# (Bitcoin paper) An Axiomatic Approach to Block Rewards

→ This paper is about incentive issues in block-chain protocols

→ our main focus is incentives for PoW (Proof of Work) miners at the time scale of a single block.

→ How to split block reward amongst the participating miners?

Ans:- As a function of contributed hash rates $h_1, h_2 \cdots h_n$ (Computational Power)

→ proportional allocation :- This means that the expected reward of a miner is equal to the fraction of the overall hash rate that belongs to it.

eg:- If any miner bring 20% of the overall hash rate then that miner gets (0.2× block reward) as a expected reward.

$$E[\text{reward of miner } i] = \frac{h_i}{\Sigma_j h_j}$$

→ can we do better than proportional rule?

→ Implementing Non-proportional Rules :-

→ An allocation rule maps hash rates $(h_1, h_2 \cdots h_n)$ to (expected) rewards $(r_1, \cdots r_n) \rightarrow (x_1(h), x_2(h), \cdots)$

→ Strong budget balance :- An allocation rule 'x' is strongly budget-balanced if $\Sigma_i x_i(h) = 1$ for every configuration h.

Weak budget-balance :- An allocation rule $x$ is weakly budget-balanced if $\sum_i x_i(h) \leq 1$ for every configuration $h$.

→ Alternative way to the proportional allocation rule?

A:- Possible implementation:-

→ Generally bitcoin does leader election as taking a single sample from a probability distribution, the probability distribution that is proportional to miners hash rates

→ You take one sample the selected miner is then one who authorizes the block gets the entire reward

→ But Now, our idea is to take one sample from the hash rate distribution but a 10,000 samples over the course of epic, with that many samples we are going to have almost an exact estimation of the hash rate that everyone contributed, If we know everybody's hash rate then the protocol can distribute rewards.

→ we can get these 10,000 samples by adding (or) giving easier (10,000 times easier version of the crypto puzzle) and collect partial solutions to the easier puzzle, b/w each two solutions of the hard puzzle, we are expecting to see 10,000 samples of the easier, which gives samples from the hash rate distribution.

## Axiom-1 :- Sybil-Proofness

eg:- uniform allocation rule : We take all the public key's and then (uniformly random) pick one of them and that public key miner gets the whole block reward

→ This above example is totally missing the point of sybil attack.

→ If we implement the above rule then certainly everybody is doing sybil attacks.

→ The more public key's you make available to protocol the higher the probability of collecting that reward

→ Sybil-Proofness :- An allocation rule $x$ is sybil-proof if: For every configuration $h \in N^*$ and every configuration $h'$ that can be derived from $h$ by replacing a miner with hash rate $h_i$ by a set $S$ of miners with total hash rate at most $h_i$ (i.e $\sum_{j \in S} h_j' \leq h_i$), the total expected reward to miners of $S$ under $h'$ is at most that of miner $i$ in the original configuration

$$\sum_{j \in S} x_j(h') \leq x_i(h)$$

## Axiom-2 : Collusion-Proofness

eg:- Winner-take-all allocation rule: We are taking 10,000 samples, we have accurate estimation of everybody's contributed hash rates then we could do is deterministically allocate the entire block reward to the biggest hash rate miner.

→ The above example is sybil-proof rule, but the above example gives incentive to collude, Try to form a 51% pool to get that reward.

Collusion-Proofness :- An allocation rule $x$ is collusion-proof if: For every configuration $h \in N^*$ and every configuration $h'$ that can be derived from $h$ by replacing a set $T$ of miners with a new miner $i^*$ with hash rate at most the total hash rate of miners in $T$ (i.e with $h'_{i^*} \leq \sum_{j \in T} h_j$), the total expected reward to miner $i^*$ under $h'$ is at most the total expected reward of miners of $T$ in the original configuration.

$$x_{i^*}(h') \leq \sum_{j \in T} x_j(h)$$

→ Strong collusion-proofness (under proportional sharing) :-

→ (i) no miner of $T$ has strictly higher expected reward in $h'$ (with proportional sharing) than in $h$

→ (ii) some miner of $T$ has strictly lower expected reward in $h'$ (with proportional sharing) than in $h$ That is, if

$$x_{i^*}(h') \cdot \frac{h_i}{\sum_{j \in T} h_j} > x_i(h)$$ for some miner $i \in T$

then $$x_{i^*}(h') \cdot \frac{h_l}{\sum_{j \in T} h_j} < x_l(h)$$ for some other miner $l \in T$

→ Weak collusion-proofness (under proportional sharing):

$$x_i(h') \cdot \frac{h_i}{\sum_{j \in T} h_j} \leq x_i(h)$$

Axiom-3: Uniqueness theorem :- Rewards depend only on the set of hash rates, not on miner names.

eg:- There are some dictator rules (give reward to lexicographically first miner)

→ proportional allocation rule satisfies three axioms

① sybil-proofness
② collusion-proofness
③ uniqueness theorem

→ If we want to deviate from proportionality rule, then we have to relax (or) give up on one of these three axioms.

## Proof of Uniqueness Theorem

Assume: hash rates are positive integers
by scaling, extends to all rational hash rates

Proof: By induction on number of miners with hash rate > 1

→ we are going to induct on the number of miners who contribute a hash rate bigger than the minimum (2 (or) more)

→ Base case: (i.e, all-1's vector)

→ all miners get same reward.

→ budget-balance → reward must be $1/H$
(where $H$ = sum of hash rates)

→ Inductive step: ($t$ miners with hash rate > 1)

→ Consider miner $j$ with $h_i > 1$ (let $H = \sum_j h_j$)

Case-1:- expected reward to $i < h_i/H$

→ Consider sybil attack by $i$ (split into $h_i$ miners with hash rate 1 each) call result $h'$

→ $h'$ has $t-1$ miners with hash rate > 1 by inductive hypothesis, sybils get $1/H$ reward each in $h'$, for a total of $h_i/H$

→ Here $h$ withesses failure of sybil-proofness.

Case 2:- Expected reward to $i > h_i/H$

→ Here $h'$ withesses failure of collusion-proofness.

Risk-neutral miners: care only about expected reward.

Risk-averse miners: want to maximize $E[u(\text{reward})]$, where $u$ = strictly concave function. prefer certainty to uncertainty

observation: with risk-averse miners, current randomized implementation of the proportional rule is not collusion-proof.

incentive to form mining pools, reduce reward variance.