区块链价值与原理

登链社区 - Tiny熊

要点

- 为什么需要区块链（区块链价值）
- 区块链关键技术

当前互联网WEB2 现状

- 带来高度**便利**：获取信息、社交互动、交易、娱乐…
- **依赖**：让互联网大厂掌控着绝大部分资源与服务，也控制着我们
- **“割裂”体验**：如：账号、跨境转账等
- **被“利用/挟持”**：利用垄断滥用权力（寻租）
  - 暴力牟利、强迫用户、互通设障、信息审查与控制、隐私泄露 …

“一切有权力的人都会滥用权力,这是一条万古不易的经验”

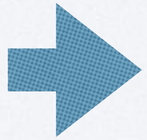
– 孟德斯鸠

问题源于：

用户没有控制权

解决问题的希望 - 区块链技术

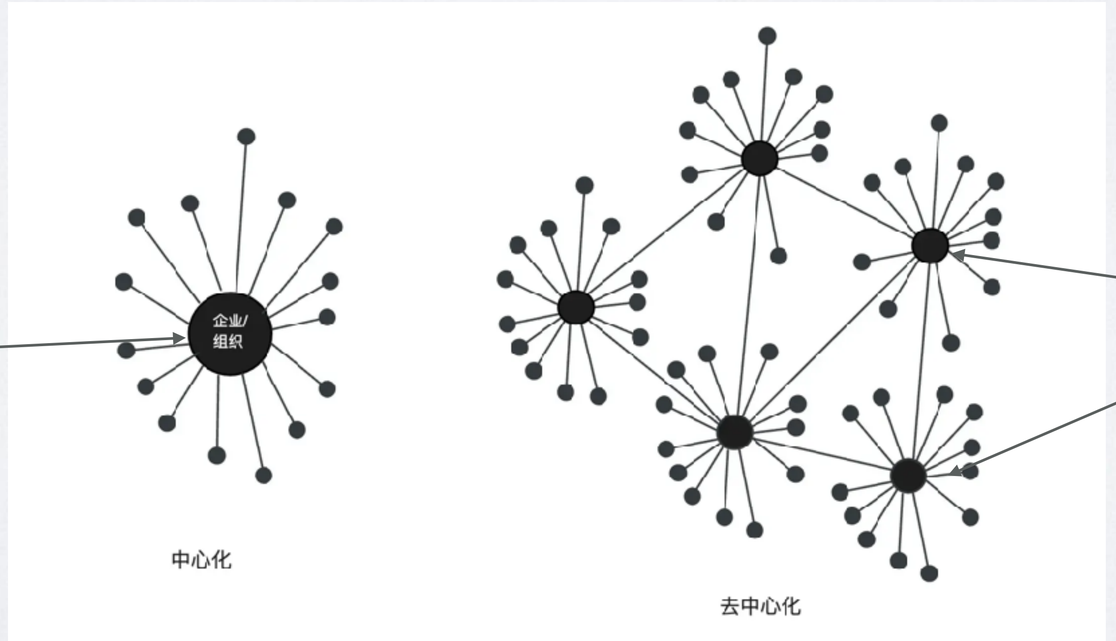
- 区块链技术利用密码学和去中心化网络搭建了一个公共技术平台
  - 密码学：所有权控制
  - 去中心化网络：节点相互验证（要求代码开源）、防止作恶
- 实现：

基于人/组织的信任  基于代码的信任

Web3 经典语录：Do not trust , verify.

