Mineração individual de *bitcoins* e *litecoins* no mundo

Guilherme Albuquerque B. Silva[1], Carlo Kleber da S. Rodrigues[1]

[1]Faculdade de Tecnologia e Ciências Sociais Aplicadas – Centro Universitário de Brasília (UniCEUB) – Brasília – DF – Brasil.

guilhermealbuquerque1@hotmail.com, carlokleber@gmail.com

Abstract. *This paper analyzes the solo mining process of the bitcoin and litecoin cryptocurrencies all over the world. The goal is to identify which one turns out to be the most profitable one. To this end, the metric named as energy efficiency is used and three continents are taken as mining regions: America, Asia and Europe. Three variables are considered to compute the above metric: the hash-processing rate of the hardware, the electrical energy consumption of the hardware, and the price of the kilowatt-hour of the mining region. The final results suggest that mining litecoins turns to be more profitable than mining bitcoins. Lastly, general conclusions and future avenues come at the end of this paper.*

Resumo. *Este artigo analisa a mineração individual das criptomoedas bitcoin e litecoin no mundo. O objetivo é identificar aquela que é economicamente mais rentável. Para tanto, utiliza-se a métrica denominada eficiência energética e consideram-se três continentes como regiões de mineração de cada criptomoeada: América, Ásia e Europa. O cálculo dessa métrica considera três variáveis: a taxa de processamento de hashes do hardware, o consumo de energia elétrica do hardware em watts, e o valor do quilowatt-hora da região de mineração. Os resultados finais indicam que minerar litecoins é mais rentável que minerar bitcoins. Conclusões gerais e possíveis trabalhos futuros finalizam este artigo.*

1. Introdução

Criptomoedas são formas de dinheiro virtual que contam com métodos criptográficos para assegurarem a geração e a distribuição de valores de forma segura por meio de uma rede de computadores [Bank for International Settlements, 2015]. As criptomoedas são livres de interferências cambiais de governos e dão relativa segurança às transações financeiras realizadas com elas. Duas criptomoedas bem populares e comercialmente atrativas são *bitcoin* e *litecoin* [Murphy, 2013].

O principal processo de obtenção de criptomoedas não advindo de uma transação financeira é denominado de *mineração*. Esse processo consiste em adquirir digitalmente a posse de um certo número de criptomoedas a partir de um esforço computacional despendido pelo *hardware* de uma pessoa (i.e., *minerador*) que realiza esse processo [Nakamoto, 2008].

O *bitcoin* foi criado em 2008 [Nakamoto, 2008] e alcançou a expressiva marca de USD 4,05 bilhões em seu mercado de transações no ano de 2015 [White, 2015]. Esse mercado é, no entanto, ainda instável. Por exemplo, o *bitcoin* teve uma valorização de 6.000% em 2013, alcançando a marca de USD 1.250,00 por *bitcoin*. No ano seguinte, porém, perdeu 2/3 do seu valor. Atualmente, um *bitcoin* (ou 1,0 BTC) é cotado em USD 454,90.

Dentre as outras criptomoedas que surgiram desde a criação do *bitcoin*, destaca-se a criptomoeda *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 um processo de mineração mais fácil e mais rápido que aquele do *bitcoin*. Além disso, como ainda não existem muitas opções de *hardware* especializado para a mineração de *litecoins*, há uma competição mais equânime entre os possíveis mineradores, pois estes tendem a utilizar o mesmo *hardware*. Diante disso, surge então a seguinte pergunta: a despeito da complexidade computacional e sob o ponto de vista da rentabilidade econômica, é mais vantajoso minerar *litecoins* que *bitcoins*?

Dentro deste contexto, este trabalho objetiva analisar a rentabilidade econômica da mineração individual das criptomoedas *bitcoin* e *litecoin*. Essa análise baseia-se na avaliação da métrica *eficiência energética* nos países com maiores Produtos Internos Brutos (PIBs) das seguintes regiões: América, Europa e Ásia, almejando-se uma rentabilidade 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 (kWh).

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

2. Fundamentos

2.1 Protocolo Bitcoin

O protocolo *Bitcoin* foi originalmente anunciado em um artigo publicado em novembro de 2008, o qual definiu uma forma de criptomoeda que funciona de forma pseudônima e sem depender da confiança em qualquer usuário do sistema [Nakamoto, 2008]. Esse protocolo foi desenvolvido considerando o paradigma de uma rede *peer-to-peer* (P2P) de alcance mundial, resultando em um sistema de transações financeiras de escala global.

