Faculdade de Informática e Administração Paulista

MBA EM BLOCKCHAIN - DEVELOPMENT & TECHNOLOGIES

1BLC / BITCOIN / Professora EMÍLIA MALGUEIRO CAMPOS

**BIP Bitcoin Improvement Proposal**

BIP: 001

Layer: Consensus

Title: Ajustes mais dinâmicos na dificuldade do Nonce

Author: Alexandre Akel, Eduardo Salvatori e Guilherme Araújo

Status: Withdrawn

Type: Standards Track

Junho/2019

**Resumo**

A proposta desse BIP é ajustar com uma frequência maior a dificuldade do Nonce, obedecendo a mesma regra da média de 10 minutos por bloco.

**Motivação**

Essa proposta não visa a condenação da plataforma pelo seu alto consumo de energia elétrica, muito pelo contrário. A disrupção que o Bitcoin trouxe é imensurável para ser diminuído pela quantidade de energia que consume.

O BIP levanta uma melhoria para diminuir o consumo em tempos que a pauta do desperdício de recursos está em alta. Uma queda significativa de energia consumida (sem comprometer a segurança) significa pontos positivos para a aceitação ainda maior da plataforma.

A quantidade de transações e mineradores na rede Bitcoin tem crescido a cada dia. Com isso, temos uma enorme quantidade de energia elétrica consumida pela rede 24 horas 7 dias por semana. Esse ponto vem causando uma série de críticas a plataforma. Calcular a dificuldade do Nonce com mais frequência e precisão irá reduzir esse impacto.

**Cenário Atual**

Com a média de um bloco minerado a cada 10 minutos, a dificuldade do Nonce é ajustada a cada 2016 blocos (2 semanas). A dificuldade pode aumentar ou diminuir de acordo com o tempo de geração dos blocos.

Segue abaixo trecho do livro Mastering Bitcoin (Andreas Antonopoulos) onde explana-se melhor sobre a definição de dificuldade:

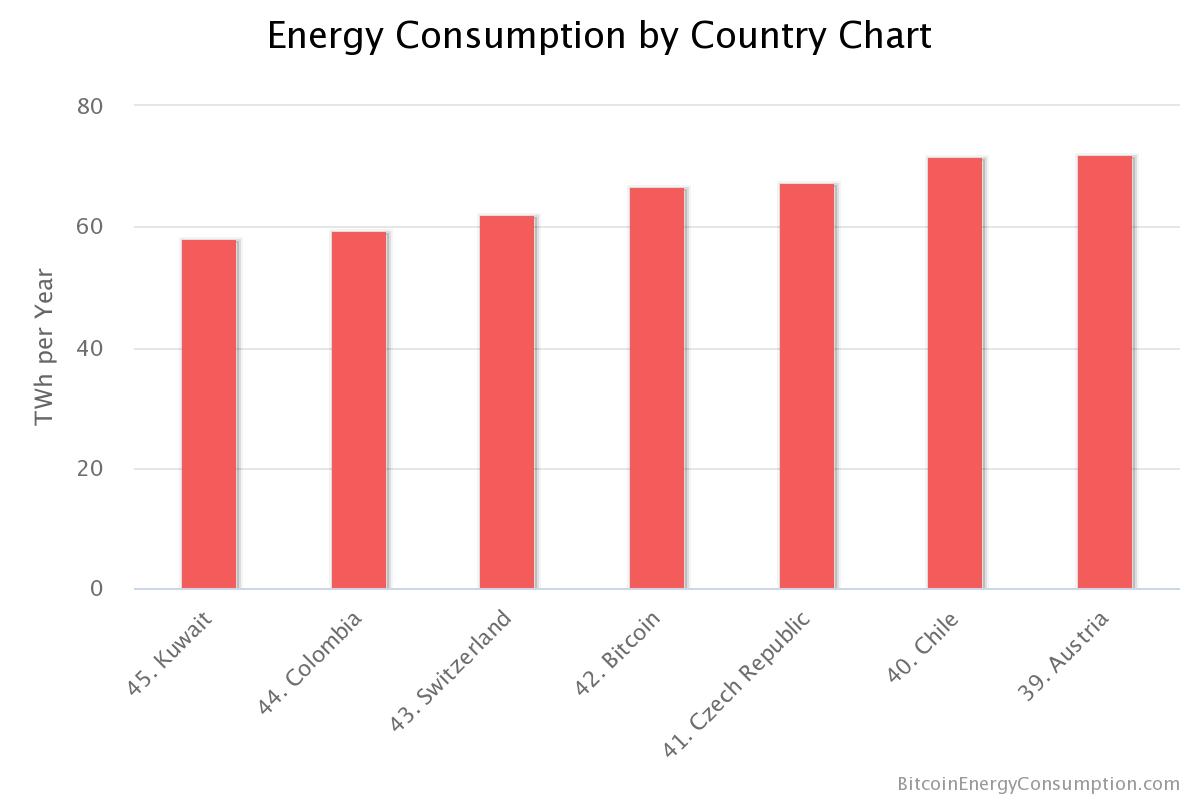
*A equação para reajustar o alvo mede o tempo que levou para encontrar os últimos 2.016 blocos e o compara com o tempo esperado de 20.160 minutos (duas semanas, baseando-se em um tempo desejado de 10 minutos para gerar um bloco). A razão entre os períodos de tempo atual e o desejado é calculada, e um ajuste correspondente (para cima ou para baixo) é feito à dificuldade. Simplificando: Se a rede estiver encontrando blocos mais rápido do que a cada 10 minutos, a dificuldade irá aumentar. E se a descoberta de blocos estiver mais lenta que o esperado, a dificuldade irá diminuir.*

