区块链价值与原理

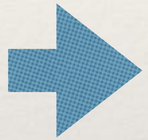
Tiny熊

要点

- 区块链提供了什么价值
- 区块链关键技术

区块链价值

基于人/组织的信任



区块链技术实现：

基于代码的信任

基础：代码开源 + 分布式执行

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
- 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

去中心化的两个问题：

- 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*

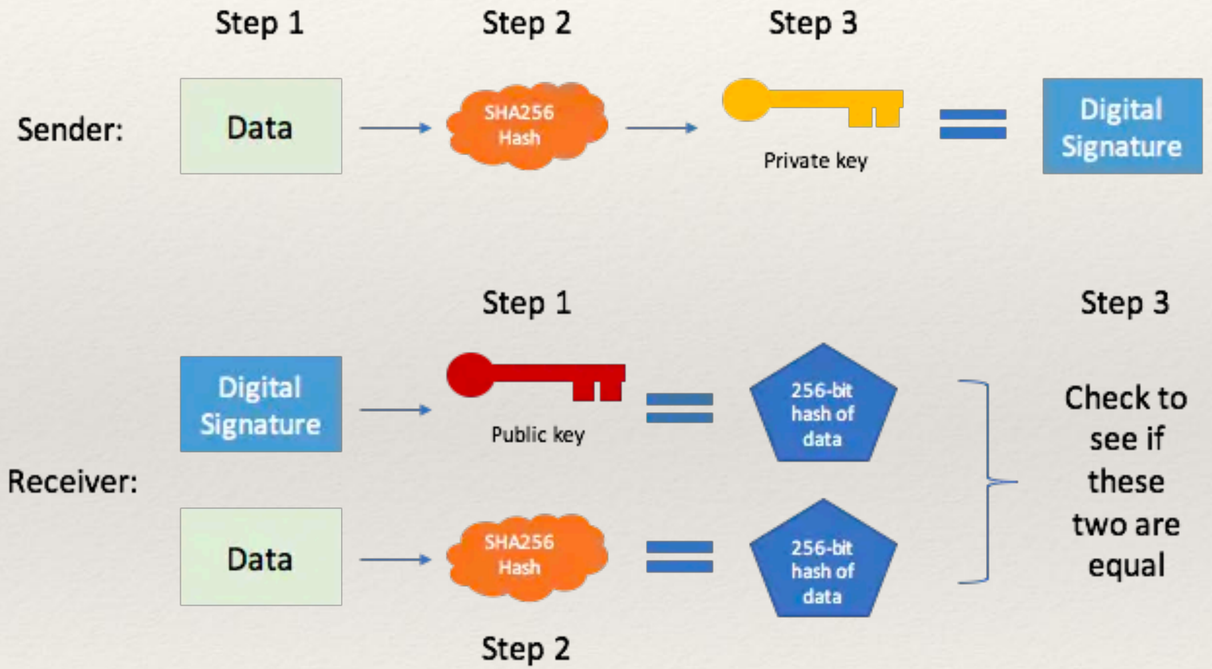
比特币核心

- 个人私钥控制资产（非对称加密）
- 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


Step 1
Step 2
Step 3
Sender:
Data
SHA256 Hash
Private key
Digital Signature
Step 1
Step 3
Digital Signature
Public key
256-bit hash of data
Receiver:
Check to see if these two are equal
Data
SHA256 Hash
256-bit hash of data
Step 2

链式结构 - 账本验证

在点对点的网络中，节点如何知道其他节点发过来的数据是正确的?

链式结构 - 账本验证

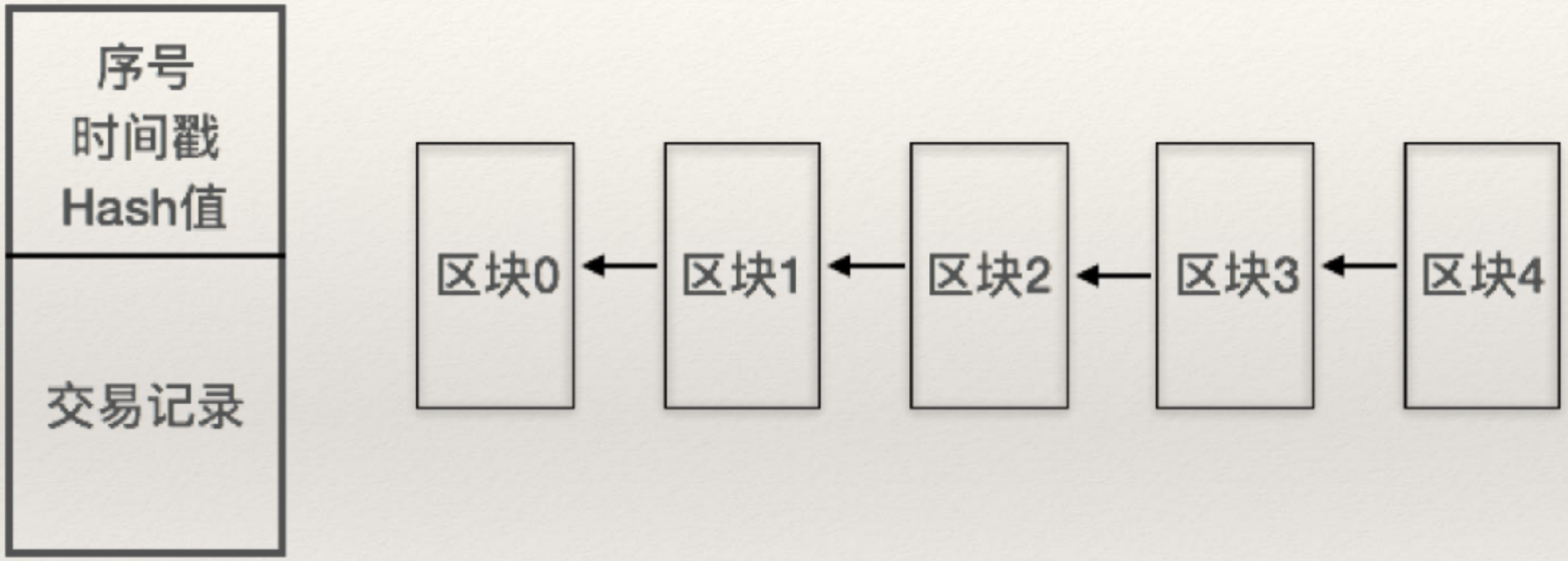
账号	收入	支出	余额
王二	100		190
张三		100	**300**
李四	120	90	170
赵五	300		500

