F1 Fee Distribution Draft-01

Dev Ojha

December 3, 2018

Abstract

In a proof of stake blockchain, validators need to split the rewards gained from transaction fees each block. Furthermore, these fees must be fairly distributed to each of a validator's constituent delegators. They accrue this reward throughout the entire time they are delegated, and they have a special operation to withdraw accrued rewards.

The F1 fee distribution scheme works for any algorithm to split funds between validators each block, with minimal iteration, and the only approximations being due to finite decimal precision. Per block there is a single iteration over the validator set, which enables only rewarding validators who signed a given block. No iteration is required to delegate, and withdrawing only requires iterating over all of that validators slashes since delegation it began. State usage is minimal as well, one state update per validator per block, and one state record per delegator.

1 F1 Fee Distribution

1.1 Context

In a proof of stake blockchain, each validator has an associated stake. Transaction fees get rewarded to validators based on the incentive scheme of the underlying proof of stake model. The fee distribution problem occurs in proof of stake blockchains supporting delegation, as there is a need to distribute a validator's fee rewards to its delegators. The trivial solution of just giving the rewards to each delegator every block is too expensive to perform on-chain. So instead fee distribution algorithms have delegators perform an explicit withdraw action, which yields the same total amount of fees as though they received it at every block.

This details F1, an approximation-free, slash-tolerant fee distribution algorithm which allows validator commission-rates, inflation rates, and fee proportions, which can all efficiently change per validator, every block. The algorithm requires iterating over the validators every block, and withdraws require iterating over all of the corresponding validator's slashes whilst the delegator was bonded. The former iteration is cheap, due to staking logic already requiring iteration over all validators, which causes the expensive state-reads to be cached.

The number of slashes is expected to be 0 or 1 for most validators, so the latter term also meets the blockchains efficiency needs.

The key point of how F1 works is that it tracks how much rewards a delegator with 1 stake for a given validator would be entitled to if it had bonded at block 0 until the latest block. When a delegator bonds at block b, the amount of rewards a delegator with 1 stake would have if bonded at block 0 until block b is also persisted to state. When the delegator withdraws, they receive the difference of these two values. Since rewards are distributed according to stake-weighting, this amount of rewards can be scaled by the amount of stake a delegator had. Section 1.2 describes this in more detail, with an argument for it being approximation free. Section 2 details how to adapt this algorithm to handle commission rates, slashing, and inflation.

1.2 Base algorithm

In this section, we show that the F1 base algorithm gives each delegator rewards identical to that which they'd receive in the naive and correct fee distribution algorithm that iterated over all delegators every block.

Even distribution of a validators rewards amongst its validators weighted by stake means the following: Suppose a delegator delegates x stake to a validator v at block h. Let the amount of stake the validator has at block i be s_i and the amount of fees they receive at this height be f_i. Then if a delegator contributing x stake decides to withdraw at block n, the rewards they receive is

$$\sum_{i=h}^{n} \frac{x}{s_i} f_i = x \sum_{i=h}^{n} \frac{f_i}{s_i}$$

Note that s_i does not change every block, it only changes if the validator gets slashed, or if someone new has bonded or unbonded. We'll relegate handling of slashes to subsection 2.2, and only consider the case with no slashing here. We can change the iteration from being over every block, to instead being over the set of blocks between two changes in validator v's total stake. Let each of these set of blocks be called a period. A new period begins every time that validator's total stake changes. Let the total amount of stake for the validator in period p be n_p. Let T_p be the total fees that validator v accrued in period p. Let h be the start of period p_{init}, and height n be the end of p_{final}. It follows that

$$x \sum_{i=h}^{n} \frac{f_i}{s_i} = x \sum_{p=p_{init}}^{p_{final}} \frac{T_p}{n_p}$$

Let p_0 represent the period which begins when the validator first bonds. The central idea to the F1 model is that at the end of the kth period, the following is stored at a state location indexable by k: $\sum_{i=0}^{k} \frac{T_i}{n_i}$. Let the index of the current period be f. When a delegator wants to delegate or withdraw their reward, they first create a new entry in state to end the current period. Then this entry

is created using the previous entry as follows:

$$Entry_f = \sum_{i=0}^{f} \frac{T_i}{n_i} = \sum_{i=0}^{f-1} \frac{T_i}{n_i} + \frac{T_f}{n_f} = Entry_{f-1} + \frac{T_f}{n_f}$$

Where T_f is the fees the validator has accrued in period f, and n_f is the validators total amount of stake in period f.

