1 Mathematical Proof

Table 1.1: Reward distribution example.

i	0	1	2	3	4	5	$R^j_{0,5}$
$R^0_{i,i}$	0	120	40	20	0	0	180
$R^1_{i,i}$	0	0	80	40	48	60	228
$R^2_{i,i}$	0	0	0	60	72	60	192

i is the block number

$R^j_{i,i}$ is the reward of user j at block i

$R^j_{0,5}$ is the reward sum between block $i = 0$ and $i = 5$ of user j

We suppose that at each block a reward is distributed, where BR_i for $i = 0, ..., 5$ is equal to 120 (the value of the reward per block can be dynamic following a precise monetary policy, we used a fixed reward for simplification only) tokens with a chronological order of events as follow:

- $user_0$ stake 100 tokens at block 1
- $user_1$ stake 200 tokens at block 2
- $user_2$ stake 300 tokens at block 3
- $user_0$ widthraw 100 tokens at block 4
- $user_1$ stake 100 tokens at block 5

Obtaining the results presented in Table **??** in a custodial or centralized solution is easy since there is no gas fee or gas block limit, however, when implementing the same algorithm in a smart contract the task is a way harder since it is nearly impossible to compute and save the reward for each user at every block due to high gas consumption when dealing with arrays (if a single user stake at a given block, the reward for all users will change).

1.1 Demonstration

We define $R^j_{K,N}$ as the reward of user j between block K and N.

$$R^j_{K,N} = \sum_{i=K}^{i=N} A^j_i * \frac{BR_i}{S_i} \quad (1)$$

where:

- BR_i is the staking reward at block i to be devided between the stakers
- S_i is the total staked amount at block i for the total number of user P

$$S_i = \sum_{j=0}^{j=P} A^j_i \quad (2)$$

- A_i^j is the amount staked by a user j at block i

If we suppose that no staking or withdrawing activity was done between block K and M, A_i^j and S_i will remain constant on every block i where $i = K, K+1, ..., M-1, M$.

The new formulation of equation **??** will be as follow:

$$R_{K,L}^j = \frac{A^j}{S} * \sum_{i=K}^{i=L} BR_i \tag{3}$$

if we assume that any user x started staking at block M, the reward of user j where $j \neq x$ will be:

$$R_{K,N}^j = R_{K,M}^j + R_{M,N}^j \tag{4}$$

$$R_{K,N}^j = A^j * (\frac{1}{S_{K,M}} * \sum_{i=K}^{i=M} BR_i + \frac{1}{S_{M,N}} * \sum_{i=M}^{i=N} BR_i) \tag{5}$$

If we define the weighted block reward (WBR) as follow:

$$WBR_{K,M} = \frac{1}{S_{K,M}} * \sum_{i=K}^{i=M} BR_i \tag{6}$$

Equation **??** will become:

$$R_{K,N}^j = A^j * (WBR_{K,M} + WBR_{M,N}) \tag{7}$$

1.2 Algorithm

As demonstrated in equation **??**, a user j reward between two blocks *(M,N)* is the sum of WBR between the same blocks multiplied by the user stake.

When a user start staking at block K we save the total sum $WBR_{0,K}$ for the specific user, once he claims, stake or withdraw at block N, we substruct the sum of $WBR_{0,N}$ from the initial sum of $WBR_{0,K}$. hence getting the reward of user j, $R^j = A^j * WBR_{K,N}$.