数字货币和区块链

- 共识与区块链

山东大学网络空间安全学院

钱宸 2023年11月29日

区块链与共识协议

- 简介与历史
- 拜占庭广播与Dolev-Strong协议
- 拜占庭广播（无签名）
- 区块链
- 区块链协议

拜占庭广播（无签名）

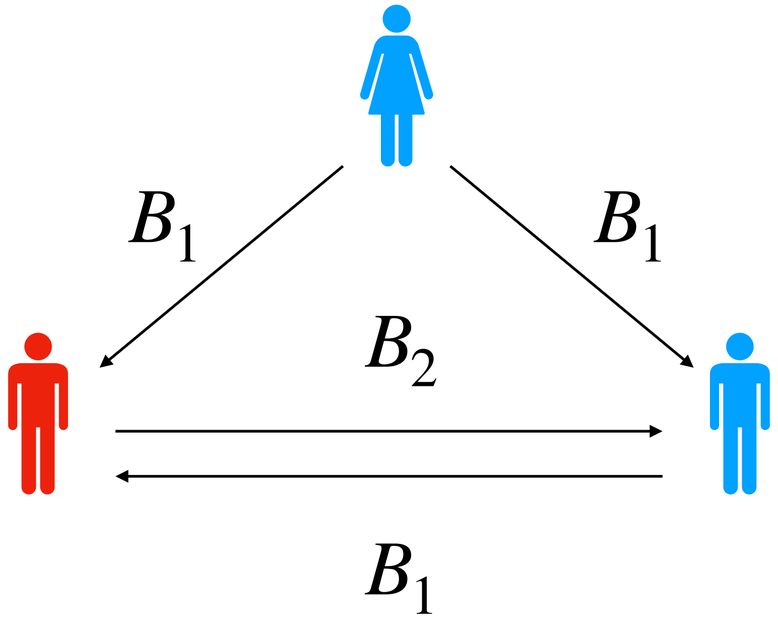
- Dolev-Strong 拜占庭协议
- 缺点：
  - 密码学假设（单向函数存在）
  - 分布式系统中密钥分发难
  - PKI设置复杂，易攻击
  - 签名算法、密码学假设效率相对较低

拜占庭广播（无签名）

- 问题：
  - 如果不基于签名算法和公钥加密系统，能否构造拜占庭协议?
- 思路：
  - Dolev-Strong协议中签名算法保证了，中间用户不能篡改信息
  - 假如Bob给出一个文件m带有Alice的签名，第三方可以确保Alice曾经发出过m

