Goal

Efficient on chain distribution of rewards/dividends to participants according to their share/stake, including frequent distribution (daily/hourly/per block), while share/stake of individual users can change freely (like an ERC20 balance).

Context

Many crypto projects need to disburse “dividends” to holders of staking tokens; other projects have a revenue sharing system where frequent events in their economy generate amounts that must be splitted proportionally between project backers. Examples that could use this technique: staking pools, cooperatives with fractional owning of rent generating assets, paying dividends to share holders, investment funds, recurring payments: salaries could be sent in a single transaction to all employees with any time granularity (hourly/etc); or even the reverse operation: taxing balances of all users by the same percentage, etc.

Solution

Instead of outbound transfers of rewards, keep a clever accounting of individual ratio of rewards based on accumultated reward per unit of stake and let users withdraw their rewards at any moment (in a pull based fashion). This allows O(1) time for all operations of reward distribution or balance change (deposit/withdraw/transfer) and maintains all distribution logic onchain. The algorithm is detailed in our 2 page paper.

It can even be implemented inside an ERC20 compatible contract that will supplimentary expose additional methods like “distribute” and “withdraw reward”.

Note that staking token and dividends token may not be of the same type. Actually, all four combinations of using Ether or an ERC20 token for staking and dividends make sense and have useful usecases.