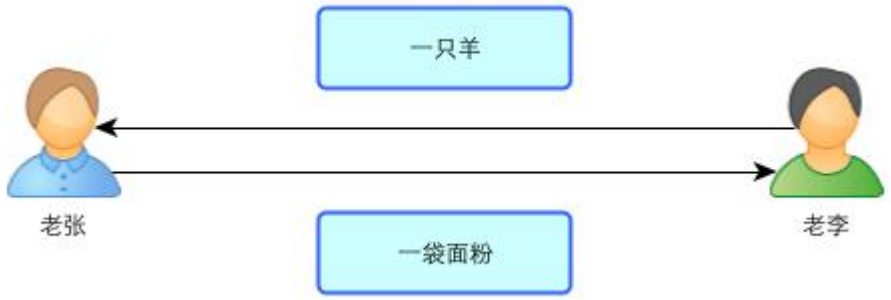
比特币原理

从人类记账故事开始

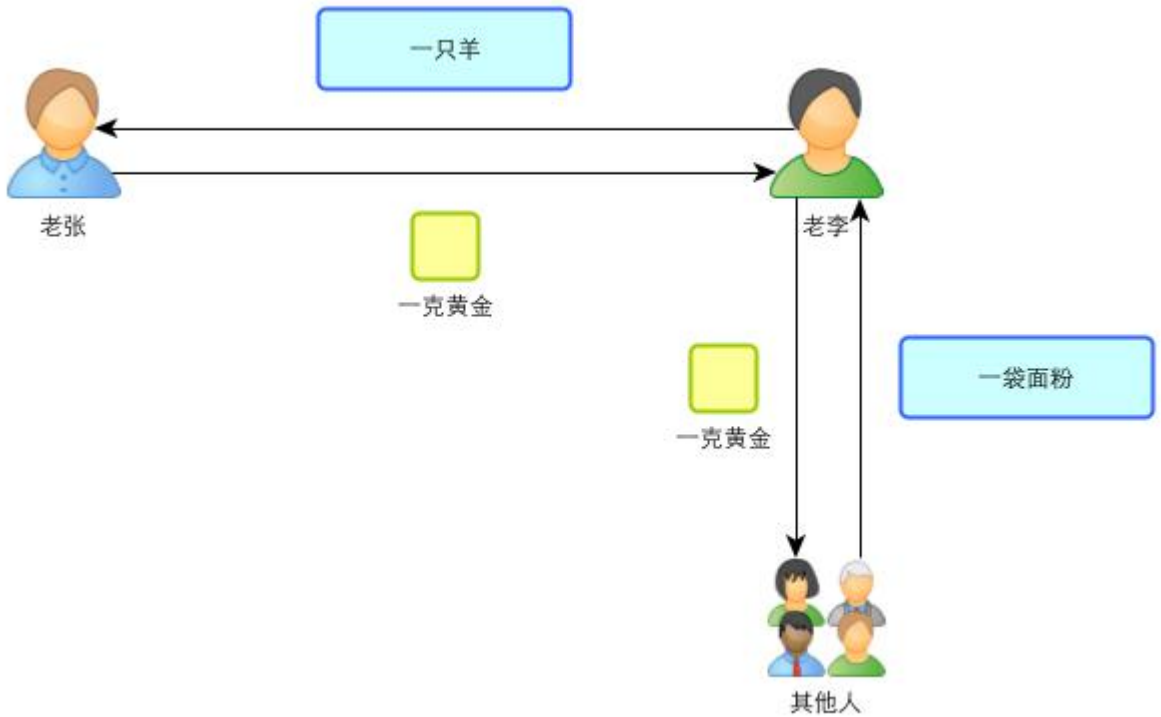
以物易物的比特村

- 话说在这个世界上，有一个叫比特村的小村庄，村庄共有几百户人家。