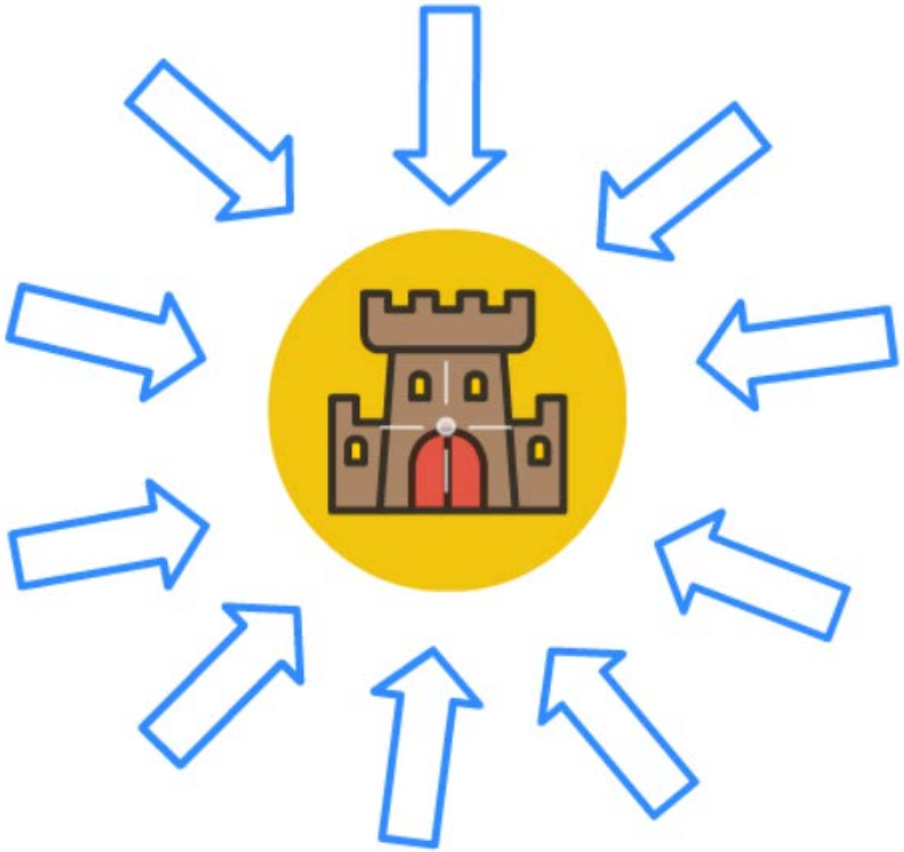
分布式系统和一致性

分布式系统问题



谁说了算的问题, 听谁的!

工作证明Pow

- 获取这个证明需要很长的时间
- 而验证它的真伪只需要很短的时间


考过高富帅 战胜官二代


高考
CFP 供图

有人说高考是千军万马过独木桥,
高中毕业,再过4年就可以获得学士学位.
学士学位再学3年,就可以获得硕士学位,
硕士学位再学3年,就可以获得博士学位,
博士学位再学3年,就可以获得壮士学位,
壮士学位再学3年,就可以获得圣斗士学位…

学士→硕士→博士→壮士→圣斗士

他们像一个链表,
不考取博士绝对成不了壮士,
不获取壮士学位就当不成圣斗士

比特币采用了类似的方式, 他降低了信息传递的速率，
增加了成为领导的难度, 通过区块链的短暂分叉。
完美的解决了拜占庭将军的问题.

记账的群众 (矿工)

故事开始了，商务男, 小男孩 和 老爷爷斗地主.
商务男输了10块钱, 要给小男孩和老爷爷每人转账5块钱.

商务男 本应该把这个转账消息大喇叭广播给所有的记账的吃瓜群众.
然而他并没有.

他冒充矿工伪造账本**单独的**发给了老爷爷和小男孩,
看这是账本, 你们卡上多了5块钱.

