DOI: 10.5102/un.gti.v7i1.3929

Rentabilidade econômica da mineração de bitcoins e litecoins*

Economic profitability of mining bitcoins and litecoins

Guilherme Albuquerque Barbosa Silva[1]
Carlo Kleber da Silva Rodrigues [2]

Resumo

Este artigo tem o objetivo de analisar a rentabilidade econômica da mineração individual de criptomoedas bitcoins e litecoins. Essa análise é baseada na avaliação da métrica eficiência energética de cada criptomoeada em cinco países da América Latina, almejando-se uma margem de lucro de 0,10 USD/hora. Três variáveis são consideradas para o cálculo da métrica em comento: a taxa de processamento de hashes do equipamento, o consumo de energia elétrica do equipamento em watts e o valor do quilowatt-hora do país onde se realiza a mineração. Os resultados obtidos indicam que a criptomoeda litecoin é uma alternativa mais viável para a mineração do que a criptomoeda bitcoin. Por fim, sugestões para trabalhos futuros encerram este artigo.

Palavras-chave: Rentabilidade. Mineração. Bitcoin. Litecoin. Criptomoeda.

Abstract

This paper has the goal of analyzing the economic profitability of the individual mining process of the bitcoin and litecoin cryptocurrencies, respectively. This analysis is based on the metric named as energy efficiency, which is evaluated for each cryptocurrency in five countries in Latin America, considering a profit goal of 0,10 USD/hour. Three variables are considered to compute the metric: the hash-processing rate of a standard hardware in a certain period of time, the electrical energy consumption, and the price of the kilowatt/hour of the region considered. The final results suggest that Litecoin is the best choice for a more profitable mining process. Lastly, future avenues are mentioned at the end of the article.

Keywords: Profitability. Bitcoin. Litecoin. Mining. Cryptocurrency.

* Recebido em: 19/03/2016.
Aprovado em: 05/01/2017.

[1] Aluno de graduação do curso de Ciência da Computação - FATECS – UniCEUB.

[2] Doutor em Engenharia de Sistemas e Computação pela Universidade Federal do Rio de Janeiro (UFRJ, 2006). Mestre em Sistemas e Computação pelo Instituto Militar de Engenharia (IME, 2000). Graduado em Engenharia Elétrica (Eletrônica e Eletrotécnica) pela Universidade Federal de Campina Grande (UFCG, 1993). Professor do Centro Universitário de Brasília (UniCEUB) nos cursos de Ciência da Computação e Engenharia de Computação.

1 Introdução

Por ser o bitcoin uma criptomoeda livre de interferências cambiais de países (MURPHY, 2013), esta tem sido uma alternativa cada vez mais atrativa para a realização de transações de pagamentos eletrônicos. Corroborando esse pensamento, o mercado de bitcoins já alcançava USD 4,05 bilhões em março de 2015 (WHITE, 2015).

Porém, é preciso dizer que esse mercado é, ainda, instável. Em 2013, o bitcoin teve uma valorização de 6.000% em apenas um ano, alcançando a marca de USD 1.250,00 por bitcoin. Mas, no ano seguinte, perdeu 2/3 do seu valor. Atualmente, um bitcoin é cotado em USD 379,00.

Além dessa instabilidade, o bitcoin sofre, também, com outros tipos de problemas como: a crescente demanda computacional para a realização da mineração e, consequentemente, o maior consumo de energia elétrica, resultando em um negativo impacto ambiental.

Alternativas de criptomoedas cresceram desde o ano de 2011, com destaque para aquela denominada de litecoin. Em 2013, essa criptomoeda teve um crescimento de 400% e, em seu ápice, chegou a ser cotada em USD 48,05. Trata-se de uma alternativa que possui a característica de um processo de mineração mais rápido que aquele do bitcoin. Além disso, como ainda não existem muitas opções de hardware especializado para mineração de litecoin, cria-se uma competição mais democrática entre os possíveis mineradores, pois estes tendem a utilizar o mesmo hardware.

Ante o exposto, surge a seguinte pergunta ainda em aberta na literatura: a despeito da complexidade computacional e sob o ponto de vista da rentabilidade econômica, é mais vantajoso minerar litecoins que bitcoins?

Dentro desse contexto, o presente trabalho tem o objetivo de analisar a rentabilidade econômica da mineração individual das criptomoedas bitcoin e litecoin, respectivamente. Essa análise baseia-se na avaliação da métrica eficiência energética nos cinco países mais ricos da América Latina, almejando-se uma margem de lucro de 0,10 USD/hora. Três variáveis são consideradas para o cálculo dessa métrica: a taxa de processamento de hashes do hardware empregado, o consumo de energia elétrica em watts e o valor em dólares do quilowatt-hora.

