随机数服务讨论会议纪要

随机数服务增加两种子服务，两种方式均既提供web3接口也提供内部接口

1. 子服务1：
   1. 用途：每个块产生一个随机数，
   2. 计算方式：给定区块高度，指定区块头高度的nonce+当前区块头的有效私钥+当前账户地址
   3. 概念性问题补充
      1. 当前区块头的有效私钥：若当前区块头的私钥与上一个自己出的块的公钥匹配，则为当前区块头的私钥，否则为0
2. 子服务2：
   1. 用途：每个广播周期产生一个随机数，
   2. 计算方式：当前广播区块内的有效私钥之和+前100块的最大nonce
   3. 概念性问题补充
      1. 当前广播区块内的有效私钥之和：获取当前区块的私钥交易列表，再获取上一个广播区块的公钥交易列表，算匹配的公私钥之和