MANX 公链共识技术

课题 **1**：**MANX** 共识的基本概念

状态机复制，也叫原子广播，是分布式系统的核心抽象。在状态机复制协议中，一组服务器需要对不断增长的线性排列的日志，达成共识。

有两个特征需要满足：

（1）一致性（consistency），也就是所有的服务器必须对日志有相同的记录；

（2）活跃性 （liveness）,也就是当客户提交一个交易，这笔交易可以迅速地被记录到日志上。

一个共识协议是可响应的（responsive），指的是任何在诚实节点上的交易输入可以被确认的时间取决于网络延迟的时间。实现可响应要求 2/3 的节点是诚实的。所有已知的可响应的协议都是很复杂的，所以不容易实现。我们定义良好响应（benign responsiveness）指的是当好条件满足时，可响应的条件满足。

我们考虑两种条件：

（1）最糟糕条件，共识协议可以提供在最坏条件下的一致性和缓慢的确认；

（2）良好性条件，共识协议可以提供可响应确认，要求有 3/4 节点是诚实的而且上线，同时有指定的“领导者”是诚实的。

课题 **2**：**MANX** 共识的设计简介

MANX 共识的主要设计是：

- 一个指定的节点：领导者，或“加速器”
- 交易发送给领导者
- 领导者对交易签名（序号不断增加）然后把签了名的交易发送给”委员会”节点
- “委员会”节点“确认”所有领导者签名了的交易，每个序号只有一次
- 如果一个交易有超过 3/4 的“委员会”签名，我们叫“公证了”
- 参与节点可以直接输出最长的连续“公证了”的交易，所有这些交易都被确认了

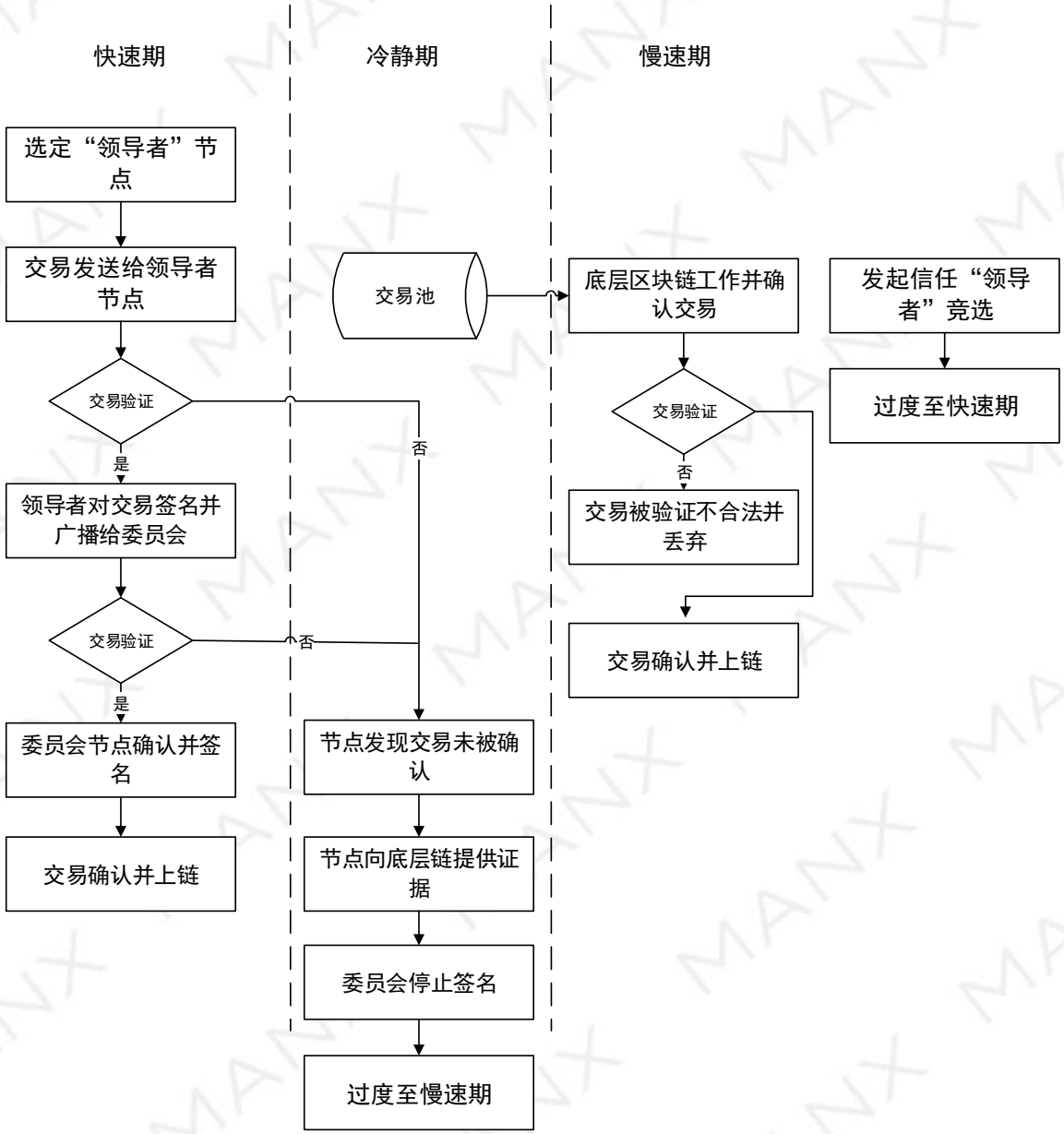
在超过 1/2 的“委员会”节点是诚实的时候，这个协议是一致性的。而且在良好响应的条件下（领导者是诚实的，3/4 委员会节点是诚实的），这个协议满足活跃性。在这些理想的条件下，只需要 2 次交流就可以确认一次交易。然而当“领导者”是在欺骗，这个协议就停止了。

如果节点发现交易没有被“领导者”或“委员会”确认，一些证据被发送到底层区块链，然后进入“冷静期”，委员会节点停止对“领导者”节点的消息签名。然而我们仍然让节点广播任何“公证了”的交易。

当“冷静期”结束后，进入“缓慢”阶段。交易通过底层区块链来确认。然后用区块链来替换掉“领导者”，然后开始一段新的机会性协议阶段。

MANX 的共识机制设计的极其简单，在良好环境下，使用快速模式只需一轮投票即可确认交易；在恶意环境下，使用慢速模式保证安全和数据真实。对于大规模分布式系统来说，简单设计至关重要。MANX 可以用来加速任何已有区块链，可以是良好性方案也可以是区块链的方案。MANX 可以承受 49%的攻击。

课题 **3**：**MANX** 共识的流程草图



MANX 共识机制流程图