作业一：

对ring signature，zk-snark进行比较，ring signature decoy的数量在多少的时候更消耗时间空间， zk-snark在使⽤上占用多少空间，计算时间相⽐哪个更快

环签名测试数据如下：

测试程序：环签名go版本

测试报告：在测试过程中，发现数值不是很稳定，偏差很大，有的多次运行后偏差在一倍之多，不知道是go版本的问题，还是其他原因导致的，decoy选取范围2-21之间（后续应该扩大decoy范围），下图是多次执行后平均值。

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| D | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 消耗时间 | 16.716619ms | 23.829181ms | 36.577541ms | 37.360589ms | 46.270684ms | 53.302757ms | 61.427054ms | 66.63443ms | 75.443852ms | 80.409618ms |
| D | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 |
| 消耗时间 | 90.499304ms | 103.524362ms | 115.617025ms | 126.823222ms | 134.110881ms | 154.308295ms | 163.158496ms | 164.974559ms | 165.635849ms | 165.172654ms |

图中显示decoy在17时斜率最大，17以后趋向稳定

zk-snark数据暂时还没出来，稍后更新

作业二：bitcoin、etheruem、monero、zcash、eos交易报告

**一、bitcoin交易report**

1、bitcoin 交易信息：

|  |  |  |  |
| --- | --- | --- | --- |
| **Field Size** | **Description** | **Data type** | **Comments** |
| 4 | version | int32\_t | Transaction data format version (note, this is signed) |
| 0 or 2 | flag | optional uint8\_t[2] | If present, always 0001, and indicates the presence of witness data |
| 1+ | tx\_in count | [var\_int](https://en.bitcoin.it/wiki/Protocol_documentation#Variable_length_integer) | Number of Transaction inputs (never zero) |
| 41+ | tx\_in | tx\_in[] | A list of 1 or more transaction inputs or sources for coins |
| 1+ | tx\_out count | [var\_int](https://en.bitcoin.it/wiki/Protocol_documentation#Variable_length_integer) | Number of Transaction outputs |
| 9+ | tx\_out | tx\_out[] | A list of 1 or more transaction outputs or destinations for coins |
| 0+ | tx\_witnesses | tx\_witness[] | A list of witnesses, one for each input; omitted if *flag* is omitted above |
| 4 | lock\_time | uint32\_t | The block number or timestamp at which this transaction is unlocked:   |  |  | | --- | --- | | **Value** | **Description** | | 0 | Not locked | | < 500000000 | Block number at which this transaction is unlocked | | >= 500000000 | UNIX timestamp at which this transaction is unlocked |   If all TxIn inputs have final (0xffffffff) sequence numbers then lock\_time is irrelevant. Otherwise, the transaction may not be added to a block until after lock\_time (see [NLockTime](https://en.bitcoin.it/wiki/NLockTime)). |

TxIn consists of the following fields:

|  |  |  |  |
| --- | --- | --- | --- |
| **Field Size** | **Description** | **Data type** | **Comments** |
| 36 | previous\_output | outpoint | The previous output transaction reference, as an OutPoint structure |
| 1+ | script length | [var\_int](https://en.bitcoin.it/wiki/Protocol_documentation#Variable_length_integer) | The length of the signature script |
| ? | signature script | uchar[] | Computational Script for confirming transaction authorization |
| 4 | [sequence](http://bitcoin.stackexchange.com/q/2025/323) | uint32\_t | Transaction version as defined by the sender. Intended for "replacement" of transactions when information is updated before inclusion into a block. |

The OutPoint structure consists of the following fields:

|  |  |  |  |
| --- | --- | --- | --- |
| **Field Size** | **Description** | **Data type** | **Comments** |
| 32 | hash | char[32] | The hash of the referenced transaction. |
| 4 | index | uint32\_t | The index of the specific output in the transaction. The first output is 0, etc. |

The Script structure consists of a series of pieces of information and operations related to the value of the transaction.

(Structure to be expanded in the future… see script.h and script.cpp and [Script](https://en.bitcoin.it/wiki/Script) for more information)

The TxOut structure consists of the following fields:

|  |  |  |  |
| --- | --- | --- | --- |
| **Field Size** | **Description** | **Data type** | **Comments** |
| 8 | value | int64\_t | Transaction Value |
| 1+ | pk\_script length | [var\_int](https://en.bitcoin.it/wiki/Protocol_documentation#Variable_length_integer) | Length of the pk\_script |
| ? | pk\_script | uchar[] | Usually contains the public key as a Bitcoin script setting up conditions to claim this output. |

The TxWitness structure consists of a [var\_int](https://en.bitcoin.it/wiki/Protocol_documentation#Variable_length_integer) count of witness data components, followed by (for each witness data component) a [var\_int](https://en.bitcoin.it/wiki/Protocol_documentation#Variable_length_integer) length of the component and the raw component data itself.