如何实现基于代码的信任

- 前提：代码开源， 以便他人可以启动运行，参与网络
- 核心：去中心化
  - 同一个代码（规则）在 N 个不相关 节点上运行
  - 节点独立行动：某个节点的数据修改不被其他节点认可
  - 没有任何特权节点



中心控制着一切

节点是平等的
限制单体作恶空间

区块链技术的两个关键问题

- 无中心，如何确权？
- 如何让独立的个体达成一致的行动？
  - 独立：不依附他人决策
  - 独立：与他们没有利益关系

“比特币：一个点对点的电子现金系统”

– 中本聪 *2008*

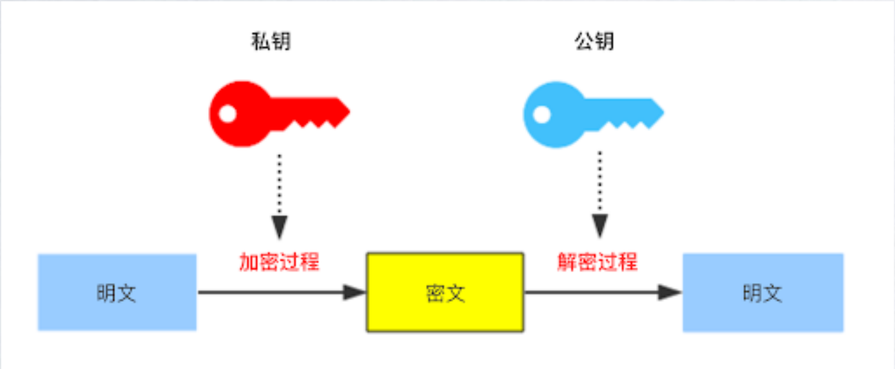
比特币核心

- 个人私钥控制资产（非对称密码学应用）
- 链式结构，防篡改、好验证（区块链名称来历）
- POW 共识：谁先完成计算，谁获奖励

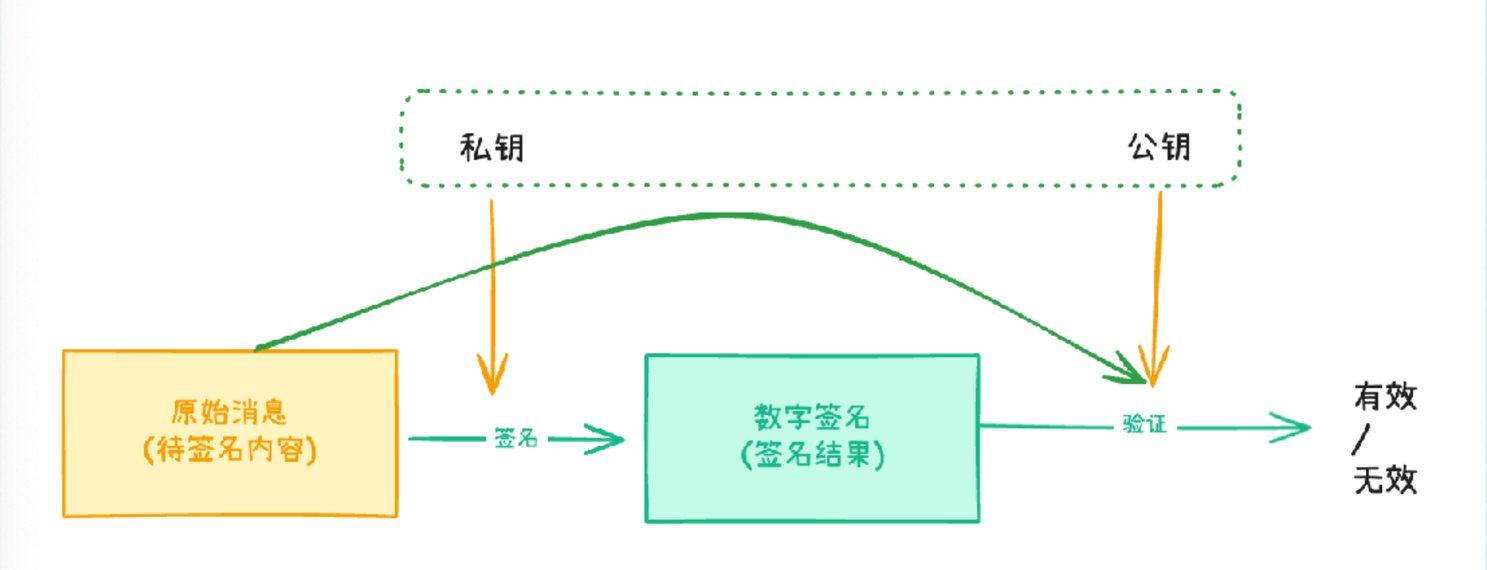
资产所有权

- 银行、金融账户
  - 账号 + 密码（只有自己知道）
  - 后台系统核对
- 比特币
  - 私钥（只有自己知道）签名交易（用钱包管理）
  - 任何人通过公钥公开校验

