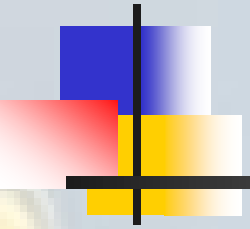
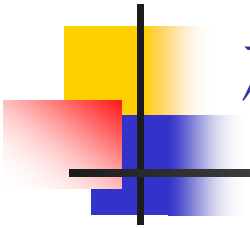
区块链技术与应用



Chapter 2 比特币如何做到去中心化

苏 明



概览

- 2.1 中心化与去中心化
- 2.2 分布式共识
- 2.3 使用区块链达成没有身份的共识
- 2.4 奖励机制与工作量证明
- 2.5 总结

去中心化

- Scoogecoin 财奴币

  中心化带来的问题

- 区块链：**技术手段**+激励机制

中心化与去中心化

- 不同的流派

  电子邮件--去中心化

  Facebook, Linkedin---中心化

- 没有一个系统是完全中心化的，或者是完全去中心化

混合模式

去中心化解决的问题

1. 谁在维护交易账本？
2. 谁有权批准哪个交易是正当有效的？
3. 谁在制造新的比特币？

4. 谁在制定系统变化规则？
5. 比特币如何取得交易价值？

去中心化解决的问题

1. **谁在维护交易账本？**
2. **谁有权批准哪个交易是正当有效的？**
3. **谁在制造新的比特币？**

4. 谁在制定系统变化规则？
5. 比特币如何取得交易价值？

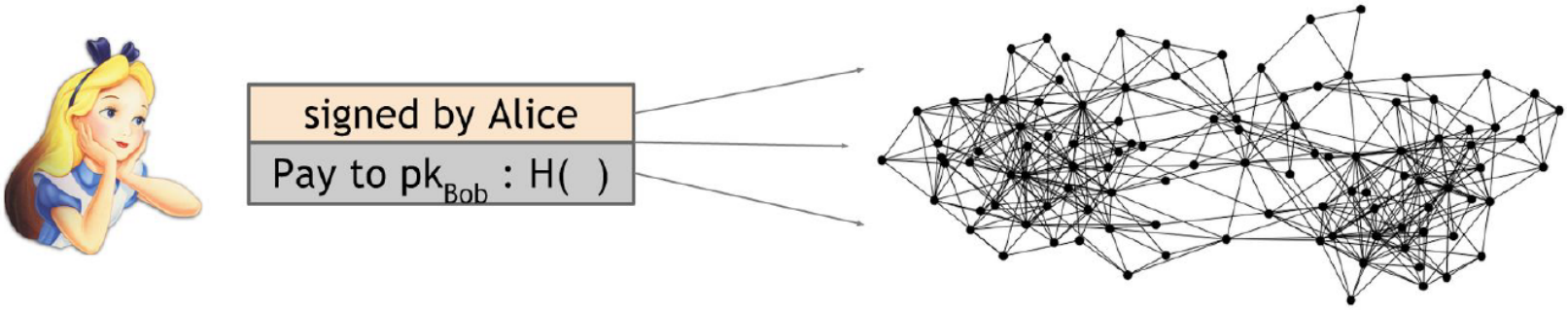
分布式共识

建立分布式电子现金系统的关键技术问题

Distributed consensus protocol. There are *n* nodes that each have an input value. Some of these nodes are faulty or malicious. A distributed consensus protocol has the following two properties:

- It must terminate with all honest nodes in agreement on the value
- The value must have been generated by an honest node

分布式共识

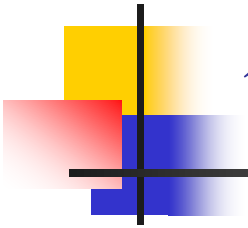


Broadcasting a transaction In order to pay Bob, Alice broadcasts the transaction to the entire Bitcoin peer-to-peer network