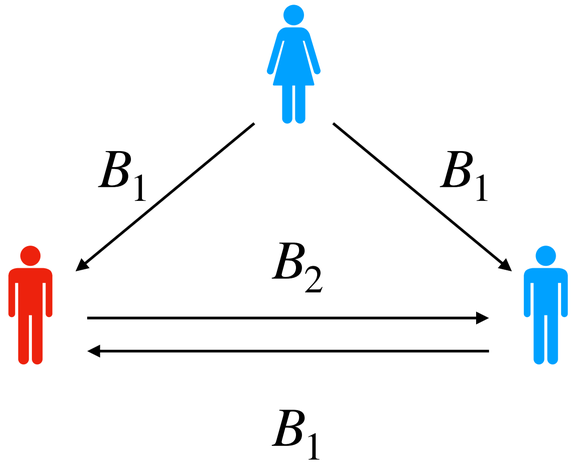
拜占庭广播（无签名）

- 想法：
  - 签名可以大幅度简化拜占庭共识协议的构造
  - 反例，如果没有签名：



拜占庭广播（无签名）

- B_2 有如下两种不同的选择
  - B_1没有遵守协议
  - A没有遵守协议
- B_2并无法判断是哪种情况

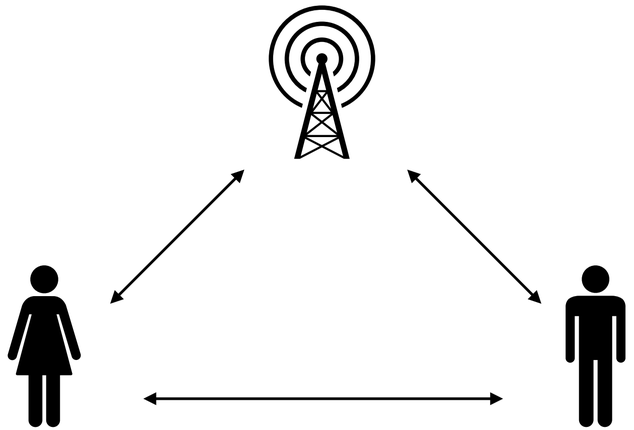


拜占庭广播（无签名）下界

- [PSL80],[FLM85]在没有初始化的情况下，不存在有1/3叛徒仍然成立的拜占庭协议。
- Dolev-Strong协议能够确保在任意$k \leq n-2$个叛徒的情况下仍然成立
  - 因为Dolev-Strong协议要求每个人都拥有一个签名公私钥对

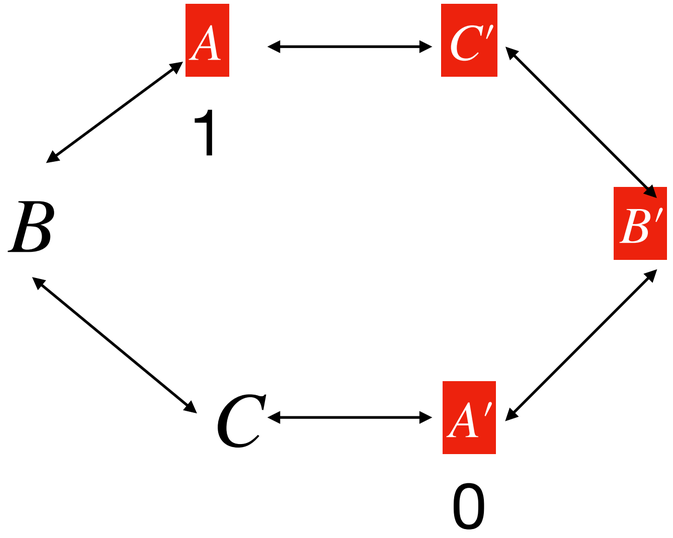
拜占庭广播（无签名）下界

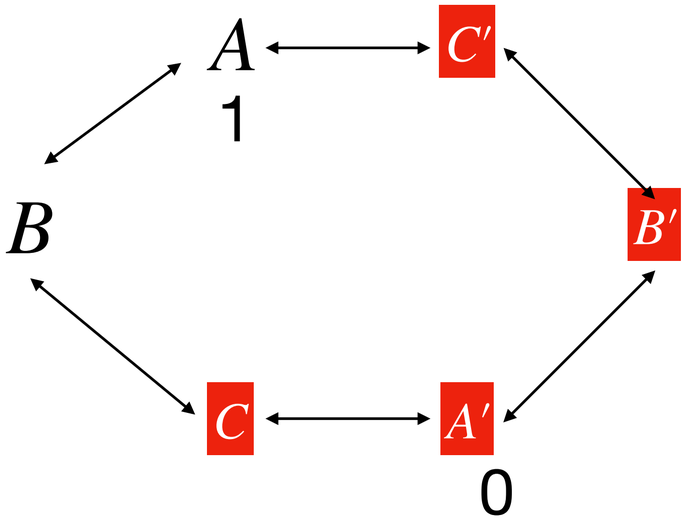
- 假设有$3k$个不同的用户，我们可以将这些用户分成数量相等的三组(A, B, C)

