When will I mint a peercoin block? How much will I mint?

Peercoin use *proof-of-stake* blocks to secure the network in a energy efficient way. While it is easy to find the probability and the reward to mine a *proof-of-work* block, I haven't found those informations for minting a *proof-of-stake* block. So here there are.

If you don't know anything about Peercoin, or about *proof-of-stake*, you should read the Peercoin white paper first.

Coin age

The minting operation is based on the concept of *coin age* which is the amount of coins multiplied by the age of a given transaction. Thus, if I've received m Peercoins α days ago I currently have a coin age of $m \times \alpha$ *coins-days*. Transferred coins lose their age.

For the purpose of minting, coins must be **at least 30 days old** [1], and the maximum age possible is 90 days [2] (if a coin is older we still counting it as a 90 days old coin). Let's call α' the *minting age*:

$$\alpha' = \max(\min(\alpha, 90) - 30, 0)$$

By definition, $0 \leq \alpha' \leq 60$.

Minting expectancy

The probability $p(T)$ to mint a block in the next period of T seconds depends on x' the *minting age*, on m the amount of coins, and on d the network *proof-of-stake* difficulty. Those variables are linked by the following formula:

$$p(T) = \frac{m \times \alpha' \times T}{d \times d_1}$$

where d_1 is the difficulty 1 target, fixed at `0xffff0000` *ie* `4294901760` [3].

[1] source code
[2] source code
[3] source code

Example 1

> If I've received `10,000` Peercoins `60` days ago, how likely will I mint a block in the next hour at a network difficulty of `7.2`?

$$p(T = 60 \times 60) = \frac{(60 - 30) \times 10000 \times 60 \times 60}{7.2 \times 4294901760} = 0.0359 = 3.59\%$$

Example 2

> In the same conditions, how much time should I wait to have a probability of `0.5` to mint a block?

$$T = \frac{0.5 \times 7.2 \times 4294901760}{(60 - 30) \times 10000} = 51538s \approx 14h19m$$

Reward

When you mint a block you create a special transaction called *coinstake*. This transaction contains newly generated Peercoins as a reward for your minting operation. The reward is calculated so you will have an annual interest of 1%, it uses the following formula:

$$r = \frac{\max(\alpha, 90) \times m \times 0.01}{365.242424}$$

where α is the *coin age* and m the amount of coins [4].

Example 3

> In the same conditions, what will be my minting reward ?

$$r = \frac{60 \times 10000 \times 0.01}{365.242} = 16.4274454 \text{ PPC}$$

I hope it helps!

[4] source code