分布式共识

达成共识

- Propose→Consensus
- 正当的交易可以等待下一次被打进区块的机会



分布式共识

技术上面临的挑战

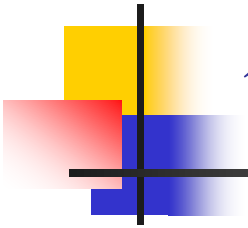
1. 达成共识是一个难题：节点会宕机或者存恶意节点
2. 点对点网络通信不完美
3. 信息传递的延迟

分布式共识

不可能性结论：Byzantine Generals Problem

- 一组拜占庭将军分别各率领一支军队共同围困一座城市。为了简化问题，将各支军队的行动策略限定为进攻或撤离两种。因为部分军队进攻部分军队撤离可能会造成灾难性后果，因此各位将军必须通过投票来达成一致策略，即所有军队一起进攻或所有军队一起撤离。因为各位将军分处城市不同方向，他们只能通过信使互相联系。在投票过程中每位将军都将自己投票给进攻还是撤退的信息，通过信使分别通知其他所有将军，这样一来每位将军根据自己的投票和其他所有将军送来的信息就可以知道共同的**投票结果而决定行动策略**。

https://zh.wikipedia.org/wiki/...



分布式共识

将军的总数为n，n里面背叛者的数量为t，则只要$n > 3t$就可以容错。

分布式共识

Byzantine Generals Problem. A commanding general must send an order to his $n - 1$ lieutenant generals such that

IC1. All loyal lieutenants obey the same order.
IC2. If the commanding general is loyal, then every loyal lieutenant obeys the order he sends.

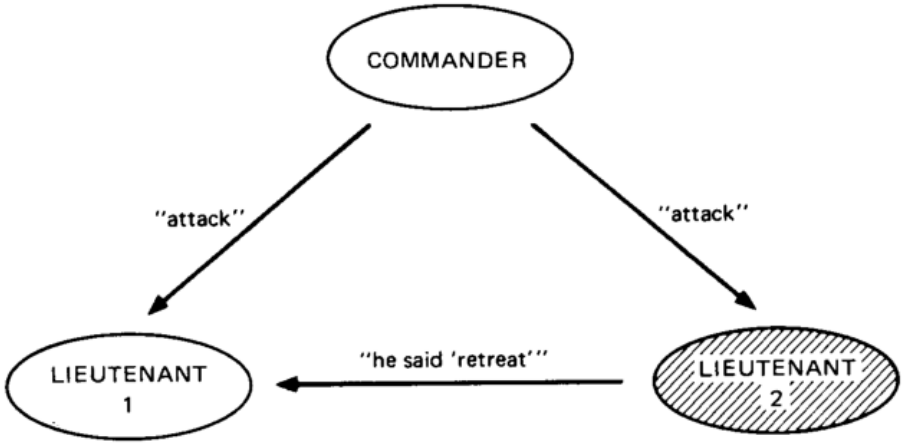


Fig. 1. Lieutenant 2 a traitor.

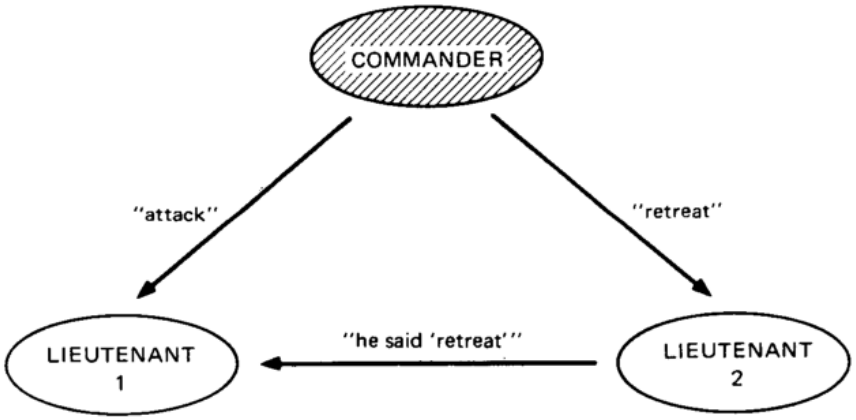


Fig. 2. The commander a traitor.