*A equação pode ser resumida como:*

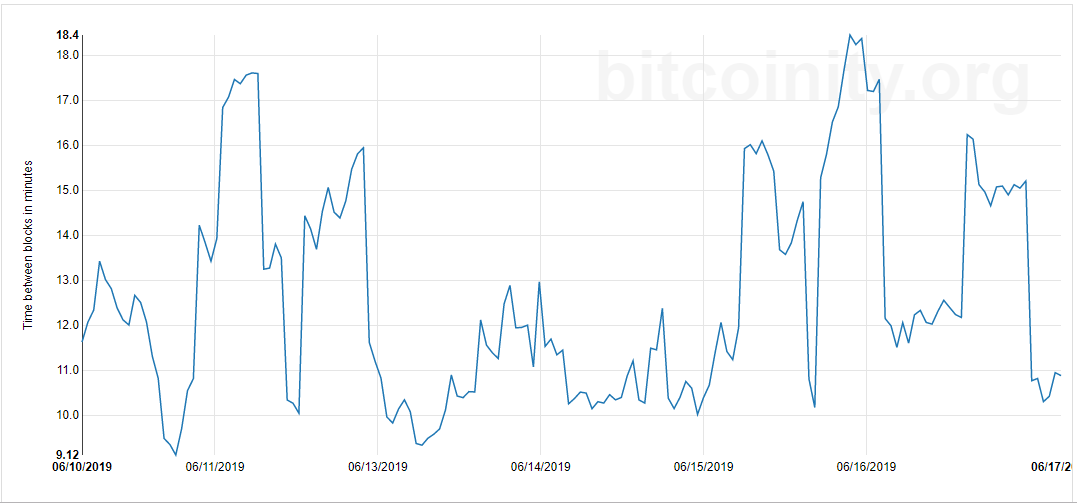
*Nova Dificuldade = Dificuldade Antiga \* (Tempo dos últimos 2.016 blocos / 20.160 minutos)*

Com isso, levantemos algumas estatísticas da rede. Como na Tabela 1 abaixo:

Imagem 1 com comparativo da rede com países:



No gráfico 2 abaixo, podemos pegar de exemplo a semana do dia 10/06/2019. Vimos que poucos blocos levaram menos de 10 minutos e um número grande de blocos mais que 10 minutos. Percebe-se que nesse período a dificuldade do Nonce estava um pouco alta, gerando um consumo de energia maior para os mineradores encontrarem o mesmo.