A organização do restante desse texto é descrita a seguir. A Seção 2 apresenta, sucintamente, o protocolo Bitcoin e as suas principais diferenças com relação ao protocolo Litecoin. Os trabalhos relacionados são discorridos na Seção 3. Na Seção 4, são apresentados e discutidos os experimentos e os resultados alcançados. Por fim, as conclusões finais e os direcionamentos para trabalhos futuros aparecem na Seção 5.

2 Fundamentos

2.1 Protocolo *Bitcoin*

O protocolo *Bitcoin* é o resultado de um artigo publicado em novembro de 2008 sobre a ideia de uma criptomoeda, denominada de *bitcoin*, que funciona, de forma anônima e, principalmente, sem depender da confiança em qualquer usuário do sistema (NAKAMOTO, 2008). *Satoshi* é o nome dado a menor quantidade de *bitcoins* que pode ser enviada em uma transação: 0,00000001 *bitcoin* (BADEV et al., 2008). Esse protocolo é implementado sobre uma rede *peer-to-peer* (P2P) de alcance mundial, redundado em um eficiente sistema de transações comerciais ou pagamentos eletrônicos.

Um ponto de significativa importância é o fato de a moeda *bitcoin* ser descentralizada, i.e., a própria arquitetura da rede *P2P* garante a autenticidade e o saldo financeiro (i.e., saldo da carteira virtual de *bitcoins*) de todas as pessoas envolvidas. Por isso, o *bitcoin* está livre de influências alfandegárias de bancos centrais de países e interferências políticas no valor da moeda (DOWD; HUTCHINSON, 2015).

A arquitetura do protocolo *Bitcoin* é baseada em um *livro-razão* ou *ledger* público, em que todos os usuários têm acesso a todas as transações e saldos, mas, como são utilizados números em vez de nomes, a privacidade é, então, preservada (NAKAMOTO, 2008).

Toda vez que uma transação em *bitcoins* é realizada, o *ledger* é atualizado em todos os computadores da rede. Para exemplificar, considere a transação fictícia explicada a seguir entre dois usuários imaginários: Amanda e Bruno. Amanda compra um produto de Bruno no valor de 1,0 BTC (BTC = *bitcoin*). Tanto o *ledger* de Bruno quanto o de Amanda vão ter seus saldos alterados: em mais 1,0 BTC (para Bruno) e menos 1,0 BTC (para Amanda). No entanto, o restante da rede inteira, também, tem que atualizar seus respectivos *ledgers* para conter os saldos atualizados de Bruno e Amanda.

2.1 Conceito de *Block-chain*

Em relação ao exemplo da subseção anterior, quando Amanda envia 1,0 BTC para Bruno, é como se

Amanda estivesse assinando um documento público que atesta: *Eu, Amanda, estou dando 1,0 BTC para Bruno*. A assinatura dessa transação é realizada pelo conceito de par de chaves assimétricas, em que Amanda, como qualquer usuário da rede *Bitcoin*, possui duas sequências de dígitos aleatórios que formam as *chaves pública* e *privada*, respectivamente.

O protocolo *Bitcoin* utiliza o algoritmo ECDSA (*Elliptic Curve Digital Signature Algorithm*) para implementar o conceito de chaves assimétricas que, nesse caso, é um número inteiro de 256 bits de tamanho (NAKAMOTO, 2008). O conhecimento da chave privada é único e exclusivo de Amanda e, juntamente a essa chave privada, é gerada outra sequência de dígitos que formam a chave pública de Amanda (ESKANDARI et al., 2015).

Esse sistema de chaves garante a autenticidade de quem e, ainda, para quem a transação é realizada, mas não garante que Amanda não possa gastar a mesma moeda mais de uma vez ou utilizar a mesma chave daquela transação em outras transações. Dado que se decorre um tempo para propagar o *ledger* atualizado, Amanda poderia realizar outra transação enquanto a antiga não se propagou por toda a rede. Nesse caso, a rede teria dificuldades em diferenciar qual é a transação legítima.

A solução para o problema anteriormente descrito se dá pelo emprego do conceito de *block-chain*, explicado a seguir. Propagam-se as transações recém-realizadas, mas, ainda, não validadas, por toda a rede. Essas transações são então agrupadas em blocos. Cada bloco é validado pelo *minerador* (i.e., *hardware* utilizado para validação) por meio de um processo matemático de alta complexidade, envolvendo *hash criptográfico* (NAKAMOTO, 2008).