A arquitetura do protocolo *Bitcoin* é baseada na implementação de um livro-razão ou *ledger* público, onde todos os usuários têm acesso a todas as transações. No entanto, como são utilizados números em vez de nomes, a privacidade é preservada [Nakamoto, 2008]. Sempre que ocorre uma transação na rede, tanto o *ledger* do beneficiário quanto o do pagador vão ser alterados. De forma semelhante, o restante dos nós da rede atualiza seus *ledgers* para conter essa transação.

2.2 Conceito de Block-chain

Quando o pagador de uma transação em *bitcoins* envia certa quantia para outro usuário é como se esse pagador estivesse assinando um documento público que atesta a transferência de posse daquela quantia para o outro usuário. A assinatura dessa transação é realizada pelo conceito de par de chaves assimétricas, onde um mesmo usuário da rede possui duas sequências de dígitos únicos que formam as chaves pública e privada, respectivamente.

O sistema de chaves criptográficas assimétricas garante a autenticidade de quem e para quem a transação é realizada, mas não garante que um mesmo usuário não possa gastar aquela mesma quantia mais de uma vez em outras transações. Dado que se decorre um tempo para propagar-se o *ledger* atualizado, qualquer usuário poderia teoricamente realizar outra transação enquanto a antiga não se propagou por toda a rede. Nesse caso, a rede teria dificuldades em diferenciar qual transação seria a legítima.

A forma encontrada pelo protocolo para solucionar 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 pelos mineradores no processo de mineração.

Após validado, o bloco é então adicionado a uma corrente (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. Os blocos que não forem validados pelos mineradores são descartados. Essa corrente é denominada de *block-chain* e é a base de informação para implementar o *ledger* público.

2.3 Conceito de Proof-of-work

Nakamoto (2008) definiu que o processo matemático realizado pelo minerador ocorre por meio do algoritmo *hash* criptográfico *SHA-256*. Esse algoritmo faz com que minerador precise 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 múltiplas tentativas, e a condição de desigualdade é estabelecida considerando-se um valor máximo, denominado de *target difficulty*, que é ajustado pelo algoritmo para garantir que, em média, apenas um bloco de transações válidas seja adicionado à *block-chain* a cada 10 minutos.

O *nonce* descoberto, também chamado de *golden nonce*, é a *proof-of-work* (prova de trabalho) que o cálculo iterativo por tentativas foi de fato realizado e que o bloco pode então ser adicionado à *block-chain* [Rocha e Rodrigues, 2016]. Para incentivar os mineradores a validar os blocos, o protocolo prevê uma *reward* (recompensa) em *bitcoins* para quem primeiro conseguir encontrar o *golden nonce*. Essa recompensa não tem um valor fixo, sendo alterada de tempos em tempos [Rosenfeld, 2016].

Quando o *Bitcoin* foi lançado, o seu *reward* era de 50,0 BTC. Esse valor de *reward* 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 dez 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.

2.4 Protocolo Litecoin

O protocolo *Litecoin* foi desenvolvido por Charles Lee, então funcionário da empresa Google, em outubro de 2011. 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, sendo o valor da *reward* atual igual a 25,0 *litecoins.* Semelhantemente ao protocolo *Bitcoin*, o *Litecoin* também passa pelo

evento de *halving* a cada quatro anos aproximadamente. O algoritmo usado pelo *Litecoin* para estabelecer o processo matemático da mineração é o *Scrypt* [Percival, 2009].

É preciso ressaltar que a ideia do protocolo *Litecoin* não foi a de substituir a mineração de *bitcoins*, mas permitir que ambas criptomoedas coexistam nos mercados financeiros. Comparativamente, a principal diferença entre os algoritmos de *proof-of-work* dos protocolos é que o *SHA-256* (do *Bitcoin*) é focado em uso intensivo do processador, enquanto que *Scrypt* (do *Litecoin*) é focado no uso intensivo de memória. Disto resulta a necessidade de *hardwares* especializados para mineração de *bitcoins*, e de *hardwares* de uso geral para mineração de *litecoins*.

Para encerrar esta seção, cabe ainda mencionar que existem basicamente três formas de se obter criptomoedas: por meio de uma transação entre criptomoedas; comprando-se criptomoedas com dinheiro real; e, por último, por meio do processo de mineração. Esta última pode ser ainda realizada de duas formas: de maneira coletiva (i.e., *pools* de mineradores) e por meio da *mineração individual*, i.e., utilizando-se um único *hardware*. O foco deste trabalho é a mineração individual.