老爷爷和小男孩看到商务男发来的账本就是这样

账本	
商务男	90
老爷爷	105
小男孩	105

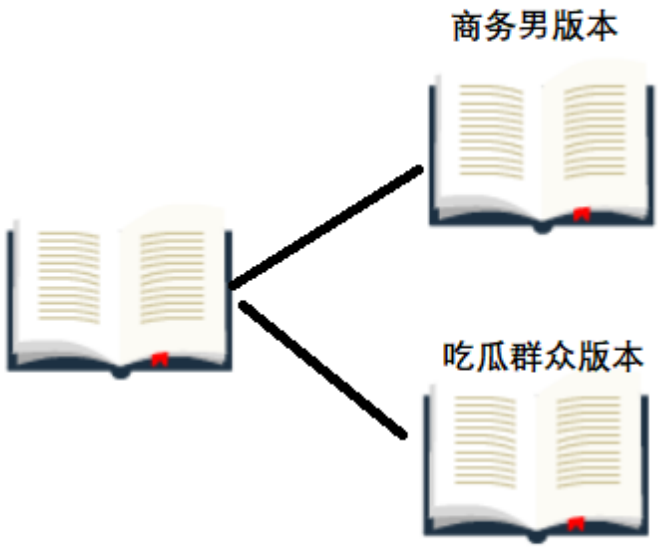
可是老爷爷和小男孩还收听着所有的吃瓜群众 ABCDEFGH 的账本

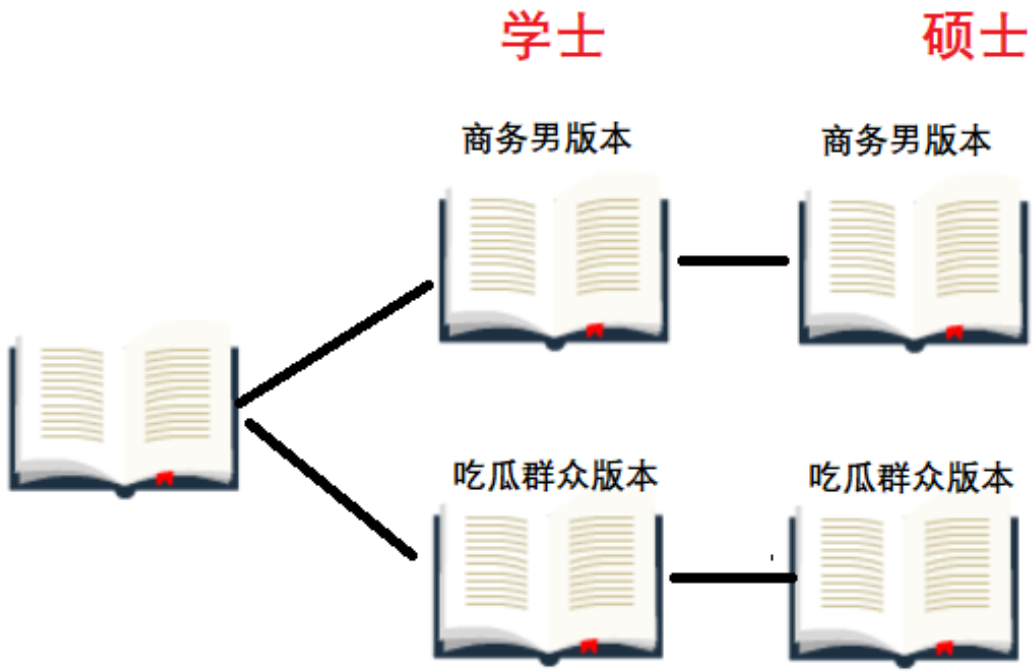
账本	
商务男	100
老爷爷	100
小男孩	100

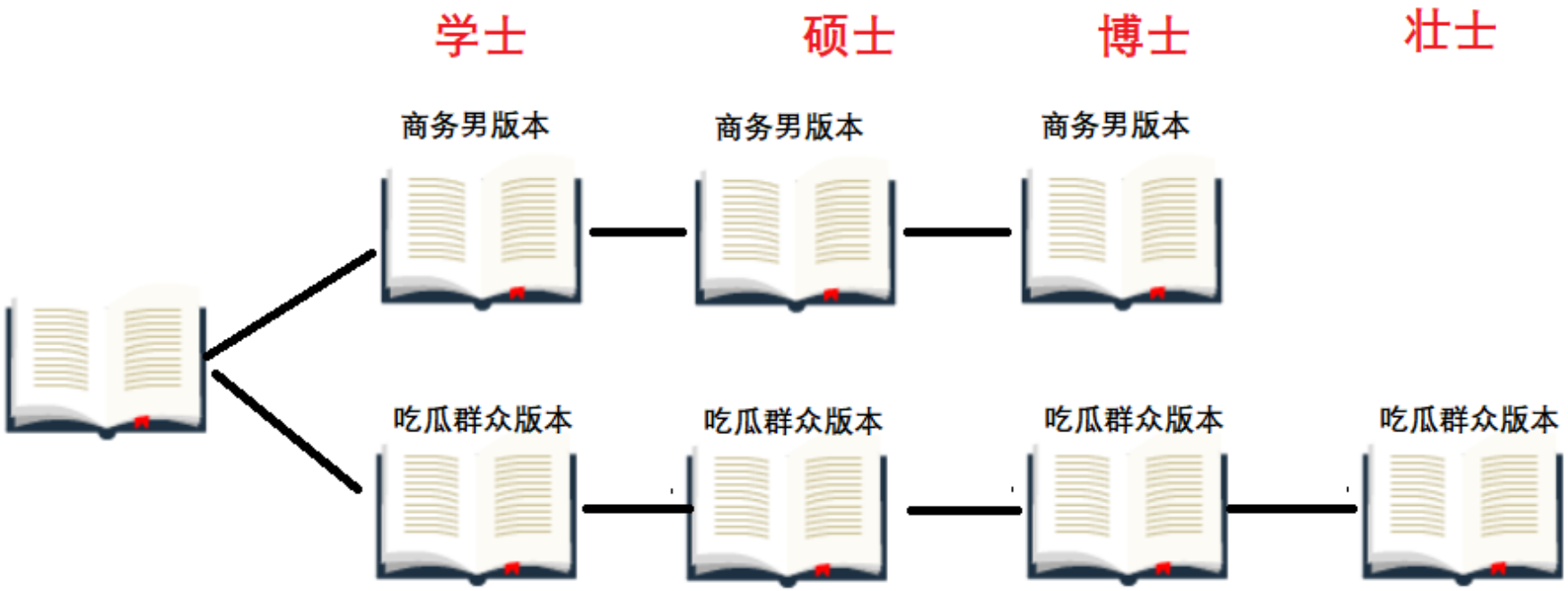
听谁的

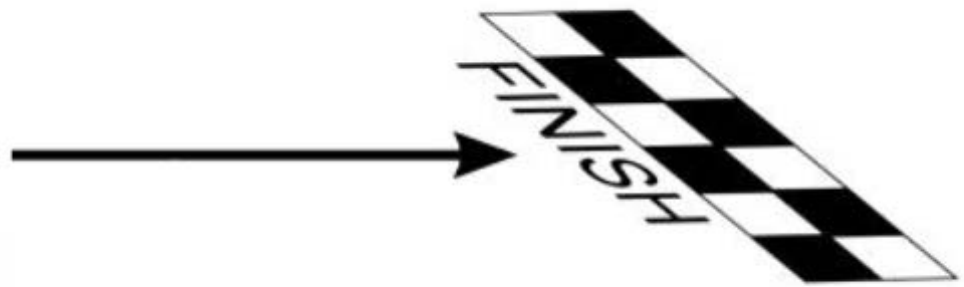
- 饭后走一走，活到九十九
- 饭后不宜百步走

学士

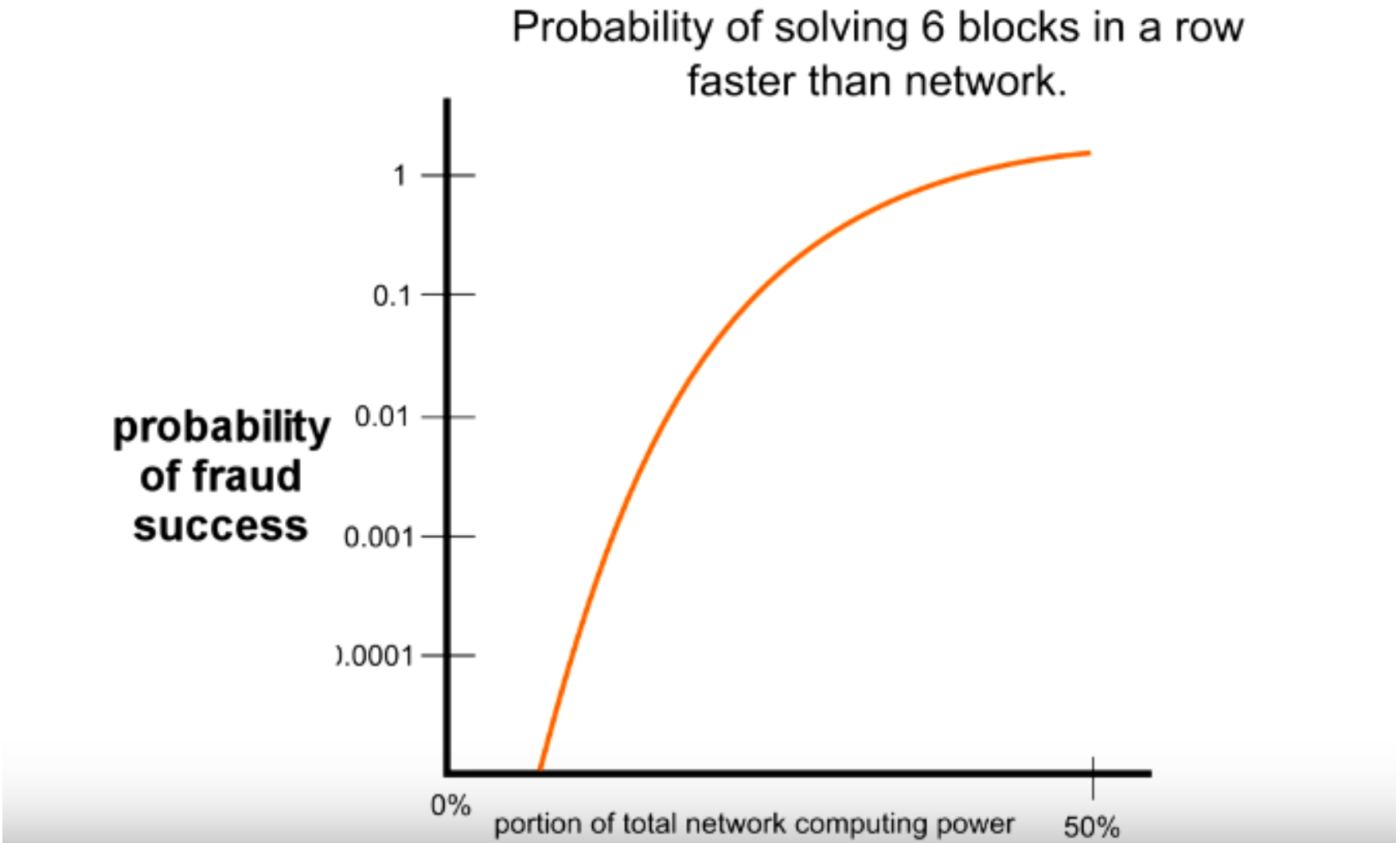



学士
硕士
商务男版本
商务男版本