The withdrawer's delegation object has the index k for the period which they ended by bonding. (They start receiving rewards for period $k+1$) The reward they should receive when withdrawing is:

$$x \sum_{i=k+1}^{f} \frac{T_i}{n_i} = x \left(\left(\sum_{i=0}^{f} \frac{T_i}{n_i} \right) - \left(\sum_{i=0}^{k} \frac{T_i}{n_i} \right) \right) = x \left(Entry_f - Entry_k \right)$$

It is clear from the equations that this payout mechanism maintains correctness, and required no iterations. It just needed the two state reads for these entries.

T_f is a separate variable in state for the amount of fees this validator has accrued since the last update to its power. This variable is incremented at every block by however much fees this validator received that block. On the update to the validators power, this variable is used to create the entry in state at f, and is then reset to 0.

This fee distribution proposal is agnostic to how all of the blocks fees are divied up between validators. This creates many nice properties, for example it is possible to only rewarding validators who signed that block.

2 Additional add-ons

2.1 Commission Rates

Commission rates are the idea that a validator can take a fixed $x\%$ cut of all of their received fees, before redistributing evenly to the constituent delegators. This can easily be done as follows:

In block h a validator receives f_h fees. Instead of incrementing that validators "total accrued fees this period variable" by f_h, it is instead incremented by $(1 - commission\_rate) * f_p$. Then $commission\_rate * f_p$ is deposited directly to the validator's account. This allows for efficient updates to a validator's commission rate every block if desired.

2.2 Slashing

Slashing is distinct from withdrawals, since not only does it lower the validators total amount of stake, but it also lowers each of its delegator's stake by a fixed percentage. Since noone is charged gas for slashes, a slash cannot iterate over

all delegators. Thus we can no longer just multiply by x over the difference in stake. The solution here is to instead store each period created by a slash in the validators state. Then when withdrawing, you must iterate over all slashes between when you started and ended. Suppose you delegated at period 0, a y% slash occured at period 2, and your withdrawal is period 4. Then you receive funds from 0 to 2 as normal. The equations for funds you receive for 2 to 4 now uses $(1-y)x$ for your stake instead of just x stake. When there are multiple slashes, you just account for the accumulated slash factor.

In practice this will not really be an efficiency hit, as we can expect most validators to have no slashes. Validators that get slashed a lot will naturally lose their delegators. A malicious validator that gets itself slashed many times would increase the gas to withdraw linearly, but the economic loss of funds due to the slashes should far out-weigh the extra overhead the honest withdrawer must pay for due to the gas.

2.3 Inflation

Inflation is the idea that we want every staked coin to create more staking tokens as time progresses. (To the purpose of driving down the worth of unstaked tokens) Each block, every staked token should produce x staking tokens as inflation, where x is calculated from a function $inflation$ which takes state and the block information as input. This inflation can be auto-bonded efficiently into the fee distribution model as follows:

Make each block store the evaluation of $inflation$, which represents the number of staking tokens a single staked token should produce. At the end of each period, increase the validators total number of tokens within the fee distribution by the amount due to inflation. This can be done by multiplying the validators number of staked tokens by (1+ sum of x over the period).

