上海交通大学
SHANGHAI JIAO TONG UNIVERSITY

第五次作业

李子龙
123033910195

2023 年 11 月 17 日

矿池管理员

工作

- 准备一个区块模板，包含区块头和块内的多个交易。
- 根据最高的支持矿工数 65536 = 2^{16}，划分 nonce 的前缀为 `0x0000` ～`0xffff`，矿池里的每个矿工都会被分配一个 nonce 前缀。
- 由于矿工的效率较高，每秒可以尝试 2^{44} 个 nounce，每个块的平均挖出时间为 10 分钟，也就是 600 秒，一般会设定最长时间为 120 分钟，即 7200 秒，所以对于一个模版，矿工大概可以尝试 2^{56} 个 nonce，这对于 32 位的 nounce 剩余的 2^{16} 空间是不足的。因此矿工将会被允许对 coinbase transcation 中的 coinbase 字段进行增添，比如添加一个 40 位以上的 extranonce，只要 coinbase 交易不超过 800 位的固定长度限制，矿池管理员也会认为这是一个合法的挖矿。
- 根据每个矿工提交的块的频率，每一轮动态调整该矿工的难度，通过限定矿工提交块的哈希值应当在某一个值以下（指定一个目标 target 值），使得矿工能够接近于一个合理的频率提交结果，避免网络占用过于频繁。
- 如果有矿工返回了一个合适的区块，经矿工管理员检查通过后，通知各个矿工本区块挖矿结束。

发送

- `coinbasetxn` coinbase 交易，包含一个 `data` 字段可供矿工增添。
- `previousblockhash` 区块前置哈希。
- `transactions` 交易信息。
- `expires` 过期时间，比如 120 分钟。
- `target` 目标哈希，矿工挖到的区块哈希不应当超过这个值。可以用于难度调整，该值越小矿工难度越大。
- `nonce(prefix)` 该矿工分配到的 nonce 前缀。
- 还可以包含一些 flags 以及其他元信息。

矿池矿工

工作

- 向矿池管理员请求一个区块模板。
- 根据交易计算 merkle root 哈希，根据得到的 `nonce(prefix)` 对剩余的 nonce 16 位空间进行搜索，计算区块哈希，观察是否不超过 `target` 目标值。
- 如果上一步找到了一个合适的 nonce 值满足条件就将结果返回给矿池管理员。

- 否则，对于每个可能的 nonce 值，再增加一个 40 位以上的 extranonce 插入 `coinbasetxn` 中的 `data` 字段。重新计算 merkle tree 上该路径上的哈希值，并计算 merkle root 哈希，计算区块哈希，观察是否不超过 `target` 目标值。
- 如果找到了一个合适的 nonce 值和 coinbase data 值，就将结果返回给服务器。如果超过一定时间仍未找到或被通知到本矿池内其他的矿工已经找到合适的区块，则放弃本次挖矿，向服务器请求下一次挖矿区块模板。

发送 矿工需要返回区块头和 coinbase transaction。为了节省网络带宽，可以协定不返回区块交易数据。