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12月25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

Streamlet 协议

- 对于第e轮，e = 1,2,…
- 提议：
  - 在第e轮开始的时候，轮领导L选择自己见到公证过的最长的链chain
  - 计算h = H(chain)
  - 收集所有未经记录的交易tx
  - 将$\langle (h, e, tx) \rangle_L$进行广播

Streamlet 协议

- 投票：
  - 每一个节点i收到$\langle (h, e, tx) \rangle_L$以后，检查收否是一个正确的区块
  - 如果$\langle (h, e, tx) \rangle_L$是目前见过公证的区块链的最长的一个区块链的延伸，则投票。即：将$\langle (h, e, tx) \rangle_i$发送给所有节点
  - 如果一个区块获得的投票超过$\frac{2}{3}n$，则确认区块被公证
- 结算：
  - 如果看到三个连续的被公证过的节点，则将第二个节点以及之前的所有都进行记账。

Streamlet 性质

- Streamlet满足无论在什么通信延迟下，都满足一致性要求。
- Streamlet在通信条件良好的情况下（在一个周期内，诚实用户可以互相收到通信），则满足活跃性要求：
- 定理（活跃性）：在良好的通信环境中，如果有连续5个时间段（e, e+1, e+2, e+3, e+4）都满足诚实信息发布者，那么在时间e+5的开始，每个诚实节点的账本都会增加至少一个新的块，并且这个新的块是由一个诚实发布者所发布的。

一些关于streamlet的讨论

- 因为每一轮的信息发布者都是随机产生的，所以能在一定的概率以后交易能够被记录。
- 与Dolev-Strong相比较，确定的共识协议必须要f+1轮才能达成共识。
- 随机性减少了达成共识的轮数。

半同步模型

- Streamlet满足半同步模型（partial synchrony - Dwork, Lynch, Stockmeyer’88）
- 一致性：无论系统延迟有多长都能满足。
- 活跃性仍然需要系统满足Δ延迟。

半同步模型

- 两种不同（但等价）的定义方式：
- 同步阶段模型：
  - 无论系统延迟有多长，一致性都能得到满足
  - 活跃性只在有一段足够长同步阶段存在的情况下满足
- 未知Δ模型：
  - 系统的一致性与活跃性的存在都独立于系统实际延迟Δ
  - 系统的确认时间T_{conf}取决于系统实际延迟Δ

一些背景

- 两种模型是等价的：如果存在一个协议满足一种模型，则可以构造另一种协议。
- 未知Δ模型常用于理论结果证明，同步阶段模型经常用于协议构造。
- 历史上来说Paxos和PBFT及其变种，基本为主流实用区块链协议。
- 这些区块链协议全部都是直接区块链的构造，并没有拜占庭协议的叠加。主要是因为直接构造通常能够获得更好的效率。

半同步模型的下界

- 我们之前看到了Streamlet是一个半同步模型下安全的区块链协议
  - 其中允许至多有n/3个攻击者存在
- 那么：
  - 是否存在允许多于n/3个攻击者的半同步协议?
  - 答案是否定的（n/3是下界）

半同步模型的下界

- 我们在“未知Δ模型”中证明这个下界。
- 证明思路：
  - 我们证明拜占庭共识在“未知Δ半同步模型”中最多允许n/3个攻击者存在
  - 一些需要注意的：
    - 拜占庭广播与拜占庭共识的区别
    - 拜占庭广播在半同步模型中只要有攻击者存在就不安全
    - 我们将要说明拜占庭共识与区块链协议可以相互构造

拜占庭广播与拜占庭共识

- 广播：一个信息发布者将一个消息发送给所有用户
- 共识：所有人都有一个输入比特，需要所有诚实用户达成一致
  - 一致性：如果两个诚实的用户输出b_1，b_2，则满足$b_1 = b_2$
  - 正确性：如果所有诚实用户都收到一个相同的比特b，那么所有诚实用户的输出应该为b
  - T-活跃性：每个诚实的节点在T轮以后必须产生一个输出。其中T是关于用户数n和系统实际延迟Δ的函数

半同步拜占庭广播

- 半同步模型中拜占庭广播在攻击者$f \geq 1$的情况下不存在
- 反例：
  - 不需要攻击者，只要延迟信息发送者的消息，使消息发送者的消息在第一个诚实接受者结束之后再发出。
  - 诚实接受者无法区分下列两种情况
    - 消息发送者因为系统延迟消息未送达
    - 消息发送者本身是攻击者，未发送信息

拜占庭共识与区块链协议

- 区块链协议⇒拜占庭共识
  - 每个用户将自己的信息签名发布在区块链协议当中
  - 当每个用户发现自己的区块链中存在$\frac{2}{3}n$个不同用户的签名时，输出前$\lceil\frac{2}{3}n\rceil$个比特中占多数的比特，如果相同则输出0
  - 因此，当攻击者小于n/3时，区块链能够构造拜占庭共识

拜占庭共识与区块链协议

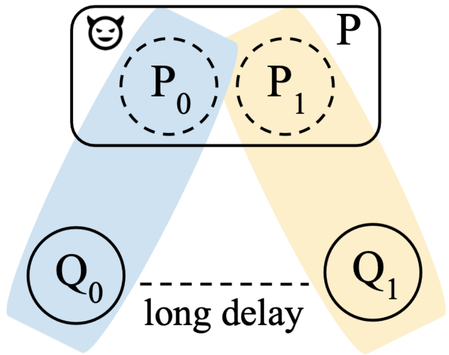
- 拜占庭共识⇒区块链协议
  - 这里对攻击者的数量并没有限制
  - 每一轮随机选取一个轮领导，并将随机选择的比特，然后所有诚实的节点通过拜占庭共识，形成共识比特，并将这个共识比特写入自己的账本
- 所以只要证明，不存在允许攻击者大于n/3的拜占庭共识协议（半同步）
  - 就可以推出，不存在允许攻击这个大于n/3的区块链协议（半同步）

半同步模型拜占庭共识下界

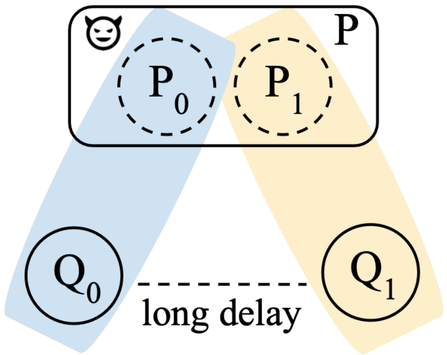
- 通过“未知Δ模型”证明
- 定理：令$T(n, \Delta)$为一个函数，如果至少有n/3个攻击者，那么就没有T-活跃的拜占庭共识协议。

半同步模型拜占庭共识下界

- 证明：
  - 反证，假设存在n=3, f=1的拜占庭共识协议
  - 考虑三种不同的情况：



半同步模型拜占庭共识下界

- 考虑三种不同的情况：
- 

- P是攻击者，分别与Q_0，Q_1关于（0，1）形成共识
- Q_0和Q_1的启动时间有很长的延迟
- 形成矛盾