Matrix账户修改方案

# 账户地址修改方案

## Matrix账户编码

1. Matrix将以太坊地址进行base58编码（"github.com/itchyny/base58-go"）
2. 加上前缀为币种名称，全部大写加点，币种名称长度限制2-8，全大写。例如man币地址为：MAN.xxxxxx
3. 将上面的全部做CRC校验，mod58，添加base58编码的一位：例如man币地址全部为：MAN.xxxxxY，Y为校验码

## Matrix多币种支持

1. Matrix的主链可以打包多个币种，每个币种为币种包
   1. 币种包包含一个键值Key：用币种名称即可，不能重复
   2. 币种包包含目前与交易有关的所有存储和状态树
2. Matrix的主链Header可包含多个币种包
   1. MAN是主币种包，每个区块必须打包
   2. 其它币种包，只有有交易的时候才打包
3. 分包存储
   1. 类似分片存储的概念，每个包要单独存储，单独下载
   2. 每个包都支持目前所有的交易类型
   3. 每个包都支持分片存储
4. 多币种跨币种交易：
   1. 与跨链，跨合约代币相似，用撮合的办法，是另外的任务

## Matrix多账户机制：

1. 多账户机制是用来实现不同账户的不同功能，是常用智能合约的简单规范实现方法
2. 多种账户在币种包下面，为二级账户。在币种包内：
   1. 每个地址有一个地址状态结构(stateObject)
   2. StateObject目前只有一个Account，现在修改为Account的Map，key值为账户类型
   3. Account需要做成接口形式，用来支持多种交易类型，目前需要支持的账户属性有：
      1. 冻结账户，在[time0-time1]之间不能转出，之后可以转到任意账户，常用于押金，抵押，定时交易等
      2. 锁仓账户，在[time0-time1]之间不能提出，之后提回主账户，用于锁仓，可得到利息。
      3. 可撤消账户，用于可撤销转账，只能用可撤销转账和撤消交易调用
      4. 委托账户，委托别的地址使用，有限额，使用限制[比如gas]

## Matrix交易扩展：

1. 定时交易类型：
   1. 普通定时交易，在某个时间后执行
   2. 可撤销转账：A->B，24小时后执行
      1. A把man币转到可撤销账户
         1. 24小时之内A撤消交易，取消交易，可撤销账户的钱回到主账户
         2. 24小时之后，A的定时交易执行
      2. 所以，可撤销交易的hash要单独做一个状态树，并且有一个状态是否撤消
      3. 要先扣足gas，保证定时交易成功
2. 委托交易
   1. 委托交易有两种，委托签名和委托转账
   2. 委托签名不需要使用委托账户
   3. 委托转账需要使用委托账户
   4. 具体参考委托交易文档