3. Trabalhos Relacionados

A análise formal da rentabilidade da mineração individual de criptomoedas ainda é um tema relativamente recente na literatura. Tendo-se conhecimento desta pouca exploração científica, esta seção busca discorrer brevemente sobre alguns dos trabalhos mais recentes da literatura que contribuíram ou se relacionaram, mesmo de forma indireta, com o objetivo deste trabalho.

Rosenfeld (2011) propõe a compreender os aspectos da rentabilidade por mineração em *pools*. O trabalho conclui 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 Kiayias e Panagiotakos (2016) compara a eficiência da tecnologia de *block-chain* sob a ótica da segurança, considerando as alternativas mais modernas para realizar transações. O trabalho consegue apontar que, nos piores cenário de segurança, os protocolos mais modernos, como o denominado GHOST, têm um desempenho pior ou na melhor das hipóteses similar à *block-chain*.

Luther (2015) investiga o emprego de criptomoedas nos distintos mercados financeiros. 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 precursor das criptomoedas.

O trabalho de Chávez e Rodrigues (2015) apresenta formas de decidir analiticamente quando é mais vantajoso trocar de *pools* a fim de se manter a rentabilidade considerada. O trabalho conclui que a mineração considerando o salto entre *pools* (i.e., troca dinâmica) é mais eficiente que a mineração considerando um único *pool*.

Pazmiño e Rodrigues (2015) avaliam o tempo de verificação de transações e, neste 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.

Por fim, o trabalho de Rocha e Rodrigues (2016) tem um viés de análise baseado em metodologias de desenvolvimento de *software* e, precipuamente, apresenta a modelagem do processo de negócio do sistema *Bitcoin*. Para tanto, são empregadas técnicas de *Engenharia de Software* e de *Business Process Model and* Notation. Os modelos desenvolvidos permitem mapear problemas críticos do sistema, explicitando em quais etapas do processo de negócio eles incidem.

4. Rentabilidade para Bitcoin e Litecoin

4.1 Definição de rentabilidade

Tanto para o *Bitcoin* quanto para o *Litecoin*, a *target difficulty*, *D*, refere-se à complexidade para se minerar um bloco, sendo ajustada de forma que qualquer número de tentativas para encontrar o *golden nonce* tenha sempre a razão de $\frac{1}{2^{32}*D}$ de chance de sucesso.

O valor atual de *D* para o protocolo *Bitcoin* é 194.254.820.283, e para o protocolo *Litecoin* é 47.760. A taxa com que um *hardware* consegue testar valores para descobrir o *golden nonce* é denominada de *hashrate*, representada por *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 [Rosenfeld, 2011].

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

O valor da *Receita total* pode ser obtido pela Equação 2, aqui definida assim como as demais equações que seguem. Esse valor é calculado levando-se em conta o valor da *reward* então recebido, bem como o valor de cotação atual em dólares da criptomoeda considerada, representado por V_c.

$$Receita\ total = reward * V_c \qquad (2)$$

A rentabilidade total esperada é calculada como *Receita total* menos *Despesa*. Por sua vez, o valor de *Despesa* é obtido pela multiplicação da *Despesa por hora*, D_h, pelo tempo *t* de mineração em horas. Explica-se que D_h está relacionada ao valor do kWh da região, V_{kWh}, onde a mineração em si é realizada. Para esse cálculo (vide Equação 3), 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 uma hora.

$$D_h = \frac{P}{1000} * V_{kWh} \qquad (3)$$

Seja V_r = USD 0,10 por hora (i.e., USD 0,10/h) a rentabilidade almejada por hora. 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.

Agora, a partir de V_r e de D_h, pode-se escrever a Equação 4 para obter-se o valor da *Receita por hora*, representada por R_h.

$$R_h = V_r + D_h \qquad (4)$$

Ainda, seja Q_h a quantidade de moedas por hora suficiente para alcançar a *Receita por hora*, representada por R_h. O cálculo de Q_h é obtido pela Equação 5.

$$Q_h = \frac{R_h}{V_c} \qquad (5)$$

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 a *Receita total*. Para tanto, é aqui considerado um valor de *hashrate* mínimo, representado por h_{min}. A Equação 6 apresenta a fórmula para obter esse valor. Essa equação é derivada a partir das Equações 1, 2, 3, 4 e 5, sendo t o período de tempo considerado de mineração.