这个村庄几乎与世隔绝，过着自给自足的生活。

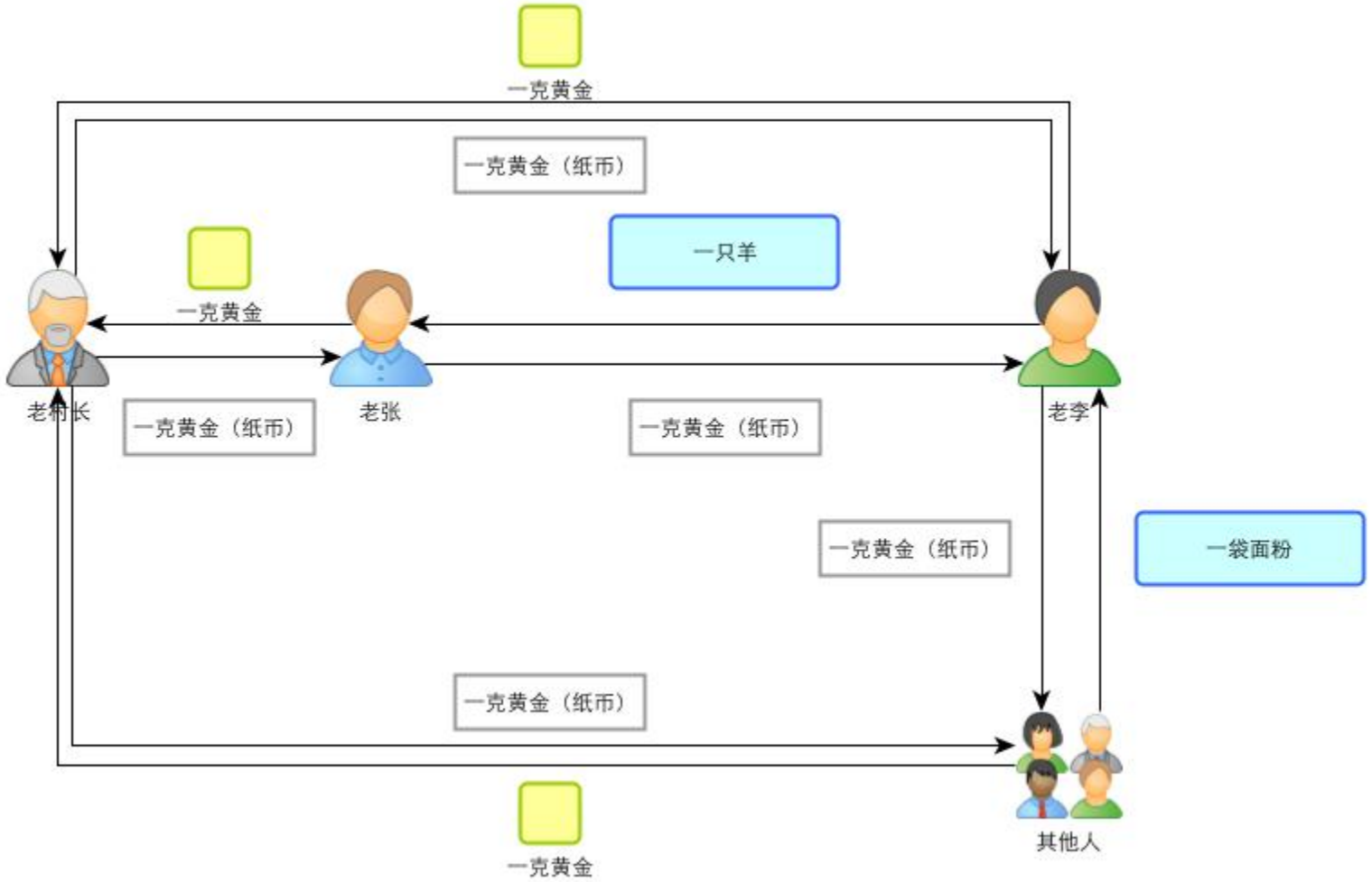
- 由于没有大规模贸易，比特村村民一直过着以物易物的生活

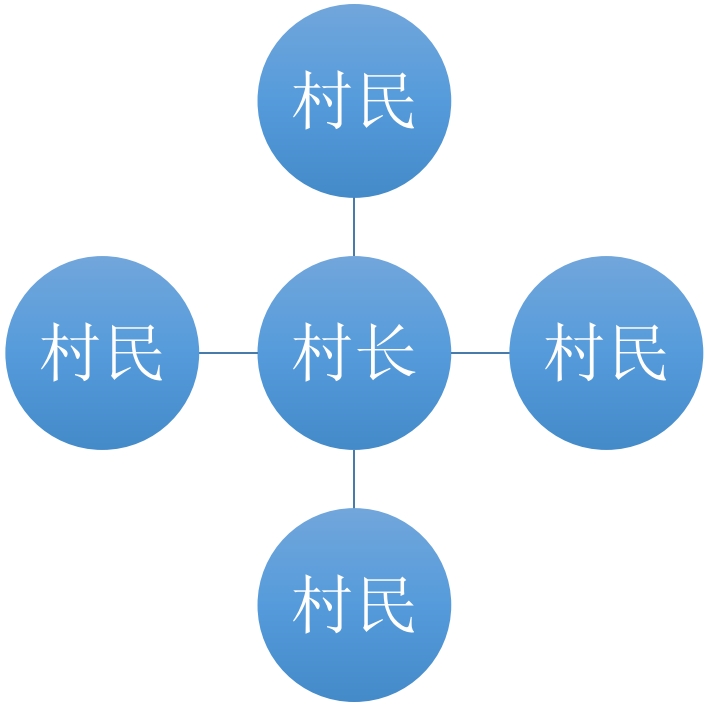


