LESSON ONE

一、对ring signature, ZK-snark进行比较，ring signature decoy的数量在多少的时侯更消耗时间空间，ZK-sanrk在使用上占用多少空间，计算时间相比哪个更快.

ring signature decoy数量大于7时更消耗时间和空间；

zk-SNARKs占用空间大约40M左右；

环形签名和zk-SNARK计算时间相比较，zk-SNARKs的运行更有效率。

二、将bitcoin, ethereum, monero, zcash, EOS的交易、相关交易易属性、块大小以及填入多少交易写在report

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 交易属性 | 共识算法 | 块大小 | 填入交易数 |
| Bitcoin | 最终一致性的确认需要多个出块来保证 | POW | 1M | 2-3K |
| Ethereum | 燃料(Gas)消耗机制，支持图灵完备的智能合约 | PoW+POS | 一块的gas上限是1500000Gas（可配置） | 一块能有多少交易，要视交易数据的大小而定 |
| Menero | 使用环签名，隐形地址保证匿名 | 防ASIC的CryptoNote的核心算法 | 不固定，最大为前100个块大小的中位数的2倍，最小块300KB | 交易数量不固定，能接近1000 |
| ZCash | zk-SNARKs实现匿名 | 抗ASIC的EquiHash算法 | 2M | 3k左右 |
| EOS | 快速，地址记忆友好，权限体系 | 异步BFT（DPOS+aBFT）共识机制 | 不固定，可以到几十M | 数据集保持在1027bytes内 |