所有权 - 数字签名



非对称加密/解密

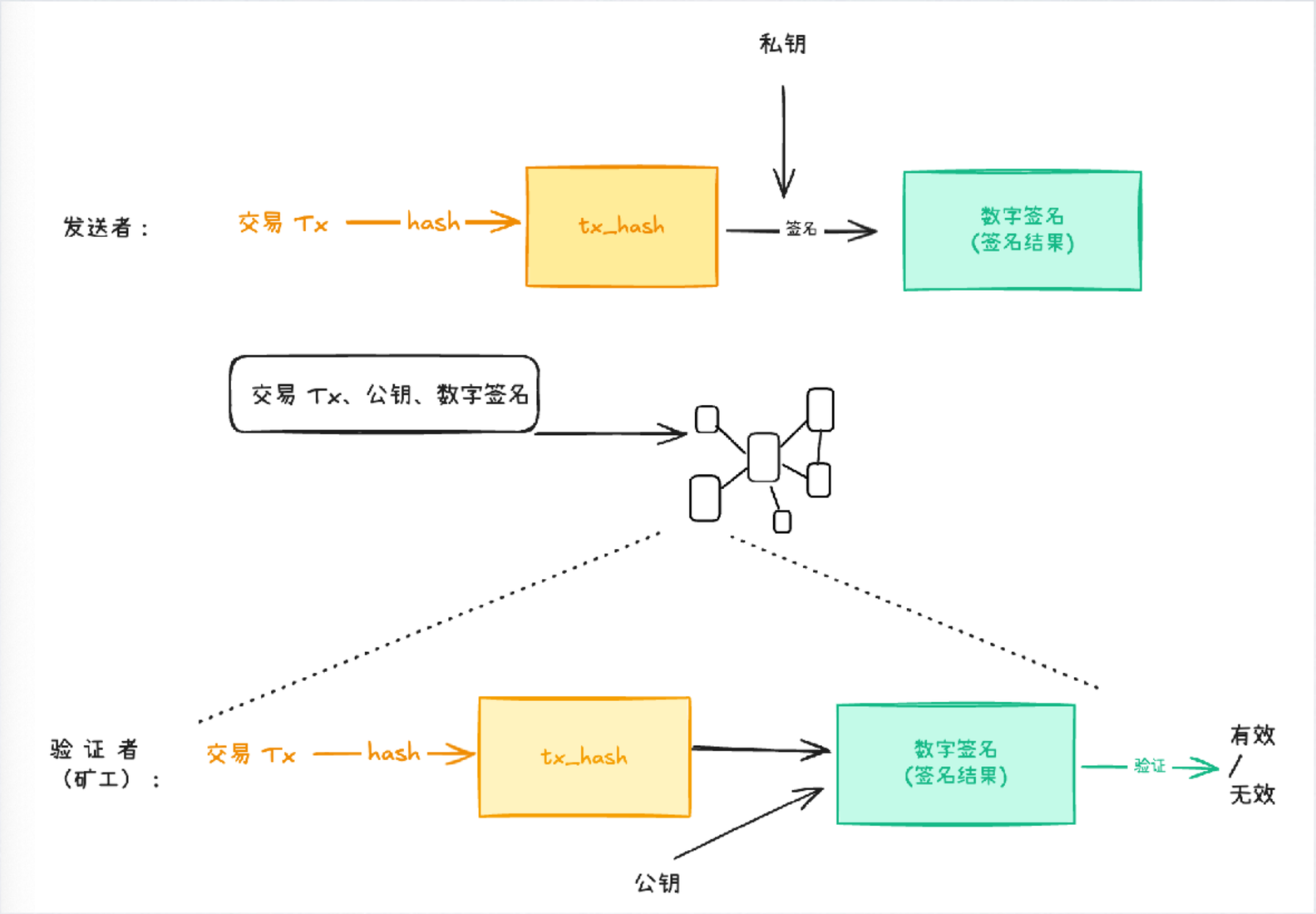


数字签名： 私钥签名、公钥验证

非对称加密与数字签名原理类似（公钥密码学）

目的不一样：前者用于隐私、后者用于证明身份

所有权 - 数字签名


私钥
发送者：
交易 Tx
hash
tx_hash