Após validado, o bloco é, então, adicionado a uma cadeia de blocos, que leva desde o primeiro bloco, contendo a primeira transação já realizada na história do *Bitcoin*, até a transação mais recentemente validada. Essa cadeia é denominada de *block-chain* e é a base de informação para implementar o *ledger* púbico.

É pouco provável que dois ou mais *mineradores* consigam resolver o processo matemático, citado anteriormente, no mesmo instante. Porém, prevendo essa situação, toda vez que o bloco é colocado na *block-chain*, ele é colocado, na verdade, em uma ramificação da *block-chain* original, denominada *branch*, e os *mineradores* posteriores vão, sempre, escolhendo a *branch* de maior tamanho (i.e., comprimento mais longo). A convergência para a *branch* a ser, definitivamente, aceita (i.e., aquela de maior comprimento entre todas existentes) ocorre em, aproximadamente, seis blocos ou, como cada bloco leva cerca de dez minutos, em uma hora (NIELSEN, 2013).

2.2 Conceito de *Proof-of-work*

O processo matemático a ser realizado pelo *minerador* está relacionado ao algoritmo *hash* criptográfico SHA-256 (NAKAMOTO, 2008). De forma simples, o *minerador* precisa descobrir um número inteiro de 4 bytes, denominado de *nonce*, capaz de satisfazer a uma desigualdade (inequação) expressa em função desse algoritmo.

O método de descobrimento usado pelo *minerador* é baseado em tentativas e a condição de desigualdade é estabelecida considerando-se um valor máximo, denominado de *target difficulty*, que é ajustado, consensualmente, pelos nós da rede para garantir que, em média, apenas um bloco de transações válidas seja adicionado à *block-chain* a cada 10 minutos.

O valor correto descoberto pelo minerador, ou seja, o *nonce* correto ou *golden nonce*, é a prova de trabalho, ou *proof-of-work*, que o cálculo iterativo (por tentativas) foi realizado e que o bloco pode ser adicionado ao *block-chain* (AUMASSON, 2009).

De forma sistêmica, para a adequada e eficiente operação do processo de *mineração*, o protocolo *Bitcoin* depende, naturalmente, de que muitos *mineradores* estejam validando blocos a todo momento, o que consome um elevado poder computacional e, consequentemente, energia elétrica.

Para incentivar os *mineradores* a validar os blocos, o protocolo *Bitcoin* prevê uma recompensa em *bitcoins* para quem primeiro conseguir encontrar o *golden nonce*. Essa recompensa é conhecida como *payout* (NAKAMOTO, 2008). É importante ressaltar que esse valor não é fixo, sendo alterado de tempos em tempos.

Quando o *Bitcoin* foi lançado, o seu *payout* era de 50,0 BTC. Esse valor de *payout* é dividido por 2 a cada 230.000 blocos minerados na rede ou, aproximadamente, a cada quatro anos, já que cada bloco leva cerca de 10 minutos para ser minerado. Esse ajuste é conhecido como *halving*. O *Bitcoin* já passou por um *halving* e, atualmente, cada bloco minerado é recompensado com 25,0 BTC.

2.3 Protocolo *Litecoin*

Em outubro de 2011, o protocolo *Litecoin* foi desenvolvido por Charles Lee, então funcionário da empre-

sa Google. É um projeto de código aberto que, na época, foi lançado em plataformas de desenvolvimento colaborativas (BRADBURY, 2013). Esse protocolo possui o tempo de mineração de cada bloco estimado em 2,5 minutos.

Ressalta-se que a ideia do protocolo *Litecoin* não foi a de substituir a mineração de *bitcoins*, mas permitir a mineração conjunta de *bitcoins* e *litecoins*. O *Litecoin*, também, passa pelo evento de *halving* a cada quatro anos aproximadamente. Por último, o algoritmo usado pelo *Litecoin*, para estabelecer o processo matemático da *mineração*, é o *Scrypt* (PERCIVAL, 2009). Para fins de mera comparação, as principais características dos protocolos *Litecoin* e *Bitcoin*, respectivamente, são destacadas na Tabela 1.

Tabela 1 - Diferenças entre *Litecoin* e *Bitcoin*.

Criptomoeda	Tempo médio para minerar um bloco	Algoritmo de hash criptográfico	Tempo para cada evento de halving	Valor atual em USD
Litecoin	2,5 minutos	Scrypt	4 anos	3,37
Bitcoin	10,0 minutos	SHA-256	4 anos	379

Fonte: Os autores.

