Bitcoin: o que é mineração e *halving*?

Um evento aguardado para o ano de 2024 no mercado de criptomoedas é o *halving* do bitcoin, usualmente associado a fortes movimentos de valorização dos preços — em novembro de 2012, julho de 2016 e maio de 2020, a criptomoeda subiu 7.956%, 270% e 533%, respectivamente.

Em essência, é um evento programado no próprio código do bitcoin que restringe a quantidade de emissão, fazendo com que o estoque já emitido (atualmente, cerca de 16.684.406 BTC) aumente mais devagar até, algum dia, chegar ao limite máximo de 21 milhões. É exatamente essa "escassez digital" que fundamenta a tese de que o bitcoin pode ser uma alternativa ao ouro enquanto reserva de valor.

Ainda que seja um evento certo e seu momento seja perfeitamente previsível, o *halving* representa um marco de "renovação das esperanças" de quem subscreve a tese de investimento em bitcoins baseada na sua escassez, com a expectativa de que os preços aumentem pela diminuição da oferta no longo prazo. Fala-se em um sistema "deflacionário" em contraposição as moedas fiduciárias dos Estados e seu regime inflacionário.

Para entender o que é o *halving*, precisamos compreender como novos bitcoins são emitidos e o que exatamente significa afirmar que estamos diante de um ativo deflacionário. De quebra, o conceito de "mineração" emerge da discussão como uma analogia útil para a explicação de todo o processo.

Como funciona a rede do bitcoin

As transações envolvendo bitcoins são realizadas em uma rede regida por um *protocolo*, isto é, um conjunto de regras que permite a comunicação entre seus participantes. Alguns nós desta rede guardam consigo cópias do histórico de todas as operações já efetivadas.

À medida que as transações são realizadas entre os participantes, o efetivo "pagamento" com saída de recursos de um nó para outro depende de algumas operações que são conduzidas por membros especializados que realizam sua validação (a identidade das partes, a suficiência de saldo para transferência e outras informações). Cada transação pretendida se torna uma mensagem, que é propagada para todos os nós da rede.

As operações são processadas em etapas, que levam cerca de dez minutos e consistem na geração de um novo bloco (como um vagão de um metrô) que receberá novas transações que ficarão na rede "para sempre". Em cada ciclo, os validadores competem entre si, resolvendo um *quebra-cabeças criptográfico* , cujos parâmetros dependem, em parte, do conteúdo das mensagens que decide processar. Quem resolver primeiro adquire o direito de incluir as transações validadas no bloco atual e a rede segue para o próximo ciclo.

A remuneração do validador – e por que se chama "minerador"

O validador que consegue resolver o problema e inserir o bloco é remunerado de duas formas.

Primeiro, pela soma das taxas de processamento estipuladas em cada transação, pois as partes indicam quanto desejam pagar. Obviamente, uma vez que o validador pode escolher quais transações incluir no bloco, irá preferir as transações em que as partes estão dispostas a pagar maiores taxas.

Segundo, o validador recolhe uma "recompensa" em uma transação especial no bloco de transações, é incluída uma em especial, que representa uma emissão primária da moeda, como se a casa da moeda estivesse distribuindo papel-moeda recém impresso pela primeira vez. Os bitcoins são gerados (emitidos) por meio desse procedimento.