实物货币

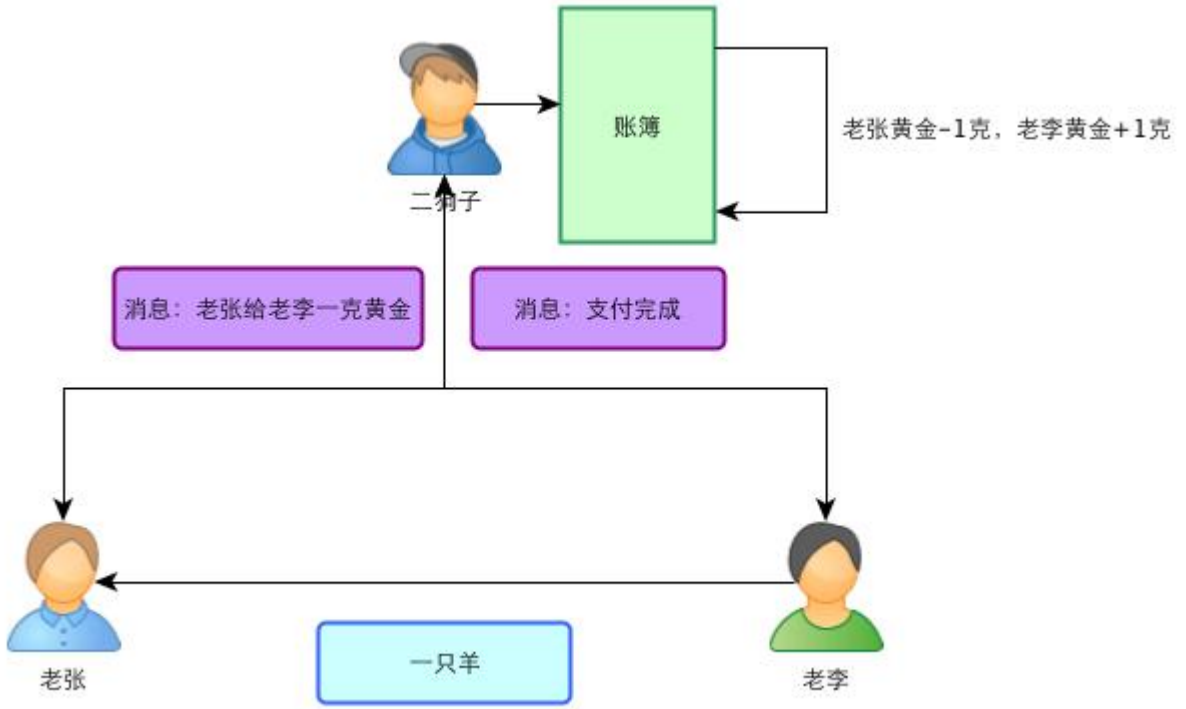


符号货币


一克黄金
一克黄金（纸币）
一只羊
一克黄金
老村长
老张
老李
一克黄金（纸币）
一克黄金（纸币）
一克黄金（纸币）
一袋面粉
一克黄金（纸币）
其他人
一克黄金