Para encerrar, cabe mencionar que existem, basicamente, três formas de se obter criptomoedas: por meio de uma transação entre criptomoedas, adquirindo criptomoedas com dinheiro real e, por último, por meio do processo de mineração. Essa última pode ser realizada em grupos de distintos hardwares (denominados de pools) ou, ainda, por meio da mineração individual, i.e., utilizando-se um único hardware. O foco deste trabalho é a mineração individual.

3 Trabalhos relacionados

A rentabilidade da mineração individual de criptomoedas ainda é um tema pouco discutido na literatura. Tendo-se ciência desse relativo ineditismo, esta seção busca, alternativamente, discorrer sobre quatro dos trabalhos mais recentes da literatura que contribuem ou se relacionam, mesmo de forma indireta, com o objetivo deste trabalho.

O trabalho de Rosenfield (2011) se propõe a compreender os aspectos da rentabilidade por mineração em pools. O trabalho concluiu que, por causa da alta variância nas recompensas da mineração individual, a necessidade de mineração em pools se faz importante e não pode ser desconsiderada.

O trabalho de Luther (2015) investiga a possibilidade de as criptomoedas serem mais amplamente usadas ou se tornaram dinheiro de um nicho *mais específico do mercado. O* trabalho conclui que o Bitcoin representa um real avanço tecnológico no processamento de pagamentos, embora seja, também, verdade que o desenvolvimento de outras criptomoedas possa vir em algum momento tornar o Bitcoin obsoleto, passando este a ser reconhecido apenas como o percursor das criptomoedas.

O trabalho de Chávez e Rodrigues (2015) demonstra formas de decidir, analiticamente, quando é mais vantajoso trocar, automaticamente, de pools a fim de manter a rentabilidade considerada. O trabalho concluiu que a mineração considerando o salto entre pools é mais eficiente do que a mineração considerando apenas um único pool.

Por fim, o trabalho de Pazmiño e Rodrigues (2015) avalia o tempo de verificação de transações e, nesse contexto, propõe um esquema para a divisão da base de dados de um nó da rede bitcoin, considerando o hardware disponível localmente no usuário. Os resultados finais são, numericamente, atrativos, resultando em otimizações de até 71,42% no tempo de verificação de transação.

4 Rentabilidade com *Bitcoin* e *Litecoin*

Tanto o *Bitcoin* quanto o *Litecoin* garantem, atualmente, 25 moedas em seu *payout*. Para ambos, a *target difficulty* (ou, simplesmente, dificuldade), representada pela letra *D*, refere-se à complexidade para se minerar um bloco, sendo ajustada de forma que qualquer valor de tentativa para encontrar o valor de *nonce* tenha, sempre, a razão de $\frac{1}{2^{32} * D}$ de sucesso.

O valor atual de *D* para o protocolo *Bitcoin* é 144.116.447.847 e, para o protocolo *Litecoin*, é 54.656. A taxa com que um *hardware* consegue testar valores para descobrir o *golden nonce* é denominada de *hashrate*, representada pela letra *h*.

Considerando-se, então, o tempo de mineração *t*, um *hardware* pode realizar um total de *h*t* tentativas (ou *hashes*) para descobrir o valor do *golden nonce*. Ainda, a quantidade de *bitcoins Q* a ser recebida, em um certo intervalo de tempo *t* de *mineração*, pode ser estimada pela Equação 1 (ROSENFIELD, 2011).

$$Q = \frac{h * t}{2^{32} * D} * payout \quad (1)$$

Propõe-se, agora, calcular a *rentabilidade econômica da mineração* de uma moeda para qualquer país

conforme raciocínio apresentado a seguir. Para esse cálculo, consideram-se os gastos de energia elétrica (*Despesa*) e o ganho durante o período (*Receita*), ambos calculados em dólares.

O valor da *Receita* é obtido pela Equação 2 e o valor de *Despesa* é obtido por meio da Equação 3. Sendo assim, a rentabilidade esperada é calculada como *Receita* menos *Despesa*, dado um certo período de tempo.

