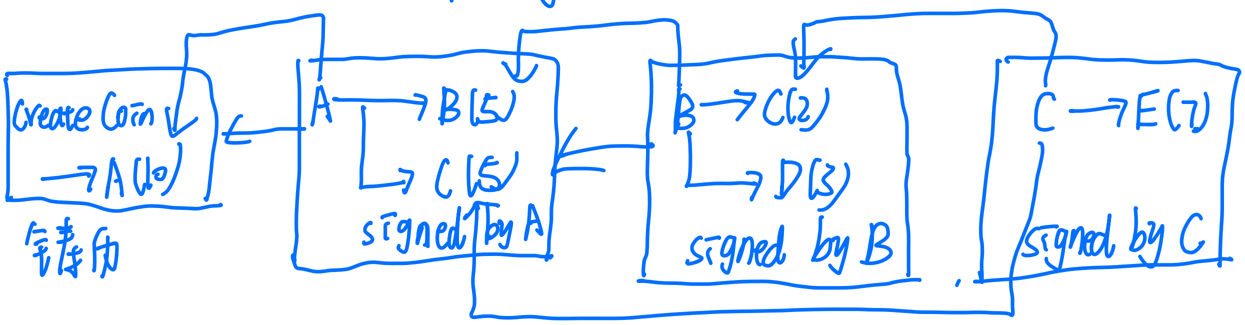
数字货币的风险: double spending attack.

发行货币:挖矿.

how to defend double spending attack.



还有A的公钥 —— 两公钥应该可对比.

比特币交易系统包含{输入: 注明币的来源,还要说明A的公钥!
{输出: 给出收款人的公钥的哈希.

转账: A need B的地址 A need prove coin 的来源

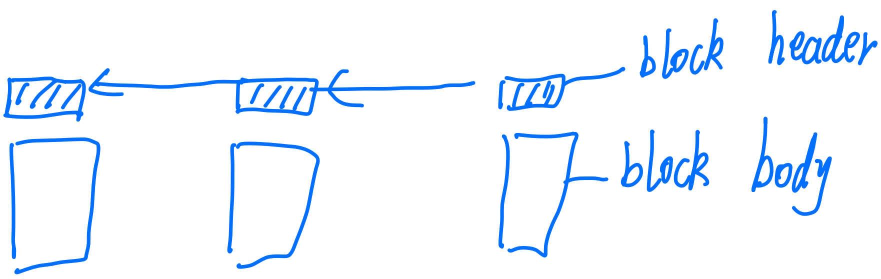
所有节点need A的public key (为了验证 public key)

当前交易的输入Script与币的来源的脚本合在一起,不报错即通过.

每个区块分为:

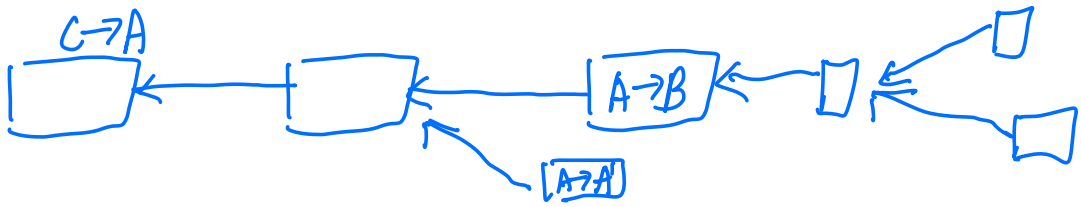
Block header: {version, hash of previous block hearder,
merkle root hash, target, nonce.

Block body: transaction list.



full node: all information. fully validating.
light node:
只长本的内容应取得: distributed consensus (分布式共识)
example: distributed hash table
impossibility result: FLP:
在一个异步的系统里，即使用一个faulty，也无法达成共识。
CAP Theorem: Consistency, Availability, Partition tolerance
任何一个分布式系统只能满足3中之2.

Consensus in BitCoin:
用 compute ability to vote
every node could make block
记录并报: get nonce, 可以发布 next block.



longest valid chain, 只接受 longest valid chain
block reward:
coinbase transaction: 产生新的 bitcoin 唯一方式。
50 BTC → 25 BTC → 12.5 BTC →
hash rate
bitcoin mining digital gold
miner