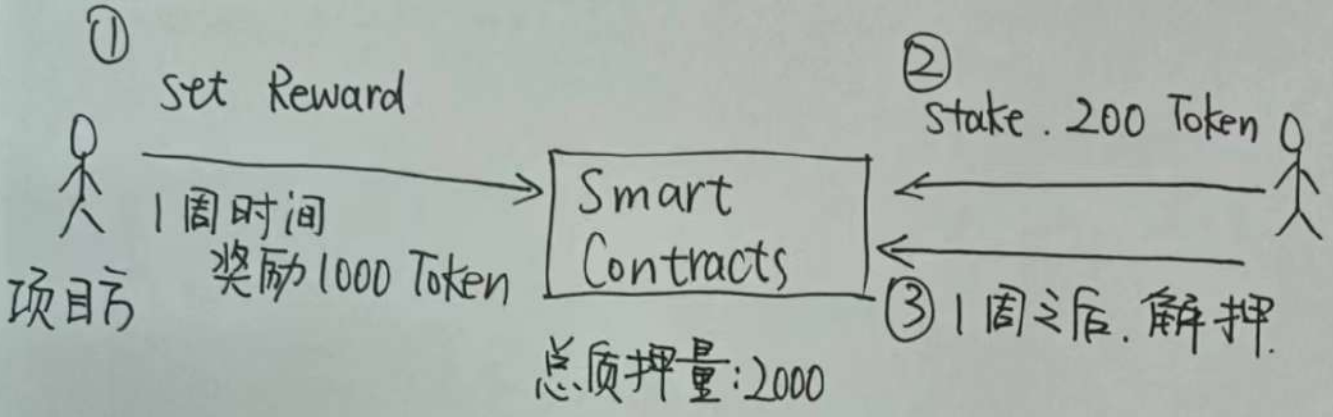
案例1：



$$reward = \frac{200}{2000} \cdot 1000/周 \cdot 1周 = 100\ token$$

建模：

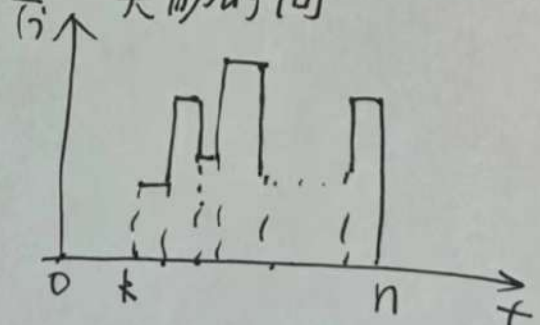
$r(u,k,n)$：用户u在时间k→n之间质押得到的奖励.

在任意时刻i. 如果有 $k<i<n$. 有：

S_i：用户u在时刻i质押的数量

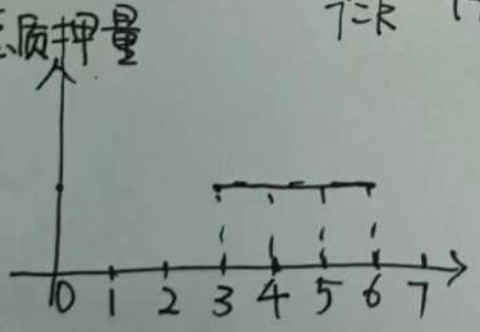
T_i：在时刻i.的总质押量

R：每秒钟的奖励数量. 其中 $R=\frac{总奖励数量}{奖励时间}$



那么：$r(u,k,n)=\sum_{i=k}^{n-1}\frac{S_i}{T_i}R$

案例2：

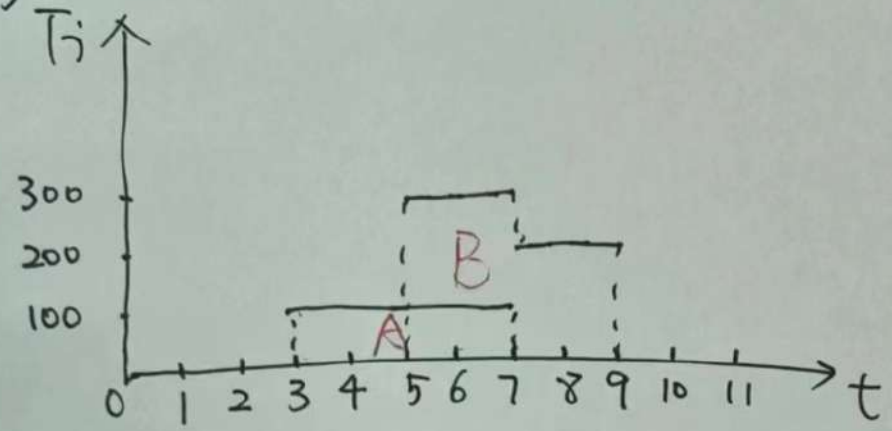


A在第3s-6s质押了100个 token. 没有别人质押.

