Fabirc 账户交易设计

目录

[结构定义及说明 3](#_Toc509212830)

[钱包 3](#_Toc509212831)

[交易结构体定义 3](#_Toc509212832)

[钱包交易日志结构体定义 3](#_Toc509212833)

[UTXO结构体定义 4](#_Toc509212834)

[交易流程 5](#_Toc509212835)

[普通交易流程 5](#_Toc509212836)

[Coinbase交易 6](#_Toc509212837)

[模型论证 6](#_Toc509212838)

[交易防双花 6](#_Toc509212839)

[交易隐私性 6](#_Toc509212840)

[攻击 6](#_Toc509212841)

# 结构定义及说明

## 钱包

**定义**

每个机构下，都有一个属于自己机构的钱包。钱包的标识由机构的唯一mspId确定。

**字段**

|  |  |  |
| --- | --- | --- |
| 字段名 | 类型 | 说明 |
| mspId | String | 由前缀“WalletAddr”与mspId组成钱包ID |
| UTXOList | String | UTXO地址加密后列表。存储的是该机构UTXO地址加密后的值 |
| Logs | [](log数组) | 钱包日志，日之内信息使用机构自己密钥加密 |
| cryptPubKey | String | 机构私密信息加密公钥，用于己方或者他方机构给己方转账时加密UTXO地址与日志信息 |
| SignKey | String | 用于验证机构交易签名的解密密钥 |

初始化：

1. 钱包初始化：
   1. 在前端框架生成两对密钥：K1，K2。其中K1密钥对（K1’，K1’’）用于加密

## 交易结构体定义

**定义**

交易是由交易发起方发送至区块链上的参数，此交易信息并不实际存储在区块链上，而是

|  |  |  |
| --- | --- | --- |
| 字段名 | 类型 | 说明 |
| From | String | 转出方mspId |
| To | String | 转入方mspId |
| TimieStamp | String | 时间戳 |
| Amount | Float64 | 金额 |
| TxType | String | 交易类型 |
| Sign | String | 转出方对交易的签名 |

## 钱包交易日志结构体定义

|  |  |  |
| --- | --- | --- |
| 字段名 | 类型 | 说明 |
| TxId |  |  |
| TimeStamp |  |  |
| Nonce |  |  |
| RemoteAddr |  |  |
| Amount |  |  |
| OpeType |  |  |
| Info |  |  |
| UTXOs |  |  |

## UTXO结构体定义

UTXO在比特币中称为：未花费输出。





# 交易流程

## 普通交易流程



## Coinbase交易

# 模型论证

## 交易防双花

在并发交易的情况下，有可能出现以下情况：机构钱包下拥有a数量余额，用户A在该机构下进行向外转账，转账数量为b的资产，B用户同时也在该机构下进行向外转账，转账c数量资产。当A的操作还未完成，机构余额为a时，B的操作也同时进行，可能发生在余额为a的情况下，同时支付b、c，导致支付后余额d≠a-b-c。

而在此模型的交易流程中：由于在进行UTXO的花费时：

1. 花费UTXO前，检查该UTXO是否所有UTXO的余额是否足够本次支付；
2. 若两笔支付的总和大于余额，则根据鸽巢原理，必有一笔UTXO是需要被两笔交易同时修改，但是根据Fabric平台目前的限制，同时修改一笔记录会导致时间稍后的一笔交易最终失败，所以此情况下不会产生双花。

## 交易隐私性

1. 钱包内UTXO的隐私性：

各个机构内只记录的了所用的UTXO的地址列表，且各个UTXO的地址都是使用该机构公钥加密后的数据，只有本机构才能解密看到所有的UTXO地址，而在链上的所有UTXO虽然公开了改UTXO所拥有的余额，但是由于无法找到该UTXO与某个机构的对应关系，保证了财产的隐私。

1. 发送交易的隐私性：

在进行交易之前，区块链智能合约会产生一对密钥，并且将公钥发送给前端框架，使得前端框架可以使用该密钥加密之后一笔交易中的敏感信息，保证在前端框架与智能合约的交易过程中的隐私性。

## 攻击

由于Fabric在接收来自框架的调用请求时，会将请求中的参数一并记录在链内，所以可能存在的攻击方式：

通过遍历区块以及区块内的交易，找出前端框架与智能合约之间传递交易密钥的记录，并且遍历该交易之后某几笔存储密钥的交易，可以得到前端框架与智能合约之间的解密密钥，根据该解密密钥可以去遍历其他块内的交易信息并且尝试解密，最终可以找到真正的已被加密的交易信息，获取到机构与机构之间的转账记录。