吃瓜群众版本
吃瓜群众版本


学士
硕士
博士
壮士
商务男版本
商务男版本
商务男版本
吃瓜群众版本
吃瓜群众版本
吃瓜群众版本
吃瓜群众版本


FINISH

6个区块确认后，就是有效的


Probability of solving 6 blocks in a row faster than network.
probability of fraud success
1
0.1
0.01
0.001
.0001
0%
portion of total network computing power
50%

学习笔记

- 比特币通过p2p技术实现账本的同步拷贝
- 比特币通过增加发送信息的成本(pow)来增加信息传播的成本,降低信息传播的速率
- 比特币通过区块链的长度,来判断数据的可信度
- 交易中6个有效区块认为转账成功. 所以比特币的交易确认需要1小时
- Pow通过sha256哈希来完成, 后面单独介绍
- 工作证明的获取需要很长时间, 但是验证只需要很短时间.
- 比特币的Pow算法导致大家通过矿池来挖矿, 矿池算力垄断. 有潜在的中心化风险.
- 矿池挖矿只是在抢夺记账权,获得比特币,消耗大量电力,并无实际价值,我国计划取缔挖矿.


Witness
图片
深山里的比特币矿场
摄影 刘行喆 | 编辑 米杜 | 新浪图片出品
法律法规网

比特币的价值

- 价值转移
- 区块链可以让物质的转移像信息流动一样快速便捷，同时又由全网的人一起来担保(全部参与的人一起担保就相当于天然存在存在不可证伪，除非其中51%的人统一口径违约)，来保证在虚拟世界中的物质转移的可靠。
- 价值转移，这就是“区块链”技术有望成为引领“第四次技术革命”的核心原因。