参选交易NodeID漏洞修复方案讨论

1. 参选交易不填NodeID，主账户发出交易，带ManAddress
   1. 曹奥建议设置一个空账户，用来签名(ManAddress)
   2. 主账户收钱
   3. 按照广播节点账户的轮换方式，如果不指定，一直用最后一个
   4. 顶层节点到了选举高度还没有下一个的轮换账户（多少个广播周期），就自动退出顶层选举
   5. 第三方代付gas，或者交易发送频率
2. 任何节点启动时：
   1. 启动参数添加一个Address和Password，就叫ManAddress
      1. 目前以太坊启动时有一个Etherbase，是一个以太坊账户，用于挖矿
      2. 我们现在需要挖矿账户，validator验证账户，广播交易签名账户
      3. 矿工和Validator不能同时存在于一个NodeID，则挖矿和验证者可用一个
      4. 签名账户可以再加一个参数，或者用轮换账户，默认使用ManAddress
   2. 启动时节点会创建node信息

|  |
| --- |
| *type Node struct {*  *IP net.IP // len 4 for IPv4 or 16 for IPv6*  *UDP, TCP uint16 // port numbers*  *ID NodeID // the node's public key*  *ManAddress*  *Signature [65]byte //sign(nodeID)*  *sha common.Hash*  *addedAt time.Time*  *}* |

* + 1. 添加一个ManAddress和ManAdress对NodeID的签名
    2. 没有设置ManAddress的node这两项为空

1. 节点建立p2p链接时
   1. 判断是否有ManAddress
   2. ManAddress签名是否正确
   3. 如果满足条件，建立ManAddress与NodeID的一对一关系
   4. 程序自动定期公布新签名，签名生命周期有300个区块的重复
   5. 从参选交易链表中确定每个nodeID的身份
2. 如果nodeID相同
   1. 某个节点启动时，nodeID是用本地私钥创建的，不丢失私钥的前提下，NodeID为当前用户自己做出修改的
   2. ManAddress的签名也保证是自己要绑定NodeID的
   3. 修改方法：以最新node信息为准
      1. 如果同一个ManAddress收到两个Node，以最新Node信息为准
      2. 如果同一个NodeID收到两个ManAddress，以最新ManAddress信息为准

现在这个版本：

参选交易不发送NodeID

添加一个ManAddress和ManAdress对NodeID的签名

没有设置ManAddress的node这两项为空