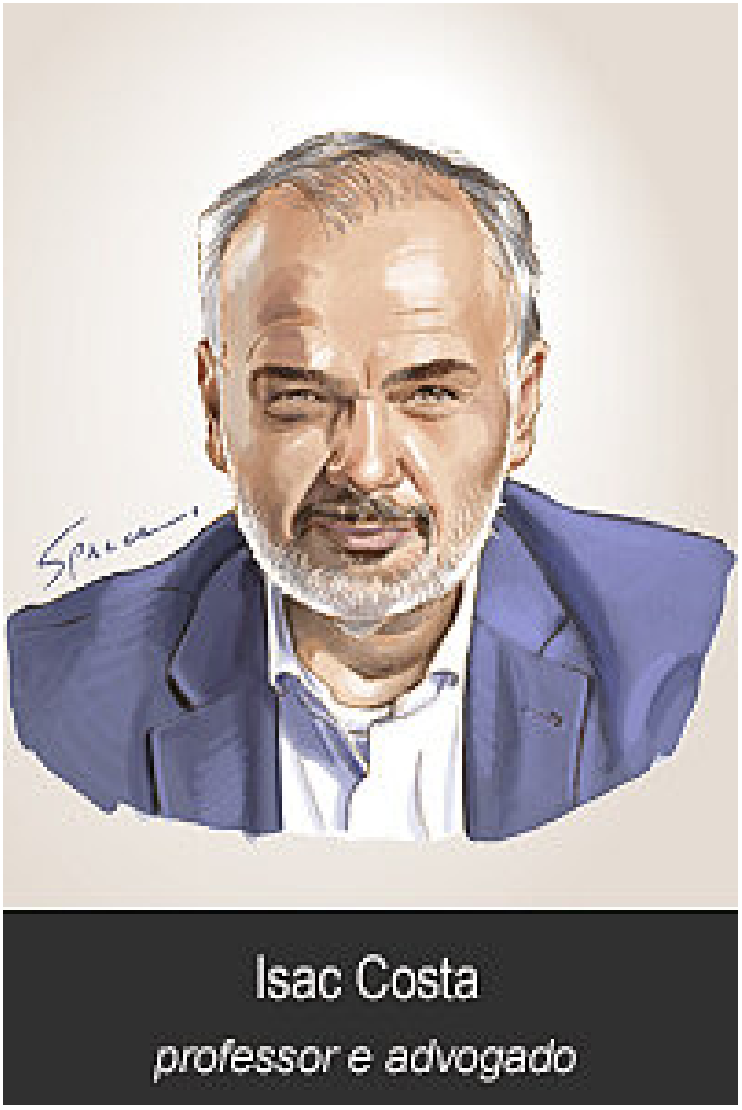
Como esta parcela é um saldo em criptomoedas, seu efetivo valor irá flutuar conforme a taxa de conversão entre o valor da criptomoeda e outras criptomoedas ou de alguma moeda soberana (1 BTC = US$ 62 mil no momento em que esse texto é escrito). Cada bloco é minerado, em média, a cada 10 minutos e no ano corrente (2024) o minerador que insere um novo bloco é remunerado com 6,25 BTC. Logo, *a cada 10 minutos, há um minerador vencedor que recolhe para si o equivalente a US$ 387,5 mil em cotações atuais*. Não é à toa que a atividade da mineração faz brilhar os olhos de muitas pessoas, que desconhecem a complexidade, a dificuldade e os custos da operação.

Afirmamos que a remuneração atual por ciclo é de 6,25 BTC, mas não foi sempre assim. Originalmente, em 2009, a emissão de criptomoedas a cada novo bloco inserido rendia BTC 50 a cada remuneração. O código que implementa o protocolo bitcoin foi programado de modo a reduzir periodicamente pela metade o valor da remuneração, após o processamento de certo número de blocos, o que ocorre por volta de cada quatro anos.

Spacca

Note que a escolha do termo “mineração” foi proposital: a remuneração dos validadores decorre de um esforço (computacional) árduo e, quanto mais recursos são extraídos, mais escassos eles ficam, como uma reserva mineral sendo exaurida. Assim, temos a seguinte sucessão de valores para a remuneração:

- 2009 – BTC 50
- 2012 – BTC 25
- 2016 – BTC 12,5
- 2020 – BTC 6,25
- 2024 – BTC 3,125
- 2028? – BTC 1,5625
- …
- ???? – BTC 10^-8 (1 satoshi)



Em algum momento, o valor da remuneração decrescerá de forma a chegar no mínimo valor do bitcoin, sua unidade indivisível denominada satoshi, que é 10^-8 = 0,00000001 BTC. A partir daí, não será possível efetuar novas divisões.

Qual o máximo de bitcoins que serão emitidos?