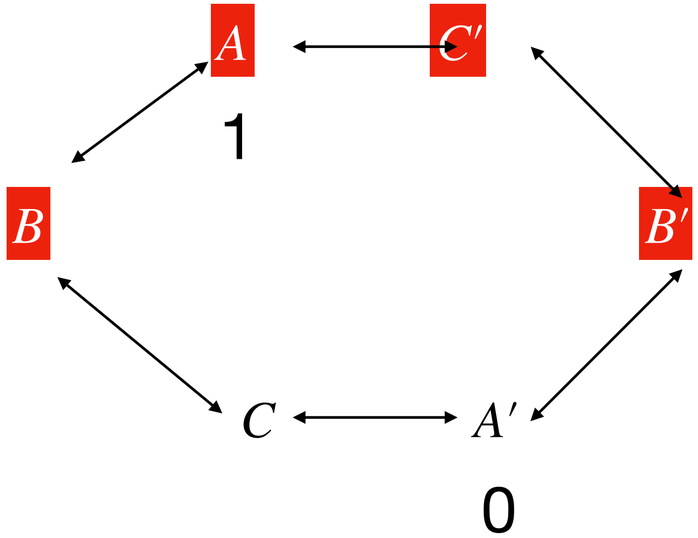


拜占庭广播（无签名）下界

- 考虑如下三种不同的世界：







拜占庭广播（无签名）上界

- 假设一共有n个节点。整个协议主要是通过投票进行的。
- 经过3k轮，其中当r = {1,2,…,k}时，分成三轮：
  - 其中对于每个r都定义L_r作为发起人，其中
    - $L_1 = 1$，$L_r = H(r)$其中$H(\cdot)$是模拟成为随机寓言机的一个哈希函数。

拜占庭广播（无签名）上界

- 经过3k轮，其中当r = {1,2,…,k}时，分成如下三个步骤：
  - 第0轮： L_r作为投票领导，按如下的方式选择一个比特b，发送给所有人。
    - 如果L_r当前相信的比特不为⊥，则b为当前相信的比特
    - 否则L_r随机选取一个比特$b \xleftarrow{\$} \{0,1\}$
  - 第1轮：每个用户对当前相信的比特进行投票。
    - 如果用户当前相信的比特不为$b \neq \perp$，则投票给b
    - 否则的话，投票给L_r发送的比特（如L_r发送的不是比特或者是⊥，则随机选取一个比特输出）
  - 第2轮：对于每个用户都进行计票，如果有 $\geq 2/3n$个投票是相同的比特b'，则将相信的比特更新为b'。否则将相信的比特更新为⊥

拜占庭广播（无签名）上界

- 定理1: 在任何一轮都无法出现，一个诚实的节点看见2/3n个1，但另一个诚实节点看到2/3n个0。
- 定理2: 在任何一轮结束的时候，不会发生一个诚实的节点相信的比特是b，而另一个诚实的节点相信的比特是1-b。
- 定义（幸运轮数）：第r轮是幸运的
  - 如果L_r是诚实的
  - 如果L_r提议b，则在这轮开始之前没有诚实节点相信比特为1-b
- 定理3：如果$r \leq k$是幸运的，则该轮结束时所有诚实节点相信的比特都为b。

拜占庭广播（无签名）上界

- 定理1: 在任何一轮都无法出现，一个诚实的节点看见2/3n个1，但另一个诚实节点看到2/3n个0。
- 证明：
  - 假设投票1的节点集合为S_1，投票0的节点集合为S_0。那么因为$\left|S_1\right| \geq 2/3n$，且$\left|S_0\right| \geq 2/3n$。所以$\left|S_0 \cap S_1\right| \geq 1/3n$。那么因为至少有2/3n个诚实的节点，所以矛盾。
- 定理2由定理1简单可得。

拜占庭广播（无签名）上界

- 定义（幸运轮数）：第r轮是幸运的
  - 如果L_r是诚实的
  - 如果L_r提议b，则在这轮开始之前没有诚实节点相信比特为1-b
- 定理3：如果$r \leq k$是幸运的，则该轮结束时所有诚实节点相信的比特都为b。
- 证明：
  - 这轮结束时，所有诚实的节点都会投票给b，所以至少有2/3n个节点投票b。
    即：该轮结束时所有诚实节点相信的比特都为b。

拜占庭广播（无签名）上界

- 确定幸运轮数的概率：
- 定理4：如果$H(\cdot)$与叛徒集合相互独立，则每一轮是幸运的概率至少是1/3。
- 证明：分两种情况讨论
  - $H(r)$为诚实的，且他相信的比特为b，那么根据定理而，所有诚实的节点在$r-1$轮结束后，相信的比特要么是b要么是⊥。
  - 如果$H(r)$为诚实的，且他相信的比特为⊥，那么则有1/2的概率选中正确的比特b。
  - 最后，$H(r)$是诚实的概率为$2/3$。所以，总概率最少为2/3* 1/2 = 1/3

拜占庭广播（无签名）上界

- 综上所述：
  - 对于一个给定的k，存在一个幸运轮数的概率为$1-\left(\frac{2}{3}\right)^k$。
- 定理（一致性）：存在$1-\left(\frac{2}{3}\right)^k$概率，所有诚实节点输出相同的值。
- 定理（正确性）：如果$H(1)$是诚实的，且输出比特为b，则所有诚实节点输出的比特都为b。