Lamport, L.; Shostak, R.; Pease, M. The Byzantine Generals Problem. ACM Transactions on Programming Languages and Systems. 1982

分布式共识

打破传统意义下的假设

- 比特币实际运行情况远比理论的研究结果好的多

？？？

1. 引入了奖励
2. 包含随机性；经过一段时间观点出现分歧的概率按指数下降

Blockchain->达成没有身份的共识

隐性共识

- 每一个回合：一个随机节点被选中，然后这个节点可以提议这个链的下一个区块
- 其他节点可以通过接龙的方式，隐性的接受或者拒绝

Blockchain->达成没有身份的共识

比特币共识算法

Bitcoin consensus algorithm (simplified)

This algorithm is simplified in that it assumes the ability to select a random node in a manner that is not vulnerable to Sybil attacks.

1. New transactions are broadcast to all nodes
2. Each node collects new transactions into a block
3. In each round a random node gets to broadcast its block
4. Other nodes accept the block only if all transactions in it are valid (unspent, valid signatures)
5. Nodes express their acceptance of the block by including its hash in the next block they create

Blockchain->达成没有身份的共识

比特币的攻击

1. **窃取比特币--->**伪造数字签名

2. **拒绝服务攻击→**如果Alice拒绝提供服务给Bob； Bob等到下一个诚实节点发起区块的时候，交易记录会被放进这个区块里。

Blockchain->达成没有身份的共识

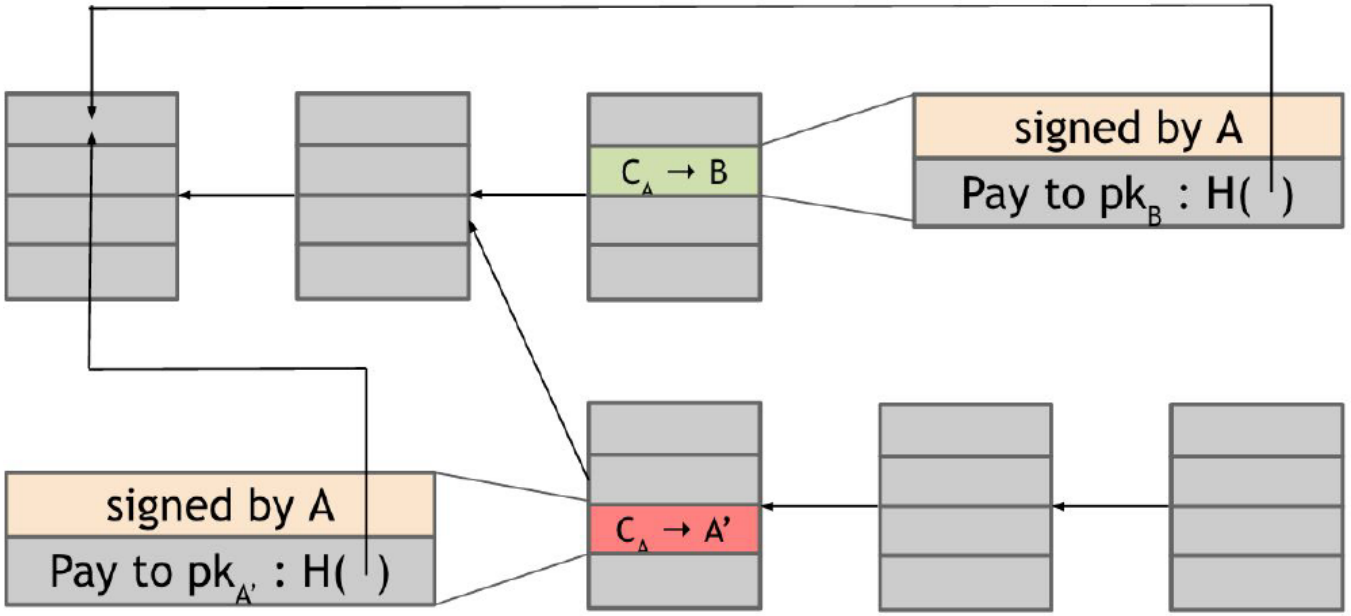
3. 双重支付攻击

Alice→Bob

Alice→转到另外一个地址

一个交易就是一个数据结构：里面有Alice的数字签名，一个付给Bob的公钥（地址），一个哈希值（指向先前的一笔交易的输出）

Blockchain->达成没有身份的共识



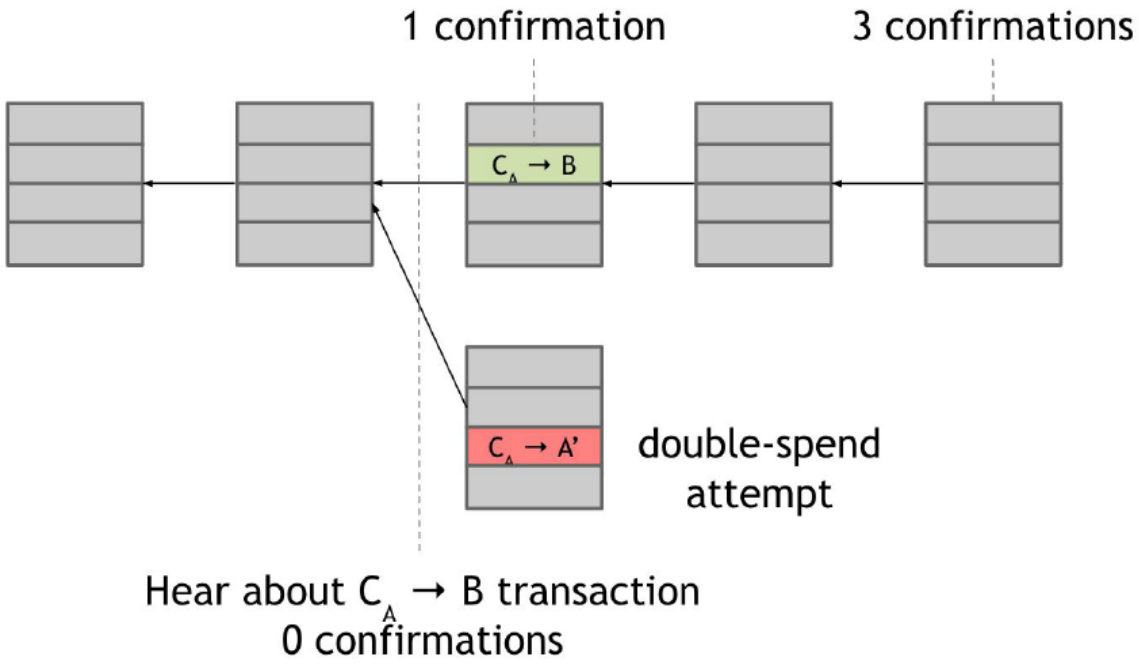
A double spend attempt

Blockchain->达成没有身份的共识

- **取决于最后哪一个区块被纳入长期的共识链**

- 从道德角度看，分支截然不同；
  但从技术角度看，两笔交易都符合规范，形式上有效

Blockchain->达成没有身份的共识



In order to protect himself from this attack, Bob should wait until the transaction with which Alice pays him is included in the block chain and has several confirmations.