签名
数字签名
(签名结果)
交易 Tx、公钥、数字签名
验证者
（矿工）：
交易 Tx
hash
tx_hash
数字签名
(签名结果)
验证
有效
/
无效
公钥

链式结构 - 账本验证

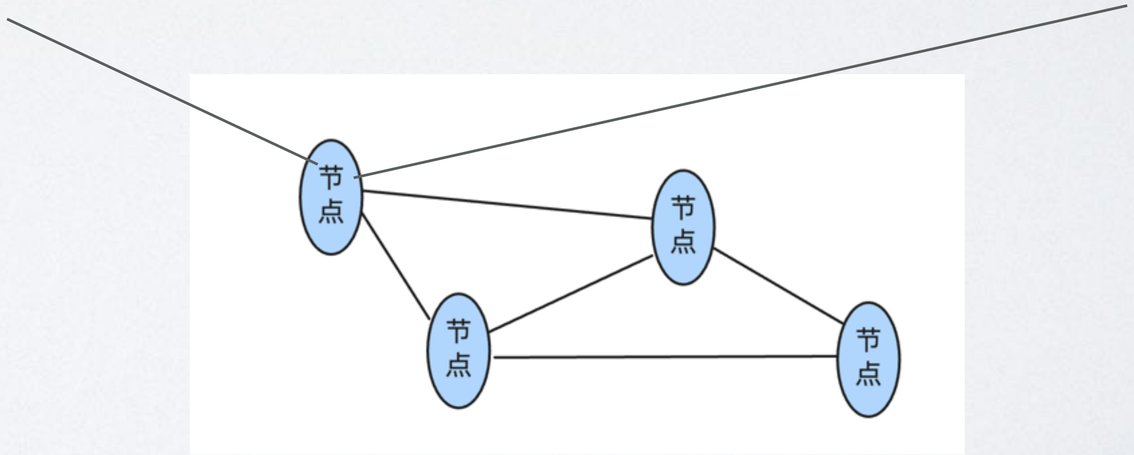
在点对点的网络中，节点如何识别其他节点发过来的数据是正确的?