Explica-se que o valor de *Receita* é calculado levando-se em conta o valor *Q* de moedas recebidas durante o período de tempo de mineração *t* (Equação 1), bem como o valor de cotação atual em dólares da criptomoeda considerada, representado por V_c.

$$Receita = Q * V_c \quad (2)$$

Ainda, explica-se, também, que *Despesa*, durante a atividade de mineração, está relacionada ao valor do kWh da região onde a mineração em si é realizada. Também se leva em conta a potência do equipamento (*hardware*) de mineração *P*, dada em watts, que serve para o cômputo de quanta energia o equipamento precisa utilizar em determinado período de tempo *T*, medido em horas.

$$Despesa = \frac{P * T}{1000} * kWh \quad (3)$$

Considere que a rentabilidade almejada seja de USD 0,10 por hora (i.e., USD 0,10/h). Esse valor é escolhido por ser compatível com o cenário atual da atividade de *mineração*, observado em *sites* populares da Internet que reportam sobre valores estimados para esse tipo de atividade. No entanto, é preciso esclarecer que esse valor absoluto não é importante para efeito das conclusões e observações a serem alcançadas neste trabalho, pois aqui tenciona-se uma análise comparativa (relativa) e não absoluta.

Considere, ainda, que a região onde a mineração é realizada seja o país Brasil. Utilizando-se, então, as Equações 1 e 2 e, também, um equipamento (*hardware*) padrão de *mineração* de potência máxima de 100 watts, chega-se aos seguintes resultados: *Despesa* = USD 0,0096 e *Receita* = USD 0,1096, ambos por hora.

Como mencionado, para se encontrar o *golden nonce*, é necessário observar a medida de *hashrate* do equipamento. Isso para que o valor de *hashrate* seja suficiente para encontrar um bloco no tempo necessário para preservar o lucro esperado ao final da mineração. É considerado um valor de *hashrate* mínimo ou h_{min}. A Equação 4 apresenta a fórmula para obter o valor de h_{min}. Observe que essa equação é derivada a partir das Equações 1, 2 e 3.

$$h_{min} = \frac{rentabilidade * 2^{32} * D}{t * payout * V_c} \quad (4)$$

A métrica *eficiência energética EE*, definida neste trabalho, é medida em hash/J e representa quantos *hashes* um *hardware* padrão precisa calcular, utilizando 1 joule de energia, para que se preserve a rentabilidade almejada. Pode-se, então, calcular *EE* a partir do valor de h_{min} (Equação 4) da região considerada e o valor de potência do equipamento empregado, conforme Equação 5.

$$EE = \frac{h_{min}}{P} \quad (5)$$

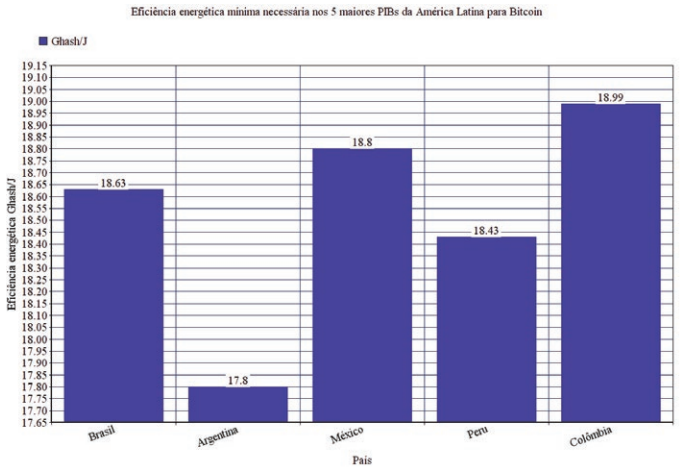
Segundo a ANEEL (Agência Nacional de Energia Elétrica), a taxa de kWh mais barata do Brasil é a da concessionária de energia do Rio Grande do Norte (RN), conhecida como COSERN (Companhia energética do Rio grande do Norte), no valor de R$ 0,37590/kWh. Considerando-se a cotação do dólar em R$ 3,93, tem-se, então, o valor de 0,096 USD/kWh. Por fim, pelo Sistema Internacional de Unidades (SI), sabe-se que: 1 watt = 1 J/s (Joule/segundo) e, ainda, 1 hora = 3600 segundos.

Admitindo-se, então, o custo de energia de kWh dado anteriormente e um equipamento que não consuma mais do que 100,0 W e, ainda, substituindo-se os valores do cenário brasileiro na Equação 4, chega-se a um valor de h_{min} de, aproximadamente, 1863,0 Ghash/s para garantir a lucratividade de 0,10 USD/h. Aplicando-se esse valor de h_{min} na Equação 5, chega-se, então, ao seguinte resultado: *EE* = 18,63 Ghash/J.

Considerando-se agora o protocolo *Litecoin* e um raciocínio análogo ao que acabou de ser descrito para o protocolo *Bitcoin*, há os seguintes resultados: h_{min} = 86,37 Mhash/s e *EE* = 0,86 Mhash/J, para o país Brasil.

