Proof of Work（工作量证明）

区块链如何在「没有老师」的情况下，全班都抄同一本答案?

这一章你会学到什么？

- 什么是「共识（Consensus）」
- 为什么区块链需要 Proof of Work
- PoW 是如何防止作弊与攻击的
- 区块分叉（Fork）、最长链规则、Finality
- 「工作量」到底在做什么?

什么是共识（Consensus）？

一句话给小学生听

共识就是：**全班同学都同意「答案本现在写到哪一页」**

区块链里的共识是什么意思？

在区块链里：

- 没有老师（没有中央银行、没有服务器）
- 每个人都有一本账本

共识 = 所有节点都同意「目前账本的正确状态」

如果没有共识会怎样？

- 有人说 Alice 还有 1 ETH
- 有人说 Alice 已经转给 Bob 了

→ 系统直接坏掉

什么是共识协议（Consensus Protocol）？

小学生版解释

共识协议 = 一套「投票 + 奖惩」的游戏规则

共识协议在做什么？

- 奖励「守规则的人」
- 惩罚「想作弊的人」
- 让作弊 **变得非常非常贵**

重要观念

区块链安全不是靠「相信好人」，而是：**让坏人赔到破产**

Proof of Work 是什么？

一句话给小学生听

Proof of Work = **谁先完成最难的作业，谁就可以写下一页答案**

PoW 在做三件事

- 决定「谁可以产生新区块」
- 防止一个人假装成很多人（Sybil Attack）
- 保护区块链不被乱改

PoW 的核心流程（一步一步）

步骤 1：矿工收集交易

发生什么事？

- 用户发出交易
- 交易进入「记忆池（mempool）」
- 矿工挑交易（手续费高的优先）

步骤 2：开始解谜（工作量）

谜题在干嘛？

矿工要找到一个随机数（**nonce**），让：

$$Hash(+ nonce) <$$

小学生版类比

- 像是在一直丢骰子
- 直到丢出「超级小的数字」

重点

没有捷径，只能一直试

为什么这件事可以保护区块链？

1. 网络安全

为什么攻击很贵？

要攻击网络，你必须：

- 买大量矿机
- 付巨额电费
- 还不一定赢

2. 防止女巫攻击（Sybil Attack）

小学生故事

- Alice：一台电脑
- Bob：一台电脑
- Charlie：假装 100 个人，但只有一台电脑

PoW 看的是「算力」，不是「名字数量」

结论

你装成几个人都没用，电脑跑多快才是真的

区块分叉（Fork）与最长链规则

为什么会分叉？

- 两个矿工几乎同时挖到区块
- 网络有延迟

→ 世界短暂出现两条链

最长链规则

- 哪一条链继续长得比较快
- 哪一条就被当作「正确答案」

Nakamoto 共识

Proof of Work + 最长链规则 = Nakamoto Consensus

Finality（最终确定性）

一句话给小学生听

等「后面又写了好几页」，前面的内容就不会被擦掉了

以 Ethereum（PoW 时代）为例

- 等 6 个区块
- 被回滚的机率 $< 0.00001\%$

为什么要等？

因为前面可能是「临时分叉」

「工作量」到底在证明什么？

重点一句话

证明矿工真的：

- 花了钱
- 用了电
- 付出算力

为什么这很重要？

- 作假会被马上发现
- 被发现 = 白烧电费

→ **诚实最划算**

本章小学生必背

- 共识 = 全世界抄同一本账
- PoW = 谁算得快谁写下一页
- 算力就是权力
- 攻击很贵，所以不值得
- 等几块 = 交易更安全

备注：Ethereum 已于 2022 年转为 Proof of Stake，但 PoW 是理解区块链安全的基础。