账本验证

如果有一些人篡改了数据：

一条一条和其他人核对么？
谁的数据作为基准呢？

序号	From	To	Amount
1	王二	张三	12
2	张三	李四	2
3	李四	赵五	3
4	赵五	…	4
5	0..0	张三	3.175



账本验证 - 链式结构

Hash (

序号	From	To	Amount
1	王二	张三	12
2	张三	李四	2
3	李四	赵五	3
4	赵五	…	4

) = 787635A

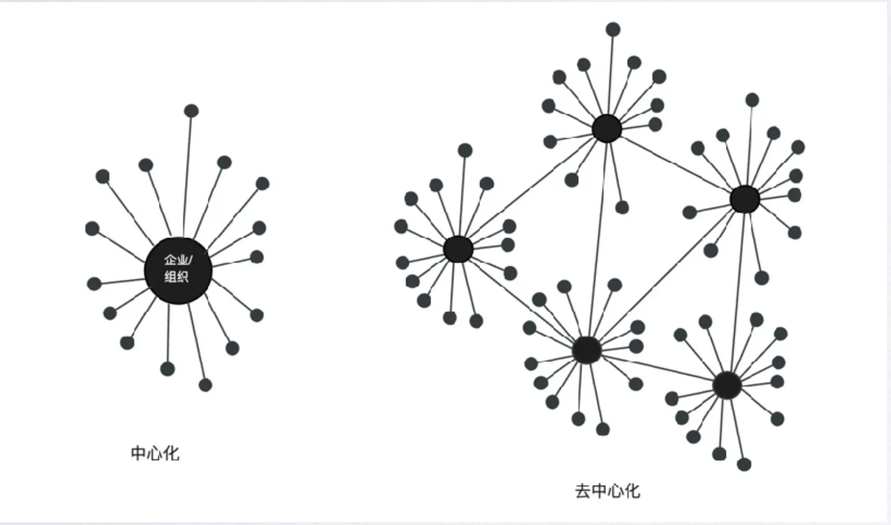
Hash (787635A +

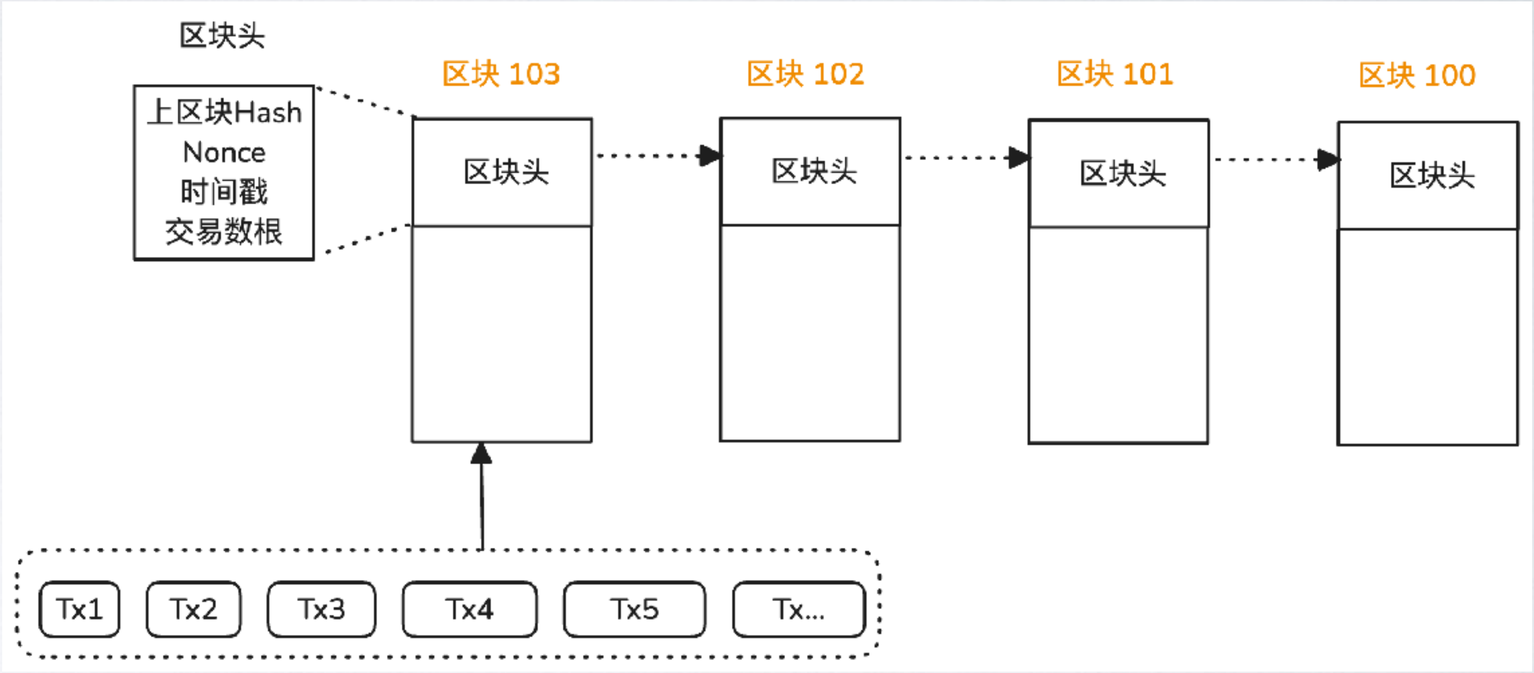
序号	From	To	Amount
1	…	张三	14
2	张三	李四	4
3	李四	赵五	1
4	赵五	…	3