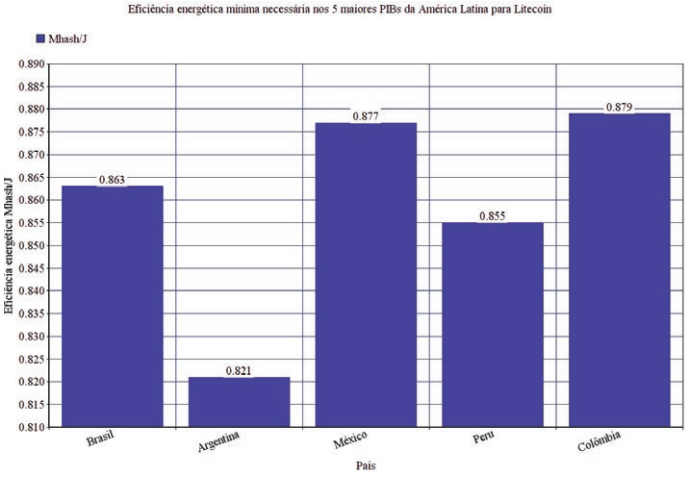
Para analisar o cenário América Latina, escolhem-se os cinco países de maiores PIBs (Produto Interno Bruto) por juntos representarem mais de 80% do PIB total da América Latina. Os resultados estão nas Figuras 1 e 2. A partir dessas figuras, é possível, imediatamente, perceber que os valores resultantes para o protocolo *Bitcoin* são bem superiores àqueles obtidos para o protocolo *Litecoin*. Os valores dos kWh dos países considerados estão na Figura 3. A partir dessa figura, observa-se, imediatamente, que a Argentina possui o menor valor, enquanto a Colômbia o maior.

Figura 1 - Eficiência energética (mínima) para o protocolo *Bitcoin*



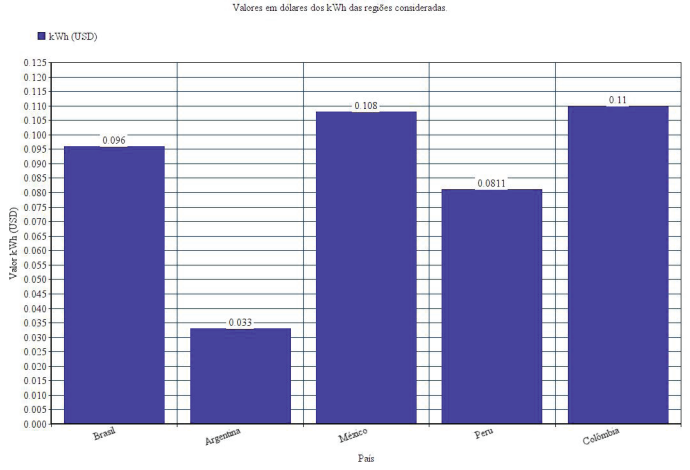
Fonte: Os autores.

Figura 2 - Eficiência energética (mínima) para o protocolo *Litecoin*.



Fonte: Os autores.

Figura 3 - Valores do kWh dos 5 países de maiores PIBs na América Latina



Fonte: Os autores.

Ressalta-se, no entanto, que, para mineração individual, o valor do *payout* é pago de uma só vez e, apenas, ao final do processo de mineração (i.e., quando o valor do *golden nonce* é encontrado). Ou seja, apenas ao término da *mineração*, o *minerador* recebe seu *payout,* o qual corresponde, atualmente, a 25 moedas.

Assim, para o estimar o tempo médio em segundos, necessário para encontrar um bloco para ambos protocolos (i.e., *Bitcoin* e *Litecoin*), devem, então, ser considerados o valor de h_{min} e o valor da dificuldade atual D, conforme Equação 6.

$$t = \frac{2^{32} * D}{h_{min}} \quad (6)$$

Por meio da Equação 6 e admitindo-se o país Brasil, onde h_{min} = 1863 Ghash/s e D = 144116447847, um bloco do *Bitcoin* seria, então, resolvido em, aproximadamente, $3{,}32 \times 10^8$ s. Convertendo-se esse valor em dias, tem-se, aproximadamente, 3.845 dias (ou seja, cerca de 10,53 anos) para se achar um bloco e receber 25 moedas (*payout* atual). Com a cotação atual, seriam USD 9.588,00 de lucro. Considerando-se agora o mesmo cenário de análise e substituindo-se os valores de D e h_{min} para o protocolo *Litecoin*, esse tempo t seria cerca de, apenas, 30 dias, e o valor das 25 moedas seria de USD 77,75.

