Protocol Change

Yunshu Liu

2020.6.11

I. Part 1 change: miners generate 1 block every 10 minutes

Implementation:

- Miners always keep trying to find new block (even when transaction pool is empty)
- Block reward: miner who successfully produces a block get it
  - Initially block reward is 50 bitcoins, it halves every 144*365*4 blocks
    (Explanation: 1 block correspond to 10 minutes, 144*365*4 blocks are roughly 4 years)
- Keep block generation time to 10 minutes
  (Explanation: More miners, more computing power, but still keep 10 minutes)
  - Mining target value for time t: D_t (Explanation: when a block's hash value is smaller than D_t, the miner successfully finds a new block)
  - Mining target value adjustment: With more computing power, set lower D. Lower D means more difficult to find a block, which can leverage more computing power.
    1) Calculate the average block generation time of past 144*14 blocks $\bar{t}$ in terms of seconds (144*14 blocks is roughly 2 weeks)
    2) Mining target value for next time slot :

$$D_{t+1} = \frac{D_t \bar{t}}{600}$$

- Block size limit: the size of a block should not exceed 1MB
  (Explanation: avoid long communication time)

II. Part 2 change: transaction pool change

Implementation:

- Transaction pool's size is infinite
- When miners select transaction into a block, they first select transaction with highest $\frac{\text{Fee}}{\text{size}}$ value, then select transaction with second-highest $\frac{\text{Fee}}{\text{size}}$ value, until there is no more transaction or block is 1MB.
  (Explanation: Block size is limited, miners prefer transaction with higher $\frac{\text{Fee}}{\text{size}}$ ratio)

III. Part 3 change: Time constraint

Implementation:

- Transaction:
  - Add generation time (in terms of second)
  - Add expire time, and

$$\text{expire time} = \text{generation time} + 1200$$

    (Set expire time 20 minutes ahead)
    (Explanation: Valid tx: generation time $\leqslant$ current time $\leqslant$ expire time)
- Miners:
  - When broadcast unrecorded transaction, verify if the transaction is valid, if not, delete it
  - When select transactions and mine a block, verify if the transaction is valid, if not, delete it from tx pool
  - When accept new block from other miners, verify if all txs in the block are valid, if not, delete the block

References