村民
村民
村长
村民
村民

中央系统虚拟货币



- 比特村进入了中央系统虚拟货币时代。每个村民都不需要用实物支付，支付过程变成了二狗子那边维护的账本上数字的变更。

分布式虚拟货币

- 这新上任的二狗子是聪明，不过这人有时候是聪明反被聪明误。有一天二狗子盯着这账本，心想这全村各户谁有多少钱就是我说的算，那我岂不是……
- 于是他头脑一热，私自从老张帐下划了十克金子到自己名下。

分布式账本

- 正当人们不知所措时，村里一个叫中本聪的宅男科学家走上了台，告诉大家他已经设计了一套不依赖任何中央处理人的叫比特币的虚拟货币系统，可以解决上述问题。

基础设施搭建

- 账簿公开和分布式存储机制
- 身份校验和签名机制（RSA加密系统）
- 成立虚拟矿工组织（挖矿群体）负责挖矿
- 建立初始账簿（创世块）

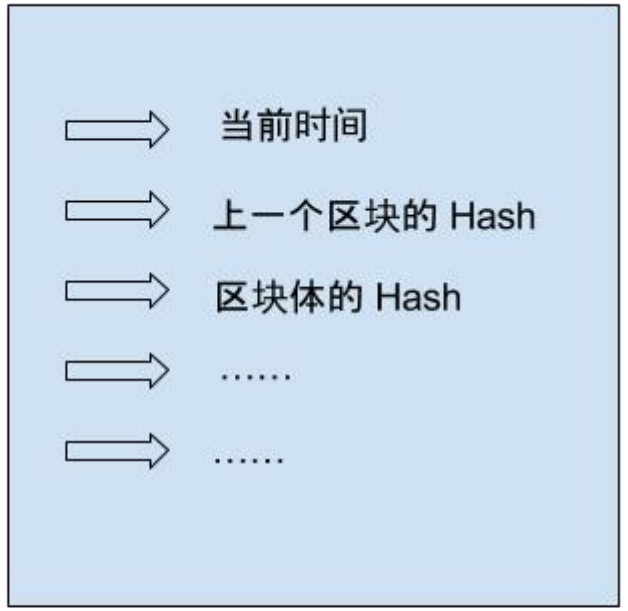
