## 2.比特币（BTC）PoW（Proof of Work，工作量证明）共识算法的详细流程

### 第一步

矿工收集网络中未确认的交易，验证其合法性，计算merkle root。

### 第二步

矿工寻找nonce，计算双SHA-256，如果hash = SHA256(SHA256(block\_header))<target，则说明此nonce可以出块。

block\_header包含：prevhash（前一个块的hash）、merkle root、timestamp（时间戳）、bits（难度目标）、nonce（随机数）

### 第三步

矿工打包完整区块（区块头+区块体），并通过P2P向全网广播。

### 第四步

其他节点收到后，验证区块内签名、交易是否合法，重新计算hash是否<target，检验prevhash是否指向当前最长链的最新区块。

### 第五步

当全网多数节点验证通过后，新区块被正式确认并追加到当前最长链的末端形成新区块。进入下一轮挖矿流程。矿工获得区块奖励（新发行的BTC）和交易手续费。

## 3.比特币（BTC）PoW共识过程会遇到问题，BTC 解决方案

1.区块分叉

问题描述：同时出现两个有效区块，链出现了分叉。

解决方式：最长链为有效链。短链会被丢弃，且矿工无法获得奖励。

2.处理效率低

问题描述：比特币**TPS仅为7**，确认时间冗长，难以满足实时支付等高频交易需求。

解决方式：建立layer2，减轻链上负担，降低能源消耗，同时提升交易速度和效率。。

3.51%的攻击问题

问题描述：对于一些算力较小的PoW链，可能会面临51%的攻击风险，攻击者可以篡改交易记录、进行**双花**等。

解决方式：鼓励全球更多矿工参与挖矿，增加攻击者的成本。

4.难度调整机制

问题描述：算力剧烈波动导致出块时间偏离 10 分钟。

解决方式：每2016个区块自动调整挖矿难度，确保区块生成的时间稳定在10分钟左右。

5.高能耗问题

问题描述：比特币挖矿需要大量算力，导致能耗巨大，不环保。

解决方式：目前无完美解决方案。

6.**孤块**

问题描述：区块的父区块尚未到达本地。

解决方式：建立孤独池，父区块到达后立即链接。