.交易结构

.交易流程

-创建

-提交

-验证执行

-完成

.交易状态跟踪

.测试例子

交易结构

类型 字段 描述

byte[] nonce 地址已经发送的交易数量,每做一次增加1

byte[] value 交易额,已wei为单位

byte[] receiveAddress 目标账户地址,取公钥的SHA3哈希最后20字节作为地址

byte[] gasPrice 汽油价格,用于计算交易费

byte[] gasLimit 允许使用的汽油量

Byte[] data 消息呼出的输入数据或新合约的初始化代码

byte v

byte[] r sigmature 椭圆曲线数字签名

byte[] s

.在ethereum中由org.ethereum.core包中的Transation类来表示交易

.在发送空地址的交易是一种特殊类型的交易,创建了一个"合约"

.交易合法的条件

-签名具有合法格式(即27<=v<=30,0<=r<p,0<=s<N)

个地址具有足够的资金支付交易金额和交易费用.

交易流程

1.创建

.生成Transation类的实例

.填写交易信息+发送者私钥签名

2.提交

.把交易光波导以太坊网络中去

3.验证交易

.验证是否合法;执行交易

4完成

.交易被写入区块链中

交易状态跟踪

通过实现EthethereumListener接口实现监听交易的状态变化

. onPendingTransationsReceived

-提交之后,未包含到区块链之前的状态

. onTransationExecuted

-被执行之后,使用TransationExcutionSummary进行描述

. onBlock

-被确认包含到区块链

测试例子

.A->B, 合法

.C->D, 余额不足,不合法

.E->F->G,合法

后序工作

.执行交易的细节

.Repository

.Transation

.TransactionExecutionSummary

TransactionExecutor (关键)

.TransactionReceipt

.Wallet

交易中用到的加密工具

untitled1.png!