) = 127635B

https://andersbrownworth.com/blockchain/blockchain

账本验证 - 链式结构





只要满足 hash 链式结构都是正确的数据，修改数据将无法满足 hash 链式结构

如果存在多个不同数据链?

- 可能会出现多个数据链?
  - 不同节点可能包含不同的交易集合，应该以谁的数据为基准?

POW - PROOF OF WORK

- 工作量证明 - 增加记账（写数据）的难度
- 最快解出密码学难题获得记账权（大概 10 分钟）
- 所有人只认同最先延长的区块（最长链）

Hash(上一个Hash值，交易记录集) = 456635BCD

16^19 0000000af

Hash(上一个Hash值，交易记录集，随机数) = 0000aFD635BCD

https://blockstream.info/block/00000000000000000000015053d4ef12dce3fac32a6c7e27f87971bf114726bb46

出块激励

- 为何要参与记账?
- 出块者有权给自己添加一笔奖励（也是 BTC 发行过程）


```
Hash(上一个Hash值，交易记录集) = 456635BCD
```

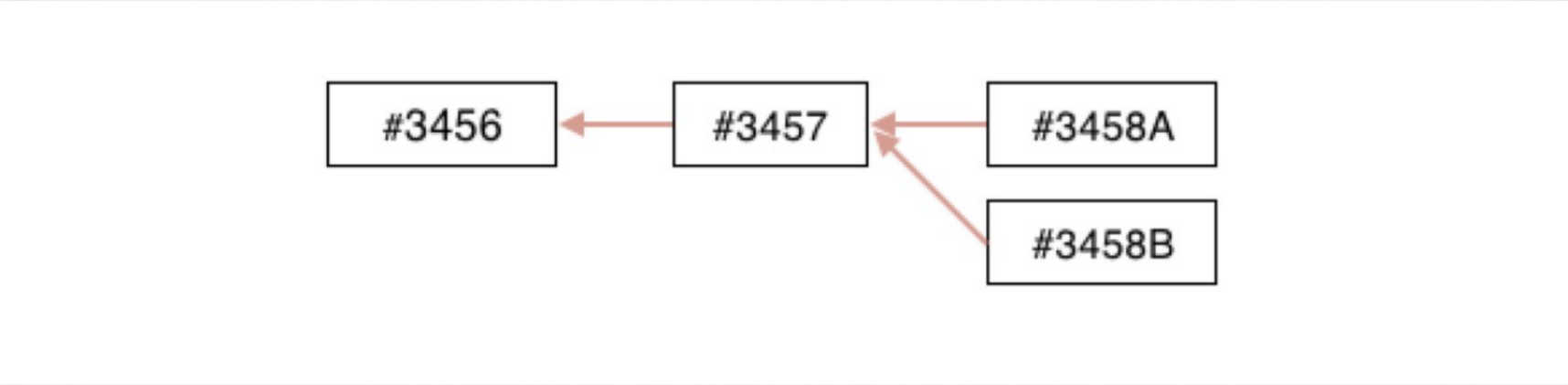
```
Hash(上一个Hash值，交易记录集，随机数) = 0000aFD635BCD
```

POW 如何保护网络安全的?