支付与交易

- 付款人签署交易单
- 收款人确认单据签署人
- 收款人确认付款人余额

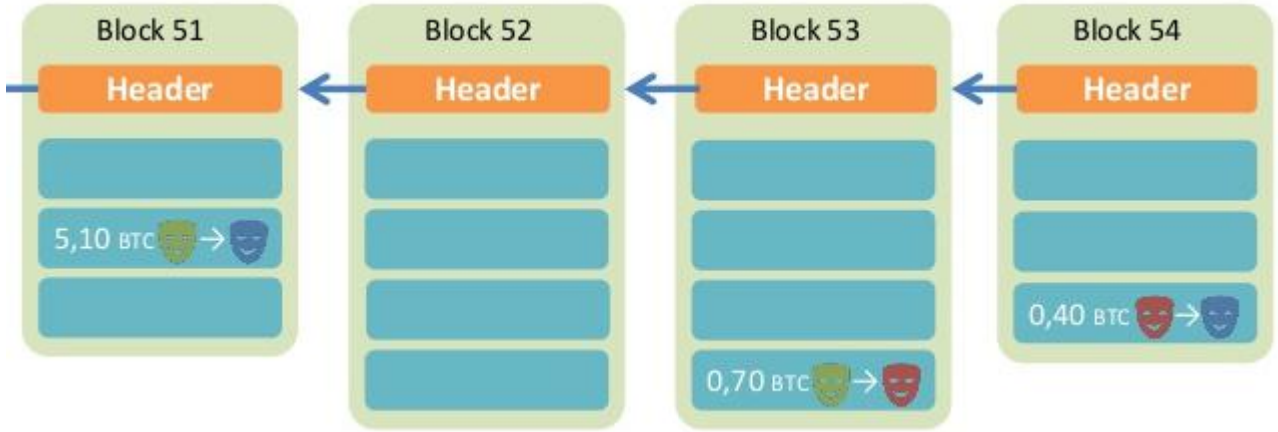
矿工的工作

- 收集交易单
- 填写账簿
- 确认账簿
- 账簿确认反馈

区块头

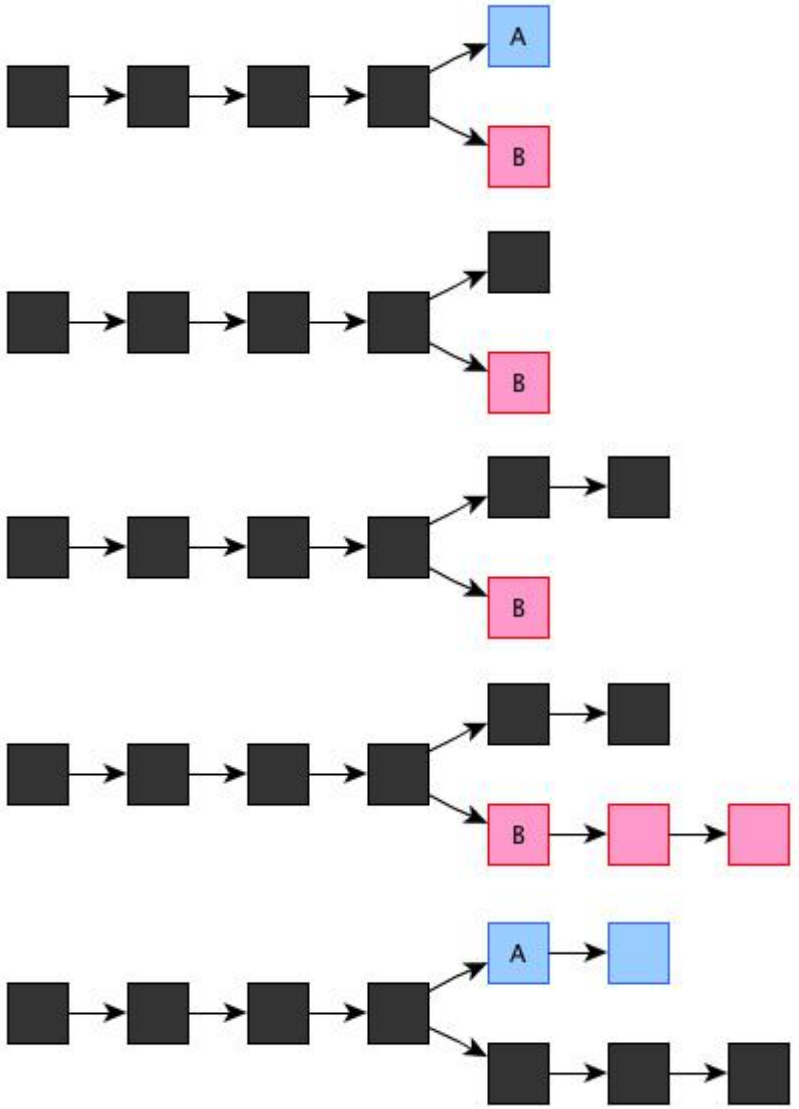


区块体



如果同时收到2份合法的账簿页怎么办？

- 同时收到2份不一样的账簿页，它们都基于当前这个小组的主账簿的最后一页，并且内容也都完全合法，怎么办？



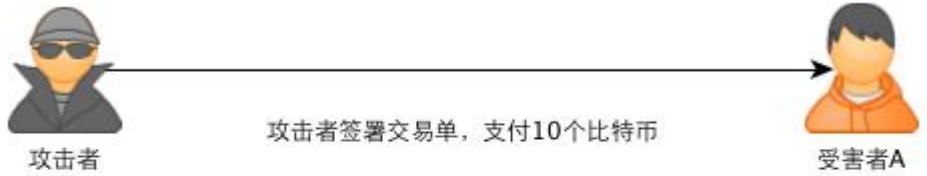
黑色表示当前账簿主干。此时，可以随便选择一个页作为当前主分支

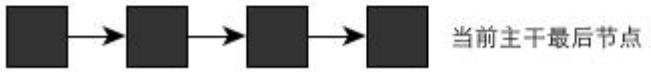
如果挖矿小组有人伪造账簿怎么办?