In state a variable should be kept for the sum of all $inflation$ evaluations from now until genesis. Then each period will store this total inflation sum in addition to what it already stores per-period. The presence of comission rates causes the distribution of delegated stake within a validator to change per block. To get around this, when accumulating the value per validator in state, instead of calculating the rewards you'd get for 1 stake, you treat it as though you have $\prod_0^{now} 1+x$ stake, where $\prod_0^{now} 1+x$ is the amount of stake accumulated since genesis until now if you had 1 stake originally bonded. When withdrawing, you take the difference as before, which yields the amount of rewards you would have obtained with $(\prod_0^{begin\ bonding\ period} 1+x)$ stake from the block you began bonding at until now. You then divide that by $(\prod_0^{begin\ bonding\ period} 1+x)$ to normalize it, and then proceed as before.

TODO: Explain this better / put equations to prove correctness

This works great in the model where the inflation rate should be dynamic each block, but apply the same to each validator. Inflation creation can trivially be epoched as long as inflation isn't required within the epoch, through changes to the $inflation$ function.

Note that this process is extremely efficient.

The above can be trivially amended if we want inflation to proceed differently for different validators each block. (e.g. depending on who was offline) It can also be made to be easily adapted in a live chain. (i.e. via governance) It is unclear if either of these two are more desirable settings. Note that this inflation model is in more fair than the currently implemented inflation algorithm, as this has inflation reward delegators not just validators.

2.4 Delegation updates

Updating your delegation amount is equivalent to withdrawing earned rewards and a fully independent new delegation occuring in the same block.

2.5 Jailing / being kicked out of the validator set

This basically requires no change. In each block you only iterate over the currently bonded validators. So you simply don't update the "total accrued fees this period" variable for jailed / non-bonded validators. Withdrawing requires *no* special casing here!

3 State pruning

You will notice that in the main scheme there was no note for pruning entries from state. We can in fact prune quite effectively. Suppose for the sake of exposition that there is at most one delegation / withdrawal to a particular validator in any given block. Then each delegation is responsible for one addition to state. Only the next period, and this delegator's withdrawal could depend on this entry. Thus once this delegator withdraws, this state entry can be pruned. For the entry created by the delegator's withdrawal, that is only required by the creation of the next period. Thus once the next period is created, that withdrawal's period can be deleted.

This can be easily adapted to the case where there are multiple delegations / withdrawals per block. Keep a counter per state entry for how many delegations need to be cleared. (So 1 for each delegation in that block which created that period, 0 for each withdrawal) When creating a new period, check that the previous period (which had to be read anyway) doesn't have a count of 0. If it does have a count of 0, delete it. When withdrawing, decrement the period which created this delegation's counter by 1. If that counter is now 0, delete that period.

The slash entries for a validator can only be pruned when all of that validator's delegators have their bonding period starting after the slash. This seems ineffective to keep track of, thus it is not worth it. Each slash should instead remain in state until the validator unbonds and all delegators have their fees withdrawn.

4 Implementers Considerations

This is an extremely simple scheme with many nice benefits.

- The overhead per block is a simple iteration over the bonded validator set, which occurs anyway. (Thus it can be implemented "for-free" with an optimized code-base)
- Withdrawing earned fees only requires iterating over slashes since when you bonded. (Which is a negligible iteration)
- There are no approximations in any of the calculations. (modulo minor errata resulting from fixed precision decimals used in divisions)
- Supports arbitrary inflation models. (Thus could even vary upon block signers)
- Supports arbitrary fee distribution amongst the validator set. (Thus can account for things like only online validators get fees, which has important incentivization impacts)
- The above two can change on a live chain with no issues.
- Validator commission rates can be changed every block
- The simplicity of this scheme lends itself well to implementation

Thus this scheme has efficiency improvements, simplicity improvements, and expressiveness improvements over the currently proposed schemes. With a correct fee distribution amongst the validator set, this solves the existing problem where one could withhold their signature for risk-free gain.

5 Future Work

- A global fee pool can be described.
- Determine if auto-bonding fees is compatible with inflation and comission rates in conjunction
- Reduce storage in the inflation case, by only having one store of the product of inflation results