收到了一条假数据怎么办?

链式结构 - 账本验证

https://andersbrownworth.com/blockchain/blockchain

链式结构 - 账本验证



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

共识问题

- 可能会出现多个数据链?
- 可能没有人参与?

共识（机制）

- 共识主要解决谁的记账有效
- 经济激励参与记账的人（出块）

共识（机制）

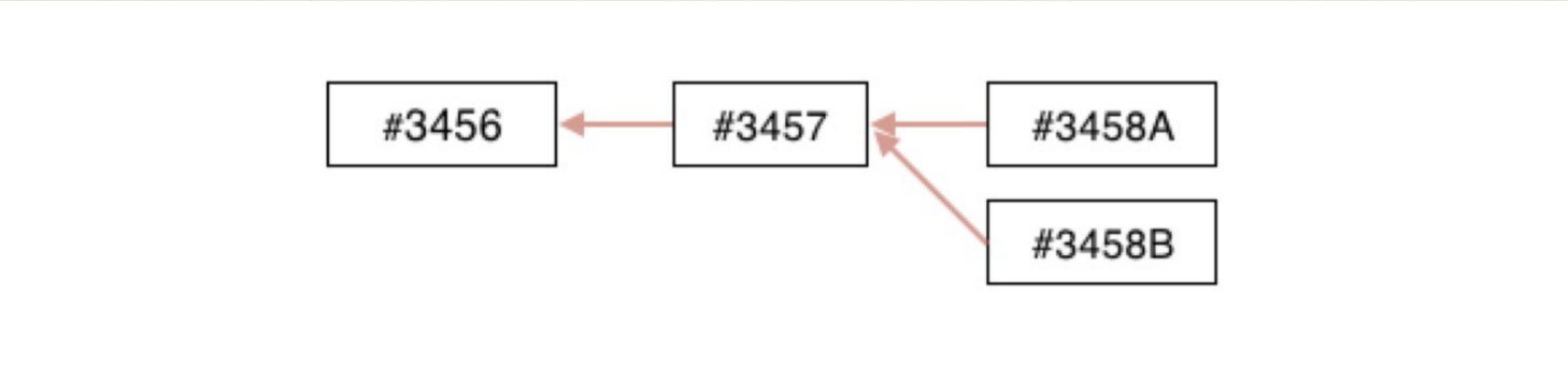
- 用代码确定一套规则（工作量证明）：
  - 最快解出密码学难题获得记账权（有权给自己添加一笔奖励）

```
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
```

共识（机制）

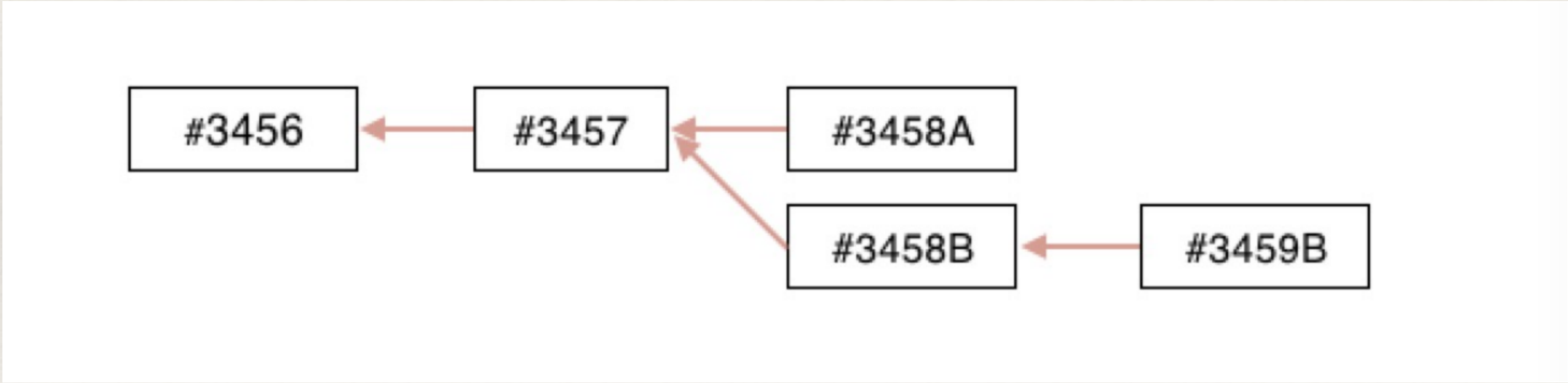
- 遇到同时解出难题怎么办?



称为：分叉

共识（机制）

- 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?

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
- 在 decert.me 领取证书

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？

思考

区块链技术有哪些不足？

有不足么?

- 较慢
- 较贵
- 代码安全问题

谢谢