Summary – Difficulty calculation

Huajing Yu

I. The new concepts

The new concepts that I have learned in this week.

1.Bitcoin uses a proof-of-work system that involves scanning for a required hash by increasing a nonce in the block, and the required hash begins with a number of zero and less than the given bits in the block. Once the calculation effort has been expended to find the required hash, the block cannot be tampered unless redoing the work. The required hash is calculated as follows:

$$Sha256(Sha256(version, parentHash, merkleRoot, time, bits, nonce)) \leqslant bits \tag{1}$$

$version$ is the block version; $parentHash$ is the previous block hash; Transactions are hashed in a Merkle Tree, with only the $merkleRoot$ included in block; $time$ is the timestamp that is included into the block by miner, $bits$ means the mining difficulty in this round, miner takes Sha256 algorithm that hashes the block items for calculating a hash less than the bits by increasing a $nonce$ in the block.

2.Ethereum has a higher fork risk than bitcoin because Ethereum adjusts the excepted block interval to 13s, which generates many uncle blocks that are not part of the main chain. A miner who mined uncle block will not be rewarded unless the uncle block is referenced by one regular block that exists in the main chain, and the rewards ranges from a $\frac{7}{8}$ block reward for an immediate inclusion to a $\frac{2}{8}$ block reward for inclusion 6 blocks later. Ethereum leverages the greedy heaviest observed subtree(ghost) to deal with the fork problems. The formula of calculating uncle-block's rewards is as follows:

$$R_{uncle} = (H_{uncle} - H_{block} + 8) \div 8 \times R_{blocks} \tag{2}$$

R_{uncle} represents rewards that should give uncle block's miner;H_{uncle}notes the height of uncle block;H_{block}means the height of block that references to the uncle block;R_{block}represents the basic rewards of usual block in the main chain.

3.Ethereum is a platform built on blockchain techniques, using smart contracts to hold state. Moreover, it aims to provide a tightly integrated p2p network to the developer for building application on a hitherto unexplored compute paradigm. Ethereum is a asic-resistance with initial 16M cache and 1G dataset, and it uses the small cache to verify the mining puzzles and the big dataset to solve the mining puzzles.

5. Ethereum calculates a new mining difficulty in every round based on the time between adjacent blocks and Moore's law that mining reliability challenges. The algorithm of adjusting mining difficulty is as follows:

$$D_{n+1} = D_n + D_n \times \frac{\max[u - \frac{T(B_{n+1}) - T(B_n)}{i}, -99]}{2048} + 2^{ph-2} \tag{3}$$

D_{n+1} is the mining difficulty in this round B_{n+1} ; D_n is the mining difficulty in last round; u equals to 2 if block B_n contains uncle block else 1; $T()$ returns the timestamp of the block; i is the excepted block interval in Ethereum; ph returns a virtual block height that returns block height minus 10,700,000 according to eip-4345 published in Dec.10 2021.

6. Bitcoin adjusts mining difficulty in every 2016 blocks according to the difference of excepted and actual mining time.

$$D_{n+1} = D_n \times \frac{T_{default}}{T_{actual}} \tag{4}$$

where, D_{n+1} is the mining difficulty in this round; D_n is the mining difficulty in last round; $T_{default}$ returns the total excepted mining time in last 2016 blocks; T_{actual} returns the total actual mining time in last 2016 blocks;