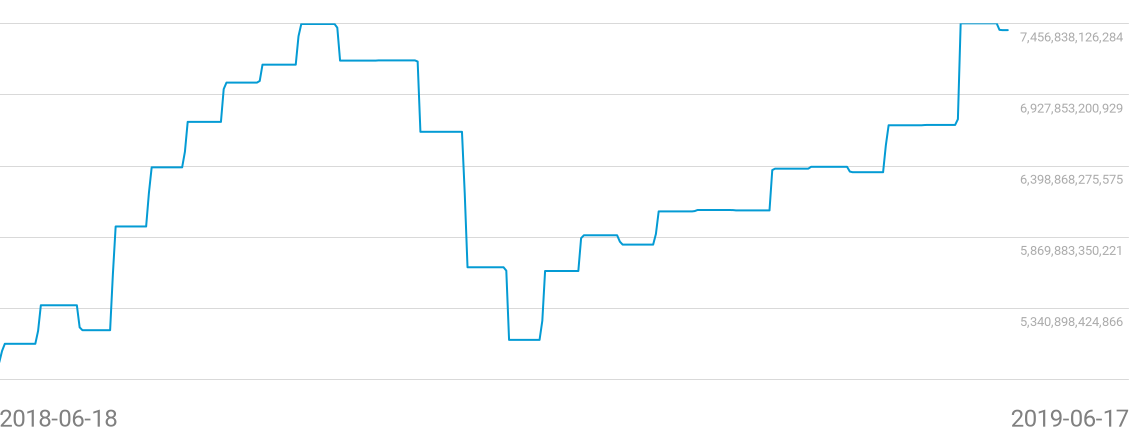
Se considerarmos uma média de 3500 transações por bloco, cada transação consumindo 540 KwH, temos 1.890.000 kwh para fecharmos um bloco.

**Cenário Proposto**

Reajustando a dificuldade do Nonce a cada 1008 blocos (1 semana) já conseguiríamos ver uma normalização maior no tempo da mineração dos blocos.

Ao longo de duas semanas, pode parecer imperceptível alguns segundos ou minutos a mais em cada bloco (como ilustrado na Figura 2). Mas em termos de consumo de energia, essas pequenas variações custam muito.

O gráfico 3 ilustra a variação da dificuldade do Nonce no último ano:



Conclui-se que existe uma grande variação, e isso é normal, deve-se variar mesmo. O ponto é, se variar ainda mais (como a proposta central desse BIP) teremos uma assertividade maior do grau de dificuldade e consequentemente um menor desperdício de tempo de processamento das máquinas (quando ultrapassa de 10 minutos por bloco) onde teremos uma redução de energia elétrica consumida pela rede. Alterando a equação, ficando assim:

*Nova Dificuldade = Dificuldade Antiga \* (Tempo dos últimos 1.008 blocos / 10.080 minutos)*

**Conclusão**

Com a implementação do BIP, em poucas semanas esperamos uma diminuição significativa no consumo de energia elétrica pela rede. Além do enfoque no desperdício mínimo, temos um ganho de imagem e aceitação na comunidade internacional levantando a bandeira da sustentabilidade. Os mineradores também perceberão este BIP como incentivo, pois os gastos diminuirão.

Enquanto não vivemos em uma era de abundância de energia sustentável, a pauta do desperdício sempre será levantada e contestada. O Bitcoin é muito maior que essa questão, mas não podemos ignora-la.

**Referências**

[https://www.blockchain.com](https://www.blockchain.com/)

[https://data.bitcoinity.org](https://data.bitcoinity.org/)

<https://digiconomist.net/bitcoin-energy-consumption>

<https://en.bitcoin.it/wiki/Block_hashing_algorithm>

# Mastering Bitcoin, Andreas Antonopoulos 2016.