- 有一种可能的攻击行为，即在收款人确认收款后，从另一条分支上建立另外的交易单，取消之前的付款，而将同一笔钱再次付款给另一个人（即所谓的*double-spending*问题）。

double-spending 双花交易攻击

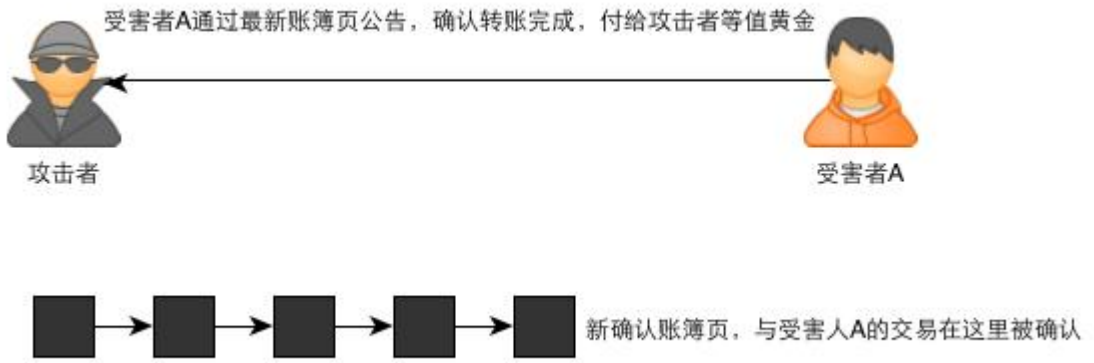
先假设有一个攻击者拥有10个比特币，他准备将这笔钱同时支付给A和B，并都得到承认：





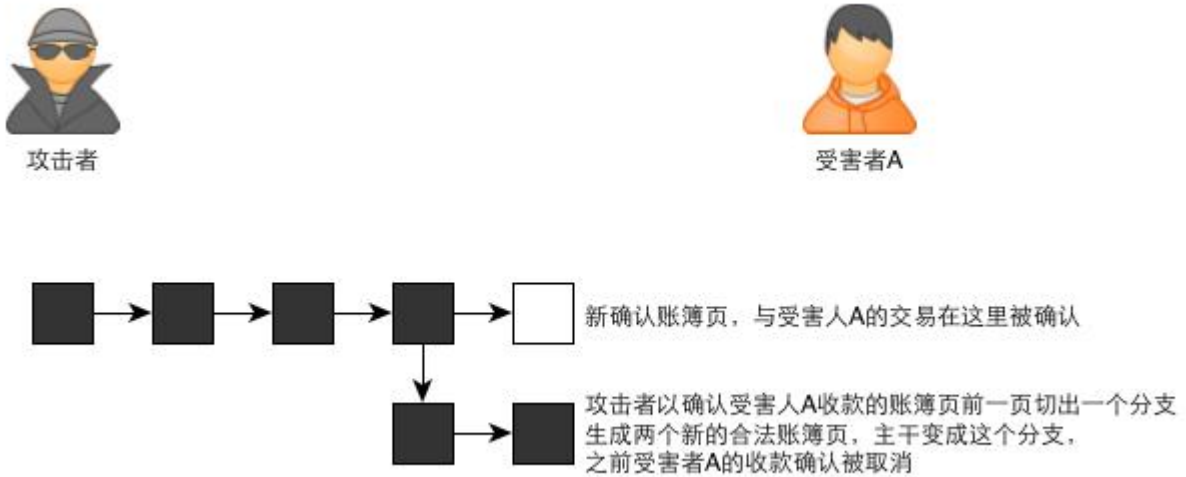
- 第一步：攻击者准备从受害者A手里买10比特币的黄金，他签署交易单给受害者A，转10个比特币给受害者A