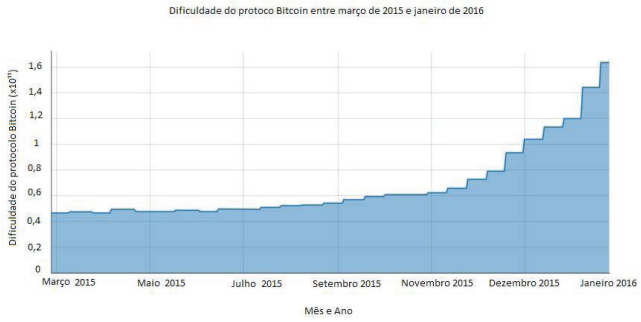
O resultado do cálculo anterior alerta para o fato de que, no período de 10 anos, tanto a moeda *bitcoin* como *litecoin* teriam passado por dois *halvings*, o que faria o valor de 25 moedas se tornar um quarto do valor original, ou seja, 6,25 moedas apenas. Nesse sentido, observe que o cálculo de *EE* proposto não leva em conta os eventos de *halvings* ao longo do tempo de *mineração*.

Para efeito de análise com a intenção de evitar-se o evento de *halving* e, portanto, garantir as 25 moedas de *payout*, admita o processo de mineração durando no máximo 4 anos (tempo limite para evitar-se o evento de *halving*), ou seja, um bloco deve ser minerado a cada 1460 dias em média. A partir da manipulação das equações anteriores, é possível mostrar que a *EE* tem que ser aumentada em, aproximadamente, 263,3%, fazendo a taxa de hash/s do Brasil igual a 4905 Ghash/s (ou o equivalente em 49,05 Ghash/J de energia).

Observe, ainda, que, ao longo de 10 anos, a dificuldade D e o valor da moeda, relacionadas ao protocolo *Bitcoin*, podem sofrer variações significativas. Isso faz com que projeções em longo prazo sejam difíceis e geralmente imprecisas. Por outro lado, tendo em vista que, no cenário considerado, o ganho obtido pelo uso do protocolo *Litecoin* seria alcançado em cerca de apenas 30 dias, as projeções se tornam mais confiáveis e o evento de

halving não influenciaria o lucro obtido ao final do período estimado para minerar um bloco. Para evidenciar essa imprevisibilidade, a Figura 4 mostra a flutuação da dificuldade *D* do protocolo *Bitcoin* no período de março de 2015 até janeiro de 2016.

Figura 4 - Flutuação da dificuldade *D* do protocolo *Bitcoin*.



Fonte: Os autores**.**

Ante as informações e discussões anteriores, os seguintes pontos gerais merecem destaque. Primeiro, o algoritmo de *proof-of-work* empregado pelo protocolo *Litecoin* (i.e., algoritmo *Scrypt*) é mais focado em uso de memória do que em uso de processador. Essa condição permite que equipamentos não necessariamente especializados (i.e., domésticos) possam ser utilizados, com o objetivo de lucro, mais facilmente para a *mineração* no caso do protocolo *Litecoin* que no caso do protocolo *Bitcoin*.

Segundo, o protocolo *Litecoin* é uma alternativa mais viável para mineração individual, tendo em vista que o tempo para receber a recompensa por bloco *minerado* (i.e., *payout*) é bem inferior do que aquele observado para o protocolo *Bitcoin*. Por isso, o protocolo *Litecoin* é bem menos susceptível a mudanças, como a variação do preço do kWh e a flutuação da dificuldade de *mineração* da moeda.

Por fim, a questão central desta pesquisa pode ser satisfatoriamente respondida como segue. É possível afirmar que: mesmo que o valor de cotação atual da moeda *litecoin* seja inferior àquele da moeda *bitcoin*, há evidências contundentes que indicam que é mais vantajoso realizar o processo de mineração individual de moedas *litecoins* que de moedas *bitcoins*.

5 Conclusões e trabalhos futuros

Este artigo teve o objetivo de analisar a rentabilidade econômica da mineração individual de criptomoedas *bitcoins* e *litecoins*. Essa análise foi baseada na avaliação da métrica *eficiência energética* de cada criptomoeada em cinco países da América Latina, almejando-se uma margem de lucro de 0,10 USD/hora. Três variáveis foram consideradas para o cálculo da métrica: a taxa de processamento de *hashes* do equipamento, o consumo de energia elétrica do equipamento, e o valor do quilowatt-hora do país da mineração.