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

A métrica *eficiência energética EE*, definida neste trabalho, é medida em hash/J e representa quantos *hashes* um *hardware* padrão precisa calcular, utilizando 1,0 joule de energia, para que se preserve a rentabilidade almejada V_r. Pode-se então calcular *EE* a partir do valor de h_{min} (vide Equação 6) da região considerada e do valor de potência do equipamento empregado, conforme Equação 7.

$$EE = \frac{h_{min}}{\mathrm{P}} \qquad (7)$$

4.2 Mineração no Brasil

Segundo a Agência Nacional de Energia Elétrica (ANEEL), a taxa de kWh mais barata do Brasil é a da concessionária de energia de Santa Catarina (SC), conhecida como Cooperativa Pioneira de Eletrificação (COOPERA), no valor de R$ 0,25/kWh, conforme ilustrado na Tabela 1 [Agência Nacional de Energia Elétrica, 2016].

Tabela 1. As três operadoras mais caras e as mais baratas de energia no Brasil.

Sigla	Tarifa (kWh/R$)	Unidade da Federação
CEDRI	0,604	SP
UHENPAL	0,583	RS
CHESP	0,582	GO
CERSUL	0,293	SC
CEA	0,273	AP
COOPERA	0,250	SC

Considerando a cotação do dólar em R$ 3,61, tem-se então o valor de 0,069 USD/kWh. Por fim, pelo Sistema Internacional de Unidades (SI), sabe-se que: 1,0 watt = 1,0 J/s (Joule/segundo) e, ainda, 1 hora = 3.600 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 6, chega-se a um valor de h_{min} de aproximadamente 2.178,4 Ghash/s para garantir a rentabilidade almejada de 0,10 USD/h. Aplicando-se este valor de $h_{\min}$ na Equação 7, chega-se então ao seguinte resultado: EE = 21,78 Ghash/J, conforme pode ser visto na Figura 1.

Considerando-se agora o protocolo *Litecoin* e um raciocínio análogo ao que acabou de ser descrito para o protocolo *Bitcoin*, tem-se os seguintes resultados: h_{min} = 63,28 Mhash/s e EE = 0,632 Mhash/J, para o país Brasil, conforme é apresentado na Figura 2.

Ante o exposto, evidencia-se então que a eficiência energética para o *Litecoin* no Brasil é menor que a do *Bitcoin*. Portanto, pode-se concluir que a mineração de *litecoins* é mais rentável que a de *bitcoins* no Brasil.

4.3 Mineração no mundo

Para analisar o cenário mundial, escolhem-se três importantes regiões econômicas: América, Ásia e Europa. Dessas regiões, são escolhidos os países de maiores PIBs. Os dados dos PIBs dos países selecionados estão na Tabela 2 [Fundo Monetário Internacional, 2016]. Os resultados da EE estão nas Figuras 1 e 2. A partir dessas figuras, é possível perceber que os valores resultantes para o protocolo *Bitcoin* são bem superiores àqueles obtidos para o protocolo *Litecoin*.

Tabela 2. Países considerados e seus respectivos valores de PIB e kWh.

País	PIB (milhões USD)	Valor kWh (USD)
Brasil	1.722.589	0,069
México	1.144.334	0,108
Estados Unidos	17.947.000	0,094
Canadá	1.552.386	0,070
Alemanha	3.357.614	0,015
França	2.421.560	0,089
Reino Unido	2.849.345	0,141
Japão	4.123.258	0,177
China	10.982.829	0,113
Indonésia	858.953	0,164

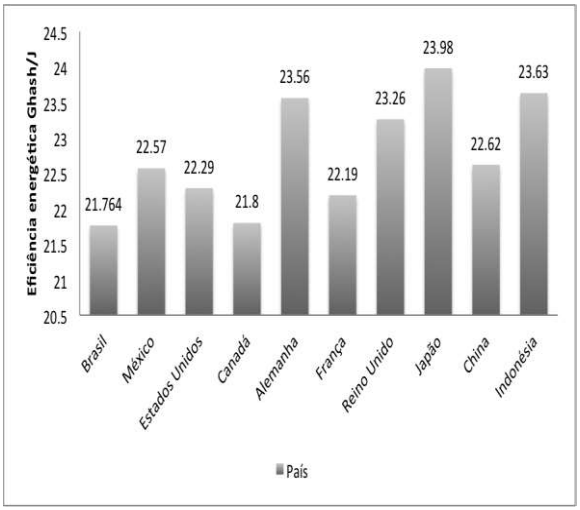

Figura 1. Eficiência energética do Bitcoin.

