para que usuários possam minerar cada uma das criptomoedas analisadas;
- Recursos para a Mineração com CPU: em termos de configuração de hardware e software suficientes para ter uma experiência satisfatória de mineração com cada uma das criptomoedas analisadas;
- Resultados Obtidos em Dois Dias de Mineração: de modo geral, reflexões sobre a experiência com a mineração de cada uma das criptomoedas analisadas.

Tomando estes critérios como categorias de análise e, com base em conhecimentos e percepções adquiridas durante a coleta dos dados da pesquisa, foram atribuídos níveis de satisfação em cada um dos critérios definidos, para cada uma das criptomoedas analisadas.

Os níveis de satisfação são “bom”, “regular” e “ruim”. Optou-se por não utilizar “excelente” como um nível de satisfação devido ao fato de tratar-se de tecnologias relativamente novas e que, de modo geral, ainda são muito dispendiosas para todo e qualquer usuário dentro de todos os critérios que foram definidos para a análise.

A Tabela 1 demonstra os critérios observados e os níveis de satisfação atribuídos para cada uma das criptomoedas analisadas.

Tabela 1. Critérios observados na pesquisa e os níveis de satisfação atribuídos para cada uma das criptomoedas analisadas.

CRITÉRIO OBSERVADO/ANALISADO	CRIPTOMOEDAS		
	Bitcoin	Litecoin	Nióbio
Popularidade	Bom	Bom	Ruim
Disponibilidade de Material	Bom	Regular	Ruim
Disponibilidade de Ferramentas	Bom	Regular	Regular
Recursos para Mineração com CPU	Bom	Regular	Ruim
Resultados Obtidos em Dois Dias de Mineração	Ruim	Ruim	Ruim

Fonte: Os autores.

A popularidade do Bitcoin continua sendo a melhor, pois, quando se trata de criptomoedas, ela é primeira a ser apresentada nos motores de busca, por exemplo, e a mídia, num contexto geral, vem ajudando a aumentar cada vez mais sua popularidade, devido ao seu valor de mercado ser maior, o que acaba incidindo no aumento da quantidade de pessoas que procuram aprender mais sobre o assunto e, conseqüentemente, no aumento da demanda por materiais e ferramentas destinadas à mineração desta criptomoeda, além de outros meios para adquiri-la, como, por exemplo, comprando frações de bitcoins.

Assim como o Bitcoin, o Litecoin também tem uma boa popularidade, devido principalmente ao fato de ter sido criado com intuito de ser uma melhoria do Bitcoin e por já ter sido a segunda criptomoeda mais minerada do mundo. Porém, diferente do Bitcoin, não possui uma grande quantidade de materiais disponíveis na internet, principalmente em português. Em relação às ferramentas e recursos para mineração com CPU, o Litecoin não possui uma ferramenta específica, criada pela equipe de desenvolvedores da criptomoeda,

apenas uma carteira virtual para depósitos. Porém, na internet há vários pools que possibilitam a sua mineração, tanto por CPU quanto por GPU.

Por ser uma criptomoeda nova, a Nióbio Cash não é tão popular no mercado, sendo considerada uma moeda emergente entre as outras existentes, e carente de materiais disponíveis, limitando-se ao *whitepaper* que pode ser encontrado na página da moeda na internet. No quesito disponibilidade de ferramentas, a própria desenvolvedora disponibiliza um software para download e, assim como as moedas anteriores, é possível encontrar *pools* que possibilitam a mineração da Nióbio Cash por CPU e GPU, diferente da aplicação disponibilizada pelos desenvolvedores, que não tem essa opção de selecionar qual hardware utilizar para mineração.

Quanto aos resultados obtidos com a mineração, em relação às três criptomoedas analisadas, os ganhos foram fracos devido ao curto período de tempo para a mineração das mesmas, que não foi o suficiente para angariar quantidades expressivas; a Mineração com CPU não se mostrou eficaz, devido aos bugs apresentados por algumas ferramentas, acarretando em sobrecarga dos recursos computacionais e gastos excessivos com energia, devido ao tempo necessário que os computadores tiveram que ficar ligados. Se comparado esse gasto de energia com os lucros obtidos em criptomoedas, fica evidente o prejuízo na atividade de mineração das mesmas.

166

CONSIDERAÇÕES FINAIS

A partir das pesquisas feitas em torno das criptomoedas, foi possível perceber o quanto estas se tornaram populares nos últimos anos, conquistando um grande espaço na mídia, em geral, revolucionando o mercado financeiro mundial, despertando o interesse de muitas pessoas em minerá-las e até mesmo sendo apontadas como a solução de muitos problemas do cenário econômico atual, devido à liberdade proporcionada e por ser propagada como uma nova maneira de ganhar dinheiro “fácil”, em relação a métodos tradicionais de investimentos.

Apesar de toda essa expectativa e estigmas em torno das criptomoedas, nem todos sabem o que realmente elas são e como funcionam, e a mídia não costuma propagar toda a verdade em relação às criptomoedas, apenas ideias superficiais, ao ponto de levar muitas pessoas a acharem que a aquisição de criptomoedas é mais fácil do que a aquisição de dinheiro comum. No entanto, na realidade, não é bem assim que acontece.

Existem basicamente duas maneiras para se adquirir alguma criptomoeda: investindo ou minerando. Para fazer investimentos, é necessário bastante conhecimento no

mercado das moedas virtuais, que funciona como uma espécie de bolsa de valores na internet.