$$r(A,3,6)=\frac{S_3}{T_3}\cdot R+\frac{S_4}{T_4}\cdot R+\frac{S_5}{T_5}\cdot R$$

$$=\frac{100}{100}\cdot R+\frac{100}{100}\cdot R+\frac{100}{100}\cdot R=3R$$

案例3:



$$r(A,3,7)=\frac{S_3}{T_3}\cdot R+\frac{S_4}{T_4}\cdot R+\frac{S_5}{T_5}R+\frac{S_6}{T_6}\cdot R$$
$$=\frac{100}{100}\cdot R+\frac{100}{100}\cdot R+\frac{100}{300}\cdot R+\frac{100}{300}\cdot R$$
$$=R+R+\frac{1}{3}R+\frac{1}{3}R$$
$$=\frac{8}{3}R$$

$r(B,5,9)$. 自行计算

缺点: 针对每个用户在每一秒的数据进行计算. 计算量大. 存储量大.

现实: stake 和 withdraw 都是低频操作.

$r(u,k,n)=\sum_{i=k}^{n-1}\frac{S_i}{T_i}R$ 在 $S=S_i$ 不变的情况下

$$=S\left(\sum_{i=0}^{n-1}\frac{R}{T_i}-\sum_{i=0}^{k-1}\frac{R}{T_i}\right)=S(r_n-r_k)$$

$\sum_{i=0}^{n-1}\frac{R}{T_i}$ 的含义: 单位token在 $t=0$ 到 $t=n$ 时刻之间可以得到的总奖励数. (结合案例3理解). 记为. 简 r_n

对A来说: $\sum_{i=0}^{n-1}\frac{R}{T_i}=0\cdot R+0\cdot R+0\cdot R+\frac{1}{100}\cdot R+\frac{1}{100}\cdot R+\frac{1}{300}\cdot R+\frac{1}{300}\cdot R$

$$=\frac{2}{100}R+\frac{2}{300}R$$

$r(A,3,7)=r(A,0,7)-r(A,0,3)=100\cdot\left(\frac{2}{100}R+\frac{2}{300}R\right)-0\cdot 0$

计算 $r(B,5,9)$ $=\frac{8}{3}R$.

化简 r_n

$$r_n = \sum_{i=0}^{n-1} \frac{R}{T_i}.$$

设在时刻 $j_0 \to j$ 之间. $T_i = T$. 不变. $j_0 < i < j$

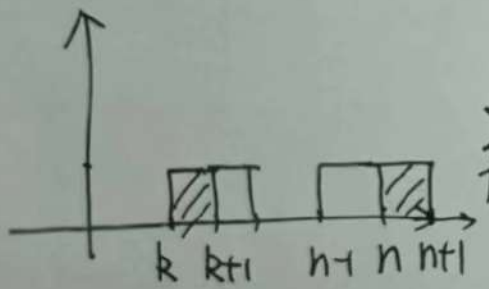
$$r_j = \sum_{i=0}^{j-1} \frac{R}{T_i} = \sum_{i=0}^{j_0-1} \frac{R}{T_i} + \sum_{i=j_0}^{j-1} \frac{R}{T_i}$$

$$= \sum_{i=j_0}^{j-1} \frac{R}{T} = \frac{R}{T} \sum_{i=j_0}^{j-1} 1.$$

$$= \frac{R}{T}(j-1-j_0+1)$$

$$= \frac{R}{T}(j-j_0)$$

$$r_j = r_{j_0} + \frac{R}{T}(j-j_0)$$



$$\sum_{i=k}^{n} 1 = n+1-k$$

案例3中. $r_3 = 0$

$$r_5 = r_3 + \frac{R}{100} \cdot (5-3)$$

$$= \frac{2}{100} R$$

$$r_7 = r_5 + \frac{R}{300}(7-5)$$

$$= (\frac{2}{100} + \frac{2}{300}) R$$

$$r(A,3,7) = 100(r_7 - r_3) = 100\left[(\frac{2}{100} + \frac{2}{300})R - 0\right] = \frac{8}{3}R.$$

求 $r(B,5,9)$

算法：

每一次有用户 stake 和 withdraw 的时候.

1. 计算 r. 也就是累加的 rewardPerToken

$$r = r + R/totalSupply * (currentTime - lastUpdateTime)$$

2. 针对于 stake 或 withdraw 的用户. 计算奖励.

rewards[user] += balanceOf[user] * (r - userRewardPerTokenPaid[user])

3. 更新该用户的 userRewardPerTokenPaid

userRewardPerTokenPaid[user] = r

4. 更新时间戳

last update time = current time

5. 更新质押总量.

balanceOf[user] +/- = amount (+ stake, - withdraw)

totalSupply +/- = amount