基础知识：Threshold 门限签名，Threshold 门限 Coin Toss(基于 DH 困难问题，且是非交互的)

第 r 轮的 Coin(TID,r)　由交易 TID 和轮数构成，总共有 n 个节点，P1,…,Pn，最多 t 个恶意节点。

(1) 每个 Pi 计算 Coin 的 coin share : CS_i ,并将其广播出去。
(2) 每个 Pi 收集 n-t 个 coinshare，可以还原 coin，计算的 toss 的值 $F(TID,r)\epsilon(0,1)$。
(3) 每个节点 Pi 给 $b\ \epsilon(0,1)$预投票 pre-vote，如果 r=1，b 的值就是一个 Pi 给的初始值 Vi，如果 r>1，则由 r-1 轮的结果决定。
   - **如果上一轮 r-1 轮第(5)步有结果输出** m=("pre-vote", TID, r-1, b)；**那么此轮的 pre-vote 投票结果和上轮结果输出一致**，$b_r=b_{r-1}$，pre-vote 的验证数据 justification 为上一轮共识输出的门限签名(门限签名的产生见(4),(5))，这种 pre-vote 称为 b 的 hard prevote。
   - **如果上一轮 r-1 轮第(5)步有结果输出**结果输出为 m=("main-vote", TID, r-1, abstain)，**那么这一轮的 pre-vote 投票结果为 b= F(TID,r)**，也就是由此轮 coin tossing 的结果决定。pre-vote 的验证数据 justification 为上一轮共识输出的门限签名(门限签名的产生见(4),(5))，这种 pre-vote 称为 b 的 soft prevote。

在投票后，Pi 为此轮投票结果("prevote", TID, r, b)产生门限签名 signature share。

那么此轮最终输出为:
("prevote", r, b, justification(上一轮第(5)步输出的门限签名)，此轮投票结果 signature share)

其中 b 为此轮的 pre-vote 结果。

注：
Hard prevote 中，此轮投票结果 b 不要和上一轮输出混淆；
原文的上一轮输出 pre-vote，main-vote 等字段没有描述清楚，应该是一个字符串，所以这里我加上了双引号。

(4) 在投完预投票 pre-vote 后，Pi 收集 r 轮的 n-1 个验证过的预投票结果，并开始主投票，主投票 $v\ \epsilon(0,1,\text{abstain})$，主投票的值由决定方法如下：
   - **如果 Pi 收集到的 n-t 预投票既包含 0，也包含 1，那么 Pi 的主投票就是 abstain。**主投票的 Justification 数据为两个冲突预投票的 justification。第一轮的 prevote 由于没有 justification，所以第一轮的 abstain 的主投票也没有 justification 数据。
   - **如果 Pi 收到 n-t 个合法的 pre-vote，且投票结果为一个确定值 $b\ \epsilon(0,1)$，没有冲突，那么此轮的 main-vote 投票结果也是 b，即主投票 v=b。**Pi 收集所有预投票的 signature share，使用门限签名，**可以恢复上轮投票结果**
     ("prevote", TID, r, b)
     的一个合法门限签名 (这里可以用来做下一轮第(3)步 hard-vote 的 justification)，此轮 main-vote 的验证数据 justification 也就是此门限签名。

产生主投票结果后，Pi 对这轮主投票结果
("main-vote", TID, r , v)
签名产生 signature share。

Pi 这一轮主投票的最终输出为消息:
("main-vote", r, v, justification, signature share)

(5) Pi 主投票完成后，等待收集其他合法的 r 轮 n-t 个 main-vote。

- 如果收到的 main-vote 都是同一个值 $\mathbf{b} \in (\mathbf{0}, \mathbf{1})$，那么 Pi 确定 TID 的最终值，但是仍然参与 TID 的下一轮共识；否则 Pi 直接跳到下一轮。

- 在进行到下一轮之前，Pi 需要为下一轮的预投票做如下准备：

如果 Pi 收集了 n-t 个弃权 abstain 的主投票，那么他可以收集所有的主投票的 signature share 产生如下消息的 Threshold signature:
("main-vote", TID, r-1, abstain)
为下一轮 soft prevote 做 justification。

否则如果有个主投票是 $\mathbf{b} \in (\mathbf{0}, \mathbf{1})$，**且投票的 justification 部分伴随着如下消息的一个 threshold signature：**

("prevote", TID, r, b)

这个签名用来做 Pi 下一轮 hard pre-vote 的 justification。