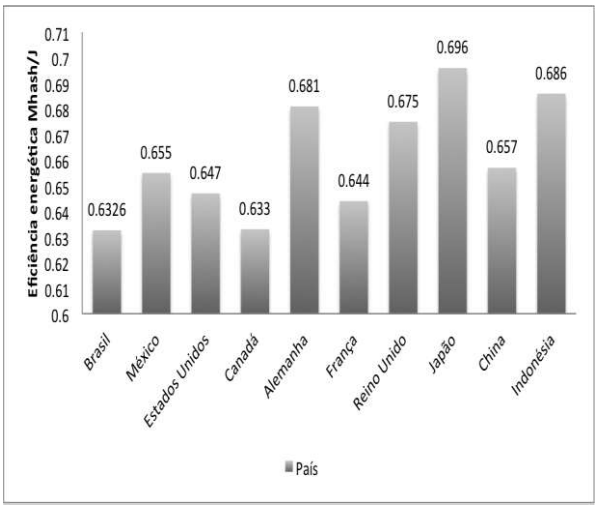

Figura 2. Eficiência energética do Litecoin.

Considerando então os resultados obtidos, pode-se concluir que no cenário mundial, assim como observado para a região brasileira anteriormente, a mineração de *litecoins* é mais rentável que a de *bitcoins.*

4.4 Tempo de mineração por bloco

Ressalta-se que, para mineração individual, o valor da *reward* é pago de uma só vez e apenas ao final do processo de mineração, quando o valor do *golden nonce* é encontrado. Ou seja, apenas ao término da mineração é que o minerador recebe sua *reward,* a qual corresponde atualmente a 25 moedas, tanto para o *Bitcoin* quanto para o *Litecoin.*

Assim, o tempo médio, $t_{médio}$, necessário para conseguir minerar um bloco se faz de importante consideração na mineração individual. Para se estimar $t_{médio}$ é necessário considerar a *target difficulty*, *D*, da criptomoeda considerada, e o valor da *hashrate, h,* do equipamento, resultando na Equação 8.

$$t_{médio} = \frac{2^{32} * D}{h} \qquad (8)$$

Para o país Brasil e o valor de *h* sendo a *hashrate* mínima, i.e., $h = h_{min} = 2.178\text{x}10^9$ hash/s, e com $D = 194.254.820.283$, a resolução da Equação 8 diz então que um bloco do protocolo *Bitcoin* seria minerado em aproximadamente $3{,}83\text{x}10^8$ s. Convertendo-se esse valor em dias, tem-se aproximadamente 4.323 dias, ou seja, cerca de 12 anos, para se minerar um bloco e receber 25 moedas (*reward* atual). Com a cotação atual da criptomoeda, seriam USD 11.372,5 de lucro.

Considerando agora o mesmo cenário de análise e substituindo-se os valores de *D* e h_{min} para o protocolo *Litecoin*, $t_{médio}$ seria de apenas 37,5 dias, e o valor das 25 moedas seria de USD 96,25. Ou seja, o tempo necessário pelo *Bitcoin* é cerca de 115,28 vezes maior para obter as 25 moedas de *reward*. Nesse tempo, o *Litecoin* obteria como *reward* 2.882 moedas, ou USD 11.095,7 de lucro, ficando bem próximo daquele provido pelo *Bitcoin*.

Além disso, o resultado do cálculo de $t_{médio}$ alerta para o fato de que, no período de 12 anos, tanto a criptomoeda *bitcoin* como a criptomoeda *litecoin* teriam passado por três *halvings*, o que faria o valor de 25 moedas se tornar um oitavo do valor original, ou seja,

3,12 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, no caso do protocolo *Bitcoin*, com a intenção de evitar-se o evento de *halving* e, portanto, garantir-se as 25 moedas de *reward*, admita o processo de mineração durando no máximo quatro anos (tempo limite para evitar-se o evento de *halving*), ou seja, um bloco deve ser minerado a cada 1.460 dias em média. A partir da manipulação das equações anteriores, é possível mostrar que a *EE* tem que ser aumentada em aproximadamente 296%, fazendo a taxa de hash/s do Brasil igual a 6.449 Ghash/s (ou 64,49 Ghash/J de eficiência energética).

Observe ainda que, ao longo de 12 anos, a dificuldade *D* e o valor da moeda 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 37 dias, o evento de *halving* não influenciaria o lucro obtido no final do período estimado para minerar um bloco.

