第一课作业

1. 需要对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当大于7时更消耗时间和空间

zk-snark空间占用：40M

zk-snark更快

1. 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中
2. bitcoin相关交易易属性、块大小及多少交易

|  |  |  |
| --- | --- | --- |
| 属性 | 描述 | 大小 |
| 版本号 | 目前为1 | 4字节 |
| 输入数量 | 正整数VI=Varlnt | 1-9字节 |
| 输入列表 | 每块的第一个交易的第一个输入叫做”coinbase”(早期版本中内容被忽略) | <in-counter>-许多输入 |
| 输出数量 | 正整数VI=Varlnt | 1-9字节 |
| 输出列表 | 块中的第一个交易的输出是花掉挖矿得到的比特币 | <out-counter>-许多输出 |
| 锁定时间lock\_time | 如果非0并且序列号小于0Xfffffff,是指块序号；如果交易已经终结，则是指时间戳 | 4字节 |

块大小：1M

可以填入：2k-3k笔交易

1. ethereum

如下为原始交易对象字段：

var rawTx = {

nonce: '0x00',

gasPrice: '0x09184e72a000',

gasLimit: '0x2710', to: '0x0000000000000000000000000000000000000000',

value: '0x00',

data:'0x7f7465737432000000000000000000000000000000000000000000000000000000600057'

}

各字段说明:

nonce: 记录发起交易的账户已执行交易总数。Nonce的值随着每个新交易的执行不断增加，这能让网络了解执行交易需要遵循的顺序，并且作为交易的重放保护。

gasPrice:该交易每单位gas的价格，Gas价格目前以Gwei为单位（即10^9wei），其范围是大于0.1Gwei，可进行灵活设置。

gasLimit:该交易支付的最高gas上限。该上限能确保在出现交易执行问题（比如陷入无限循环）之时，交易账户不会耗尽所有资金。一旦交易执行完毕，剩余所有gas会返还至交易账户。

to：该交易被送往的地址（调用的合约地址或转账对方的账户地址）。

value：交易发送的以太币总量。

data: 若该交易是以太币交易，则data为空；若是部署合约，则data为合约的bytecode；若是合约调用，则需要从合约ABI中获取函数签名，并取函数签名hash值前4字节与所有参数的编码方式值进行拼接而成

块大小：一块的gas上限是21000个（可配置）

填入多少交易：以太坊中，对交易大小或者块大小都没有直接或固定的上限，具体一块能有多少交易，要视交易数据的大小而定

1. monero

monero交易易属性：

1. 不可链接性(Unlinkability) :无法证明两个交易是发送给同一个人的，也就是无法知道交易的接收者是谁。
2. 不可追踪性(Untraceability) : 无法知道交易的发送者是谁。
3. 环签名(ring signatures)将发送者的输入与其它的输入进行混合，使确定后续的交易关联变得成倍的困难
4. 隐形地址(stealth addresses)为每个交易生成隐形地址，使除了该交易的发送者和接收者之外的其他人不可能找到该交易的实际发送地址
5. 环机密交易(ring configential transactions)通过该机制隐藏交易的金额

Monero 在区块大小上限以及区块奖励上是动态的，最大块最多可以多达上n(当前为100)个块的中间块的两倍，该协议还保持最小块300KB。这意味着矿可以构建300KB的块却不违规，如果选择构建这些参数之外的区块，则会收到罚款

**罚款=基础奖励\*（（区块大小/MN）-1）²**

1. Zcash

Zcash交易易属性:

隐私地址和透明地址，用户可以选择使用隐私方式或公开方式发送zcash

Zcash块大小：

1. 透明资金地址taddr 类bitcoin地址，保存在UTXOs中，长度为34位。
2. 私有资金地址 zaddr 保存在notes对象中，长度为96位，前2位为标记，主链地址前2位是”zc”, spendingkey的前2位是“SK“，测试链的地址前2位是”tn”.

块大小：2M

1. EOS交易属性

transactin\_id: 当前这笔交易的hash值

processed: 其中包括的信息比较丰富，重点是如下的几个

“refBlockNum”: 2206

“refBlockPrefix”: 221394282

这里是前一个区块的信息，refBlockPrefix,是取了最近一个区块的hash值的一部分

Messgae：包括了代币所属的智能合约名称(eos),类别：transfer,所需要的权限：inita的active权限，以及交易数据结构(data)

ref\_block\_num:引用的区块号

ref\_block\_prefix:引用的区块头

expiration:交易过期时间

scope:账户范围

transaction\_merkle\_root:SHA256用于区块产生时的校验

producer\_account\_id:区块生产者的账户名

signatures:签名集合

采用异步BFT（DPOS+aBFT）共识机制，验证交易的数据集保持在1027bytes内。