诚实大多数原理

- 算力主要消耗在挖矿、区块链的生成、交易确认中
- 系统稳定性的缺省信任基础：算力掌握在大多数诚实的用户手中，出于自身利益的考虑，这些用户也愿意维护区块链系统
- 比特币51%攻击理论：**攻击者要创造一条新链条，然后长度超越旧链条，覆盖旧链条**。如果现在只有1次确认，被覆盖的概率稍高，而到了6次确认，被覆盖的概率下降为接近"0"。

诚实大多数原理

- Consider the scenario of an attacker trying to generate an alternate chain faster than the honest chain.
- 诚实链和攻击链的之间比赛的特征是一个二项分布的随机漫步。成功的事件是诚实的节点被一个数据块扩展，它的领先增加一个点，失败的事件是攻击者的链扩展一个数据块，差距减少一个点。

诚实大多数原理

- 攻击者从一个给定的赤字追上成功的可能性和赌徒破产问题相似。假设一个赌徒从一个赤字开始拥有无限的信用，同时无限尝试的次数去赌以达到盈亏平衡。我们可以计算他达到盈亏平衡的可能性，那也就是一个攻击者追上诚实的链：

- p = 诚实节点发现下一个数据块的可能性
- q = 攻击者发现下一个数据块的可能性
- q_z = 攻击者尝试从z数据块以后追上的可能性

$$q_z = \begin{cases} 1 & if\ p \le q \\ (q/p)^z & if\ p > q \end{cases}$$

诚实大多数原理

- 假设诚实的数据块按每个数据块的期望的平均值生成，攻击者可能的进展的期望值将呈柏松分布。 $\lambda = z\frac{q}{p}$
- 为了得到攻击者在这时追上的概率，我们用柏松分布密度，乘以他在这个点上追上的可能概率：

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & if\ k \le z \\ 1 & if\ k > z \end{cases} = 1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right)$$

诚实大多数原理

模拟概率结果

q=0.1

z=0 P=1.0000000

z=1 P=0.2045873

z=2 P=0.0509779

z=3 P=0.0131722

z=4 P=0.0034552

z=5 P=0.0009137

z=6 P=0.0002428

z=7 P=0.0000647

z=8 P=0.0000173

z=9 P=0.0000046

z=10 P=0.0000012

奖励机制与工作量证明

- 高明的激励设计

无法判断那笔交易是道义上合法；
很难惩罚，因为节点没有身份

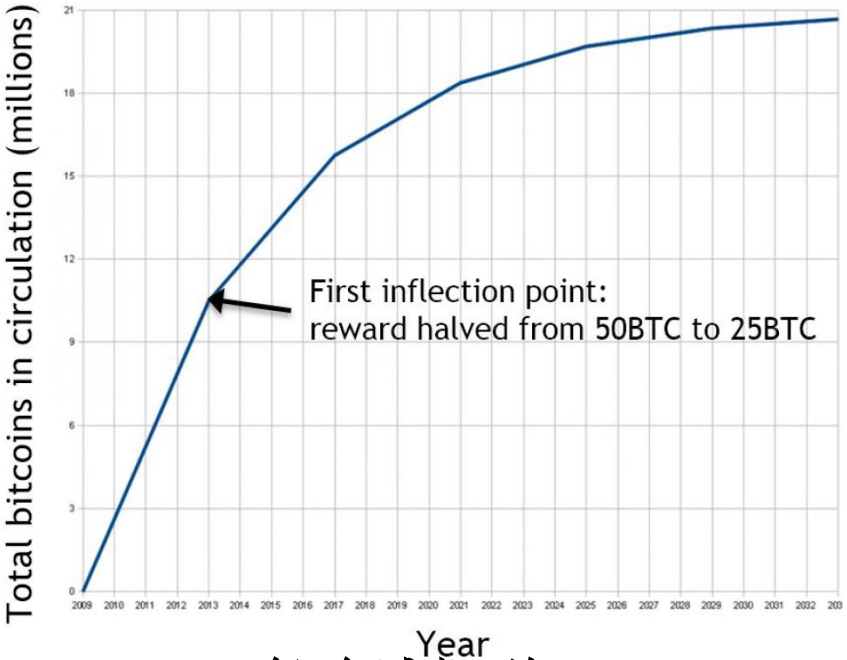
- **给予表现诚实的节点奖励：**
  用比特币来奖励创造区块的节点

激励机制

- 区块奖励
- 交易费奖励

区块奖励

- 比特币规则：创建区块的节点可以在区块中一笔特别的交易：**造币交易**，**指定这笔交易的接收地址**

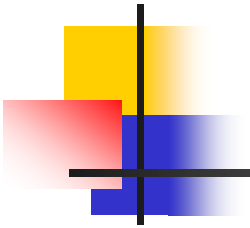


每**4**年减半一次

区块奖励

微妙和强大的设计 (Subtle but powerful trick)

