交易所与TRX区块链对接手册

为安全起见，建议交易所自己部署TRX区块链的一个FullNode和一个SolidityNode节点。其中FullNode会同步区块链所有数据，SolidityNode只会同步已经被区块链确认且不可回退的区块。可以通过FullNode进行交易广播等操作，通过SolidityNode查询账号余额等查询操作。

1. 部署FullNode和SolidityNode的前置条件：
   1. 安装JDK1.8（目前不支持JDK1.9）
   2. 如果系统是Linux Ubuntu system，请确保安装Oracle JDK 8，而不是OPEN JDK 8。
2. FullNode节点部署方法如下：
   1. git clone <https://github.com/tronprotocol/java-tron.git>
   2. cd java-tron
   3. ./gradlew clean shadowJar
   4. ./gradlew run

至此，FullNode节点启动完成，等待同步区块链数据。等控制台提示Sync Block Completed !!!，同步数据完成。

1. SolidityNode节点部署方法如下：
   1. git clone <https://github.com/tronprotocol/java-tron.git>
   2. cd java-tron
   3. ./gradlew clean shadowJar
   4. ./gradlew run -PmainClass=org.tron.program.SolidityNode

至此，SolidityNode节点启动完成，等待同步不可逆区块数据。等控制台提示Sync with trust node completed!!!，同步数据完成。

1. 部署grpc-gateway连接SolidityNode（非必选步骤）
   1. 安装go1.10.1
   2. go get -u github.com/tronprotocol/grpc-gateway
   3. cd $GOPATH/src/github.com/tronprotocol/grpc-gateway
   4. go run tron\_http/main.go

SolidityNode对外提供gRPC接口，通过grpc-gatewa提供对应的gRPC接口的Http接口。注意：该步骤是可选，非必选步骤，主要是针对gRPC接口提供Http接口，方便用户使用。

1. 生成账号
   1. 随机生成私钥32字节私钥 d：

d = ab586052ebbea85f3342dd213abbe197ab3fd70c5edf0b2ceab52bd4143e1a52

* 1. 私钥计算公钥：ecc SECP256K1N曲线，P = d\*G公钥 P

P = 5ed0ec89eaec33d359b0632624b299d1174ee2aec5a625a3ce9145dd2ba4e48e049327d454fbf7ec700a9464f87dc4b73a592e27fd0d6d1fe7faf302e9f63306

* 1. 公钥计算地址：sha3-256(P)

Hash = c7bcfe2713a76a15afa7ed84f25675b364b0e45e2668c1cdd59370136ad8ec2f

取Hash的后20字节

End20Bytes = f25675b364b0e45e2668c1cdd59370136ad8ec2f

在End20Bytes前面填充a0(testNet) 或 b0(mainNet)

address = a0f25675b364b0e45e2668c1cdd59370136ad8ec2f

* 1. 地址转base58check格式：(bip-13)

hash0 = sha256(address);

//hash0=cd398dae4f5294804c83093ee043c13fa3037603a4e7d76ed895bb3aa316e93

hash1 = sha256(hash0);

//hash1=7e5ff07e733c2bb52e56cef8cfb5af6f61e50d515eb3a57e38b5889a1f653ac8

checkSum = hash0的前4字节

//checkSum = 7e5ff07e

addressCheckSum = address || checksum

//addressCheckSum = //a0f25675b364b0e45e2668c1cdd59370136ad8ec2f7e5ff07e

addressbase58 = base58Encode(addressCheckSum)

//addressbase58=

//27mAse8NBVPM4M7Mpp5sxZcLcYkpSqrcoHX

注意：所有交易、区块存储的地址应该还是byte[]，这样比base58chcek 少14字节（21 vs 35）。区块链节点上，除了配置文件里设置的初始化地址及witness节点地址，采用base58check格式，其它地方都用原有格式。钱包这一边，涉及到输入、输出的地方要做格式转换，展示给用户的都是base58check格式。其中输入base58check的地址，需要校验正确性。

1. 连接SolidityNode或者grpc-gateway查询余额

通过步骤5生成的地址，连接SolidityNode通过gRPC接口GetAccount查询该地址的余额信息；或者连接grpc-gateway通过Http接口htpp://localhost:8080/Wallet/GetAccount查询该地址的余额信息。