Dessa maneira, o cliente pode obter lucros expressivos ou corre o risco de sofrer perdas significativas, pelo fato de que o valor atribuído às criptomoedas ser extremamente volátil, propício a alterações a cada momento. Se o usuário optar por uma das diversas maneiras de se minerar alguma criptomoeda, será necessário fazer um bom investimento em hardware de ponta, que proporcione os resultados esperado em lucros e que, em pouco tempo, possam cobrir o investimento inicial e os gastos em energia durante o processo de mineração, sem falar do conhecimento técnico que é pré-requisito para colocar esse equipamento para funcionar.

Contudo, fica evidente que ganhar dinheiro com moedas virtuais não é uma tarefa tão simples e “mágica”, como é comum ser propagado na mídia. No entanto, este é um mercado novo e revolucionário, de fato, e que está em constante crescimento, desde o seu surgimento.

REFERÊNCIAS

ABDALLA, Ricardo. A Evolução dos Meios de Pagamento: da pré-história à internet das coisas. In: **Canaltech**. 25 Jun. 2017. Disponível em: <<https://canaltech.com.br/mercado/a-evolucao-dos-meios-de-pagamento-da-pre-historia-a-internet-das-coisas-97812/>>. Acesso em: 30 mar. 2018.

ABOBOREIRA, Edgar. **Moedas Virtuais: regulamentação no japão e tendência no Brasil**. Disponível em <<https://www.jota.info/opiniao-e-analise/artigos/moedas-virtuais-regulacao-no-japao-e-tendencia-no-brasil-10052017>>. Acesso em: 20 abr. 2018.

ALVARENGA, Darlan. **Monopólio Brasileiro do Nióbio gera Cobiça Mundial, Controvérsia e Mitos**. Disponível em: <<http://g1.globo.com/economia/negocios/noticia/2013/04/monopolio-brasileiro-do-niobio-gera-cobica-mundial-controversia-e-mitos.html>>. Acesso em: 05 mai. 2018.

BITCOIN BRASIL. **O Que Você Precisa Saber Sobre o Litecoin**. Disponível em: <<https://www.bitcoinbrasil.com.br/o-que-voce-precisa-o-litecoin/>>. Acesso em: 15 mai. 2018.

CALDERON, Barbara. **Deep e Dark Web: a internet que você conhece é apenas a ponta do iceberg**. Rio de Janeiro: Alta Books, 2017.

COLLADO, Carlos; LUCIO, Maria; SAMPIERI, Roberto. **Metodologia de Pesquisa: 5 ed.** São Paulo: Penso Editora, 2013.

GOODRICH, Michael; TAMASSIA, Roberto. **Introdução à Segurança de Computadores**. São Paulo: Bookman, 2013.

Kayo Alexandre Lacerda; Leonardo da Silva Cunha; Cássio Cipriano Nogueira. **MINERAÇÃO DE CRIPTOMOEDAS: ESTUDO COMPARATIVO PÓS-REGULAMENTAÇÃO DO BITCOIN COM ALTERNATIVAS EMERGENTES**. JNT-Facit Business And Technology Journal - ISSN: 2526-4281 QUALIS B1. Março 2021 - Ed. Nº 24. Vol. 1. Págs. 150-168.

HUGHES, Eric. **A Cypherpunk's Manifesto**. Disponível em: <<https://www.activism.net/cypherpunk/manifesto.html>>. Acesso em: 14 mar. 2018.

KOZINETS, Robert. **Netnografia**: realizando pesquisa etnográfica online. São Paulo: Penso Editora, 2010.

MORSE, Eric. **Bitcoin**: uma introdução simples. Babelcube, 2017.

MORTETZ, Tassia. O Que é Paypal e Como Funciona o Serviço? In: **Techtudo**. 23 nov. 2017. Disponível em: <<http://www.techtudo.com.br/noticias/noticia/2014/07/o-que-e-e-como-funciona-o-paypal.html>>. Acesso em: 12 abr. 2018.

NAKAMOTO, Satoshi. **Bitcoin**: a peer-to-peer electronic cash system. Disponível em: <<http://bitcoin.org/bitcoin.pdf>>. Acesso em: 25 de mai. 2018.

NIÓBIO CASH. **Nióbio Cash**: whitepaper. Disponível em: <<https://niobiocash.org/wp-content/uploads/2018/03/WhitePaper-2Fbr.pdf>>. Acesso em: 27 abr. 2018.

OLIVEIRA, Rita. **(Entre)Linhas de uma pesquisa**: o diário de campo como dispositivo de (in)formação na/da abordagem (auto)biográfica. Revista Brasileira de Educação de Jovens e Adultos, v. 2, n. 4, 2014.

PRASS, Ronaldo. **Bitcoin**: o que é a mineração de criptomoedas. Disponível em: <<http://g1.globo.com/tecnologia/blog/tira-duvidas-detecnologia/post/bitcoin-o-que-e-mineracao-de-criptomoedas.html>>. Acesso em: 20 abr. 2018.

PISA, Pedro. **O que é Hash?** Disponível em: <<http://www.techtudo.com.br/artigos/noticia/2012/07/o-que-e-hash.html>> Acesso em: 03 jun. 2018.

RAPAZZO, Lino. **Metodologia Científica**. 3 ed. São Paulo: Edições Loyola, 2005.

SETTI, Rennan; URBIM, Emiliano; VASCONCELLOS, Nelson. **Bitcoin Vira Investimento Mais Sedutor do Planeta em 2017**. Disponível em: <<https://oglobo.globo.com/cultura/bitcoin-vira-investimento-mais-sedutor-do-planeta-em-2017-1-22199179#ixzz5GLYeSPva>>. Acesso em: 03 mai. 2018

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