- 奖励只有当区块最终被纳入长期共识链才会**兑现**
- 造币交易和其他每一笔交易一样，只有最终被纳入共识链，才会被其他节点**接受**



区块奖励

- 总的区块奖励是多少？

- 约2100万Bitcoins

交易费奖励

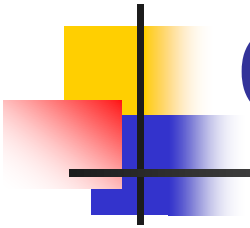
- 比特币区块奖励迟早会发完（比如2140年）
- 系统还能继续运行下去吗？
- 交易费奖励

交易费奖励

- 随着区块奖励逐渐发完，交易费会变得日益重要：需要通过交易费(**小费**)来保障合理的服务质量

201 Created

```
{
 "tx": {
  "block_height": -1,
  "block_index": -1,
  "hash": "b200bb0f872a56350a62f6e2231f153d8da5d0b507395c685cf9679c49313d14",
  "addresses": [
   "n4LNixE753aRKJsBFTERfhFCpHfUjA5fsW",
   "mv4rnyY3Su5gjcDNzbMLKBQkBicCtHUtFB"
  ],
  "total": 370000,
  "fees": 24457,
  "size": 192,
  "preference": "high",
   ……
```



Challenges

1. 如何**随机**选取一个节点？
2. 都来争抢奖励，系统是否会变得不**稳定**？
3. 攻击(Sybil Attack)： 创建大量的女巫节点来尝试颠覆整个共识过程

挖矿与工作量证明

- 工作量证明 (Proof of Work)
- 把随机选取节点改为根据节点占有某种资源的比例来选取节点

比如：计算能力—工作量证明系统(PoW)

某种币的拥有量—权益证明(PoS, Proof of Stake)

挖矿与工作量证明

工作量证明: **算力的竞争**

- 比特币：哈希函数谜题：求解nonce

$$H(nonce \,||\, prev\_hash \,||\, tx \,||\, tx \,||\, \ldots \,||\, tx) < target$$

如果一个节点发现一个**nonce,** 就可以提议创建下一个区块

完全去中心化的方式：*没有任何人决定谁可以提交下一区块*

难于计算

- 要有一定难度

- 2014年底： 产生一个区块：平均要做 10^{20} 运算

挖矿系统需要消耗大量能源

可参数化成本

- 成本是通过参数来进行调整的
- 大约每两个星期（24*6*14=2016个区块），目标区域的难度会调整一次
- **期望10分钟出一个区块**

可参数化成本

大约每两个星期(2016个区块)，区块难度重新调整一次

$$mean\ time\ to\ next\ block = \frac{10\ minutes}{fraction\ of\ hash\ power}$$

易于证实

基于哈希函数的单向性：挖矿很难，但容易验证

总结

挖矿成本

If

mining reward > mining cost

then miner profits

where

mining reward = block reward + tx fees

mining cost = hardware cost + operating costs (electricity, cooling, etc.)

总结

- 系统的安全性不是来自于P2P网络的完美，而是来自于区块链和共识协议。

- 比特币系统深度使用了分布式共识：
  拥有比特币就是其他节点对给定的一方拥有这些比特币的***共识***

启动加密货币

- 区块链的安全性、挖矿生态系统的健康程度，货币的价值 之间紧密相连

- 虚拟货币想要成功：**初始化的自举**(bootstrapping)过程很关键

51%攻击

- 51%攻击主要会摧毁大家对数字货币（比特币）的信心

- 深度影响的是共识：

不能改变数字签名的确认，交易信息的广播；仅可以局部‘指鹿为马’