2、bitcoin 块信息：

* 块大小：算上隔离见证2M，不算1M
* 块最大交易数：每笔交易大小在250B以上，在隔离见证之前大概在4-5k，隔离见证后最大能容纳9-10k左右交易
* 出块时间：10分钟
* 块确认时间：6个以上块确认
* 每秒交易数：7tps/s

**二、ethereum交易report**

1、ethereum交易信息

根据以太坊黄皮书，以太坊交易属性如下：

* nonce：该字段表示的是交易发送者的交易序列号，它是账号的一个交易计数器，这个字段能够防止重放攻击（replay attack）。
* gasPrice：gas的价格，用于计算交易费用
* gasLimit：执行这笔交易所花费的gas的上限
* from: 交易发送者的地址或者合约调用者的地址
* to：交易接收者的地址或者合约的地址
* value：要发送的以太币数量，以wei为单位
* v, s, r：签名相关的参数，通过这三个参数可以得到发送者的公钥和地址（更详细的内容参见以太坊黄皮书）

如果该交易是一个创建合约的交易，还可能包括以下字段：

* init：用于初始化交易的EVM（以太坊虚拟机）操作码
* data：数据域（理论上数据域的大小是不受限制的）

2、ethereum块信息

* 块大小：不固定，用gas limit限制
* 块最大交易数：不固定
* 出块时间：14-15秒
* 块确认时间：6个确认
* 每秒交易数：15tps

**三、monero交易report**

1、monero交易信息

* ring size ： 参与环签名的大小
* From Block： 区块高度
* Output total：匿名，隐藏交易金额
* Fee：交易花费
* Tx size ： 交易大小
* Tx version：交易版本号
* RingCT/type: yes/2，环机密，隐藏金额
* Extra：
* Mixin：
* Unlock：
* In：交易输入数
* Inputs：交易输入列表，包含所有参与的交易输入方 Key Image密钥镜像信息（和某个交易输入方一起参与环签名的所有公钥信息），隐藏交易金额
* Out：交易输出数
* Outputs：交易输出列表，包含输出的stealth address列表，隐藏交易金额

2、monero块信息

* 块大小：自适应区块大小，

工作原理：系统有一个区块奖励的惩罚，最后 100 个区块大小的中位数叫做 M100。假设矿工挖出了一个新的块，大小记为 NBS（New Block Size）。如果 NBS > M100，那么区块奖励会随着 NBS 超过 M100 的平方递减。系统不允许超过2倍M100，小于等于60没有任何奖励

* 块最大交易数：动态决定数值，如果按照最近查询的M100数约等于300k，每个交易约13k以上，能容纳最大交易数约在22笔左右
* 出块时间：2分钟
* 块确认时间：
* 每秒交易数：

**四、Zcash交易report**

1、zcash交易信息

* **Size**
* **Fee Rate**
* **Received Time**
* **Mined Time**
* **Included in Block**
* **LockTime**
* **Version**
* **Overwintered**
* **VersionGroupId**
* **Expiry Height**

proof size

2、zcash块信息

* 块大小：2m
* 块最大交易数：
* 出块时间：2.5分钟
* 块确认时间：
* 每秒交易数：

**五、Eos交易report**

1、eos交易信息

EOS采用账户模型设计， 交易设计成三层体系，从上到下分别是：block、transaction、message

Transaction交易属性如下：

| **Field** | **Type** | **Ref ID** | **Description** |
| --- | --- | --- | --- |
| transaction\_id | ObjectId | **PK** | System unique id （系统唯一标识符） |
| ref\_block\_num | Integer |  | Reference block number （引用的区块号） |
| ref\_block\_prefix | Integer |  | Reference block header （引用的区块头） |
| expiration | String |  | Expiration time of transaction （交易过期时间） |
| scope | Array |  | Account scopes （账户范围） |
| transaction\_merkle\_root | String |  | checksum (SHA256) of block when generated （区块产生时的校验和 (SHA256)） |
| producer\_account\_id | String | FK | Account nmae of block producer （区块生产者的账户名） |
| signatures | Array |  | Array of signatures （签名集合） |

Message交易属性如下：

| Field | Type | Description |
| --- | --- | --- |
| code | String | Name of contract （合约名称） |
| type | String | Name of action （行为名称）：transfer| |
| authorization | Nested\_Document | Authorizing account and permission  （授权账户和权限） |
| data | Nested document | A nested document, any format, specific to message in use （内嵌文档, 任何形式的消息） |
| hex\_data | String | Hexadecimal representation of data （数据的16进制的表现形式） |

### Data Nested Document

| **Field** | **Type** | **Ref ID** | **Description** |
| --- | --- | --- | --- |
| from | String | FK | Authorizing account name （授权账户名） |
| to | String | FK | Authorizing account name （授权账户名） |
| amount |  |  | 转账金额 |
| memo |  |  | 备注 |

2、eos块信息

* 区块容量：每个块目前可以容纳约2000笔交易
* 出块时间：0.5s
* 块确认时间：0s确认
* 每秒交易数：目前3000-4000tps

参考：

1、比特币交易信息<https://en.bitcoin.it/wiki/Protocol_documentation#tx>

2、以太坊黄皮书 <https://ethereum.github.io/yellowpaper/paper.pdf>

3、门罗币浏览器 <https://moneroblocks.info/tx/c47dfef38e883bd1948c847d5c748831d9964354ca838df2134fa3d959700404>

<https://moneroexplorer.com/tx/faad6f50e1cb9cb69b4c5b9466470c0dfa1748e9e594ffe5be9e4dbd5aa97f91/1#show-json>

<https://segmentfault.com/a/1190000013310648#articleHeader5>

4、Zcash浏览器

<https://zcash.blockexplorer.com>

<https://bitinfocharts.com/zh/>

5、EOS wiki <https://github.com/BlockchainTranslator/EOS/blob/master/wiki/Database-Schema.md>

<https://eospark.com>

<https://eosmeta.io>

<https://eostracker.io>