- 链上唯一的作恶方式是双花（双重花费：在一段时间后，用另一个交易替换原有的交易）
- 要实现双花，需要获得连续 N 个块的出块权。
- POW 与链式结构，让攻击或作恶，几乎没有空间，除非超过 51% 算力

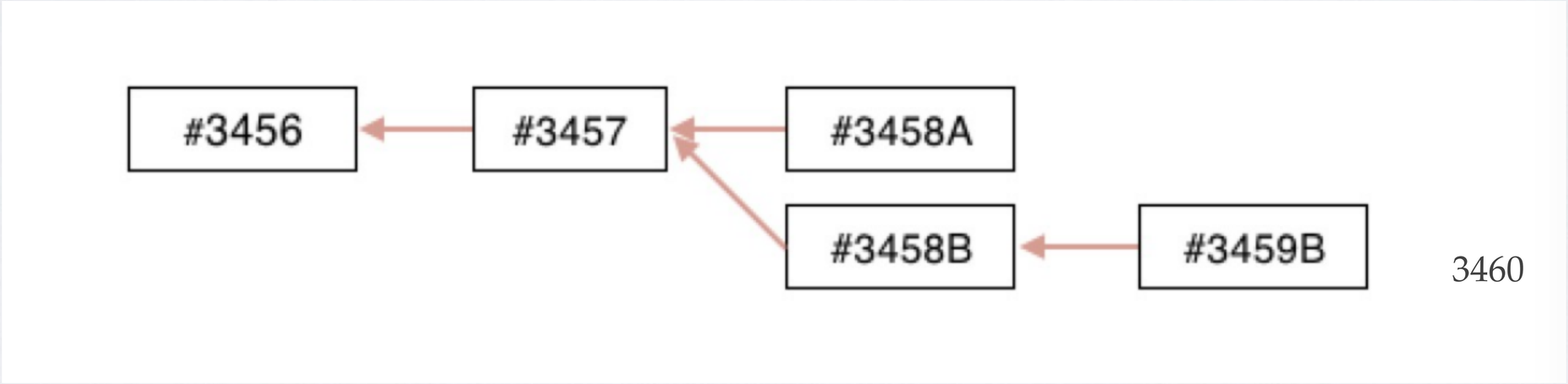
分叉

- 遇到同时解出难题怎么办?



等待

- 等待下一个区块谁先解出



为什么交易所充值需要等待数个区块?
等待确认区块不会被重组（最终确定性）

共识问题 - 共识机制

去中心化网络中的节点协作与激励问题通常称为共识问题
解决共识问题的机制（方法）称为共识机制

比特币共识称为中本聪共识（或笼统称为 POW 共识）

小结

- Web2 的便利也带来了：大厂垄断、挟持用户、隐私问题等
- 区块链通过密码学让数据控制权回归用户、通过去中心化网络来防止组织的作恶。
- 共识机制用来协调去中心化网络中的节点运行。
- BTC 共识：谁先完成 POW 难度计算，谁获奖励，同时使用 Hash区块链式结构让验证简单。

作业

- 实践 POW 用自己的昵称 + nonce， 不断的 sha256 Hash :
  - 直到满足 4 个0开头，打印出花费的时间
  - 直到满足 5 个0开头，打印出花费的时间
- 实践非对称加密 RSA
- 先生成一个公私钥对
- 用私钥对符合POW一个昵称 + nonce 进行私钥签名
- 用公钥验证

https://decert.me/challenge/45779e03-7905-469e-822e-3ec3746d9ece

作业（可选）

- 实践区块链原理（编程语言不限）：
  - 工作量证明出块
  - 交易打包进入区块
  - 节点同步区块（加分）

https://decert.me/quests/ed2d8324-54b0-4b7a-9cee-5e97d3c30030

作业说明

- 代码在自己的 github 提交
- 通过后在 decert.me 领取 NFT 证书

课外阅读

- 加密朋克宣言
- 《读、写、拥有》、京东繁体版
- 比特币白皮书
- 《精通比特币第 2 版》

思考

比特币（区块链技术）有哪些不足？

有不足么?

- 较慢
- 较贵
- 代码安全问题
- 用户体验：助记词/私钥

开放思考题

- 比特币有价值么？　庞氏么？
- 货币的价值来源是什么？
- 解决信任问题会给社会带来什么样的？