Sendo assim, as projeções para o *Bitcoin* de longo prazo tornam-se mais imprecisas que a do *Litecoin*. Isso leva à conclusão de que o retorno monetário advindo da mineração individual é bem mais incerto no caso do protocolo *Bitcoin*.

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 criptomoeda. 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 da região da mineração.

Os seguintes resultados podem ser destacados: (1) para uma mesma rentabilidade econômica do processo de mineração individual, o protocolo *Litecoin* demanda menos *eficiência energética* que o protocolo *Bitcoin* para o país Brasil; (2) em países de outros continentes, ainda que os valores de kWh variem, a demanda inferior de *eficiência energética* do protocolo *Litecoin* em relação ao protocolo *Bitcoin* se mantém; (3) devido ao tempo necessário para mineração de um bloco de transações ser menor no protocolo *Litecoin*, as suas projeções de investimento a longo prazo são mais precisas e confiáveis que no caso do protocolo *Bitcoin*. Esses resultados levam à conclusão geral de que a mineração individual de *litecoins* é mais rentável e previsível que a de *bitcoins.*

Por fim, como trabalho futuro, sugerem-se o estudo e o desenvolvimento 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 e Thaddeus, 2016]. Conjectura-se que, ao reduzir-se a demanda por esse poder de processamento, o consumo de energia elétrica diminui e, ainda, *hardwares* mais simples e, consequentemente, mais economicamente acessíveis, podem ser utilizados, resultando em um maior grau de competitividade do protocolo *Bitcoin* frente a outros protocolos de mesma finalidade.

Referências

Agência Nacional de Energia Elétrica (2016). "Ranking nacional de tarifas residenciais (grupo B1)". Disponível em: < http://www.aneel.gov.br/ranking-das-tarifas>. Acesso em: 21 jun. 2016.

Bank for International Settlements (2015). "Digital currencies". Disponível em: <https://www.bis.org/cpmi/publ/d137.pdf>. Acesso em: 9 jun. 2016.

Bradbury, D. (2013). "Litecoin founder Charles Lee on the origins and potential of the world's second largest cryptocurrency". Disponível em: <http://www.coindesk.com/litecoin-founder-charles-lee-on-the-origins-and-potential-of-the-worlds-second-largest-cryptocurrency/>. Acesso em: 20 de fev. 2016.

Chávez, J. J. G.; Rodrigues, C. K. S. (2015). A simple algorithm for hopping among Pools in the Bitcoin Mining Network. *The SIJ Transactions on Computer Networks & Communication Engineering (CNCE)*, v. 3, n. 2., p. 22-27.

Fundo Monetário Internacional (2016). "Report for Selected Country Groups and Subjects". Disponível em: <http://www.imf.org/external/pubs/ft/weo/2016/01/weodata/index.aspx>. Acesso em: 19 jun. 2016.

Kiayias, A.; Panagiotakos, G. (2016). "On Trees, Chains and Fast Transactions in the Blockchain". Disponível em: <https://eprint.iacr.org/2016/545>. Acesso em: 09 de jul. 2016.

Luther, W. J. (2015). "Bitcoin and the Future of Digital Payments". Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2631314>. Acesso em: 10 fev. 2016.

Murphy, R. P. (2013). "The Economics of Bitcoin". *Library and Liberty*. Disponível em: <http://www.econlib.org/library/Columns/y2013/Murphybitcoin.html>. Acesso em: 10 fev. 2016.

Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System". Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 30 dez. 2015.

Pazmiño, J. E.; Rodrigues, C. K. S. (2015). Simply Dividing a Bitcoin Network Node May Reduce Transaction Verification Time. *The SIJ Transactions on Computer Networks & Communication Engineering (CNCE)*, v. 3, n. 2., p. 17-21.

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

Poon, J.; Thaddeus, D. (2016). "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments". Disponível em: <http://lightning.network/lightning-network-paper.pdf>. Acesso em: 25 jan. 2016.

Rocha, J. G.; Rodrigues, C.K.S. (2016). O processo de negócio do sistema de transações financeiras Bitcoin. *Universitas: Gestão e TI*, v.6, n. 1., p. 1-14.

Rosenfeld, M. (2011). "Analysis of Bitcoin Pooled Mining Reward Systems". Disponível em: <https://bitcoil.co.il/pool_analysis.pdf>. Acesso em: 30 jan. 2016.

White, L. H. (2015). The Market for Cryptocurrencies. *Cato Journal*, v. 35, n. 2., p. 383-402.