Talvez você tenha notado que a série numérica acima é uma progressão geométrica decrescente (sua razão é menor que 1), com termo inicial a1 = 50 e razão = 0,5.

Em média, a cada quatro anos, ocorrem 4 anos = 4 x 365 dias = 4 x 365 x 24 horas = 4 x 365 x 24 x 60 minutos = 4 x 365 x 24 x 6 x (10 minutos) = 4 x 365 x 24 x 6 = 210.240 ciclos (ou seja, em média, a cada 4 anos são inseridos novos 210.240 blocos no livro descentralizado de transações).

Na verdade, o protocolo estabelece que a cada 210.000 blocos, ocorre a divisão do valor da remuneração por dois, logo você agora pode entender como, a partir do dado de que cada bloco é inserido em média a cada dez minutos, estimamos que cada divisão pela metade (*halving*) da quantidade emitida ocorrerá, em média, a cada quatro anos.

Então, temos um passo importante no raciocínio que nos levará ao cálculo do total de bitcoins que será emitido. Para facilitar o raciocínio indutivo, considere que:

- No 1º período de 4 anos (210.000 blocos) foram emitidos 50 x 210.000 BTC
- No 2º período de 4 anos, foram emitidos 25 x 210.000 BTC

- No 3º período de 4 anos, terão sido emitidos 12,5 x 210.000 BTC
- No 4º período de 4 anos, serão emitidos 6,25 x 210.000 BTC
- … e o raciocínio se repete.

Para calcular o total de bitcoins emitidos, basta somarmos os infinitos termos da progressão geométrica indicada, utilizando a fórmula S = a1 / (1-q), onde a1 é o primeiro termo da PG = 50 x 210.000 e q é a sua razão = 0,5. Substituindo os valores na fórmula chegamos a S = 210.000 x 50 / (1-0,5) = 21.000.000.

Portanto, *na história do bitcoin, serão emitidos, no máximo 21.000.000 (21 milhões) BTC*.

E quando isso irá ocorrer?

O limite máximo será atingido quando a remuneração dos mineradores chegará ao valor mínimo (1 satoshi). Neste caso, considerando a progressão geométrica de termo a1 = 50 e razão q = 0,5, precisamos saber qual o n que satisfaz an = a1*q^(n-1) = 10^-8. Logo, 50*0,5^(n-1) = 10^-8 => log 50 + (n-1)*log 0,5 = -8 => n = 1 + (-8-log 50)/(log 0,5) = 33. Logo, após a 32ª divisão pela metade, a remuneração chegará em 50*0,5^(33-1) = 1,16 x 10^-8. Como cada divisão ocorre, em média, a cada 4 anos e a rede bitcoin começou a funcionar em 2009, então este momento ocorrerá no ano de 2009 + 32*4 = 2137.

Assim, *espera-se que, por volta do ano de 2137 tenham sido minerados praticamente todos os BTC 21 milhões possíveis*.

E daí?

Em teoria, se os mercados são racionais e eficientes, os preços já deveriam refletir todas as informações disponíveis e, uma vez que o *halving* não é nenhuma novidade, sua ocorrência já deveria estar precificada, não sendo possível afirmar que qualquer variação das cotações do bitcoin teriam alguma relação com o evento no futuro próximo.

Entretanto, racionalidade e investimentos – especialmente em crioptomoedas – não costumam andar lado a lado. Por isso, o tema é associado a narrativas sobre "como lucrar com o *halving*" ou que buscam algum fundamento para os abruptos movimentos do bitcoin e demais criptoativos neste ano em que o mercado está amplamente aquecido, após a popularização dos ETFs criados por grandes gestoras.

Espero que, com esse breve texto, você tenha aprendido um pouco sobre bitcoin e sobre como certos números que vemos serem repetidos com alguma frequência foram obtidos e, ainda, possa ter adquirido uma noção de quanto tempo ainda será necessário para que a tese de bitcoin como investimento de longo prazo seja corroborada.

Autores: Isac Costa