double-spending 双花交易攻击



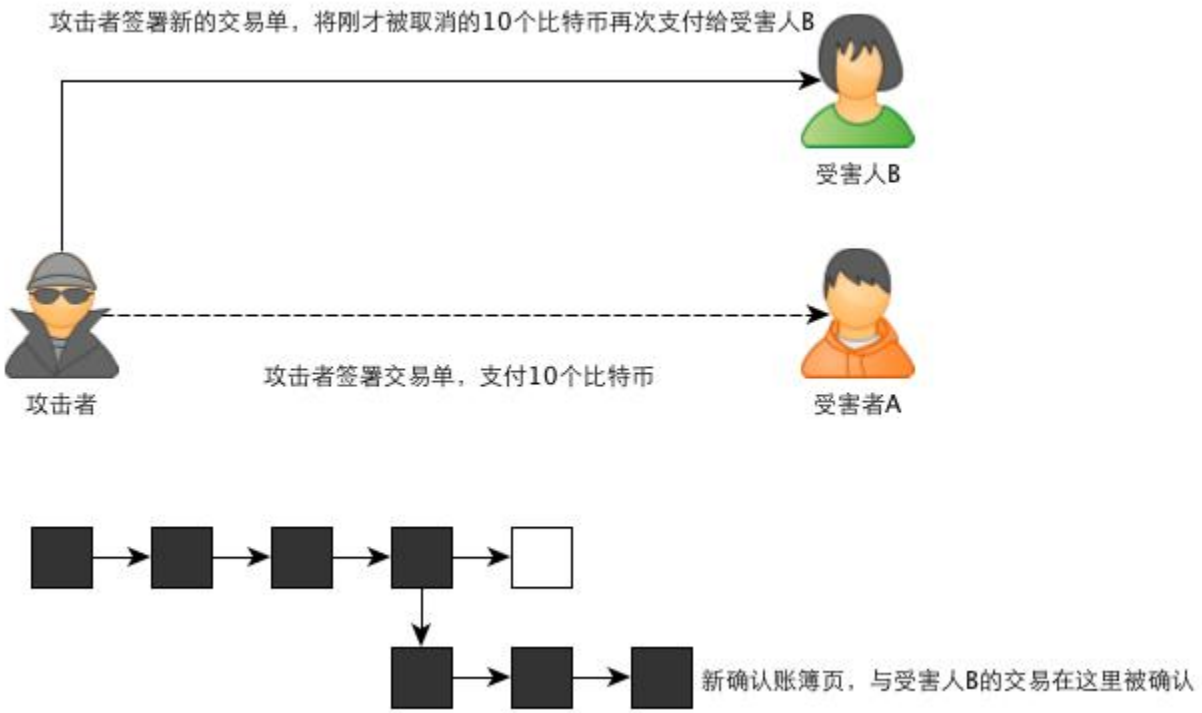
- 第二步：这笔交易在最新的账簿页中被确认，并被各个挖矿小组公告出来。受害人A看到公告，确认比特币到账，给了攻击者10个比特币等值的黄金。

double-spending 双花交易攻击



- 第三步：攻击者找到账簿，从包含刚才交易的账簿页的前一页做出一个分支，生成更多的账单页，超过刚才的分支。由于此时刚才攻击者制造的分支变成了主干分支，而包含受害者A得到钱的分支变成了旁支，因此挖矿组织不再承认刚才的转账，受害者A得到的10比特币被取消了。

double-spending 双花交易攻击



- 第四步：攻击者可以再次签署交易单，将同一笔钱支付给受害者B。受害者B确认钱到账后，支付给攻击者等值黄金

double-spending 双花交易攻击

- 解决方案：建议收款人不要在公告挂出时立即确认交易完成，而是应该再看一段时间，等待挂出6张确认账簿，并且之前的账簿没有被取消，才确认钱已到账。

比特币会一直增加下去，岂不是会严重通货膨胀？

中本聪说，这一点我也想到了。前面忘了说了，我给矿工组织的操作细则手册会说明，刚开始我们协议每生成一页账簿，奖励小组50个比特币，后面，每当账簿增加21,000页，奖励就减半，例如当达到210,000页后，每生成一页账簿奖励25个比特币，420,000页后，每生成一页奖励12.5个，依次类推，等账簿达到6,930,000页后，新生成账簿页就没有奖励了。此时比特币全量约为21,000,000个，这就是比特币的总量，所以不会无限增加下去。

没有奖励后，就没人做矿工了，岂不是没人帮忙确认交易了？

- 到时，矿工的收益会由挖矿所得变为收取手续费。例如，你在转账时可以指定其中1%作为手续费支付给生成账簿页的小组，各个小组会挑选手续费高的交易单优先确认。

结束

- 谢谢