Dentre os resultados mais importantes, os seguintes podem ser destacados: (1) para uma mesma rentabilidade econômica do processo de *mineração* individual, o protocolo *Litecoin* demanda menor *eficiência energética* que o protocolo *Bitcoin*; (2) o processo de mineração do protocolo *Bitcoin* exige o emprego de *hardwares* especializados de alto poder de processamento computacional, o que faz com o processo de mineração em *pools* seja o mais indicado; (3) o processo de mineração do protocolo *Litecoin* admite o emprego de *hardwares* domésticos, o que torna bem viável o processo de mineração individual; (4) a mineração individual do protocolo *Litecoin* tende a ser mais vantajosa que a mineração individual do protocolo *Bitcoin*.

Por fim, como possível trabalho futuro, sugere-se o estudo de métodos de *proof-of-work* para o protocolo *Bitcoin* que não sejam amparados exclusivamente no poder de processamento de *hashes* dos *hardwares* utilizados (POON; THADDEUS, 2016). Caso fosse possível reduzir a demanda por poder de processamento computacional, a demanda por energia elétrica, consequentemente, diminuiria, bem como *hardwares* mais simples poderiam ser utilizados. Isso proporcionaria um maior grau de competitividade ao protocolo *Bitcoin* frente a protocolos de mesma finalidade.

Referências

AUMASSON, Jean-Phillipe et al. *Cryptanalysis of Dynamic SHA* (2). 2009. Disponível em: <https://eprint.iacr.org/2009/184.pdf>. Acesso em: 8 fev. 2016.

BADEV, A.; CHEN, M. *Bitcoin:* technical background and data analysis. 2014. Disponível em: <http://www.federalreserve.gov/econresdata/feds/2014/files/2014104pap.pdf>. Acesso em: 4 fev. 2016.

BRADBURY, D. *Litecoin founder Charles Lee on the origins and potential of the world's second largest cryptocurrency.* 2013. Disponível em: <http://www.coindesk.com/

litecoin-founder-charles-lee-on-the-origins-and-potential-of-the-worlds-second-largest-cryptocurrency/>. Acesso em: 20 fev. 2016.

DOWD, K.; HUTCHINSON. M. Bitcoin will bite the dust. *Cato Journal*, v. 35, n. 2. 2015. Disponível em: <http://object.cato.org/sites/cato.org/files/serials/files/cato-journal/2015/5/cj-v35n2-12.pdf>. Acesso em: 8 fev. 2016.

ESKANDARI, S. et al. *A first look at the usability of Bitcoin key management*. 2015. Disponível em: <http://www.internetsociety.org/sites/default/files/05_3_3.pdf>. Acesso em: 9 fev. 2016.

WHITE, L. H. The market for cryptocurrencies. *Cato Journal*, v. 35, n. 2, 2015. Disponível em: <http://object.cato.org/sites/cato.org/files/serials/files/cato-journal/2015/5/cj-v35n2-13.pdf>. Acesso em: 2 fev. 2016.

LUTHER, W. J. *Bitcoin and the future of digital payments*. 2015. Disponível em: <http://ssrn.com/abstract=2631314>. Acesso em: 10 fev. 2016.

MURPHY, R. P. The economics of Bitcoin. *Library and Liberty*. 2013. Disponível em: <www.econlib.org/library/Columns/y2013/Murphybitcoin.html>. Acesso em: 10 fev. 2016.

NAKAMOTO, Satoshi. *Bitcoin:* a peer-to-peer electronic cash system. 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 30 dez. 2015.

NIELSEN, M. *How the Bitcoin protocol actually works*. 2013. Disponível em: <http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/>. Acesso em: 9 fev. 2016.

PERCIVAL, C. *Stronger key derivation via sequential memory-hard functions*. 2009. Disponível em: <http://www.tarsnap.com/scrypt/scrypt.pdf>. Acesso em: 30 jan. 2016.

POON, J.; THADDEUS, D. *The Bitcoin lightning network:* acalable off-chain instant payments. 2016. Disponível em: <http://lightning.network/lightning-network-paper.pdf>. Acesso em: 25 jan. 2016.

ROSENFIELD, Meni. *Analysis of Bitcoin pooled mining reward systems*. 2011. Disponível em: <https://bitcoil.co.il/pool_analysis.pdf>. Acesso em: 30 jan. 2016.

CHÁVEZ, J. J. G.; RODRIGUES, C. K. S. Hopping among pools in the Bitcoin mining network. *The SIJ Transactions on Computer Networks & Communication Engineering (CNCE),* v. 3, n. 2, 2015.

PAZMIÑO, J. E.; RODRIGUES, C. K. S. Simply dividing a Bitcoin network node may reduce transaction verification time. *The SIJ Transactions on Computer Networks & Communication Engineering (CNCE),* v. 3, n. 2, 2015.