

Rješenja inicijalnih zadataka

Nikola Pavković

I. Teoretsko ograničenje broja Bitcoina

Uz predefiniranu konstantu prepolavljanja nagrade za rudarenje novog bloka (svakih **210 000** blokova), te početnu nagradu za rudarenje prvog (**genesis**) bloka, u iznosu od **50 BTC** ($50 \cdot 10^{-8}$ Satoshi), može se izvesti sljedeći izraz za izračun ukupnog teoretskog broja Bitcoina:

$\alpha \rightarrow$ broj izrudarenih blokova nakon kojih se prepolavlja nagrada
 $\rho \rightarrow$ nagrada za rudarenje genesis bloka
 $r \rightarrow$ zajednički omjer

$$\alpha = 210\,000$$

$$\rho = 50\text{ BTC}$$

$$\sum_{i=0}^{\infty} \alpha \frac{\rho}{2^i}$$

Uvrštavanjem konstanti dobiva se sljedeći izraz:

$$210\,000 \cdot 50 \sum_{i=0}^{\infty} 2^{-i}$$

Generalizacija u geometrijski red:

$$r = \frac{1}{2}$$

$$210\,000 \cdot 50 \cdot \lim_{i \rightarrow \infty} \left(\sum_{i=0}^{\infty} 2^{-i} \right)$$

Izračun limesa sume:

$$s = \frac{1}{1-r} = \frac{1}{1-\frac{1}{2}} = 2$$

Uvrštavanjem s u prethodni izraz dobiva se sljedeći rezultat:

$$\begin{aligned}|BTC| &= 210\,000 \cdot 50 \cdot 2 = 21\,000\,000 \\ |Satoshi| &= 21\,000\,000 \cdot 10^8\end{aligned}$$

II. *Praktično ograničenje broja Bitcoina*

S obzirom na činjenicu da je osnovna jedinica Bitcoina, Satoshi, nedjeljiva i konstantna (**0.00000001 BTC**) i pretpostavku da se nagrada za rudarenje jednog bloka prepolavlja svakih **210 000** blokova, nužno će doći do zaokruživanja prilikom prelaska osme decimale zbog kontinuiranog dijeljenja.

Oduzimanjem ukupnog zbroja pogrešaka zbog zaokruživanja od teoretskog ograničenja, praktično ograničenje broja Bitcoina iznosi: **20999999.97690000 BTC**

III. *Implementacija sustava prepolavljanja u Bitcoin Core izvornom kodu*

```
CAmount GetBlockSubsidy(int nHeight, const Consensus::Params& consensusParams)
{
    int halvings = nHeight / consensusParams.nSubsidyHalvingInterval;
    // Force block reward to zero when right shift is undefined.
    if (halvings >= 64)
        return 0;

    CAmount nSubsidy = 50 * COIN;
    // Subsidy is cut in half every 210,000 blocks which will occur approximately every 4 years.
    nSubsidy >>= halvings;
    return nSubsidy;
}
```

Način na koji Bitcoin Core rukuje prepolavljanjem implementiran je pomoću funkcije `GetBlockSubsidy(...)` koja na osnovu trenutnog broja blokova u blockchainu – **nHeight** i **consensusParams.nSubsidyHalvingInterval** parametra koji iznosi 210 000, računa

broj prepolavljanja koji se prethodno dogodio te u konačnici vraća nagradu za rudarenje jednog bloka.

S obzirom na činjenicu da je broj prepolavljanja cijeli broj, doći će do odbacivanja decimalnog dijela kvocijenta duljine blockchaina i perioda prepolavljanja te će se broj prepolavljanja zaokružiti na integer vrijednost kvocijenta (pr. $2.5 \rightarrow 2$) i spremiti u varijablu **halvings**.

U sljedećoj liniji koda nalazi se varijabla **nSubsidy** koja skladišti nagradu za rudarenje **genesis** bloka u Satoshijima. Ona će se koristiti prilikom izračuna nagrade za rudarenje jednog bloka u nastavku. Konstanta COINS predstavlja faktor pretvaranja Bitcoina u Satoshije.

Nagrada za rudarenje jednog bloka prepolavlja se svakih 210 000 blokova stoga je potrebno nagradu (**nSubsidy**) skalirati s prethodnim brojem prepolavljanja. Skaliranje nagrade postignuto je korištenjem **right-shift bitwise operatora** koji, pomicanjem svih bitova za **halvings** mjesta udesno, prepolavlja vrijednost nagrade. U nastavku je prikazan **primjer korištenja right-shift bitwise operatora**.

Nagrada za rudarenje prvog bloka iznosi: $50 \cdot 10^8$ Satoshi

Pretvaranjem tog iznosa u binarni zapis dobivamo sljedeći broj:

1001010100000001011111001000000000

Korištenjem right-shift bitwise operatora naredbom:

nSubsidy>>=halvings;

i imajući na umu pretpostavku da je prethodno došlo do 3 prepolavljanja, potrebno je 3 puta pomaknuti sve bitove iznosa udesno kako bi se nagrada prepolovila 3 puta. Kao rezultat ove operacije dobivamo broj:

1001010100000001011111001000000 ili, nakon pretvorbe, 6.25 BTC po izrudarenom bloku.

Zanimljivo je primijetiti uvjet „**if(halvings >= 64) return 0;**“. Navedeni uvjet vraća nagradu iznosa 0 BTC u slučaju da je broj prepolavljanja veći ili jednak **64**. Unatoč tomu što praktično ograničenje broja prepolavljanja iznosi **33**, odabrana je konstanta 64 kako bi se spriječio overflow prilikom pomicanja bitova udesno te time izazvalo nedefinirano ponašanje. Konstanta 64 uvedena je tek 2014. u svrhu sigurnosti prilikom prepolavljanja koje će se dogoditi tek za otprilike 250 godina.

Naposlijetku funkcija vraća skaliranu nagradu za rudarenje jednog bloka s obzirom na prethodni broj prepolavljanja ili nagradu u iznosu 0 BTC u slučaju prelaska predefiniranog broja prepolavljanja.