POW即工作量证明，区块链是由网络上互不相识、匿名的节点共同维护，每个区块就是所投入工作量的证明，要确保妄图修改历史区块的节点比那些诚实的、仅仅是要增加新区块的节点耗费更大的工作量，那么与其耗费大力气篡改区块，还不如老老实实的竞争出块权，还能得到区块链奖励。

那么比特币的POW到底在做什么？真如大家传说中的挖矿吗？当然不是真的挖矿啦，比特币利用了哈希的随机性，一点小小的改动，哈希值变化会很大，无法进行预测。

POW具体在做什么呢？计算区块头的哈希值，好像大家忘记了，好吧，我把上个文章的图在贴过来，

```
UniValue generate(const JSONRPCRequest& request)
{
    CWallet * const pwallet = GetWalletForJSONRPCRequest(request);

    if (!EnsureWalletIsAvailable(pwallet, request.fHelp)) {
        return NullUniValue;
    }

    if (request.fHelp || request.params.size() < 1 || request.params.size() > 2) {
        throw std::runtime_error(
            "generate nblocks ( maxtries )\n"
            "\nMine up to nblocks blocks immediately (before the RPC call returns) to an address in the wallet.\n"
            "\nArguments:\n"
            "1. nblocks      (numeric, required) How many blocks are generated immediately.\n"
            "2. maxtries     (numeric, optional) How many iterations to try (default = 1000000).\n"
            "\nResult:\n"
            "[ blockhashes ]     (array) hashes of blocks generated\n"
            "\nExamples:\n"
            "\nGenerate 11 blocks\n"
            + HelpExampleCli("generate", "11")
        );
    }
```

这个generate函数下面调用了generateBlocks

代码位置：bitcoin/src/rpc/mining.cpp