可验证随机函数（VRF）讨论方案

1. 可验证随机函数整体流程
   1. 生成一对公私钥Pk，Sk，（以太坊中即账户的公私钥）
   2. 证明者通过（SK，msg）算出vrfValue和vrfProof
   3. 验证者根据（msg，vrfValue,vrfProof,Pk）验证vrfValue,vrfProof的合法性，
2. 修改点：
   1. 对区块头的改造
      1. 加入VrfValue：即随机数
      2. 加入VrfProof：即零知识证明数据
      3. 加入出块账户的PK：即出块人的公钥（用于验证出块人的随机数的正确性）
   2. 修改策略
      1. 创世区块：通过配置在创世区块内填入VrfValue，VrfProof，（创世区块不验证）
      2. 其他区块：
         1. Leader：通过上一区块的msg（header内的VrfValue,VrfProof，hash）和leader账户的Sk生成新的VrfValue\_New，VrfProof\_New，并将其和自己的PK放入区块头中发给其他人验证
         2. 验证者：验证者通过header的VrfValue、VrfProofPK、PK和上一区块内的msg（由上一区块的VrfValue、VrfProof、hash组成）验证其合法性