以太坊难度调整

2018.10

什么是难度

- **难度(Difficulty)** 一词来源于区块链技术的先驱比特币，用来度量挖出一个区块平均需要的运算次数。
- 挖矿本质上就是在求解一个谜题，不同的电子币设置了不同的谜题。比特币使用SHA-256、莱特币使用Scrypt、以太坊使用Ethash。一个谜题的解的所有可能取值被称为解的空间，挖矿就是在这些可能的取值中寻找一个解
- 这些谜题都有如下共同的特点：
  - 没有比穷举法更有效的求解方法
  - 解在空间中均匀分布，从而使每一次穷举尝试找到一个解的概率基本一致
  - 解的空间足够大，保证一定能够找到解

什么是难度

- 现在我们为谜题设置一个参数 **Difficulty**，那么谜题就变成了求解某个空间内符合 **x<Difficulty** 的 x，这个参数Difficulty 就是所谓的**难度**
- 难度(Difficulty) 通过控制合格的解在空间中的数量来控制平均求解所需要尝试的次数，也就可以间接的控制产生一个区块需要的时间，这样就可以使区块以一个合理而稳定的速度产生
- 当挖矿的人很多，单位时间能够尝试更多次时，难度就会增大，当挖矿的人减少，单位时间能够尝试的次数变少时，难度就降低。这样产生一个区块需要的时间就可以做到稳定

以太坊中的难度计算

- 难度计算的规则
  - 以太坊中有三种计算难度的规则，分别对应着以太坊中三个不同阶段的版本：Frontier，Homestead 和 Metropolis，现在用的方法叫做 calcDifficultyByzantium ()，对应大都会的拜占庭阶段
- 计算一个区块的难度时，需要以下输入：
  - parent_timestamp：上一个区块产生的时间
  - parent_diff：上一个区块的难度
  - block_timestamp：当前区块产生的时间
  - block_number：当前区块的序号

以太坊中的难度计算

计算步骤：

- block_diff = parent_diff + 难度调整 + 难度炸弹
- 难度调整 = parent_diff / 2048 * max((2 if len(parent.uncles) else 1) - ((timestamp - parent.timestamp) // 9), -99))
- 难度炸弹 = 2^((parent.Number - bombDelay) //100000 - 2)

- 目前拜占庭阶段， bombDelay = 3000000
- 另外，区块难度不能低于以太坊的创世区块，创世区块的难度为131072，这是以太坊难度的下限。

Q&A


尚硅谷